US 20210368314A1

(54) **MTC KEY MANAGEMENT FOR KEY DERIVATION AT BOTH UE AND NETWORK**

(71) Applicant: **NEC CORPORATION**, Tokyo (JP)

(72) Inventors: **XIAOWEI ZHANG**, Tokyo (JP); **ANAND RAGHAWA PRASAD**, Tokyo (JP)

(21) Appl. No.: **17/394,930**

(22) Filed: **Aug. 5, 2021**

Related U.S. Application Data

(63) Continuation of application No. 16/444,517, filed on Jun. 18, 2019, now Pat. No. 11,122,405, which is a continuation of application No. 14/652,456, filed on Jun. 16, 2015, now abandoned, filed as application No. PCT/JP2014/000015 on Jan. 7, 2014.

(30) **Foreign Application Priority Data**

Jan. 10, 2013 (JP) 2013-002981

Publication Classification

(51) **Int. Cl.**
H04W 4/70	(2006.01)
H04W 12/041	(2006.01)
H04W 12/0433	(2006.01)
H04W 12/03	(2006.01)

(52) **U.S. Cl.**
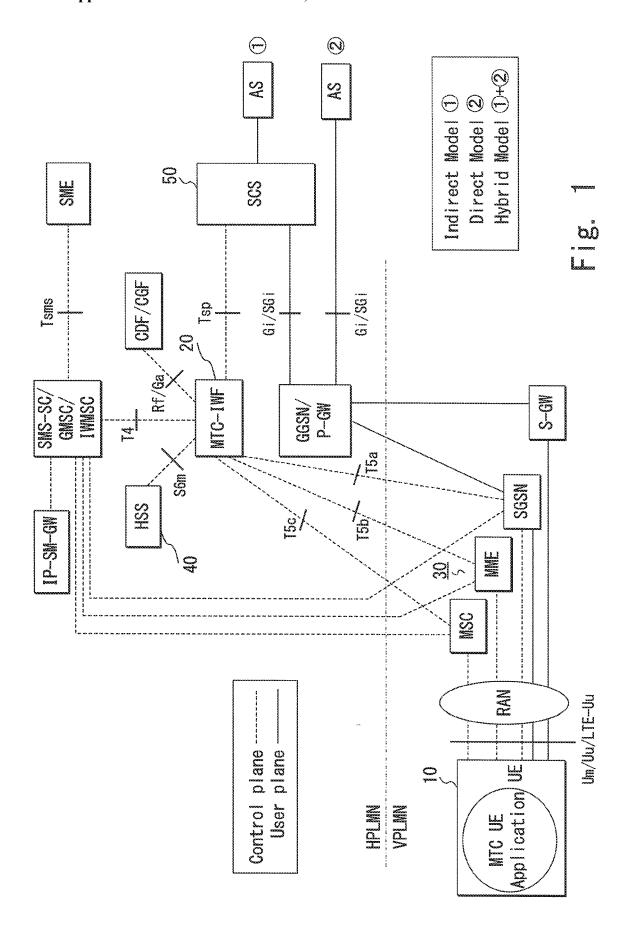CPC *H04W 4/70* (2018.02); *H04W 12/041* (2021.01); *H04L 2463/081* (2013.01); *H04W 12/03* (2021.01); *H04W 12/0433* (2021.01)

(57) **ABSTRACT**

There is provided a new IWF SMC procedure for establishing security association between an MTC UE (**10**) and an MTC-IWF (**20**). The MTC-IWF (**20**) sends to the UE (**10**) at least an algorithm identifier which instructs the UE (**10**) to select one of algorithms for deriving a root key (K_iwf). The UE (**10**) derives the root key (K_iwf) in accordance with the selected algorithm, and derives at least a subkey for checking the integrity of messages transferred between the UE (**10**) and the MTC-IWF (**20**) by using the derived root key (K_iwf). The UE (**10**) protects uplink messages transmitted to the MTC-IWF (**20**) with the derived subkey. The MTC-IWF (**20**) protects downlink messages transmitted to the UE (**10**) with the same subkey derived at a core network.
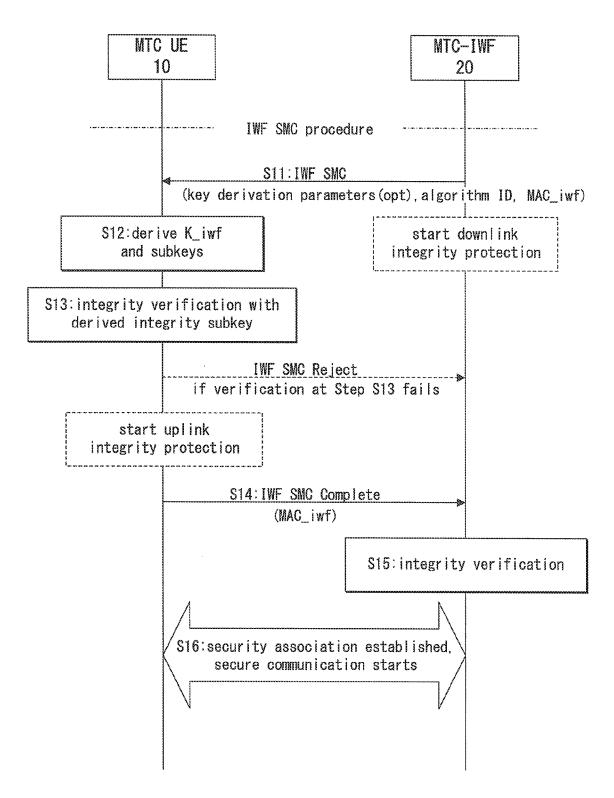
Fig. 1

MTC UE
10

MTC-IWF
20

IWF SMC procedure

S11:IWF SMC
(key derivation parameters(opt),algorithm ID, MAC_iwf)

S12:derive K_iwf
and subkeys

start downlink
integrity protection

S13:integrity verification with
derived integrity subkey

IWF SMC Reject
if verification at Step S13 fails

start uplink
integrity protection

S14:IWF SMC Complete
(MAC_iwf)

S15:integrity verification

S16:security association established,
secure communication starts

Fig. 2

Fig. 3

MTC UE 10	MME/SGSN 30	HSS 40	MTC-IWF 20	SCS 50

S31:security established

S32:MTC device trigger(UE ID)

S33:Subscriber Information Request
(msg type=trigger,UE ID)

S34:Authentication procedure,if it is not done earlier

S35:opt:send key derivation parameters in NAS message

Alt1:MTC-IWF derives K_iwf

S36:Subscriber Information Response
(opt:key derivation parameters)

S37:derive K_iwf
and subkeys

S38:IWF SMC procedure(independent or carried by NAS SMC)

Alt2:HSS derives K_iwf

S46:derive K_iwf

S47:Subscriber Information Response(K_iwf,algorithm ID)

S48:store K_iwf and
derive subkeys

S49:IWF SMC procedure(independent or carried by NAS SMC)

Alt3:MME derives K_iwf

S56:Authentication data response/Insert Subscriber Data
(key derivation parameter,algorithm ID(opt))

S57:derive K_iwf

S58:sending key toghether with algorithm ID

S59:store K_iwf and
derive subkeys

S60:IWF SMC procedure(independent or carried by NAS SMC)

Fig. 4

10

11

NEGOTIATION UNIT

Fig. 5

20

21

NEGOTIATION UNIT
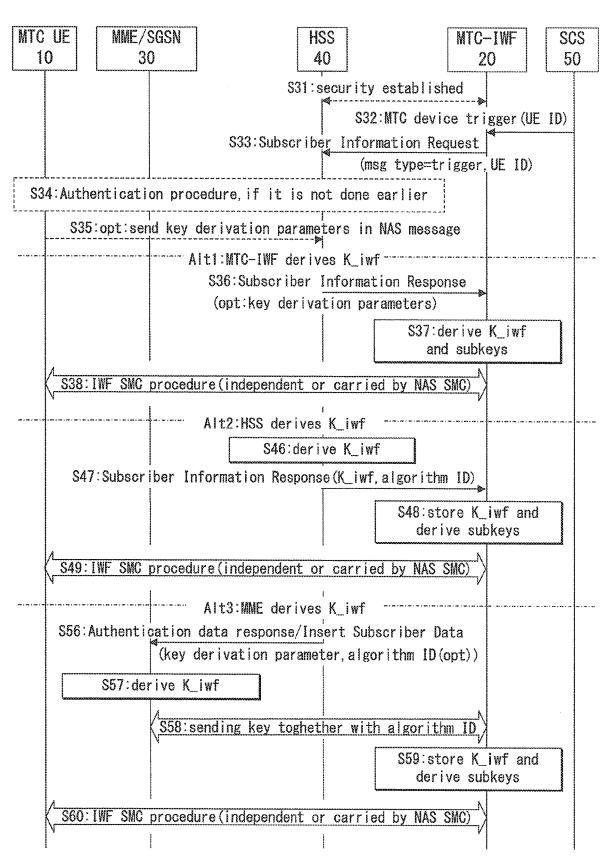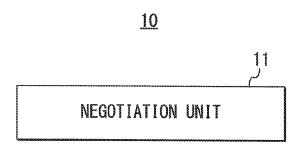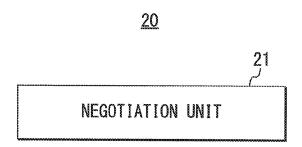
Fig. 6

MTC KEY MANAGEMENT FOR KEY DERIVATION AT BOTH UE AND NETWORK

TECHNICAL FIELD

[0001] The present invention relates to key management in MTC (Machine-Type Communication) system, in particular to a technique to derive a key at both of a UE (User Equipment) and a network.

BACKGROUND ART

[0002] As disclosed in NPL 1, the security over the interface between an MTC device and an MTC-IWF (MTC inter-Working Function) should be studied.

[0003] Note that the MTC device is a UE equipped for MTC, which will be sometimes referred to as "MTC UE" or "UE" in the following explanation.

CITATION LIST

Non Patent Literature

[0004] NPL 1: 3GPP TR 33.868, "Security aspects of Machine-Type and other Mobile Data Applications Communications Enhancements; (Release 12)", V0.10.0, 2012-09

[0005] NPL 2: 3GPP TS 33.401, "3GPP System Architecture Evolution (SAE); Security architecture (Release 12)", V12.5.1, 2012-10

SUMMARY OF INVENTION

Technical Problem

[0006] However, in 3GPP (3rd Generation Partnership Project), the study has not been fulfilled. Therefore, secure communication solution is required between an MTC device and an MTC-IWF.

[0007] Accordingly, an exemplary object of the present invention is to ensure secure communication between an MTC device and an MTC-IWF.

Solution to Problem

[0008] In order to achieve the above-mentioned object, this invention deals with the following issues:

[0009] Deriving the same root key at both UE and network side.

[0010] In this invention, there is proposed that network and UE derive the root key K_iwf separately. There is no key sent between them. Key derivation parameters can be either sent from network to UE or from UE to network. Inside the core network, the key derivation parameters can be sent from HSS (Home Subscriber Server) to MTC-IWF and MME (Mobility Management Entity), or from MTC-IWF to HSS or MME. The derivation algorithms are available in the UE and the network node. Network indicates UE which algorithm should be used for root key derivation by using an algorithm identifier.

[0011] There is also proposed a new IWF Security Mode Command (SMC) procedure for the security association establishment between UE and MTC-IWF.

[0012] A communication system according to a first aspect of the present invention includes: an MTC-IWF; and a UE. The MTC-IWF stores a master key, derives subkeys for confidentiality and integrity protection, and informs the UE about an algorithm for key derivation. The UE derives, by using the algorithm, the master key and the subkeys such that the UE shares the same master key and the same subkeys with the MTC-IWF. Security association is established between the UE and the MTC-IWF by using the shared master key and subkeys.

[0013] An MTC-IWF according to a second aspect of the present invention is configured to store a master key, derive subkeys for confidentiality and integrity protection, and inform a UE about an algorithm for key derivation to cause the UE to derive the master key and the subkeys such that the UE shares the same master key and the same subkeys with the MTC-IWF. Security association is established between the UE and the MTC-IWF by using the shared master key and subkeys.

[0014] A UE according to a third aspect of the present invention is configured to derive, by using an algorithm for key derivation informed from an MTC-IWF, a master key and subkeys for confidentiality and integrity protection such that the UE shares the master key and the subkeys with the MTC-IWF. Security association is established between the UE and the MTC-IWF by using the shared master key and subkeys.

[0015] An HSS according to a fourth aspect of the present invention is configured to derive a master key, and to send the master key to an MTC-IWF. The master key is shared between the MTC-IWF and a UE, and used for establishing security association between the MTC-IWF and the UE.

[0016] An MME according to a fifth aspect of the present invention is configured to carry, to a UE, a NAS SMC message that includes an IWF SMC message for informing the UE about an algorithm for key derivation. The algorithm is used for the UE and an MTC-IWF to share a master key and subkeys for confidentiality and integrity protection, and security association is established between the UE and the MTC-IWF by using the shared master key and subkeys.

[0017] A method according to a sixth aspect of the present invention provides a method of securing MTC communication. This method includes: storing, by an MTC-IWF, a master key; deriving, by the MTC-IWF, subkeys for confidentiality and integrity protection; informing, by the MTC-IWF, a UE about an algorithm for key derivation; and deriving, by the UE using the algorithm, the master key and the subkeys such that the UE shares the same master key and the same subkeys with the MTC-IWF. Security association is established between the UE and the MTC-IWF by using the shared master key and subkeys.

Advantageous Effects of Invention

[0018] According to the present invention, it is possible to solve the above-mentioned problems, and thus to ensure secure communication between an MTC device and an MTC-IWF.

BRIEF DESCRIPTION OF DRAWINGS

[0019] FIG. 1 is a block diagram showing a configuration example of a communication system according to an exemplary embodiment of the present invention.

[0020] FIG. 2 is a sequence diagram showing one example of IWF SMC procedure in the communication system according to the exemplary embodiment.

[0021] FIG. **3** is a sequence diagram showing another example of the IWF SMC procedure in a case where IWF SMC is carried in NAS SMC.

[0022] FIG. **4** is a sequence diagram showing an example of root key derivation at both UE and network in a case where communication is triggered by an SCS.

[0023] FIG. **5** is a block diagram showing a configuration example of an MTC device according to the exemplary embodiment.

[0024] FIG. **6** is a block diagram showing a configuration example of a network node according to the exemplary embodiment.

DESCRIPTION OF EMBODIMENTS

[0025] Hereinafter, an exemplary embodiment of the present invention will be described with the accompany drawings.

[0026] As shown in FIG. **1**, a communication system according to this exemplary embodiment includes a core network (3GPP network), and one or more MTC UEs **10** which are UEs equipped for MTC and connect the core network through a RAN (Radio Access Network). While the illustration is omitted, the RAN is formed by a plurality of base stations (i.e., eNBs (evolved Node Bs)).

[0027] The MTC UE **10** attaches to the core network. The MTC UE **10** can host one or multiple MTC Applications. The corresponding MTC Applications in the external network are hosted on an SCS (Service Capability Server) **50**. The SCS **50** connects to the core network to communicate with the MTC UE **10**.

[0028] Further, the core network includes an MTC-IWF **20** as one of its network nodes. The MTC-IWF **20** serves as a gateway to the core network for the SCS **50**. The MTC-IWF **20** relays messages between the MTC UE **10** and the SCS **50**. The core network includes, as other network nodes, an HSS (Home Subscriber Server) **40**, an MME, an SGSN (Serving GPRS (General Packet Radio Service) Support Node), an MSC (Mobile Switching Centre) and the like. In the following description, the MME and the SGSN are sometimes referred to as "MME/SGSN", and collectively or individually denoted by the symbol **30**. Communication between the MTC UE **10** and the MTC-IWF **20** is conducted through the MME/SGSN **30** (or the MSC).

[0029] Next, operation examples of this exemplary embodiment will be described in detail with reference to FIGS. **2** to **4**.

1. IWF SMC Procedure

[0030] FIG. **2** shows IWF SMC procedure using SAE/LTE (Long Term Evolution) NAS (Non Access Stratum) SMC mechanism for establishing security association between UE **10** and MTC-IWF **20**. This procedure will be described below.

[0031] Assume that MTC-IWF **20** has either received or derived the root key K_iwf and has derived subkeys. Note that the root key K_iwf is used for deriving the subkeys. The subkeys include at least an integrity key for checking the integrity of messages transferred between the MTC UE **10** and the MTC-IWF **20** (hereinafter, this key will be referred to as "integrity subkey"). The subkeys may also include a confidentiality key for encrypting and decrypting messages transferred between the MTC UE **10** and the MTC-IWF **20**.

[0032] S11: MTC-IWF **20** sends IWF SMC message to UE **10**, with key derivation parameters (optional) and algorithm ID. The IWF SMC message is protected by the integrity subkey. Integrity protection at downlink is started.

[0033] S12: UE **10** derives K_iwf and subkeys, by using the key derivation parameters and algorithm sent from MTC-IWF **20**.

[0034] S13: UE **10** verifies the received IWF SMC message with the derived integrity subkey. Integrity protection at uplink is started. UE **10** sends IWF SMC Reject message if the verification fails.

[0035] S14: If the integrity verification is successful. UE **10** sends IWF SMC Complete message to MTC-IWF **20** with integrity protection by using the integrity subkey that UE **10** has derived. Uplink integrity protection is started.

[0036] S15: MTC-IWF **20** verifies the IWF SMC Complete message with integrity subkey it has derived.

[0037] S16: If the verification at Step S15 is successful, the security association is established between UE **10** and MTC-IWF **20** and they can start secure communication.

[0038] Meanwhile, as shown in FIG. **3**, IWF SMC messages can also be carried in NAS SMC procedure.

[0039] S21: MTC-IWF **20** sends integrity protected IWF SMC message (same as Step S11 in FIG. **2**) or the necessary parameters for UE **10** to perform key derivation, with UE ID to MME **30**.

[0040] S22: MME **30** carries the IWF SMC message with NAS SMC message and sends it to UE **10**.

[0041] S23: UE **10** performs NAS integrity verification.

[0042] S24: If NAS integrity verification fails, UE **10** sends NAS SMC Reject message carrying IWF SMC Reject message to MME **30**. MME **30** forwards the IWF SMC Reject message to MTC-IWF **20**.

[0043] S25: If NAS integrity verification is succeed, UE **10** derives K_iwf and subkeys.

[0044] S26: UE **10** performs integrity verification on the IWF SMC, if the IWF SMC message was sent at Step S21 with integrity protection. The integrity verification is by using the integrity subkey derived by UE **10**.

[0045] S27: UE **10** sends the NAS SMC Complete carrying IWF SMC Complete to MME **30**. The IWF SMC Complete message can be integrity protected.

[0046] Or UE **10** sends IWF SMC Reject message carried in NAS SMC Complete, if the verification at Step S26 fails.

[0047] S28: MME **30** forwards the IWF SMC Complete or IWF SMC Reject message to MTC-IWF **20**.

[0048] S29: MTC-IWF **20** performs integrity verification on the IWF SMC Complete message, if it was integrity protected.

[0049] S30: Security association is established between UE **10** and MTC-IWF **20** and they can start secure communication. If MTC-IWF **20** received IWF SMC Complete, and integrity verification is passed at Step S29 (when it is carried).

[0050] In this procedure, the integrity protection for IWF SMC message by integrity subkey, NAS SMC message protection and verification follows the requirement in NPL 2.

2. Root Key Derivation at Both Network and UE

[0051] The initial key derivation at both sides of the UE and the core network can be triggered by:

[0052] Attaching of a MTC capable UE to the network where the UE does not have K_iwf yet, and network verifies it is a MTC UE;

[0053] First time there is a trigger need to be delivered to UE and no security association exists between the UE and MTC-IWF.

[0054] In this exemplary embodiment, take as an example a case where communication is initiated by trigger from SCS 50. The details are shown in FIG. 4.

[0055] S31: Assume that security between HSS 40 and MTC-IWF 20 has been established.

[0056] S32: SCS 50 sends MTC device trigger message to MTC-IWF 20, including target UE ID.

[0057] S33: MTC-IWF 20 sends Subscriber Information Request message to HSS 40 with msg type=trigger and UE ID. The msg type is to indicate HSS 40 that the request from SCS 50 is trigger.

[0058] S34: Mutual authentication with UE 10 is carried if UE 10 has not been authenticated yet.

[0059] S35: As an option, UE 10 can send some key derivation parameters to network in NAS message.

[0060] In a case where MTC-IWF 20 derives K_iwf, the following Steps S36 to S38 are performed.

[0061] S36: If MTC-IWF 20 does not have the key derivation 20 parameters itself, HSS 40 can send them to MTC-IWF 20 in Subscriber Information Response message.

[0062] S37: MTC-IWF 20 derives K_iwf and subkeys accordingly.

[0063] S38: IWF SMC procedure is carried, either as an independent procedure as shown in FIG. 2 or embedded in NAS SMS procedure as shown in FIG. 3.

[0064] Alternatively, in a case where HSS 40 derives K_iwf, the following Steps S46 to S48 are performed.

[0065] S46: HSS 40 derives the K_iwf. If MTC-IWF 20 has the key derivation parameters, it can send it to HSS 40 at Step S33.

[0066] S47: HSS 40 sends K_iwf to MTC-IWF 20 in Subscriber Information Response message.

[0067] S48: MTC-IWF 20 stores K_iwf and derives subkeys.

[0068] S49: IWF SMC procedure is carried, either as an independent procedure or embedded in NAS SMS procedure.

[0069] Alternatively, in a case where MME 30 derives K_iwf, the following Steps S56 to S60 are performed.

[0070] S56: HSS 40 sends the key derivation parameters, algorithm ID MME 30 in Authentication data response or Insert Subscriber Data.

[0071] S57: MME 30 derives K_iwf.

[0072] S58: MME 30 sends the derived K_iwf to MTC-IWF 20, in any one of the following two ways, for example.

[0073] One way is that MME 30 sends K_iwf in a new message to IISS 40, then HSS 40 sends it to MTC-IWF 20 in a new message called Update Subscriber Information message.

[0074] The other way is that MME 30 directly sends K_iwf over interface T5 in a new message or in a Report message to MTC-IWF 20.

[0075] S59: MTC-IWF 20 will store the K_iwf and derives the subkeys.

[0076] S60: IWF SMC procedure is carried, either as an independent 30 procedure or embedded in NAS SMS procedure.

[0077] The IWF SMC procedure is the same for the case where UE 10 initiates communication. At Step S36 and Step S47, the above-mentioned Update Subscriber Information can be used for HSS 40 to send key derivation parameter or K_iwf.

[0078] Next, configuration examples of the MTC UE 10 and the MTC-IWF 20 according to this exemplary embodiment will be described with reference to FIGS. 5 and 6. Note that in the following explanation, there will be described only elements which are specific to this exemplary embodiment. However, it will be understood that the MTC UE 10 and the MTC-IWF 20 also include elements for functioning as typical MTC UE and MTC-IWF, respectively.

[0079] As shown in FIG. 5, the MTC UE 10 includes a negotiation unit 11 which negotiates with the MTC-IWF 20 to establish the security association with the MTC UE 10 and the MTC-IWF 20 as shown in FIGS. 2 to 4. The negotiation unit 11 can transfer messages for the negotiation to the MTC-IWF 20 thorough the MME 30 as shown in FIG. 3. The negotiation unit 11 can send the key derivation parameters to the core network as shown at Step S35 in FIG. 4. The negotiation unit 11 can receive the algorithm ID from the MTC-IWF 20 as shown at Step S11 in FIG. 2. At the same Step S11, the negotiation unit 11 can further receive the key derivation parameters from the MTC-IWF 20. The negotiation unit 11 can derive the root key K_iwf and subkeys as shown at Step S12 in FIG. 2, and can verify the IWF SMC message received from the MTC-IWF 20 with the derived integrity subkey as shown at Step S13. As shown at Step S14, upon succeeding in the verification, the negotiation unit 11 protects the IWF SMC Complete message with the integrity subkey, and sends the protected IWF SMC Complete message to the MTC-IWF 20. Upon failing in the verification, the negotiation unit 11 sends the IWF SMC Reject message to the MTC-IWF 20. This negotiation unit 11 can be configured by, for example, a transceiver which conducts communication with the MTC-IWF 20 through the MME 30 and the RAN, a controller such as a CPU (Central Processing Unit) which controls this transceiver.

[0080] As shown in FIG. 6, the MTC-IWF 20 includes a negotiation unit 21 which negotiates with the MTC UE 10 to establish the security association with the MTC UE 10 and the MTC-IWF 20 as shown in FIGS. 2 to 4. The negotiation unit 21 can transfer messages for the negotiation to the MTC UE 10 thorough the MME 30 as shown in FIG. 3. The negotiation unit 21 can send the algorithm ID to the MTC UE 10 as shown at Step S11 in FIG. 2. At the same Step S11, the negotiation unit 21 can further send the key derivation parameters to the MTC UE 10. The negotiation unit 21 can protect the IWF SMC message with the integrity subkey. The negotiation unit 21 can verify the IWF SMC Complete message received from the MTC UE 10 with the integrity subkey as shown at Step S15 in FIG. 2. This negotiation unit 21 can be configured by, for example, a transceiver which conducts communication with the MTC UE 10 through the MME 30 and the RAN, a controller such as a CPU which controls this transceiver.

[0081] Based on the above description, solutions will be proposed to 3GPP TR 33.868 as follows.

4

1. Discussion

[0082] In MTC device triggering, application security between SCS and UE can protect trigger with confidentiality and integrity protection from eavesdropping or alteration.

[0083] However, since the communication for trigger delivery happens via mobile network, when we consider the security issues that the (unauthorized) triggering from SCS can bring, we also need to study the attacks to the network and the UEs attached to it. As described in threats section of TR 33.868, section 5.1.2, the attacks can cause UE power consumption, DoS attack to network, waste of network resources, overload NAS, and privacy issues. Since application security cannot solve these issues, security at transport and network layer should be considered.

[0084] In the existing system at NAS layer, MME and UE can establish NAS security. The trigger forwarded from MME to UE can have NAS security protection but MME was not designed for MTC purposed such that it does not perform any verification of SCS or the trigger from it. MME forwards any trigger it receives, which makes NAS security insufficient. Meanwhile, hop-by-hop security among MTC-IWF, MME and UE requires MME performing encryption/decryption, integrity check on both direction with MTC-IWF and UE when each trigger and response is received. The large amount of communication between UE and SCS will overload MME and NAS layer communication.

[0085] MTC-IWF, as the entrance element in the 3GPP network domain, authorizes SCS and its trigger request to a given UE, with support from HSS. MTC-IWF retrieves subscriber information and forwards the trigger from SCS to UE.

[0086] However, the security over interface T5 has not been studied. MitM attack can happen over the interface for a roaming UE. On top of that, a compromised MTC-IWF can replay, discard or alter the trigger message. The UE, which is mutually authenticated to MME and HSS and has NAS security context established with MME, trusts messages received from MME. Thus a fake trigger will be easily delivered to UE since MME does not perform any verification.

[0087] Therefore, it is necessary that UE and MTC-IWF have mutual authentication; message integrity, authentication, authorization, confidentiality protection, replay protection. MTC-IWF should ensure the security of trigger delivery, provide the proof when SCS is authenticated and authorized to the network.

2. Proposal

[0088] We propose a new key hierarchy for UE and MTC-IWF to protect the communication between them, and present how the keys are derived and shared between the two ends, key management and also the extension to mobility case.

[0089] Communication between UE and MTC-IWF should have confidentiality and integrity protection using the subkeys.

2.1 New Key Hierarchy

[0090] The key hierarchy constitutes of a root key and a pair of confidentiality and integrity protection subkeys. Using a pair of subkeys makes it easy to perform key management. When the subkeys are expired or exposed, UE and MTC-IWF can simply derive another pair of subkeys from the root key they hold, instead of going all over again for key derivation and allocation.

[0091] K_IWF is a root key that should be shared only between UE and MTC-IWF. It is used to derive a pair of subkeys K_IWFe and K_IWFi at UE and MTC-IWF separately. K_IWFe is the confidentiality key and K_IWFi is the integrity key. The two subkeys are used for protecting the control plane communication between UE and MTC-IWF.

2.2 Key Derivation at Both Network and UE

[0092] We propose in this document that the same root key K_IWF is derived independently at both MTC-IWF and UE.

[0093] HSS send Kasme to MTC-IWF over interface S6m, and MTC-IWF derives the root key K_IWF from Kasme. The K_IWF should be stored in MTC-IWF and used for subkeys derivation.

[0094] Deriving the same key at different ends requires UE and MTC-IWF have the same seed and parameters and use the same algorithm. Necessary parameters for key derivation and algorithm identifier can be indicated by HSS to UE. We propose a IWF SMC procedure, using the NAS SMC mechanism [TS33.401].

[0095] After MTC-IWF derived subkeys from the root key, it indicates the parameters and algorithms to UE in the IWF SMC message. The message is integrity protected with integrity subkey K_IWFi.

[0096] In the same way as NAS SMC procedure, the UE should verify the integrity of the IWF security mode command message. If successfully verified, UE should start uplink confidentiality and integrity security protection. UE sends the IWF security mode complete message to MTC-IWF with integrity protection by using the integrity subkey K_IWFi it derived.

[0097] The MTC-IWF should check the integrity protection on the IWF Security Mode Complete message using K_IWFi. The downlink ciphering at the MTC-IWF with the subkeys can start after receiving the IWF Security mode complete message. The uplink deciphering at the MTC-IWF with the subkeys can start after sending the IWF security mode command message.

[0098] If any verification of the IWF security mode command is not successful in the UE, the UE should reply with a IWF security mode reject message.

[0099] The IWF SMC procedure can be an independent procedure or carried in NAS SMC procedure, with the full message or necessary parameters only.

2.3 Key Management

2.3.1 Root Key Derivation and Renew

[0100] For root key K_IWF derivation, the same Key derivation function (KDF) for LTE/SAE key derivation [TS33.401] is used.

[0101] Root key should be renewed when a new Kasme is derived and sent to MTC-IWF. For handover between MMEs, there is no need to renew root key. For handover between MTC-IWF, a new root key should be derived.

2.3.2 Subkey Derivation

[0102] The subkeys K_IWFe and K_IWFi should be derived once after the root key is derived. The subkeys derivation also uses the same KDF, with K_IWF as input key. The truncation procedure as described in [TS33.401]

5

can be used to obtain the subkeys K_IWFe and K_IWFi. Other input parameters include: counter, length of counter.

[0103] K_IWFe is a key, which shall only be used for the protection of traffic between UE and MTC-IWF with a particular encryption algorithm.

[0104] K_IWFi is a key, which shall only be used for the protection of traffic between UE and MTC-IWF with a particular integrity algorithm.

[0105] When there is a new root key derived, new subkeys should be derived from the new root key. Network can decide to derive new subkeys from the same root key according to its policy at any time.

[0106] 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.

[0107] The whole or part of the exemplary embodiment disclosed above can be described as, but not limited to, the following supplementary notes.

(Supplementary Note 1)

[0108] New IWF SMC procedure for establishing security association between UE and MTC-IWF.

(Supplementary Note 2)

[0109] Modification of NAS SMC to carry messages of IWF SMC.

(Supplementary Note 3)

[0110] MTC-IWF sends key derivation parameters (optional) and

[0111] algorithm ID to UE in the IWF SMC message.

(Supplementary Note 4)

[0112] IWF SMC message is protected by integrity subkey.

(Supplementary Note 5)

[0113] UE derives K_iwf and subkeys, verify the received IWF SMC message with the derived integrity subkey.

(Supplementary Note 6)

[0114] UE sends IWF SMC Complete message to MTC-IWF, integrity protects the message with the integrity subkey UE has derived.

(Supplementary Note 7)

[0115] MTC-IWF performs integrity verification of IWF SMC Complete with the integrity subkey it derived.

(Supplementary Note 8)

[0116] UE sends IWF SMC Reject message if the verification fails.

(Supplementary Note 9)

[0117] MTC-IWF indicates to HSS that the SCS initiated communication to a given UE, with msg type=trigger and UE ID inserted in the Subscriber Information Request.

(Supplementary Note 10)

[0118] Root key derivation parameter provision:

[0119] 1) UE sends root key K_iwf derivation parameters in NAS message to network.

[0120] 2) HSS sends K_iwf derivation parameters to MTC-IWF, by re-using Subscriber Information Response message or a new message of Update Subscriber Information.

[0121] 3) MTC-IWF sends K_iwf derivation parameters to HSS, for example in Subscriber Information Request message.

(Supplementary Note 11)

[0122] HSS or MME sends MTC-IWF the algorithm ID that they used to derive K_iwf.

(Supplementary Note 12)

[0123] HSS sends key derivation parameters and algorithm ID (optional) to MME.

(Supplementary Note 21)

[0124] A communication system comprising:

[0125] an MTC (Machine-Type-Communication) device; and

[0126] a network relaying traffic between the MTC device and a server that can communicate with the MTC device,

[0127] wherein the network includes a first node that serves as a gateway to the network for the server, and

[0128] the first node negotiates with the MTC device to establish security association between the MTC device and the first node itself.

(Supplementary Note 22)

[0129] The communication system according to Supplementary note 21,

[0130] wherein the network further includes a second node that can establish confidentiality and integrity protected connection with the MTC device, and

[0131] the first node and the MTC device transfer messages for the negotiation through the second node.

(Supplementary Note 23)

[0132] The communication system according to Supplementary note 22,

[0133] wherein the MTC device sends, to the network that can be confidential and integrity protected, parameters for the network to derive a root key, and

[0134] the root key is used for deriving at least a subkey to check the integrity of messages transferred between the MTC device and the first node.

(Supplementary Note 24)

[0135] The communication system according to Supplementary note 21 or 22,

[0136] wherein the first node sends an algorithm identifier to the MTC device,

[0137] the algorithm identifier instructs the MTC device to select one of algorithms for deriving a root key, and

[0138] the root key is used for deriving at least a subkey to check the integrity of messages transferred between the MTC device and the first node.

(Supplementary Note 25)

[0139] The communication system according to Supplementary note 24, wherein the first node further sends, to the MTC device, parameters for the MTC device to derive the root key.

(Supplementary Note 26)

[0140] The communication system according to Supplementary note 24 or 25, wherein the first node protects the message with the subkey.

(Supplementary Note 27)

[0141] The communication system according to Supplementary note 26,
[0142] wherein the MTC device derives the root key and the subkey, and verifies the message with the derived subkey.

(Supplementary Note 28)

[0143] The communication system according to Supplementary note 27,
[0144] wherein upon succeeding in the verification, the MTC device sends to the first node a response message indicating the success, and
[0145] the MTC device protects the response message with the derived subkey upon sending the response message.

(Supplementary Note 29)

[0146] The communication system according to Supplementary note 28, wherein the first node verifies the response message with the subkey.

(Supplementary Note 30)

[0147] The communication system according to any one of Supplementary notes 27 to 29, wherein upon failing in the verification, the MTC device sends to the first node a response message indicating the failure.

(Supplementary Note 31)

[0148] A node that is included in a network relaying traffic between an MTC device and a server being able to communicate with the MTC device, and that serves as a gateway to the network for the server, the node comprising:
[0149] negotiation means for negotiating with the MTC device to establish security association between the MTC device and the node itself.

(Supplementary Note 32)

[0150] The node according to Supplementary note 31, wherein the negotiation means is configured to transfer messages for the negotiation to the MTC device through a different node that is included in the network and that can establish confidentiality and integrity protected connection with the MTC device.

(Supplementary Note 33)

[0151] The node according to Supplementary note 31 or 32, wherein the negotiation means is configured to send an algorithm identifier to the MTC device, the algorithm identifier instructing the MTC device to select one of algorithms

for deriving a root key, the root key being used for deriving at least a subkey to check the integrity of messages transferred between the MTC device and the node.

(Supplementary Note 34)

[0152] The node according to Supplementary note 33, wherein the negotiation means is configured to further send, to the MTC device, parameters for the MTC device to derive the root key.

(Supplementary Note 35)

[0153] The node according to Supplementary note 33 or 34, wherein the negotiation means is configured to protect the message with the subkey.

(Supplementary Note 36)

[0154] The node according to Supplementary note 35,
[0155] wherein the MTC device derives the root key and the subkey, verifies the message with the derived subkey, and upon succeeding in the verification, sends to the node a response message indicating the success, the response message being protected with the derived subkey,
[0156] wherein the negotiation means is configured to verify the response message with the subkey.

(Supplementary Note 37)

[0157] The node according to any one of Supplementary notes 31 to 36, comprising an MTC-IWF (MTC Inter-Working Function).

(Supplementary Note 38)

[0158] An MTC device that communicates with a server through a network relaying traffic between the MTC device and the server, the MTC device comprising:
[0159] negotiation means for negotiating, with a first node that is included in the network and that serves as a gateway to the network for the server, to establish security association between the MTC device and the node.

(Supplementary Note 39)

[0160] The MTC device according to Supplementary note 38, wherein the negotiation means is configured to transfer messages for the negotiation to the first node through a second node that is included in the network and that can establish confidentiality and integrity protected connection with the MTC device.

(Supplementary Note 40)

[0161] The MTC device according to Supplementary note 39, wherein the negotiation means is configured to send, to the network that can be confidential and integrity protected, parameters for the network to derive a root key, the root key being used for deriving at least a subkey to check the integrity of messages transferred between the MTC device and the first node.

(Supplementary Note 41)

[0162] The MTC device according to Supplementary note 38 or 39, wherein the negotiation means is configured to receive an algorithm identifier from the first node, the algorithm identifier instructing the MTC device to select one

of algorithms for deriving a root key, the root key being used for deriving at least a subkey to check the integrity of messages transferred between the MTC device and the first node.

(Supplementary Note 42)

[0163] The MTC device according to Supplementary note 41, wherein the negotiation means is configured to further receive, from the first node, parameters for the MTC device to derive the root key.

(Supplementary Note 43)

[0164] The MTC device according to Supplementary note 41 or 42,

[0165] wherein the first node protects the message with the subkey,

[0166] wherein the negotiation means is configured to derives the root key and the subkey, and to verify the message with the derived subkey.

(Supplementary Note 44)

[0167] The MTC device according to Supplementary note 43, wherein upon succeeding in the verification, the negotiation means is configured to:

[0168] protect, with the derived subkey, a response message indicating the success; and

[0169] send the response message to the first node.

(Supplementary Note 45)

[0170] The MTC device according to Supplementary note 43 or 44, wherein upon failing in the verification, the negotiation means is configured to send to the first node a response message indicating the failure.

(Supplementary Note 46)

[0171] A method of controlling operations in a node that is included in a network relaying traffic between an MTC device and a server being able to communicate with the MTC device, and that serves as a gateway to the network for the server, the method comprising:

[0172] negotiating with the MTC device to establish security association between the MTC device and the node.

(Supplementary Note 47)

[0173] A method of controlling operations in an MTC device that communicates with a server through a network relaying traffic between the MTC device and the server, the method comprising: negotiating, with a first node that is included in the network and that serves as a gateway to the network for the server, to establish security association between the MTC device and the node.

[0174] This application is based upon and claims the benefit of priority from Japanese patent application No.

2013-002981, filed on Jan. 10, 2013, the disclosure of which is incorporated herein in its entirety by reference.

REFERENCE SIGNS LIST

What is claimed is:

1. A User Equipment (UE) in a communication system including a network node, the UE comprising:

at least one processor; and

at least one memory coupled to the at least one processor, the at least one memory storing instructions that when executed by the at least one processor cause the at least one processor to:

receive, from the network node, a message comprising a parameter, the parameter related to derivation of a confidentiality key and an integrity key, wherein the message is protected by the integrity key;

derive the confidentiality key and the integrity key based on the parameter;

verify integrity of the message using the integrity key; and

send a reject message to the network node if there is a failure of verification of the integrity of the message.

2. The UE of claim **1**, wherein, upon execution of the instructions, the at least one processor is further caused to:

perform secure communication with the network node using the confidentiality key and the integrity key if there is a successful verification of the integrity of the message.

3. The UE of claim **1**, wherein the UE is a Machine Type Communication (MTC) device.

4. A method of a User Equipment (UE) in a communication system including a network node, the method comprising:

receiving, from the network node, a message comprising a parameter, the parameter related to derivation of a confidentiality key and an integrity key, wherein the message is protected by the integrity key;

deriving the confidentiality key and the integrity key based on the parameter;

verifying integrity of the message using the integrity key; and

sending a reject message to the network node if there is a failure of verification of the integrity of the message.

5. The method of claim **4**, further comprising:

performing secure communication with the network node using the confidentiality key and the integrity key if there is a successful verification of the integrity of the message.

6. The method of claim **4**, wherein the UE is a Machine Type Communication (MTC) device.

*   *   *   *   *