Symmetry **2014**, *6*, 1011-1025; doi:10.3390/sym6041011

OPEN ACCESS

symmetry

ISSN 2073-8994

www.mdpi.com/journal/symmetry

Article

Privacy-Enhancing Security Protocol in LTE Initial Attack

Uijin Jang [1], Hyungmin Lim [2] and Hyungjoo Kim [2,*]

[1] Korea Copyright Commission, 619 Gaepo-Ro, Gangnam-Gu 135-240, Korea;
E-Mail: neon7624@gmail.com

[2] Department of Computing, Soongsil University, 369 Sangdo-Ro, Dongjak-Gu, Seoul 156-743, Korea;
E-Mail: atskyo@gmail.com

* Author to whom correspondence should be addressed; E-Mail: hyungjoo.kim@ssu.ac.kr;
Tel.: +82-2-826-6526; Fax: +82-2-828-7346.

External Editor: Young-Sik Jeong

*Received: 14 August 2014; in revised form: 24 October 2014 / Accepted: 1 December 2014 /
Published: 12 December 2014*

Abstract: Long-Term Evolution (LTE) is a fourth-generation mobile communication technology implemented throughout the world. It is the communication means of smartphones that send and receive all of the private date of individuals. M2M, IOT, *etc.*, are the base technologies of mobile communication that will be used in the future cyber world. However, identification parameters, such as International Mobile Subscriber Identity (IMSI), Radio Network Temporary Identities (RNTI), *etc.*, in the initial attach section for accessing the LTE network are presented with the vulnerability of being exposed as clear text. Such vulnerability does not end in a mere identification parameter, but can lead to a secondary attack using the identification parameter, such as replication of the smartphone, illegal use of the mobile communication network, *etc.* This paper proposes a security protocol to safely transmit identification parameters in different cases of the initial attach. The proposed security protocol solves the exposed vulnerability by encrypting the parameters in transmission. Using an OPNET simulator, it is shown that the average rate of delay and processing ratio are efficient in comparison to the existing process.

Keywords: future cyber world (FCW); initial attach; Long-Term Evolution (LTE); privacy enhancing; security protocol

1. Introduction

LTE is an abbreviation for Long-Term Evolution, which is a fourth generation mobile communication technology. LTE is designed for high-speed transmission, reduced cost per bit, low transmission delay and applicability to existing frequency bands. It is currently implemented worldwide.

LTE technology is not only used as the base technology of smartphones, which store, send and receive the sensitive personal information of individuals [1,2], but as the base technology of mobile communication technology to be used in the future cyber world, such as M2M, IOT [3,4], *etc.*, and as the research base technology of the fifth generation mobile communication technology to be used in the future cyber world [5].

However in the current LTE technology, vulnerability of the identification parameter values of UE (user equipment) exists, being exposed as clear text in the initial attach process [6–9]. The vulnerability has existed since the initial release of the LTE standards and is still present in Release 12. In the LTE technical documentation, according to the "Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long-Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE) (Release 9)", there is a vulnerability during the initial attach process in the access to the LTE network, in which the UE identifying parameters are transmitted in plain text. Problems, such as tracing and privacy infringement, could occur.

This paper proposes a plan for safely transmitting identification parameters by classifying the initial attach processes into two tasks, initial attach with the International Mobile Subscriber Identity (IMSI) and initial attach with the Global Unique Temporary Identifier (GUTI).

The proposed paper consists of six sections. Section 2 analyzes the structure of the LTE, initial attach process, security process and threats. Section 3 proposes a security protocol by classifying the initial attach process into multiple cases in order to safely transmit identification parameters. Section 4 carries out a security analysis of the proposed protocol, and Section 5 compares and evaluates the performances between the proposed process with a security protocol and the existing process. Section 6 concludes the discussion.

Please see Table 1 for definitions and terms used in this paper.

2. LTE

2.1. LTE Network Structure

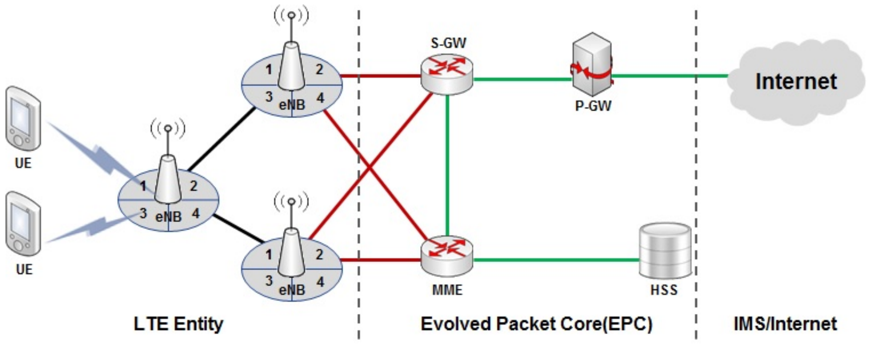
The LTE network consists of LTE entities dealing with wireless access network technology and EPC entities dealing with core network technology. Its structure is shown in Figure 1.

Of the LTE entities, UE accesses the evolved Node B (eNB) through the LTE-Uu Uu wireless interface. eNB, serving as the base station, provides the user with a wireless interface and provides wireless remote resource management (RRM) features, such as radio bearer control, wireless admission control, dynamic wireless resource allocation, load balancing and inter cell interference control (ICIC) [10].

EPC entities consist of the mobility management entity (MME), S-GW, P-G and home subscriber server (HSS). MME is an E-UTRAN control plane entity, communicating with HSS for user authentication and user profile download, and through NAS signaling, it provides the user terminal with EPS rambling management (EMM) and EPS session management (ESM) features. S-GW is the termination point between E-UTRAN and EPC and the anchoring point in the handover with eNB and the handover with the 3GPP system. P-GW connects UE to an external PDN network and provides packet filtering. In addition, P-GW allocates an IP address to the user terminal and serves as the mobile anchoring point in the handover between 3GPP and non-3GPP. Lastly, HSS manages the users' personal profiles [8,10–14].

The IMS/Internet domain is the domain commonly calling external Internet services.

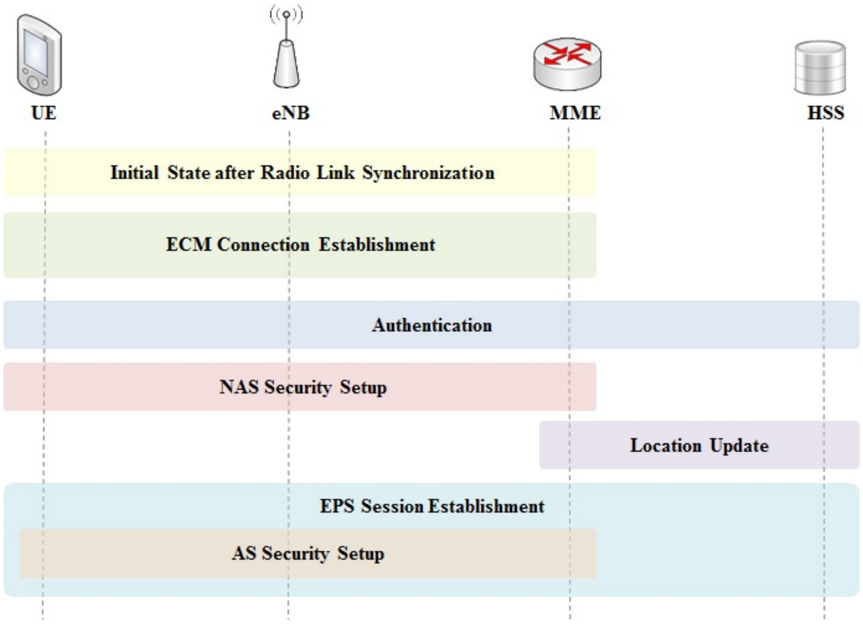
Figure 1. LTE network.



2.2. LTE Initial Attach for UE

The "initial attach for UE" process is a case of the first access to the network by the user subscribing to the LTE network using UE [15–17]. LTE Initial attach process is shown in Figure 2.

Figure 2. Initial attach process.


UE
eNB
MME
HSS
Initial State after Radio Link Synchronization
ECM Connection Establishment
Authentication
NAS Security Setup
Location Update
EPS Session Establishment
AS Security Setup

The "initial state after radio link synchronization" process is one in which UE selects eNB and synchronizes a wireless link. The "ECM connection establishment" process is a NAS layer, that is a process of transmitting IMSI to request MME for net access. Through the relevant process, the RRC connection and S1signaling connection are established.

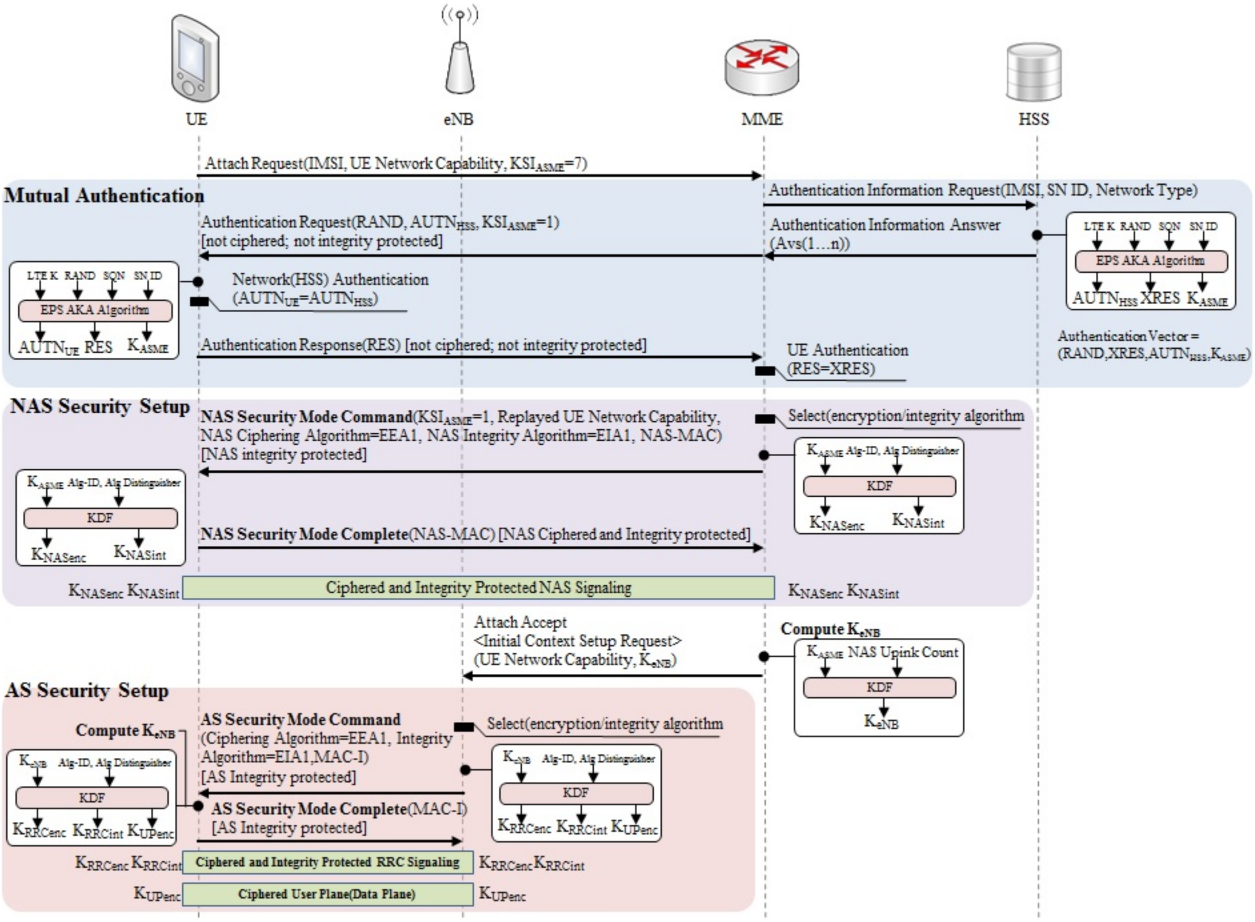
The "authentication" process is a mutual authentication procedure between UE and MME using EPS-AKA,and the "NAS security setup" process is a key setting process to safely transmit NAS messages between UE and MME [18,19].

The "location update" process is the one that receives personal profile information from HSS after registering the location, and the "EPS session establishment" process is the one that allocates network resources, so that the users can be provided with the services [20,21].

2.3. LTE Security

After the "ECM connection establishment" process between UE and eNB, the UE starts mutual authentication by transmitting IMSI to MME. Centering around the LTE security layer, the LTE network carries out mutual authentication based on EPS-AKA. The LTE security is divided broadly into three processes: UE-HSS mutual authentication process, UE-MME NAS security setup process and UE-eNB ASsecurity setup process [6,7,9,14,22–24]. LTE security process is shown in Figure 3.

Figure 3. LTE security.


UE
eNB
MME
HSS
Attach Request(IMSI, UE Network Capability, KSI$_{ASME}$=7)
Mutual Authentication
Authentication Information Request(IMSI, SN ID, Network Type)
Authentication Request(RAND, AUTN$_{HSS}$, KSI$_{ASME}$=1)
[not ciphered; not integrity protected]
Authentication Information Answer
(Avs(1…n))
LTE K RAND SQN SN ID
EPS AKA Algorithm
AUTN$_{HSS}$ XRES K$_{ASME}$
LTE K RAND SQN SN ID
EPS AKA Algorithm
AUTN$_{UE}$ RES K$_{ASME}$
Network(HSS) Authentication
(AUTN$_{UE}$=AUTN$_{HSS}$)
Authentication Response(RES) [not ciphered; not integrity protected]
UE Authentication
(RES=XRES)
Authentication Vector =
(RAND,XRES,AUTN$_{HSS}$,K$_{ASME}$)
NAS Security Setup
NAS Security Mode Command(KSI$_{ASME}$=1, Replayed UE Network Capability, NAS Ciphering Algorithm=EEA1, NAS Integrity Algorithm=EIA1, NAS-MAC) [NAS integrity protected]
Select(encryption/integrity algorithm
K$_{ASME}$ Alg-ID, Alg Distinguisher
KDF
K$_{NASenc}$ K$_{NASint}$
K$_{ASME}$ Alg-ID, Alg Distinguisher
KDF
K$_{NASenc}$ K$_{NASint}$
NAS Security Mode Complete(NAS-MAC) [NAS Ciphered and Integrity protected]
K$_{NASenc}$ K$_{NASint}$
Ciphered and Integrity Protected NAS Signaling
K$_{NASenc}$ K$_{NASint}$
Attach Accept
<Initial Context Setup Request>
(UE Network Capability, K$_{eNB}$)
Compute K$_{eNB}$
K$_{ASME}$ NAS Upink Count
KDF
K$_{eNB}$
AS Security Setup
Compute K$_{eNB}$
AS Security Mode Command
(Ciphering Algorithm=EEA1, Integrity Algorithm=EIA1,MAC-I)
[AS Integrity protected]
Select(encryption/integrity algorithm
K$_{eNB}$ Alg-ID, Alg Distinguisher
KDF
K$_{RRCenc}$ K$_{RRCint}$ K$_{UPenc}$
K$_{eNB}$ Alg-ID, Alg Distinguisher
KDF
K$_{RRCenc}$ K$_{RRCint}$ K$_{UPenc}$
AS Security Mode Complete(MAC-I)
[AS Integrity protected]
K$_{RRCenc}$ K$_{RRCint}$
Ciphered and Integrity Protected RRC Signaling
K$_{RRCenc}$ K$_{RRCint}$
K$_{UPenc}$
Ciphered User Plane(Data Plane)
K$_{UPenc}$

2.4. LTE Threats

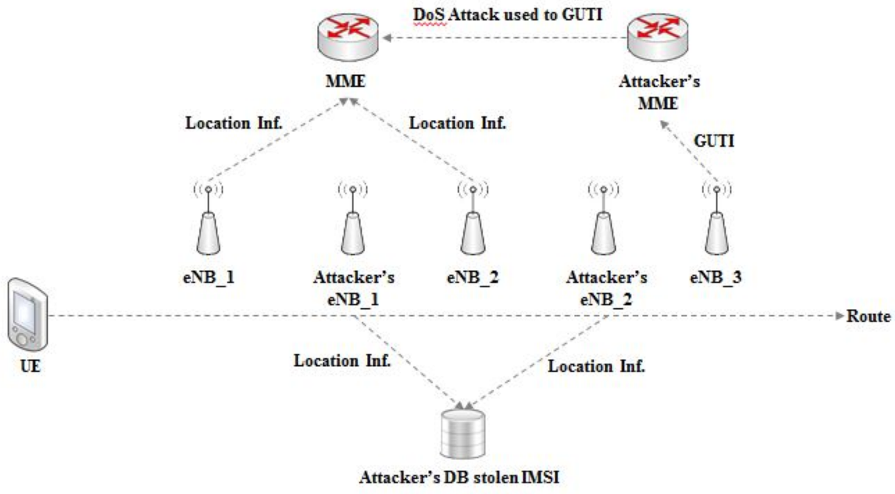
IMSI refers to the unique ID requested from each user when the net administrator registers the user to the service, and this value refers to the unique number of identifications saved in the USIM in the user device [14].

Yet, when "initial attach for UE" is carried out, in the "ECM connection establishment" process, the UE transmits IMSI to MME in plain text. The IMSI transmitted in plain text is transmitted to MME through a number of eNB, which has a vulnerability in which it is leaking to an attacker through malicious eNB. In addition, for a user tracking an attack using the leaked IMSI, a device tracking attack and a privacy abuse attack may take place.

RNTI, the unique ID to differentiate UE from eNB, and GUTI, used instead of IMSI after a series of the process, also, are transmitted in a variety of initial attach processes in plain text, so that the same vulnerability and the threat of attack of IMSI may occur [6,7,9,25].

An attack that could allow an attacker to use the stolen identification parameter is shown in Figure 4. UE constantly transmits location information to the eNB and MME; an attacker can track the user using a leaked IMSI. Furthermore, the attacker can make a DoS attack using a leaked IMSI and GUTI, which is used for requesting RNTI [26,27]. LTE threat model and its process are shown in Figure 4.

Figure 4. Threat model.



3. Proposed Security Protocol for Initial Attach in LTE

The proposed security protocol was designed to protect unique information about identification, such as IMSI and RNTI transmitted in plain text when the UE attempts an initial attach to the network. It consists of four types by the initial connection of the UE, and the terms and symbols used in the proposed security protocol are shown in Table 1.

Table 1. The terms and symbols used in the proposed security protocol.

UE	User Equipment
eNB	evolved Node B
MME	mobility management entity
HSS	home subscriber server
IMSI	International Mobile Subscriber Identity
RNTI	Radio Network Temporary Identity
GUTI	Global Unique Temporary Identifier
PLMN ID	Public Land Mobile Network ID (MCC + MNC)
MCC	Mobile Country Code
MNC	Mobile Network Code
RN	random number
h()	hash function
F	4n bit string by f()
C	challenge bits

3.1. Initial Attach with IMSI

The first protocol is shown in Figure 5 and is carried out after the "initial state after radio link synchronization" process in the initial attach with the IMSI case. It was designed to protect IMSI leaked from the "ECM connection establishment" process in plain text and RNTI leaked from the "EPS session establishment" process in plain text.

After the "initial state after radio link synchronization" process, UE and MME start an "ECM Connection" process. The UE transmits a generated random number and the "UE network capability" to MME for the attach request. MME receiving the attach request MME generates a random number and transmits it to the UE, and the UE and the MME carry out a series of arithmetic operations to safely transmit IMSI.

The UE and the MME enter the transmitted and received random numbers and the Public Land Mobile Network ID (PLMN ID) into the f() function, secretly shared according to Mobile Network Code (MNC), and generate an F string with 4n bits. The generated F string is divided into four numerical progressions with n bits each. After this process, the MME generates a random number progression used as challenge bits, the UE the second random number, and through lrnumerical progression and exclusive OR arithmetic operation, it generates RN'_{UE_2}.

$$\mathrm{f() = hash(\ Expansion\ P\text{-}Box(\ hash(\ S\text{-}Box(RN}_{UE\_1}\mathrm{),\ S\text{-}Box(RN}_{MME\_1}\mathrm{\ ),\ PLMN\ ID\ )\ )\ )}$$

The MME generates challenge bits C_i using lr_i, ad_i and c_i. If lr_i is zero, $\mathrm{C}_i = \mathrm{c}_i||\mathrm{ad}_i$ and if lr_i is one, $\mathrm{C}_i = \mathrm{ad}_i||\mathrm{c}_i$. The MME transmits C_i to UE to verify it through the response value, and the UE verifies the MME through C_i.

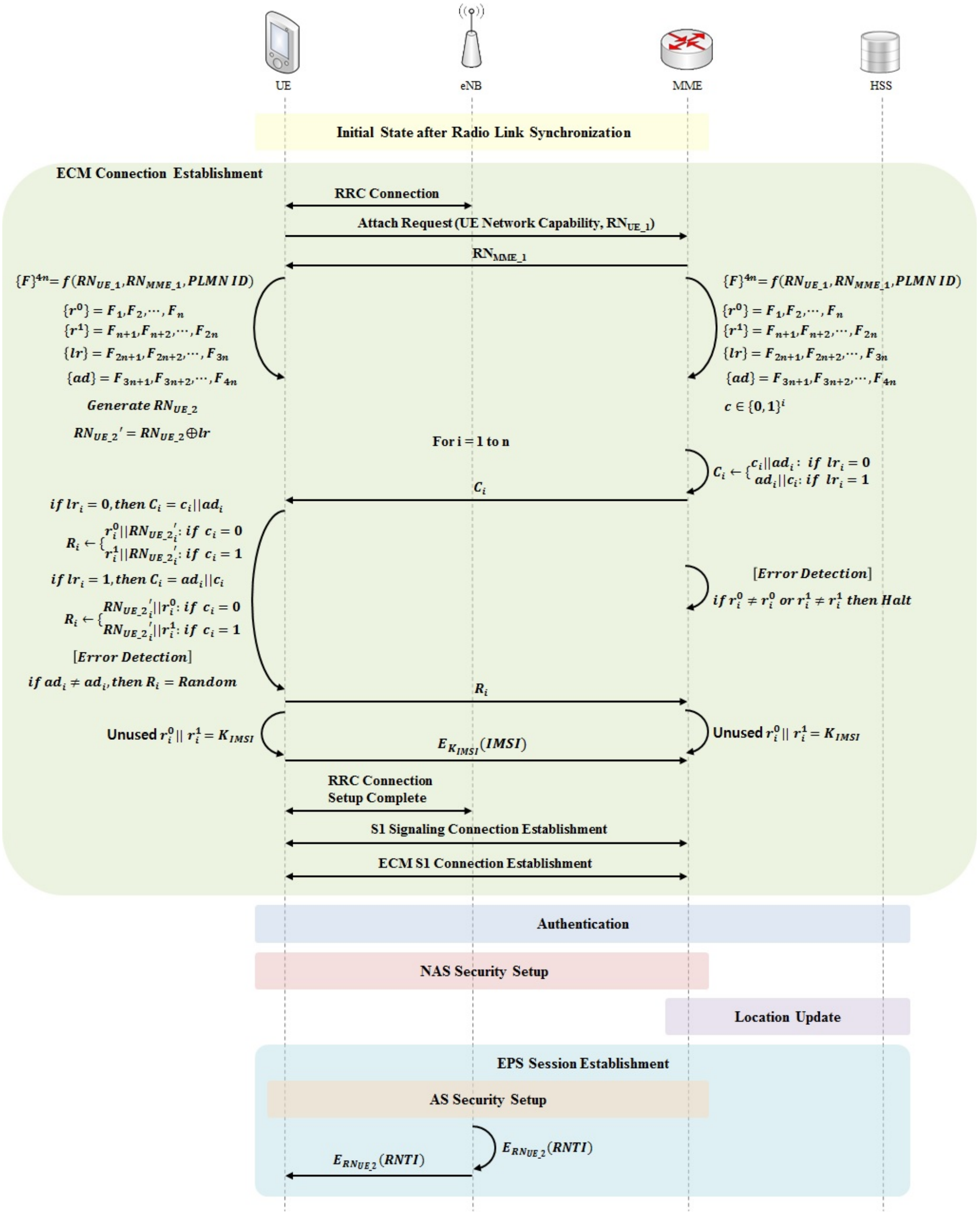
The UE is aware of lr, so it can differentiate C_i transmitted by the MME into $\mathrm{C}_i = \mathrm{c}_i||\mathrm{ad}_i$ and $\mathrm{C}_i = \mathrm{ad}_i||\mathrm{c}_i$. The UE generates $\mathrm{R}_i = \mathrm{RN}'_{UE\_2i}||\mathrm{r}_i^0$ or $\mathrm{R}_i = \mathrm{RN}'_{UE\_2i}||\mathrm{r}_i^1$ if lr_i is zero and $\mathrm{R}_i = \mathrm{r}_i^0||\mathrm{RN}'_{UE\_2i}$ or

$\mathrm{R}_i = \mathrm{r}_i^1 || \mathrm{RN}'_{UE\_2i}$ if lr_i is one. At this time, r_i^0 and r_i^1 transmits r_i^0 if c_i transmitted by the MME is zero and r_i^1 if c_i is one. At this time, the MME receives the transmission of RN_{UE_2} of the UE and saves it.

For ad_i transmitted by the MME ($\mathrm{ad}_i \neq \mathrm{ad}_i$), the UE detects an error and transmits the response value as a random value. The MME, too, halts the attach process if an error is detected through $\mathrm{r}_i^0 \neq \mathrm{r}_i^0$ and $\mathrm{r}_i^1 \neq \mathrm{r}_i^1$.

After the challenge-response process, the UE uses unused r_i^0 and r_i^1 concatenated value as a key to encrypt IMSI to transfer it to the MME. The MME generates a key through the same process as that of the UE and then decrypts the transmitted cypher text to get the IMSI.

Figure 5. Proposed protocol: initial attach with IMSI.


UE
eNB
MME
HSS
Initial State after Radio Link Synchronization
ECM Connection Establishment
RRC Connection
Attach Request (UE Network Capability, RN_{UE_1})
RN_{MME_1}
$\{F\}^{4n} = f(RN_{UE\_1}, RN_{MME\_1}, PLMN\ ID)$
$\{r^0\} = F_1, F_2, \cdots, F_n$
$\{r^1\} = F_{n+1}, F_{n+2}, \cdots, F_{2n}$
$\{lr\} = F_{2n+1}, F_{2n+2}, \cdots, F_{3n}$
$\{ad\} = F_{3n+1}, F_{3n+2}, \cdots, F_{4n}$
$Generate\ RN_{UE\_2}$
$RN_{UE\_2}' = RN_{UE\_2} \oplus lr$
$\{F\}^{4n} = f(RN_{UE\_1}, RN_{MME\_1}, PLMN\ ID)$
$\{r^0\} = F_1, F_2, \cdots, F_n$
$\{r^1\} = F_{n+1}, F_{n+2}, \cdots, F_{2n}$
$\{lr\} = F_{2n+1}, F_{2n+2}, \cdots, F_{3n}$
$\{ad\} = F_{3n+1}, F_{3n+2}, \cdots, F_{4n}$
$c \in \{0,1\}^i$
For i = 1 to n
$C_i \leftarrow \{ \begin{matrix} c_i || ad_i: if\ lr_i = 0 \\ ad_i || c_i: if\ lr_i = 1 \end{matrix}$
C_i
$if\ lr_i = 0, then\ C_i = c_i || ad_i$
$R_i \leftarrow \{ \begin{matrix} r_i^0 || RN_{UE\_2}{}_i': if\ c_i = 0 \\ r_i^1 || RN_{UE\_2}{}_i': if\ c_i = 1 \end{matrix}$
$if\ lr_i = 1, then\ C_i = ad_i || c_i$
$R_i \leftarrow \{ \begin{matrix} RN_{UE\_2}{}_i' || r_i^0: if\ c_i = 0 \\ RN_{UE\_2}{}_i' || r_i^1: if\ c_i = 1 \end{matrix}$
$[Error\ Detection]$
$if\ ad_i \neq ad_i, then\ R_i = Random$
$[Error\ Detection]$
$if\ r_i^0 \neq r_i^0\ or\ r_i^1 \neq r_i^1\ then\ Halt$
R_i
Unused $r_i^0 || r_i^1 = K_{IMSI}$
$E_{K_{IMSI}}(IMSI)$
Unused $r_i^0 || r_i^1 = K_{IMSI}$
RRC Connection Setup Complete
S1 Signaling Connection Establishment
ECM S1 Connection Establishment
Authentication
NAS Security Setup
Location Update
EPS Session Establishment
AS Security Setup
$E_{RN_{UE\_2}}(RNTI)$
$E_{RN_{UE\_2}}(RNTI)$

3.2. Initial Attach with GUTI

After the IMSI is safely transmitted, UE, eNB, MME and HSS carry out up to the “AS security setup” process during the “ECM connection establishment”, “authentication”, “NAS security setup”, “location update” and “EPS session establishment” processes.

After the “AS security setup”, the eNB encrypts RNTI to MME using the secret key of the “AS security setup” to allocate the RNTI to the UE. The MME encrypts the transmitted RNTI to RN$_{UE\_2}$ saved in the “ECM connection establishment” process to transmit to the eNB, and the eNB allocates the RNTI by transmitting the relevant value to the UE.

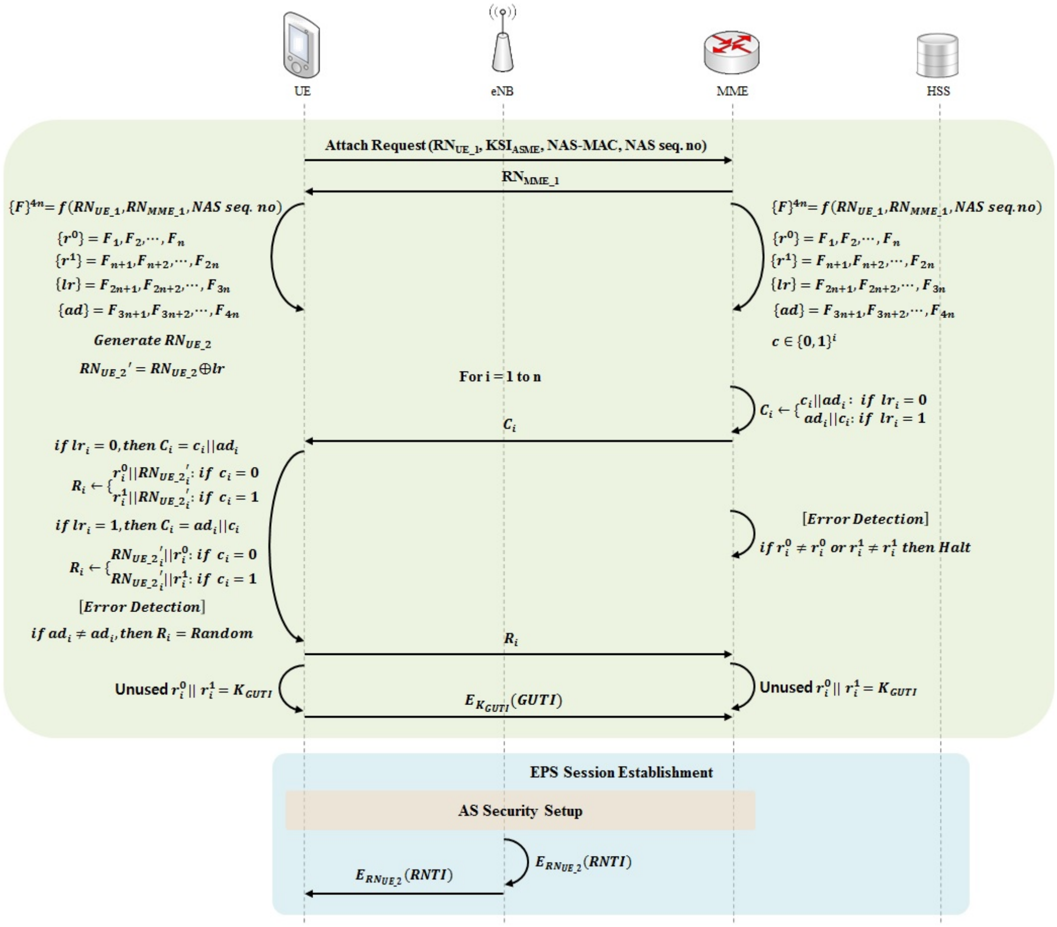
Initial attach with GUTI is the initial attach process of the case in which the UE that successfully performed an initial attach with the IMSI process re-accesses, due to a series of events. f() functions that are used in Section 3.2, are as the following formula.

$$\text{f()} = \text{hash(Expansion P-Box(hash(S-Box(RN}_{UE\_1}\text{), S-Box(RN}_{MME\_1}\text{), NAS seq. no.)))}$$

3.2.1. Case 1: MME Unchanged

The first case is that the connected MME in an initial connection with the UE is not changed, and the UE re-accesses through the same MME. Security protocol for the first case is shown in Figure 6.

Figure 6. Case 1: MME Unchanged.

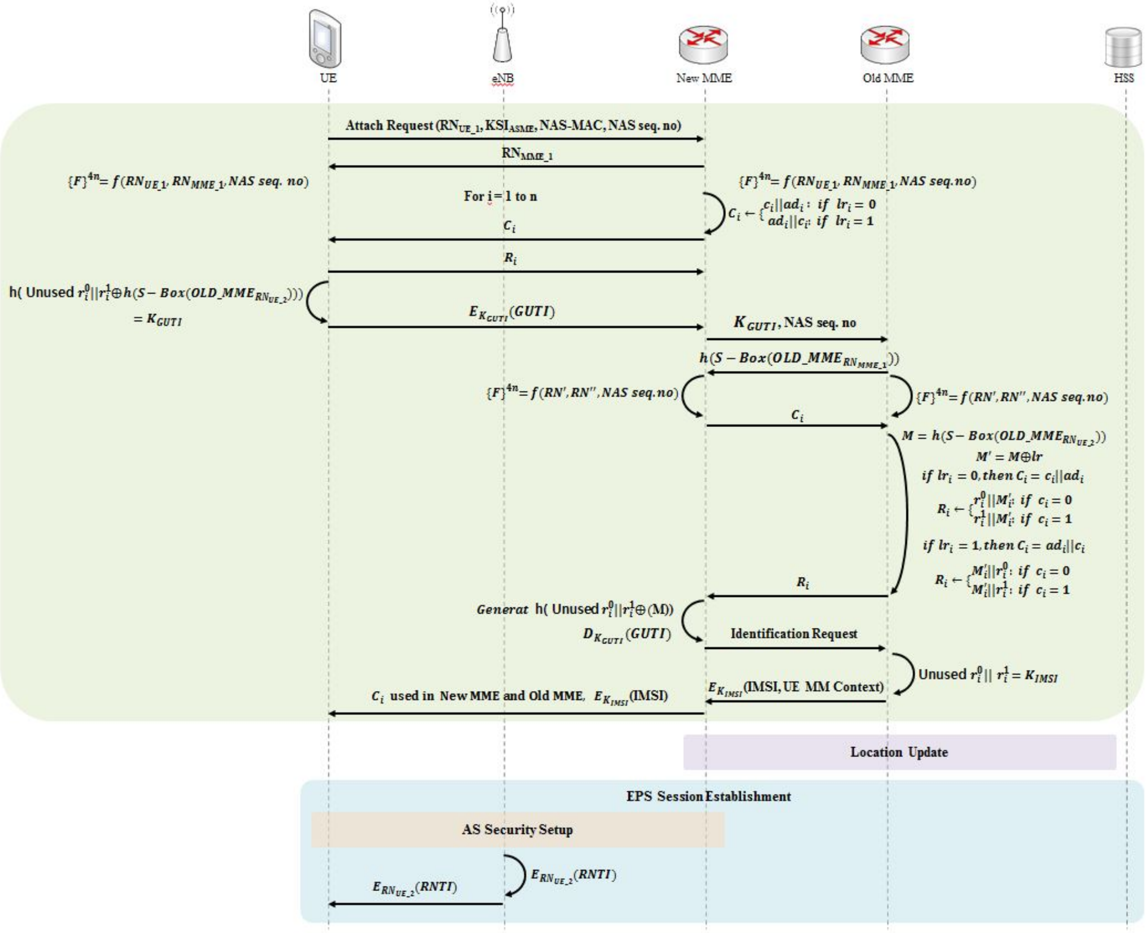

UE
eNB
MME
HSS
Attach Request (RN$_{UE\_1}$, KSI$_{ASME}$, NAS-MAC, NAS seq. no)
RN$_{MME\_1}$
$\{F\}^{4n} = f(RN_{UE\_1}, RN_{MME\_1}, NAS\ seq.\ no)$
$\{r^0\} = F_1, F_2, \cdots, F_n$
$\{r^1\} = F_{n+1}, F_{n+2}, \cdots, F_{2n}$
$\{lr\} = F_{2n+1}, F_{2n+2}, \cdots, F_{3n}$
$\{ad\} = F_{3n+1}, F_{3n+2}, \cdots, F_{4n}$
$Generate\ RN_{UE\_2}$
$RN_{UE\_2}' = RN_{UE\_2} \oplus lr$
$\{F\}^{4n} = f(RN_{UE\_1}, RN_{MME\_1}, NAS\ seq.no)$
$\{r^0\} = F_1, F_2, \cdots, F_n$
$\{r^1\} = F_{n+1}, F_{n+2}, \cdots, F_{2n}$
$\{lr\} = F_{2n+1}, F_{2n+2}, \cdots, F_{3n}$
$\{ad\} = F_{3n+1}, F_{3n+2}, \cdots, F_{4n}$
$c \in \{0,1\}^i$
For i = 1 to n
$C_i \leftarrow \{ \begin{matrix} c_i \| ad_i : if\ lr_i = 0 \\ ad_i \| c_i : if\ lr_i = 1 \end{matrix}$
C_i
$if\ lr_i = 0, then\ C_i = c_i \| ad_i$
$R_i \leftarrow \{ \begin{matrix} r_i^0 \| RN_{UE\_2}{}_i' : if\ c_i = 0 \\ r_i^1 \| RN_{UE\_2}{}_i' : if\ c_i = 1 \end{matrix}$
$if\ lr_i = 1, then\ C_i = ad_i \| c_i$
$R_i \leftarrow \{ \begin{matrix} RN_{UE\_2}{}_i' \| r_i^0 : if\ c_i = 0 \\ RN_{UE\_2}{}_i' \| r_i^1 : if\ c_i = 1 \end{matrix}$
$[Error\ Detection]$
$if\ ad_i \neq ad_i, then\ R_i = Random$
$[Error\ Detection]$
$if\ r_i^0 \neq r_i^0\ or\ r_i^1 \neq r_i^1\ then\ Halt$
R_i
Unused $r_i^0 \| r_i^1 = K_{GUTI}$
$E_{K_{GUTI}}(GUTI)$
Unused $r_i^0 \| r_i^1 = K_{GUTI}$
EPS Session Establishment
AS Security Setup
$E_{RN_{UE\_2}}(RNTI)$
$E_{RN_{UE\_2}}(RNTI)$

In a re-access, the initial attach process carries out authentication using GUTI to protect the IMSI. The process of transmitting the GUTI is the same as the Section 3.1. IMSI transmission process, and the initial attach process is carried out using existing information saved in the MME according to information, such as GUTI, NAS-MAC and NAS Seq. No. Since a series of information about the UE has already been saved in the MME, no "authentication", "NAS security setup" or "location update" process is carried out, but the "EPS session establishment" process only is carried out.

3.2.2. Case 2: MME Changed

The second case is that the MME is changed, but the old MME saves the information about the UE, so it transmits the information about the UE to the new MME. UE transmits the old MME's information to encrypt GUTI, so the new MME is transmitted the encryption key from the old MME using the challenge response method. Security protocol for the second case is shown in Figure 7.

Figure 7. Case 2: MME changed.


UE
eNB
New MME
Old MME
HSS
Attach Request (RN_{UE_1}, KSI_{ASME}, NAS-MAC, NAS seq. no)
RN_{MME_1}
$\{F\}^{4n} = f(RN_{UE\_1}, RN_{MME\_1}, NAS\ seq.\ no)$
For i = 1 to n
C_i
$\{F\}^{4n} = f(RN_{UE\_1}, RN_{MME\_1}, NAS\ seq.no)$
$C_i \leftarrow \{ c_i \| ad_i : if\ lr_i = 0;\ ad_i \| c_i : if\ lr_i = 1$
R_i
h(Unused $r_i^0 \| r_i^1 \oplus h(S - Box(OLD\_MME_{RN_{UE\_2}})))$
$= K_{GUTI}$
$E_{K_{GUTI}}(GUTI)$
K_{GUTI}, NAS seq. no
$h(S - Box(OLD\_MME_{RN_{MME\_1}}))$
$\{F\}^{4n} = f(RN', RN'', NAS\ seq.no)$
C_i
$\{F\}^{4n} = f(RN', RN'', NAS\ seq.no)$
$M = h(S - Box(OLD\_MME_{RN_{UE\_2}}))$
$M' = M \oplus lr$
$if\ lr_i = 0, then\ C_i = c_i \| ad_i$
$R_i \leftarrow \{ r_i^0 \| M_i' : if\ c_i = 0;\ r_i^1 \| M_i' : if\ c_i = 1$
$if\ lr_i = 1, then\ C_i = ad_i \| c_i$
$R_i \leftarrow \{ M_i' \| r_i^0 : if\ c_i = 0;\ M_i' \| r_i^1 : if\ c_i = 1$
R_i
Generat h(Unused $r_i^0 \| r_i^1 \oplus$ (M))
$D_{K_{GUTI}}(GUTI)$
Identification Request
Unused $r_i^0 \| r_i^1 = K_{IMSI}$
$E_{K_{IMSI}}$(IMSI, UE MM Context)
C_i used in New MME and Old MME, $E_{K_{IMSI}}$(IMSI)
Location Update
EPS Session Establishment
AS Security Setup
$E_{RN_{UE\_2}}(RNTI)$
$E_{RN_{UE\_2}}(RNTI)$

3.2.3. Case 3: MME Changed and IMSI Needed

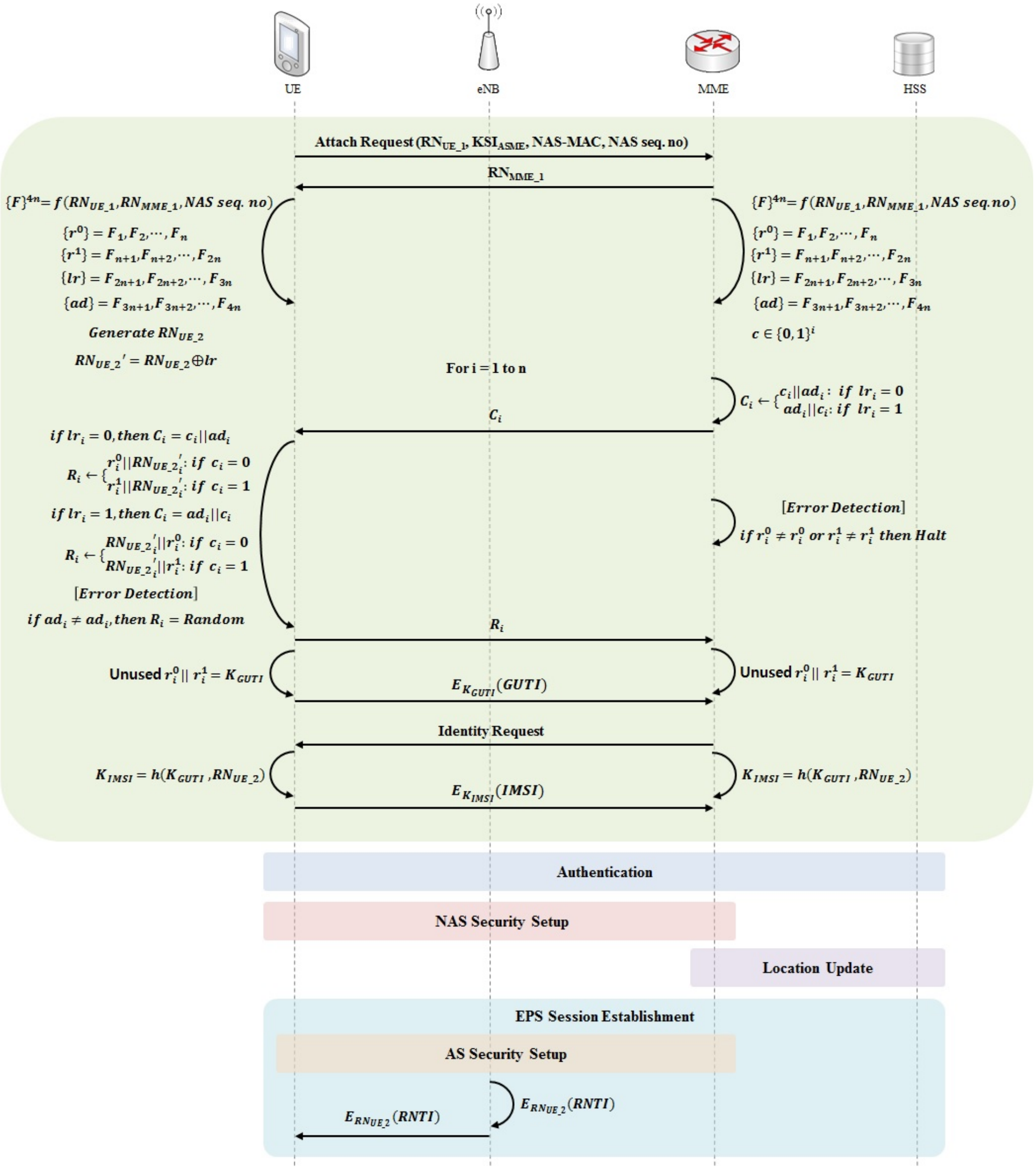
The third case is that the MME connected during the initial connection has been changed to a new MME, and there is no information about the UE in the MME connected during the initial connection.

In a re-access, the initial attach process carries out authentication using GUTI to protect the IMSI. The process of transmitting the GUTI is the same as the Section 3.1. IMSI transmission process.

When the MME is changed, the new MME requests the old MME for the information about the UE according to the information, such as GUTI, NAS-MAC and NAS Seq. No. At this time, if there is no information about the relevant UE in the old MME, the new MME requests the UE for the IMSI.

In this process, to safely transmit the IMSI, this proposed protocol transmits the GUTI, encrypts IMSI and transmits it using the generated series of values. For the encryption, the UE hashes KGUTIand RN$_{UE\_2}$ (RN, random number) to generate a key and encrypts the IMSI using the generated key, KIMSI, to transmit to the MME. After the transmission of the IMSI, the "authentication", "NAS security setup", "location update" and "EPS session establishment" processes are carried out. Security protocol for the third case is shown in Figure 8.

Figure 8. Case 3: MME changed and IMSI needed.


UE
eNB
MME
HSS
Attach Request (RN$_{UE\_1}$, KSI$_{ASME}$, NAS-MAC, NAS seq. no)
RN$_{MME\_1}$
$\{F\}^{4n} = f(RN_{UE\_1}, RN_{MME\_1}, NAS\ seq.\ no)$
$\{r^0\} = F_1, F_2, \cdots, F_n$
$\{r^1\} = F_{n+1}, F_{n+2}, \cdots, F_{2n}$
$\{lr\} = F_{2n+1}, F_{2n+2}, \cdots, F_{3n}$
$\{ad\} = F_{3n+1}, F_{3n+2}, \cdots, F_{4n}$
$Generate\ RN_{UE\_2}$
$RN_{UE\_2}' = RN_{UE\_2} \oplus lr$
$c \in \{0,1\}^i$
For i = 1 to n
$C_i \leftarrow \{ c_i||ad_i: if\ lr_i = 0;\ ad_i||c_i: if\ lr_i = 1$
C_i
$if\ lr_i = 0, then\ C_i = c_i||ad_i$
$R_i \leftarrow \{ r_i^0||RN_{UE\_2}{}_i': if\ c_i = 0;\ r_i^1||RN_{UE\_2}{}_i': if\ c_i = 1$
$if\ lr_i = 1, then\ C_i = ad_i||c_i$
$R_i \leftarrow \{ RN_{UE\_2}{}_i'||r_i^0: if\ c_i = 0;\ RN_{UE\_2}{}_i'||r_i^1: if\ c_i = 1$
$[Error\ Detection]$
$if\ ad_i \neq ad_i, then\ R_i = Random$
$[Error\ Detection]$
$if\ r_i^0 \neq r_i^0\ or\ r_i^1 \neq r_i^1\ then\ Halt$
R_i
Unused $r_i^0 || r_i^1 = K_{GUTI}$
$E_{K_{GUTI}}(GUTI)$
Unused $r_i^0 || r_i^1 = K_{GUTI}$
Identity Request
$K_{IMSI} = h(K_{GUTI}, RN_{UE\_2})$
$E_{K_{IMSI}}(IMSI)$
$K_{IMSI} = h(K_{GUTI}, RN_{UE\_2})$
Authentication
NAS Security Setup
Location Update
EPS Session Establishment
AS Security Setup
$E_{RN_{UE\_2}}(RNTI)$
$E_{RN_{UE\_2}}(RNTI)$

4. Security Analysis

The initial attach for UE process specified in the LTE Standards Release 12 transmits the parameters to identify the UE in plain text, and the proposed security protocol encrypts and safely transmits the relevant identification parameters. Security comparative analysis table is shown in Table 2.

Table 2. Security comparative analysis.

Identify Parameter	Original Initial Attach	Proposed Initial Attach
IMSI	Plain Text Transmission	Cipher Text Transmission
RNTI	Plain Text Transmission	Cipher Text Transmission
GTUI	Plain Text Transmission	Cipher Text Transmission

4.1. Key Definition, Encryption and Decryption

The proposed security protocols generate a key value used to encrypt identification parameters through the challenge-response process. The key used to encrypt IMSI and GUTI is defined as the value not used in the challenge-response process during the numerical progression generated through the f() function of the secret sharing between the UE and the MME. The relevant key value is defined only in the UE and MME, but not transmitted through the communication process to the outside. Therefore, an attacker can find the identification parameters only through the attack on the encryption algorithm, like AES-256, to know the encrypted IMSI and GUTI.

The key value encrypting the RNTI is transmitted through the challenge-response process, but the location of the bit continues to change for the transmission. Even if an attacker collects the bit string through an attack, like tapping, the probability of finding the key value with a total of *n* bits is $(1/4)^n$.

4.2. Error Detection and Verification

In the proposed security protocols, since the challenge-response and encryption are carried out through the f() function of the secret sharing between the UE and the MME and the key definition method, the UE and MME can verify if the other is a legitimate entity. In addition, in the challenge-response process, the UE can detect errors through $\mathrm{ad}_i \neq \mathrm{ad}_i$, and the MME can detect errors through $\mathrm{r}_i^0 \neq \mathrm{r}_i^0$ and $\mathrm{r}_i^1 \neq \mathrm{r}_i^1$.

4.3. Reliability

In order to secure the credibility of new MME, communication is only made possible when the UE, old MME and new MME have cross-authenticated each other. In this process, as the challenge-response method supports error detection, even a 1-bit mis-transmission will put a stop to the communication. Additionally, since IMSI is transmitted in the new MME using the values mutually shared by the UE and old MME during the past communication, the credibility of the new MME can be secured. In essence, since the UE constantly alters the MME, during which the key maintains continuity, like a hash-chain, safety against IMSI takeover through fake MME can be enhanced.

5. Performance Analysis

The performance analysis environment is shown Table 3 and original process's performance analysis is shown in Table 4. It was carried out on the LTE network components, UE, eNB and MME.

Table 3. Performance analysis environment.

Element	Values	Description
Cell	1	–
Number of UE	1, 50, 100	–
Test time	9000 s	Initial data (0–150 s) not reflected
Initial Attach Attempt Cycle	150 s	The UE service uses the initial attempt only
Portability Model	Deactivation	–

Table 4. Performance analysis: original process.

Device	Original Initial Attach		
	Time(s)	Delay(s)	Traffic Received (bits/s)
1	–	0.004600	1.214
50	–	0.007210	1.233
100	–	0.010302	1.033

All three initial attach processes include an initial attach with the IMSI process. The arithmetic operation of the encryption algorithm is carried out between the UE and the MME, and the eNB is used for passing through the communication process, so based on the initial attach with IMSI between the UE and the MME node, the average of overhead (time (s)), average delay (s) and average transmission rate (traffic received (bits/s)), the arithmetic operation of the encryption algorithm was measured and compared. In addition, for a performance analysis when the number of terminal users in the base station increases, the terminals were analyzed based on units of 1, 50 and 100 machine(s).

Since the existing initial attach does not perform encryption, time (s) was excluded. It was found that the delay according to the encryption process in the proposed algorithm decreased a little (somewhat), and since there was no packet switching other than the initial access process, it did not have an impact on the transmission rate. Performance analysis for proposed process is shown in Table 5 and Summary of performance analysis is shown in Table 6.

The maximum permissible delay in the LTE access network, based on the QCIdefined in 3GPP TS 23.203, is 100 ms (0.1 s) for FTP and web browsing, 50 ms (0.05 s) for video streaming and 30 ms (0.03 s) for VoIP. Based on VoIP with the lowest delay (0.03 s, 100%), the overhead and delay turned out to be 35.3% and 32.0%, respectively, for the arithmetic operation of encryption, so it was found that the initial attach of the proposed algorithm had less overhead. Since the transmission rate dealt with the initial entry process only prior to the security setup, it turned out to have no impact.

Table 5. Performance analysis: proposed process.

Device	**Proposed Initial Attach**		
	Time(s)	**Delay(s)**	**Traffic Received (bits/s)**
1	0.0110	0.007615	1.156
50	0.0103	0.010510	1.301
100	0.0109	0.014006	1.100

Table 6. Summary of performance analysis.

Device	**Summary (Based on VoIP 100%)**		
	Time(s)	**Delay(s)**	**Traffic Received (bits/s)**
1	36%	39%	1%
50	34%	31%	0.9%
100	36%	26%	0.9%
Total Average	35.3%	32.0%	0.93%

6. Conclusions

In this paper, a security protocol was proposed in order to solve the vulnerability of the unique identification value being transmitted as clear text, which is constantly being pointed out in LTE standards and related technical documents, and to be used as a basic study of mobile communication technology to be used in the future cyber world.

The proposed security protocol was designed to safely transmit IMSI, RNTI and GUTI in a variety of initial attach processes when the UE accesses the LTE network. The proposed security protocol generated a key through the challenge-response method to encrypt and transmit the unique ID and support error detection and verification. As a result of a performance analysis, the security protocol encrypted and safely transmitted vulnerability parameters and turned out to have a performance of an average of 32.0% based on VoIP 100%, demanding a lower rate of delay, so that the safety and performance of the proposed encryption algorithm were found to be efficient.

After all of the analyses, the proposed security protocols had less overhead and fully satisfied the privacy requirements and the maximum permissible delay defined in LTE standards.

Author Contributions

Uijin Jang researched relation work; Hyungjoo Kim designed the shceme; Uijin Jang and Hyungmin Lim performed and analyzed the data; Uijin Jang and Hyungjoo Kim wrote the paper.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Park, S.-W.; Lee, I.-Y. Anonymous Authentication Scheme based on NTRU for the Protection of Payment Information in NFC Mobile Environment. *J. Inf. Process. Syst.* **2013**, *9*, 461–476.
2. Teraoka, T. Organization and exploration of heterogeneous personal data collected in daily life. *Hum.-Centric Comput. Inf. Sci.* **2012**, *2*, 1–15.
3. Carvalho, G.H.S.; Woungang, I.; Anpalagan, A.; Dhurandher, S.K. Energy-Efficient Radio Resource Management Scheme for Heterogeneous Wireless Networks: A Queueing Theory Perspective. *J. Converg.* **2012**, *3*, 15–22.
4. Luo, H.; Shyu, M.-L. Quality of service provision in mobile multimedia—A survey. *Hum.-Centric Comput. Inf. Sci.* **2011**, *1*, 1–15.
5. Crowell, A.; Ng, B.H.; Fernandes, E.; Prakash, A. The Confinement Problem: 40 Years Later. *J. Inf. Process. Syst.* **2013**, *9*, 189–204.
6. Bikos, A.N.; Sklavos, N. LTE/SAE Security Issues on 4G Wireless Networks. *IEEE Secur. Priv.* **2013**, *11*, 55–62.
7. *Technical Specification Group Services and System Aspects; Rationale and Track of Security Decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE)*; 3GPP: Valbonne, France, 2010; Release 8.
8. *Policy and Charging Control Architecture*; 3GPP: Valbonne, France, 2009; Release 10.
9. *Telecommu-nication management; Security Management concept and requirements*; 3GPP: Valbonne, France, 2012; Release 10.
10. Kwak, H.; Lee, P.; Kim, Y.; Saxena, N.; Shin, J. Mobility Management Survey for Home-eNB Based 3GPP LTE Systems. *J. Inf. Process. Syst.* **2008**, *4*, 145–152.
11. Lee, P.; Jeong, J.; Saxena, N.; Shin, J. Dynamic Reservation Scheme of Physical Cell Identity for 3GPP LTE Femtocell Systems. *J. Inf. Process. Syst.* **2009**, *5*, 207–220.
12. Singh, R.; Singh, P.; Duhan, M. An effective implementation of security based algorithmic approach in mobile adhoc networks. *Hum.-Centric Comput. Inf. Sci.* **2014**, *4*, doi:10.1186/s13673-014-0007-9.
13. Algur, S.P.; Kumar, N.P. Novel user centric, game theory based bandwidth allocation mechanism in WiMAX. *Hum.-Centric Comput. Inf. Sci.* **2013**, *3*, doi:10.1186/2192-1962-3-20.
14. Jang, U.; Lim, H.; Kim, H. Security Scheme for Initial Attach in LTE. In Proceedings of the 2nd FTRA International Conference on Ubiquitous Computing Application and Wireless Sensor Network, Jeju, Korea, 7–10 July 2014.
15. Sharma, M.J.; Leung, V.C.M. IP multimedia subsystem authentication protocol in LTE-heterogeneous networks. *Hum.-Centric Comput. Inf. Sci.* **2012**, *2*, doi:10.1186/2192-1962-2-16.
16. Netmanias. EMM Procedure 1. Initial Attach for Unknown UE (Part 1)—Case of Initial Attach. NMC Consulting Group Co. Ltd.: Seoul, Korea, 26 Decmeber 2013.
17. Netmanias. EMM Procedure 1. Initial Attach for Unknown UE (Part 2)—Call Flow of Initial Attach. NMC Consulting Group Co. Ltd.: Seoul, Korea, 16 January 2014.

18. Hwang, K.I.; Nam, S.-W. Near Real-time M2M Communication for Bidirectional AMR Systems. *J. Converg.* **2014**, *5*, 1–7.
19. Cho, H.; Choi, M. Personal Mobile Album/Diary Application Development. *J. Converg.* **2014**, *5*, 32–37.
20. Chong, J.H.; Ng, C.K.; Noordin, N.K.; Ali, B.M. A low computational complexity V-BLAST/STBC detection mechanism in MIMO system. *Hum.-Centric Comput. Inf. Sci.* **2014**, *4*, doi:10.1186/s13673-014-0002-1.
21. Chung, Y.; Choi, S.; Won, D. Lightweight anonymous authentication scheme with unlinkability in global mobility networks. *J. Converg.* **2013**, *4*, 23–29.
22. Escudero-Andreu, G.; Phan R.C.-W.; Parish, D.J. Analysis and Design of Security for Next Generation 4G Cellular Networks. In Proceedings of the 13th Annual Post Graduate Symposium on the Convergence of Telecommuni-Cations, Networking and Broad-Casting (PGNET), Liverpool, UK, 25–26 June 2012.
23. Netmanias. LTE Security I: LTE Security Concept and Authenti-cation. NMC Consulting Group Co. Ltd.: Seoul, Korea, 31 July 2013.
24. Netmanias. LTE Security II: NAS and AS Security. NMC Consulting Group Technical Specifications. NMC Consulting Group Co. Ltd.: Seoul, Korea, 5 August 2013.
25. Peng, K. A Secure Network for Mobile Wireless Service. *J. Inf. Process. Syst.* **2013**, *9*, 247–258.
26. Kambourakis, G.; Kolias, C.; Gritzalis, S.; Park, J.H. DoS Attacks Exploiting Signaling in UMTS and IMS. In *Computer Communications*; Elsevier: Oxford, UK, 2011; pp. 226–235.
27. Angermeier, D.; Kiening, A.; Stumpf, F. PAL-privacy augmented LTE: A privacy-preserving scheme for vehicular LTE communication. In Proceedings of the Tenth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications, Taipei, Taiwan, 25 June 2013; pp. 1–10.