symmetry

MDPI

Article

Security Scheme Based on Parameter Hiding Technic for Mobile Communication in a Secure Cyber World

Jong Hyuk Park [1], Hyungjoo Kim [2] and Jungho Kang [3,*]

1 Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), 232 Gongneung-ro, Nowon-gu, Seoul 01811, Korea; jhpark1@seoultech.ac.kr
2 Convergence Laboratory, KT Research and Development Center, 151 Taebong-ro, Seocho-gu, Seoul 06763, Korea; hyungjoo.kim@kt.com
3 Department of Computer Science and Engineering, Soongsil University, 369 Sangdo-Ro, Dongjak-gu, Seoul 06978, Korea
* Correspondence: kjh7548@ssu.ac.kr; Tel.: +82-2-826-6526

Academic Editor: Young-Sik Jeong
Received: 6 September 2016; Accepted: 2 October 2016; Published: 17 October 2016

Abstract: Long Term Evolution (LTE) and Long Term Evolution-Advanced (LTE-A) support a better data transmission service than 3G dose and are globally commercialized technologies in a cyber world that is essential for constructing a future mobile environment, since network traffics have exponentially increased as people have started to use more than just one mobile device. However, when User Equipment (UE) is executing initial attach processes to access LTE networks, there is a vulnerability in which identification parameters like International Mobile Subscriber Identity (IMSI) and Radio Network Temporary Identities (RNTI) are transmitted as plain texts. It can threat various services that are commercialized therewith in a cyber world. Therefore, a security scheme is proposed in this paper where identification parameters can be securely transmitted and hidden in four cases where initial attach occurs between UE and Mobility Management Entity (MME). The proposed security scheme not only supports encrypted transmission of identification parameters but also mutual authentication between Evolved Node B (eNB) and MME to make a secure cyber world. Additionally, performance analysis results using an OPNET simulator showed the satisfaction of the average delay rate that is specified in LTE standards.

Keywords: initial attach; mutual authentication; LTE; hiding technic; session management

1. Introduction

Long Term Evolution (LTE) is 4th generation mobile communication technology and can provide a better data transmission service than 3G dose in the cyber world that is essential for constructing a future mobile environment [1–3]. Since network traffics have exponentially increased as people have started to use more than just one mobile device, they has become more important [4–6]. Release 12 is currently underway in LTE standards, and LTE networks where part of Release 10 technologies are applied based on Release 9 can be classified as a LTE advanced technology introduction country [7]. Even though LTE standards that have been drafted since 2004 solved various security vulnerabilities found in LTE, some vulnerabilities have still not been security-updated, but they are specified as vulnerabilities in the standards [8–10]. The most issued vulnerability among various vulnerabilities is the one where the identification parameter values in user equipment (UE) are exposed as plain texts [11,12].

Therefore, a method is proposed in this paper for transmitting identification parameters securely and for hiding key parameter based on mutual authentication between UE, eNB, and MME in 4 initial attach cases to make a secure cyber world.

Table 1 displays the definitions and terms used in this paper.

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

UE	User Equipment (e.g., Smart Phone)
eNB	Evolved Node B
MME	Mobility Management Entity
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
RNTI	Radio Network Temporary Identities
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	4 n bits String by h()
C	Challenge Bits
SSK	Secret Sharing Key
S-Box	Substitution-Box

This paper consists of six sections. Section 2 analyzes LTE. In Section 3, four kinds of initial attach security schemes in each case are to be proposed so that identification parameters can be securely transmitted. Section 4 compares a security analysis of the proposed scheme, and Section 5 evaluates the performances between the proposed scheme and the existing process. Section 6 concludes the discussion.

2. LTE

2.1. The LTE Network

The LTE network consists of LTE entities that are wireless access network technology and Evolved Packet Core (EPC) entities that are core network technology [13]. UE refers to user devices such as smart-phones among LTE entities. eNB is the base station [14,15]. eNB provides the user with wireless interface and 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). MME communicates with Home Subscriber Server (HSS) for downloading user authentication and user profiles and executes initial attach and authentication. In other words, authentication of user personal profile information that is saved in HSS is executed using MME; at this time, eNB is used as a connection instrument [16,17]. However, there are various threats that can harm the entire LTE network by tracing attacks, terminal tracing attacks, and privacy infringement attacks during a LTE initial attach process [18–20].

2.2. LTE Initial Attach for UE and Threats

Initial attach is the first access process to the mobile network by the user subscribing the LTE network using UE. For this, eNB is selected in the initial state process; after matching synchronization, IMSI, which is an identification parameter, is transmitted to request that MME access the network in the ECM connection establishment process [21].

IMSI refers to the unique ID requested of each user when the mobile network administrator registers the user to the service, and IMSI refers to the unique binary code of identifications saved in a Universal Subscriber Identity Module (USIM) [22].

IMSI transmitted as plain text is transmitted to MME through thousands of eNBs and has the vulnerability that IMSI is leaked to attackers by malicious eNBs. 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 RAN/3GPP System Architecture Evolution(SAE) (Release 9)," there are vulnerabilities during the initial attach process for using the LTE mobile network, in which the UE identifying parameters are transmitted in plain text. Tracing and privacy issues easily occur with this vulnerability [11,12,21,22].

However, current LTE initial attach processes are executing EPS-AKA based mutual authentication and encrypted communication focusing on classes such as Non Access Stratum (NAS) security setup after completing ECM connection establishment processes between UE and eNB [23,24]. In other words, because communication protocols that transmit identification parameters as plain texts are already used before mutual authentication and encrypted communication, related user tracing attacks, terminal tracing attacks, and privacy infringement attacks can occur using leaked IMSI [25,26]. Additionally, RNTI, which is the only identification value sorting UE in eNB, and Global Unique Temporary Identifier (GUTI), which is used instead of IMSI after a series of processes, are transmitted as plain texts in various cases; therefore, vulnerabilities and attack threats of IMSI are equally likely to occur [27,28].

3. Proposed Security Scheme

The proposed scheme was designed to protect original identification information such as IMSI and RNTI that are transmitted as plain texts when UE tries an initial attach in the network. It is composed of four cases in total, according to UE's initial access types, and eNB and MME are assumed to be a secure channel along with the backbone network.

3.1. Secret Sharing

MNO applies the secret sharing method to UE, eNB, and MME for the secure initial attach process; in other words, UE is executed in MNO before distributing UICC.

MME selects three points of SSK_{UE}, SSK_{eNB}, and SSK_{MME} in the curve that has a secret value, S, and passes $Y = aX^2 + bX + S$. SSK_{UE} is stored in UE, and SSK_{MME} is stored in MME. Finally, SSK_{eNB} is stored in eNB; at this moment, h(SSKUE) is saved together with eNB as a corresponding value with SSK_{eNB}.

3.2. Initial Attach with IMSI

The first protocol is shown as Figure 1 and carried out after the Initial State after Radio Link Synchronization process is completed in the initial attach in the IMSI case. The first protocol is based on mutual authentication between UE and eNB MME and is designed to protect IMSI, which is leaked as plain texts in the ECM connection establishment process, and RNTI, which is leaked as plain texts in the EPS session establishment process.

UE transmits a random number and the UE network capability generated for the attach request to MME. MME, which receives the attach request, generates random numbers and transmits them to UE, and UE and MME execute a series of calculation to transmit IMSI securely.

UE and MME inputs transmitted and received random numbers and PLMN ID to the hash function, which has secret sharing according to MNC and generates 4 n bits F string. Generated F stings are divided into four sequences with each n bits. MME generates random number sequences that are used as challenge bits, and UE generates SSKUE' and calculates a lr sequence and exclusive.

MME generates challenge bits Ci using lr$i$, ad$i$, and ci. Ci is composed of Ci = ci || ad$i$ when lr$i$ is 0, and of Ci = ad$i$ || ci when lr$i$ is 1. MME transmits Ci to UE and verifies UE through response values, and UE verifies MME through Ci.

Because UE knows lr, UE can distinguish Ci which is transmitted by MME between Ci = ci || ad$i$ and Ci = ad$i$ || ci. In case lr$i$ is 0, UE generates Ri = SSK_{UEi}' || r_i^0 or Ri = SSK_{UEi}' || ri^1; in case lr$i$ is 1, UE generates Ri = r_i^0 || SSK_{UEi}' or Ri = r_i^1 || SSK_{UEi}'. At this moment, r_i^1 transmits r_i^0 when ci transmitted by MME is 0, and transmits to ri1 when ci is 1. Through this process, MME receives UE's SSK_{UE}.

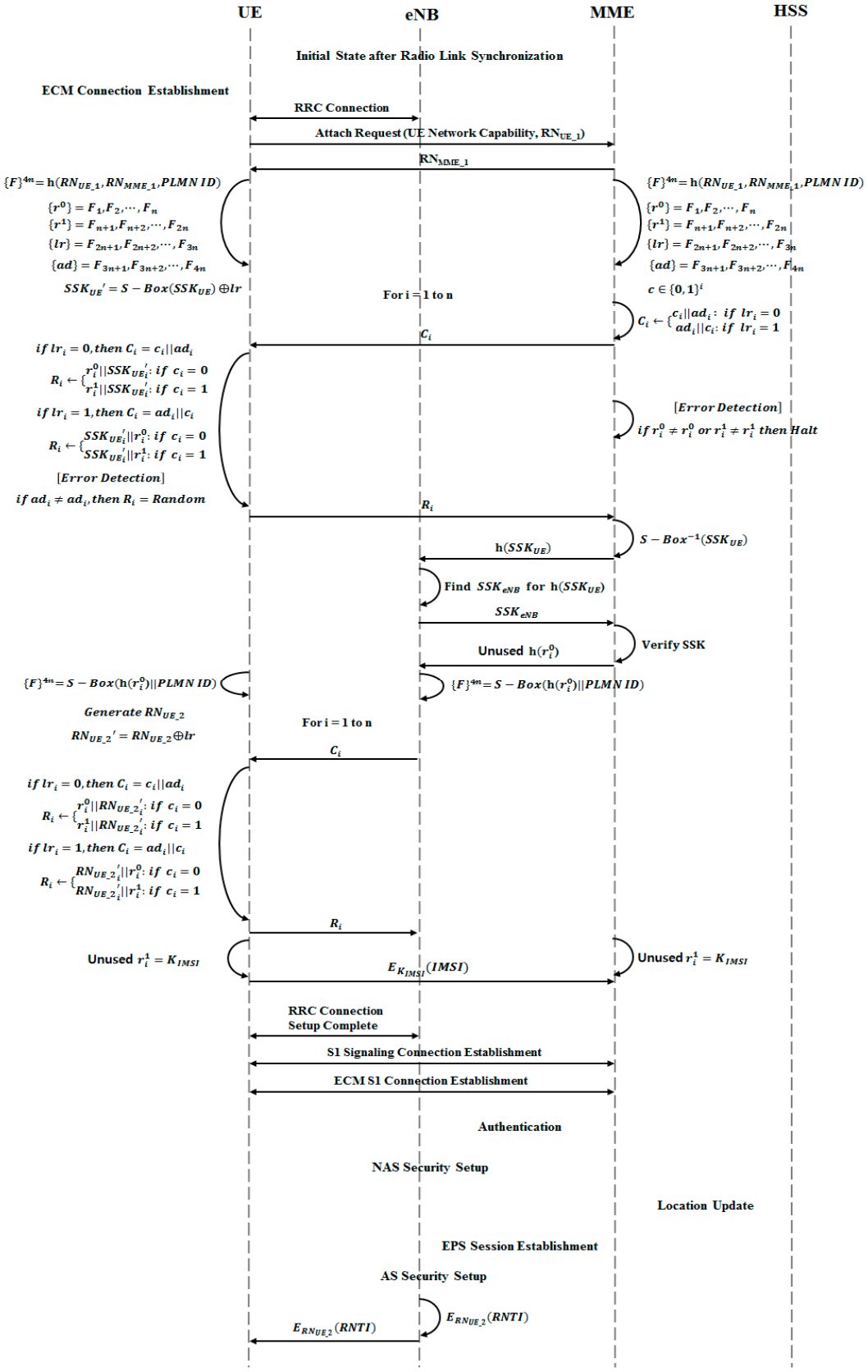

Figure 1. Proposed protocol: Initial attach with International Mobile Subscriber Identity (IMSI).

After the challenge response process, MME transmits SSK_{UE}, which is drawn through s-box inverse function and transmits to eNB after hashing SSKUE. eNB transmits SSK_{eNB}, which corresponds with $h(SSK_{UE})$ to MME. MME verifies whether a correct secret value, S, is drawn by substituting SSK_{MME}, SSK_{UE}, and SSK_{eNB}, which are corresponding with SSK_{UE} in $Y = aX^2 + bX + S$. In case verification of all SSK is successful, MME makes a hash calculation of unused r_i^0 and subsequently transmits to eNB.

UE and eNB execute the challenge response process using $h(r_i^0)$, and the random number, RN_{UE_2}, which is generated by UE, is transmitted to eNB.

After the second challenge response process is completed, UE transmits encrypted IMSI to MME using unused ri1 as a key. MME obtains ISMI by decoding received encrypted messages through the same process with UE.

After IMSI is securely transmitted, it executes down to the Access Stratum (AS) security setup process among the processes of ECM connection establishment, verification, NAS security setup, location update, and EPS session establishment. After AS security setup is completed, eNB transmits encrypted RNTI to MME using a secret key of the AS security setup in order to allocate RNTI to UE. eNB allocates received RNTI by encrypting received RNTI to RN_{UE_2}, which is saved in the ECM connection establishment process, and by transmitting to UE.

3.3. Initial Attach with GUTI

3.3.1. MME Unchanged

The first case is shown as Figure 2. The "MME Unchanged" case is the one where the MME connected with UE at initial access is not changed, and UE accesses through identical MME at the time of re-access. At the time of re-access, the initial attach process executes verification using GUTI in order to protect ISMI. The process that transmits GUTI is identical to the IMSI transmission process in Section 3.2, and the initial attach process is executed using existing information which is saved in the MME according to information such as GUTI, NAS-MAC, and NAS sequence number. Because the series of information about UE is saved in MME, processes of authentication, the NAS Security Setup, and the location update are not executed, and only the EPS session establishment process is executed.

3.3.2. MME Changed

The second case is shown as Figure 3. The second case is the one that the information about UE is transmitted to new MME because the information about UE is saved in old MME, even though MME is changed. Processes that transmit GUTI are the same as that in other cases, and new MME receives UE information from old MME using information such as GUTI, NAS-MAC, and NAS sequence number.

3.3.3. MME Changed and IMSI Needed

The third case is shown as Figure 4. The third case is the one where MME connected with UE at the initial access is changed to new MME, and UE information connected at the time of initial access does not exist in MME. At the time of re-access, the initial attach process executes authentication using GUTI. The process that transmits GUTI is identical to the IMSI transmission process in Section 3.2.

In case MME is changed, new MME requests UE information according to information such as GUTI, NAS-MAC, and NAS sequence number. At this moment, when relevant UE information does not exist in old MME, new MME requests IMSI to UE.

In order to securely transmit IMSI in this process, UE generates a key by hashing KGUTI and RN_{UE_2}, and transmits to MME by encrypting IMSI using a generated key KIMSI. After IMSI is transmitted, processes of authentication, the NAS security setup, the location update, and the EPS session establishment are executed.

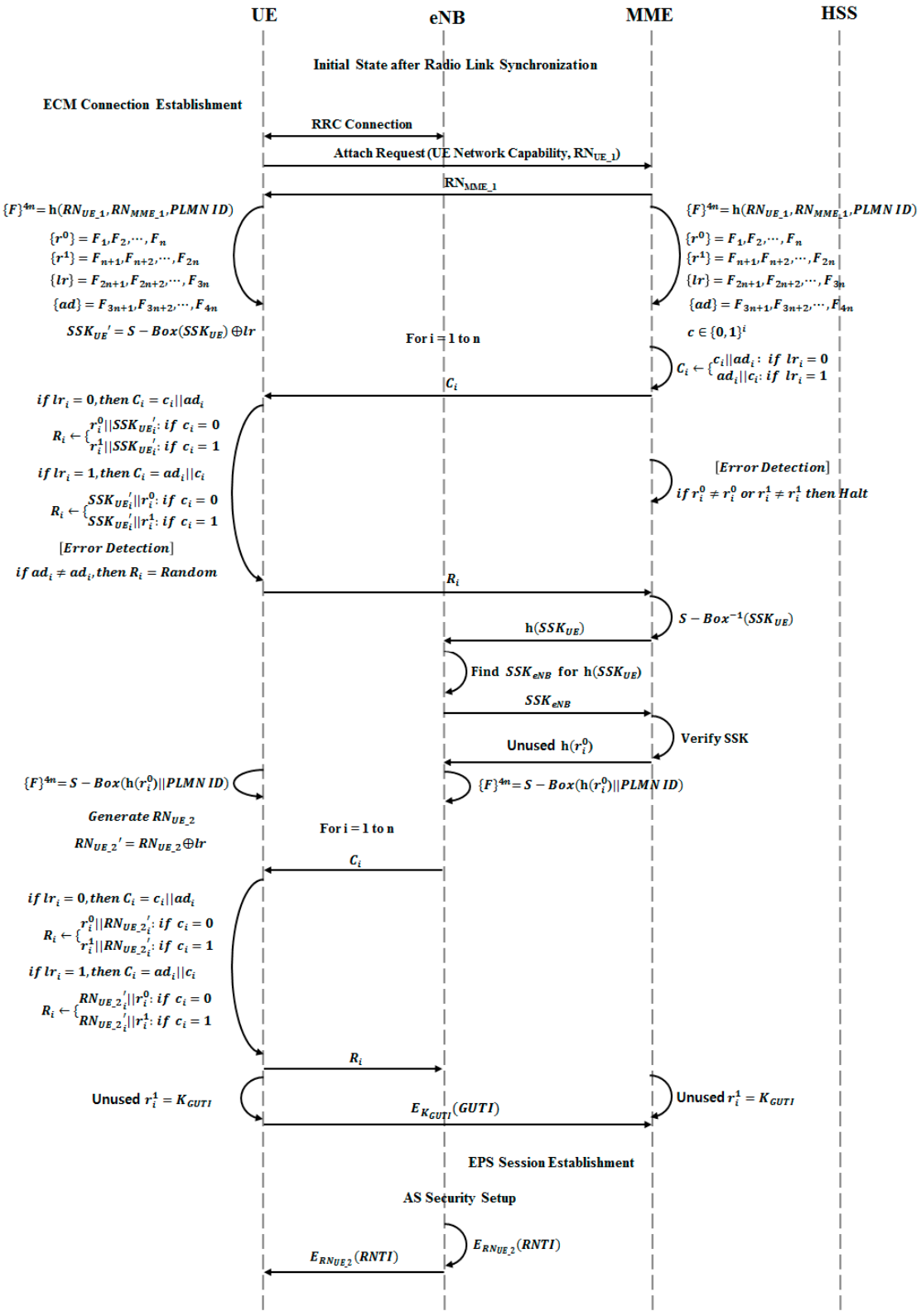

Figure 2. Case 1: Mobile Management Entity (MME) unchanged.

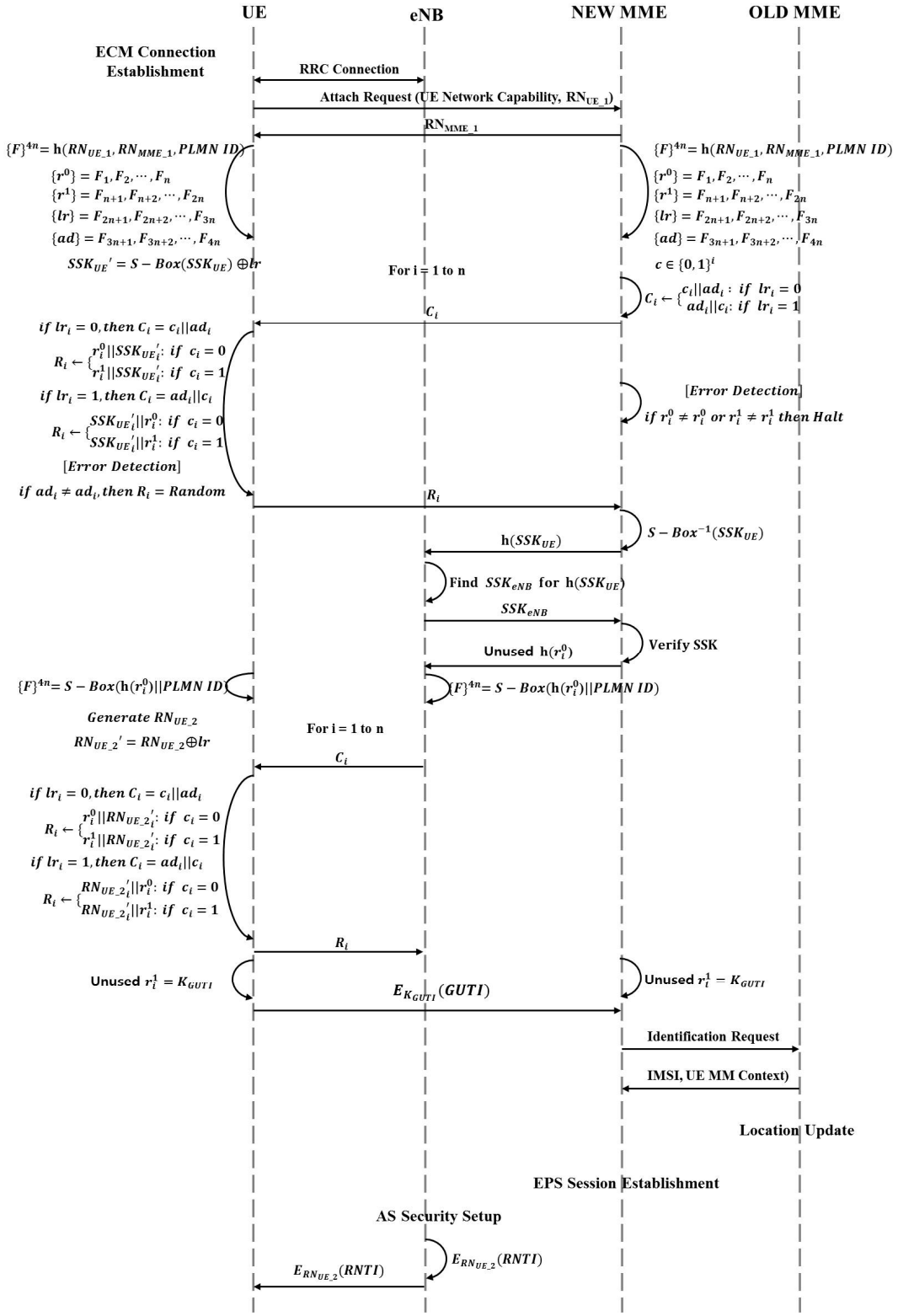

Figure 3. Case 2: MME changed.

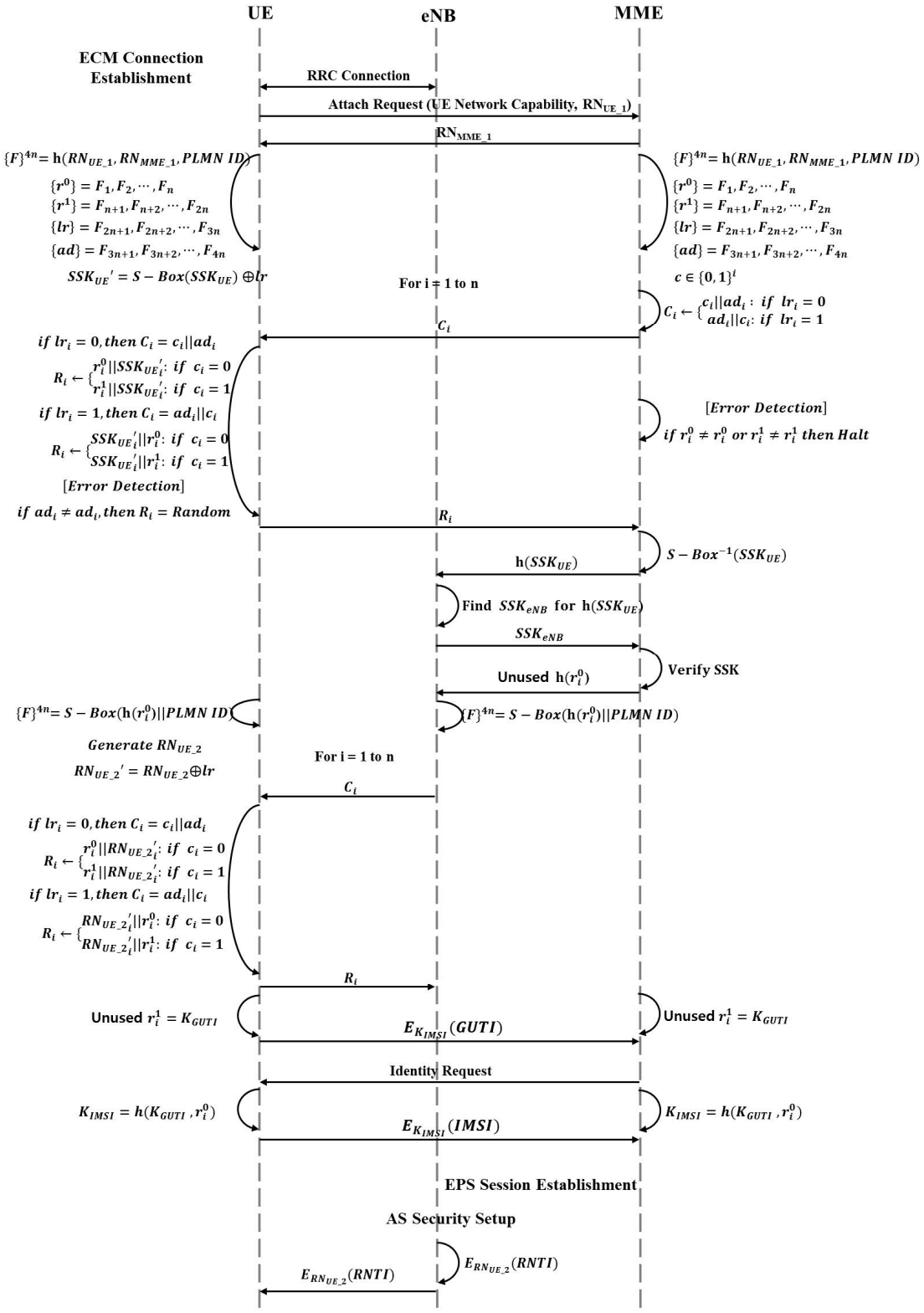

Figure 4. Case 3: MME changed and IMSI needed.

4. Security Analysis

As shown in Table 2, the existing initial attach specified in the LTE standards transmits identification parameters as plain texts; in the proposed security scheme, relevant identification parameters are securely transmitted through encryption. Additionally, it supports mutual authentication before identification

parameters are transmitted and eNB also supports authentication. Therefore, it is also secure in identification parameter exposure through malicious eNB.

Table 2. Security analysis.

Vurnerable Information and Layer	Original Initial Attach	Proposed Initial Attach
Mutual Authentication between UE and eNB	Not Supported	Supported
Mutual Authentication between UE and MME	Not Supported	Supported
Mutual Authentication between eNB and MME	Not Supported	Supported
IMSI	Plain Text Transmission	Cipher Text Transmission
RNTI	Plain Text Transmission	Cipher Text Transmission
GTUI	Plain Text Transmission	Cipher Text Transmission

4.1. Mutual Authentication

In the proposed security scheme, methods are being provided that UE, eNB, and MME can mutual authenticate at least twice.

In the first challenge response process, UE and MME can mutual authenticate each other by generating and transmitting a series of bit strings through previously shared hash functions. Subsequently, MME can verify UE and eNB again using SSKUE and SSKeNB in restoring process of secret value, S.

In the second challenge response process, UE can verify eNB because UE uses r0 bit sequences that are not used in the first challenge response and previously shared S-BOX. Additionally, eNB can verify UE through the challenge response process and verify MME as well because the authentication about r0 sequence is executed.

4.2. Error Detection and Verification

In the proposed security scheme, error detection and verification are provided through challenge response process. If adi transmitted by MME is adi $\neq$ adi, UE can detect errors and transmit responding values as random values. MME also halts the attach process when error is detected through $ri^0 \neq ri^0$ and $ri^1 \neq ri^1$.

Errors in the challenge response process between UE and eNB can also be detected through adi $\neq$ adi and can be detected through $ri^0 \neq ri^0$ and $ri^1 \neq ri^1$.

4.3. Mafia and Terrorist Attack

Mafia attack success probability which can be executed in the challenge response process is $(1/4)n$ and terrorist attack success probability is $(1/4)n$. Assuming the length of key as 256 bits, f string is 512 bit; therefore, success probabilities of both attacks are (1/4)512, which are more secure than AES-256 algorithm [29].

4.4. Key Definition, Encryption, and Decryption

In the proposed security scheme, key values used to encrypt identification parameters are generated through the challenge response process. A key value used for IMSI and GUTI encryption is defined as the value that is not used in the challenge response process among the generated sequences through hash functions, which are secretly shared between UE and MME. Relevant key values are defined only within UE and MME and are not transmitted outside through communication processes. Therefore, in order to detect the encrypted IMSI and GUTI, attackers can detect identification parameters only through the attacks to encrypted algorithms such as AES-256.

5. Performance Analysis

The performance analysis environment is shown in Table 3. It was carried out on the LTE mobile network components—UE, eNB, and MME.

Table 3. Performance analysis environment.

Variable	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 initial attempt only
Portability Model	Deactivation	-

All three initial attach processes evaluating network components include an initial attach with an IMSI process. The arithmetic operation such as hash and s-box function of the encryption algorithm is carried out between the UE and the MME; therefore, based on the initial attach with the IMSI between the UE and the MME node, the average of delay and overhead (time (s)), the average delay (s), the average transmission rate (traffic received (bits/s)), and the arithmetic operation of the encryption algorithm was measured and compared. Additionally, the terminals were analyzed based on the units of 1, 50, and 100 machine (s), because the number of terminal users in the base station could be increased.

Since the existing initial attach does not compute encryption operation, time was excluded. We also found that the delay according to the encryption operation in the proposed scheme decreased a little because there was no packet switching or transmission other than the original initial access process. It was analyzed and evaluated: it did not have a delay on the transmission rate according Tables 4 and 5.

Table 4. Performance analysis: Original process.

Device	Original Initial Attach		
	Time (s)	Delay (s)	Traffic Received (bits/s)
1	-	0.004700	1.234
50	-	0.007260	1.249
100	-	0.010292	1.039

Table 5. Performance analysis: Proposed process.

Device	Proposed Initial Attach		
	Time (s)	Delay (s)	Traffic Received (bits/s)
1	0.0113	0.007715	1.159
50	0.0105	0.010539	1.331
100	0.0114	0.014576	1.108

The maximum permissible delay in the LTE access network, defined in 3GPP (TS 23.203), is 30 ms for Voice over Internet Protocol (VoIP). Based on VoIP with the lowest delay, the overhead and delay turned out to be 35.5% and 33.0%, respectively, for the arithmetic operation of encryption, so we found that the initial attach of the proposed scheme had less overhead and fully satisfied the maximum permissible delay as shown Table 6.

Table 6. Summary of performance analysis.

Device	Summary (Based on VoIP 100%)		
	Time (s)	Delay (s)	Traffic Received (bits/s)
1	36%	40%	1%
50	34%	32%	0.9%
100	36%	28%	0.9%
Total Avg.	35.5%	33.0%	0.93%

6. Conclusions

In this paper, a security scheme for LTE initial attach conforming to LTE standards was proposed in order to solve vulnerability where identification parameters are transmitted as plain texts before mutual authentication. The proposed security scheme was designed so that UE, eNB, and MME can transmit identification parameter after mutual authentication according to four cases where initial attach occurs.

The proposed security scheme generated a security key through a challenge response process to hide and transmit the IMSI and RNTI, and support error detection and verification. As a result of a performance analysis, the security scheme turned out to use the performance of an average of 33.0% based on VoIP 100% demanding a lower rate of delay. Through security analysis, the proposed scheme is more secure than the original initial attach process.

Therefore, the proposed scheme employs the initial attach process in real LTE mobile networks and helps future cyber worlds such as IoT (Internet of Things) and CPS (Cyber Physical System), which is needed for mobility devices to function.

Acknowledgments: This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2016-H8601-16-1009) supervised by the IITP (Institute for Information & communications Technology Promotion).

Author Contributions: Hyungjoo Kim researched relation work; Jong Hyuk Park designed the protocol; Jungho Kang and Hyungjoo Kim performed and analysed the data; Jong Hyuk Park and Hyungjoo Kim wrote the paper; Jungho Kang totally supervised for this paper work, review and comments, etc.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Martin, S.; Nicolae, P.; Rosario, G. *5G: Towards Secure Ubiquitous Connectivity Beyond 2020*; SICS: Kista, Sweden, 2015.
2. Forsberg, D.; Horn, G.; Moeller, W.-D.; Niemi, V. *LTE Security*; John Wiley & Sons: Hoboken, NJ, USA, 2012.
3. Gohar, M.; Koh, S. Inter-domain mobility management based on the proxy mobile IP in mobile networks. *J. Inf. Process. Syst.* **2016**, *12*, 196–213.
4. Rahman, M.A.; Lee, Y.-D.; Koo, I. An efficient transmission mode selection based on reinforcement learning for cooperative cognitive radio networks. *Hum.-Centric Comput. Inf. Sci.* **2016**, *6*, 2. [CrossRef]
5. Gaur, M.S.; Pant, B. Trusted and secure clustering in mobile pervasive environment. *Hum.-Centric Comput. Inf. Sci.* **2015**, *5*, 32. [CrossRef]
6. Dahane, A.; Berrached, N.-E.; Loukil, A. A virtual laboratory to practice mobile wireless sensor networks: A case study on energy efficient and safe weighted clustering algorithm. *J. Inf. Process. Syst.* **2015**, *11*, 205–228.
7. Amsavalli, A.; Kashwan, K.R. Smart patch antenna array for uplink in 4G mobile communication based on LMS algorithm for DS-CDMA technique. *J. Converg. Inf. Technol.* **2014**, *9*, 16–24.
8. 3GPP. *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; 3GPP TR 33.821; 3GPP: Sophia Antipolis, France, 2010.
9. 3GPP. *Telecommunication Management; Security Management Concept and Requirements*; Release 10; 3GPP TS 32.371; 3GPP: Sophia Antipolis, France, 2012.
10. 3GPP. *Policy and Charging Control Architecture*; Release 10; 3GPP TS 23.203; 3GPP: Sophia Antipolis, France, 2009.
11. Kim, S. A Design of MILENAGE Algorithm-Based Mutual Authentication Protocol for the Protection of Initial Identifier in LTE. Master's Thesis, Soongsil University, Seoul, Korea, 2013.
12. Jang, U.; Lim, H.; Kim, H. Privacy-enhancing security protocol in LTE initial attack. *Symmetry* **2014**, *6*, 1011–1025. [CrossRef]
13. Forsberg, D.; Horn, G.; Moeller, W.-D.; Niemi, V. Security in Intra-LTE State Transitions and Mobility. In *LTE Security*; John Wiley & Sons: Hoboken, NJ, USA, 2013; pp. 147–164.

14. Shahzad, A.; Lee, M.; Lee, C.; Xiong, N.; Kim, S.; Lee, Y.-K.; Kim, K.; Woo, S.-M.; Jeong, G. The protocol design and New approach for SCADA security enhancement during sensors broadcasting system. *Multimed. Tools Appl.* **2015**, 1–28. [CrossRef]
15. Shahzad, A.; Lee, M.; Kim, S.; Kim, K.; Choi, J.Y.; Cho, Y.; Lee, K.K. Design and development of layered security: Future enhancements and directions in transmission. *Sensors* **2016**, *16*, 37. [CrossRef] [PubMed]
16. Bikos, A.N.; Sklavos, N. LTE/SAE security issues on 4G wireless networks. *IEEE Sec. Priv.* **2013**, *11*, 55–62. [CrossRef]
17. Niemi, V.; Blommaert, M. 3GPP security hot topics: LTE/SAE and home eNB. In Proceedings of the 4th ETSI Security Workshop, Sophia Antipolis, France, 13–14 January 2009.
18. Salam, M.I.; Yau, W.-C.; Chin, J.-J.; Heng, S.-H.; Ling, H.-C.; Phan, R.C.-W.; Poh, G.S.; Tan, S.-Y.; Yap, W.-S. Implementation of searchable symmetric encryption for privacy-preserving keyword search on cloud storage. *Hum.-Centric Comput. Inf. Sci.* **2015**, *5*, 19. [CrossRef]
19. Peng, K. A secure network for mobile wireless service. *J. Inf. Process. Syst.* **2013**, *9*, 247–258. [CrossRef]
20. Joo, J.W.; Lee, J.K.; Park, J.H. Security considerations for a connected car. *J. Converg.* **2015**, *6*, 1–9.
21. Netmanias. *EMM Procedure: 1. Initial Attach for Unknown UE (Part 1)—Case of Initial Attach*; NMC Consulting Group Technical Specifications; Netmanias: Seattle, WA, USA, 2012.
22. Netmanias. *EMM Procedure: 1. Initial Attach for Unknown UE (Part 2)—Call Flow of Initial Attach*; NMC Consulting Group Technical Specifications; Netmanias: Seattle, WA, USA, 2011.
23. Prasad, A. 3GPP SAE-LTE Security. In Proceedings of the Niksun Wwsmc, Princeton, NJ, USA, 25–27 July 2011.
24. Cao, J.; Ma, M.; Li, H.; Zhang, Y.; Luo, Z. A survey on security aspects for LTE and LTE-A networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 283–302. [CrossRef]
25. Netmanias. *LTE Security I: LTE Security Concept and Authentication*; NMC Consulting Group Technical Specifications; Netmanias: Seattle, WA, USA, 2012.
26. Netmanias. *LTE Security II: NAS and AS Security*; NMC Consulting Group Technical Specifications; Netmanias: Seattle, WA, USA, 2012.
27. Wang, J.; Zhang, Z.; Ren, Y.; Kim, J.-U. Issues toward networks architecture security for LTE and LTE-A networks. *Int. J. Sec. Its Appl.* **2014**, *8*, 17–24. [CrossRef]
28. Escudero-Andreu, G.; Raphael, C.P.; 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 Telecommunications, Networking and Broad-Casting (PGNET), Liverpool, UK, 25–26 June 2012.
29. Kwon, T.; Lee, J.; Choi, H.; Yi, O.; Ju, S. Efficiency of LEA compared with AES. *J. Converg.* **2015**, *6*, 16–25.