디지털산업정보학회 논문지 제13권 제1호-2017년 3월
http://dx.doi.org/10.17662/ksdim.2017.13.1.087

Efficient and Security Enhanced Evolved Packet System Authentication and Key Agreement Protocol

Shi Shanyu* · Choi Seungwon**

〈Abstract〉

As people increasingly rely on mobile networks in modern society, mobile communication security is becoming more and more important. In the Long Term Evolution/System Architecture Evolution (LTE/SAE) architecture, the 3rd Generation Partnership (3GPP) team has also developed the improved Evolved Packet System Authentication and Key Agreement (EPS AKA) protocol based on the 3rd Generation Authentication and Key Agreement (3G AKA) protocol in order to provide mutual authentication and secure communication between the user and the network. Unfortunately, the EPS AKA also has several vulnerabilities such as sending the International Mobile Subscriber Identity (IMSI) in plain text (which leads to disclosure of user identity and further causes location and tracing of the user, Mobility Management Entity (MME) attack), man-in-middle attack, etc. Hence, in this paper, we analyze the EPS AKA protocol and point out its deficiencies and then propose an Efficient and Security Enhanced Authentication and Key agreement (ESE-EPS AKA) protocol based on hybrid of Dynamic Pseudonym Mechanism (DPM) and Public Key Infrastructure (PKI) retaining the original framework and the infrastructure of the LTE network. Then, our evaluation proves that the proposed new ESE-EPS AKA protocol is relatively more efficient, secure and satisfies some of the security requirements such as confidentiality, integrity and authentication.

Key Words : LTE/SAE, Security, EPS AKA, PKI, Pseudonym

Ⅰ. INTRODUCTION

The rapid development and expansion of mobile networks make it possible for convenient access to integrated services such as voice, data and multimedia. However, to some extent, the mobile network is an opening system since the openness of the radio channels and randomness of the mobility of the users[1]. Hence, within the range of a wireless device, anyone can capture the

* 한양대학교 전자컴퓨터통신공학과 석사과정
** 한양대학교 전자컴퓨터통신공학과 교수(교신저자)

communication content without interrupting the data flow between both communication sides, resulting in man-in-middle attack, replay attack, eavesdropping etc. Therefore, the security of mobile communication system has been taken as one of the most challenging and important issues.

Even though at the beginning phase of mobile communication (the 1th Generation 1G mobile telephone systems) provided essentially no security features, global efforts to strengthen security mechanisms have been made starting from the Global System for mobile communication (GSM) for the more and more wide application of mobile communication. With the continuous development of the mobile communication system, the security mechanisms of 2nd Generation (2G, GSM), 3rd Generation (3G, CDMA) and 4th Generation (4G, LTE) has been proposed one after another. The 3G security mechanism provides some new security characteristics based on 2G system which only offers security like avoiding cloning of mobile identity and eavesdropping of fixed phones[2]. Nevertheless, the 3G security construction primarily aims at improving the system flexibility and adaptability to new challenges instead of providing complete security[2]. There are still some flaws in the security protocol such as easiness of the subscriber's identity leakage, the operation difficulty of sequence number etc. Therefore, for further improvement of the system security, in the 4th Generation mobile communication system, 3GPP developed and adopted the EPS AKA protocol which improves the security and performance without changing the framework of the 3G AKA[3]. However, the results of some related research works show that the LTE security architecture still has several security deficiencies, especially in AKA. Although many researches have been done, such as PKI based scheme, most of their efforts were concentrated on confidentiality and authentication requirements[2]. In terms of the User Equipment with limited computing resources, the efficiency of the security scheme is very critical for the sake of practical application while achieving the security requirements. In this paper, we present a more efficient and secure EPS AKA protocol named ESE-EPS AKA utilizing hybrid of Dynamic Pseudonym Mechanism (DPM) and Public Key Infrastructure (PKI) without changing the original framework and the infrastructure of the LTE network. The DPM is used to address the IMSI exposure issue while PKI is for protecting the transferred information between MME and Home Subscriber Server (HSS). By analyzing and evaluation of the proposed ESE-EPS AKA protocol, we show that it is relatively more efficient and achieves the security requirements of LTE/SAE network. The remainder of this paper is organized as follows: Section II analyzes and points out the vulnerabilities of EPS AKA. The related works of settling the issues of EPS AKA and their deficiencies, and the security requirements for wireless network are illustrated section III. Section IV introduces the proposed protocol, ESE-EPS AKA. In section V, we analyze our protocol as compared with others. Finally, a conclusion of the whole paper is given in section VI.

Ⅱ. ANALYSIS OF EPS AKA

EPS AKA can broadly be divided into two stages[4]: (1) Subscriber authentication. It is the process of the mutual authentication between the User Equipment (UE, in general, UE consists of Universal Subscriber Identity Module (USIM) and Mobile Equipment (ME)) and the corresponding home network; (2) None-access stratum (NAS) and access stratum (AS) security functions activation. It is the Keys and security algorithms negotiation process between the UE and the corresponding home network. The former is realized under the "challenge/response" mode. After receiving the attach request from the UE, the MME will make a different treatment according to different cases, respectively. The different cases will be described as follows: Case 1: the MME cannot identify the UE. In other words, the MME does not have or cannot get the UE's IMSI from the old MME (to which the UE attached last time) for integration checkout failure. Then the MME will request the UE to send its IMSI (in clear text in EPS AKA); Case 2: the MME can identify the UE. That is MME has or can get the UE's IMSI from the old MME with a successful integration checkout. In this case, the MME will not initiate the AKA procedure. However, in case 1, after the MME received the IMSI sent by the UE, then the subsequent AKA procedure includes two subcases: Subcase 1: If the MME has effective authentication tokens, then it will immediately initiate the authentication procedure for the mutual authentication between the UE and the home network; Subcase 2: If not, firstly, the MME must request new authentication tokens from the HSS. And then initiate the authentication procedure. If the authentication between the UE and the home network is successful in both sides, then the key agreement procedure will be initiated by the MME for NAS between the UE and the MME, and will be initiated by the evolved Node B (eNodeB) for AS between the UE and the eNodeB. Compared with the 3G AKA, EPS AKA enables new security functions as follows[3]:

(1) Effectively resisting attacks of pseudo base station via the authentication to Serving Network (SN);
(2) The key hierarchy and layer-wise session key production scheme enhance the safety strength of the system;
(3) For addressing the pseudo synchronization failure issue of Serial Number (SQN), the independent SQN management, the sequence storage and usage mechanism of the authentication vector (AV) are adopted.

However, there are still existing several vulnerabilities in the EPS AKA protocol[3]:

(1) During the user's initial registration or the SN requests UE to send its IMSI, UE sends IMSI in plain-text. It is very easy to capture IMSI from the wireless channel and then initiate man-in-middle attack, user location and business tracking, etc.
(2) The wired or wireless link among the network entities has no necessary protection. Especially the AVs transmitted between HSS and MME can be easily captured.

(3) There is no protection of service network identity (SNID) in both wireless and wired link, which leads to the easy leakage of the legal SNID and then causes the attacks such as pseudo base station or network fraud, etc.

Ⅲ. RELATED WORK ANALYSIS

Because it is not easy to address some weaknesses (such as man in middle attack and replay attack) by Symmetric Key Cryptosystem (SKC), most of the researchers focused on the PKI cryptosystems. Nevertheless, in terms of the UE with limited computing resources and unstable wireless mobile communication environment, all of the PKI based cryptosystems have the following disadvantages:

(1) The maintenance and management of the certificate repository as well as the huge communication overhead caused by the transfer of the public key certificate are unavoidable.

(2) The Public Key Cryptography (PKC), such as RSA, is a relatively low efficiency cryptography. That is to say, it requires a relatively (compared to SKC, such as Advanced Encryption Standard (AES)) much higher time cost in both encryption and decryption which means a relatively long time delay in communication. And also, it consumes more power and is not very efficient in hardware and software implementation. The following Table 1 and Table 2 shows the details:

Table 1. Comparison between AES and RSA[5,6]

No.	Factors Analyzed	AES	RSA
1.	Developed	2000	1978
2.	Key Size	128, 192, 256 bits	>1024 bits
3.	Block Size	128bits	Minimum 512bit
4.	Algorithm Type	Symmetric	Asymmetric
5.	Encryption	Fast	Slow
6.	Decryption	Fast	Slow
7.	Power Consumption	Low	High
8.	Security Strength	Excellent Secured	Timing Attack
9.	Key Used	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
10.	Hardware & Software Implementation	Fast and efficient	Not efficient
11.	Ciphering & Deciphering Algorithm	Different	Same

Table 2. Encryption and Decryption Time Comparison between AES and RSA[5,6]

No.	Algorithm	Packet Size (KB)	Encryption Time (Sec)	Decryption Time (Sec)	Buffer Size
1.	AES	153	1.6	1.1	152
	RSA		7.3	4.9	222
2.	AES	196	1.7	1.24	200
	RSA		8.5	5.9	257
3.	AES	312	1.8	1.3	300
	RSA		7.8	5.1	416
4.	AES	868	2.0	1.8	889
	RSA		8.2	5.1	934

(3) The AES provides high security while the RSA is relatively worse secure due to timing attack[5,6]. Hence, for higher security strength, the key length of RSA should be longer. Unfortunately, the increment of the key size means the fast growth of time cost in both encryption and especially in decryption[7]. Furthermore, The128 bits AES symmetric key algorithm can provide the same security strength as 3072 bits RSA cryptography[8].

(4) For the sake of safety, the key length of RSA should be at least 2048 bits (for the 1024 bits RSA had been thought as insecurity starting

from 2014[8]), which means the length of cipher-text will be close to 2048 bits even though the encrypted plain-text may be only tens of bits. That means a lot of useless redundancy, much more communication resources (like transmit power, bandwidth etc.) cost and lower success rate of information transfer between the UEs and the networks especially in bad wireless communication environment.

Above all, from a survey of the most recent and important works on AKA techniques based on PKI in[2], we can see that the time cost of the most efficient scheme which is based on PKI is also much higher than that of AES-128 (AES with key size 128 bits). We have to stress it again that for the UE, the limitation of the computing power and battery capacity as well as the communication bandwidth and the unstable wireless communication quality result in difficulties in practical application of the Public Key Cryptography. However, for the other network entities, such as MME and HSS, they can obtain enough energy and can be equipped with high performance computation module.

Finally, according to some relevant works, the security requirements for mobile communication networks can be summarized as follows[9,10,11]:

(1) Confidentiality: it includes the encryption protection of the transmitted traffic data and signaling data, preventing sensitive privacy information, like UE identity, from being disclosed to an adversary, and encryption algorithm and key agreement.
(2) Integrity: this means that it shall not be possible to undetectable modify the user traffic data and signaling data. And alse, it contains integrity algorithm and key agreement.
(3) Authentication: authentication corroborates the identity of the entities which are communicating. In other words, all the entities within a session utilizing the mobile communication network should be possible be authenticated to be legal and valid.
(4) Network Availability: it ensures that all resources of the communications network are always utilizable be authorized parties. Hence, Denial of Service (DoS) attack is the main threat, such as Authentication Flood Attack, RF Jamming Attack etc[12,13].

Ⅳ. ESE-EPS AKA Protocol

In order to address the above mentioned security issues existing in EPS AKA and overcome the drawbacks of the PKI based solutions, we propose an Efficient and Security Enhanced Authentication and Key agreement (ESE-EPS AKA) protocol based on hybrid of Dynamic Pseudonym Mechanism (DPM) and Public Key Infrastructure (PKI).

4.1 Notes on nomenclature

- KSIS: denotes the Integrity Key shared between UE and HSS;
- XXX: denotes the value of the corresponding variable.

- RAND-I: denotes the random number for integrity code calculation shared between UE and HSS;
- AES-128 CMAC: AES-128 in Cipher-based Message Authentication Code (CMAC) mode;
- MAC-I: denotes Message Authentication Code for Integrity;
- MsgX: denotes the transmitted message X between the network entities, X = 1, 2, 3, …;
- SQ, SQ-I: denotes the sequences of Pseudonym and RAND-I, respectively; the additional subscript 1 and 2 indicate Current (the new one) and Last Time (the old one), respectively.
- {m}K-X: denotes the encrypted or integrity computation to message m via cipher or integrity key K-X ;
- PK-MME, PK-HSS: denotes the public key of MME and HSS, respectively;
- KASME : denotes the intermediate key which is also the top-level key of the access network ;
- KSIASME : denotes the key identification allocated by MME for KASME ;

4.2 The ESE-EPS AKA Protocol

The core idea of ESE-EPS AKA scheme is that utilizing DPM to address the IMSI exposure issue (Pseudonym is transferred between the network entities instead of IMSI) for its lower consumption (battery, bandwidth etc. as mention above) especially from a UE's perspective. PKI is employed to protect the information transferred between MME and HSS for its flexibility.

Based on PKI, when the new MME is to be added to the network, the new MME and HSS shall acquire the digital certificate and public key via Certificate Agency (CA). Based on DPM, prior to communication, the initial value (a random sequence with length of 7 bytes) of Pseudonym and random number RAND-I as well as the corresponding integrity key K_{SIS} have already been shared between UE and HSS. There is a one-to-one correspondence between IMSI and Pseudonym (even though one Pseudonym may correspond to two different random sequence, Current – the new one, Last Time – the old one) as well as integrity key K_{SIS}. Table 3 shows some parameters should be stored in UE, MME and HSS, respectively. Figure 1 shows the procedure of the ESE-EPS AKA protocol, and the details are described in Step 1 ~ Step 10 (Note: some further details are not shown because they are the same as EPS AKA).

Table 3. Some parameters stored in UE, MME and HSS

UE	
Parameter	Value
Pseudonym	SQ
RAND-I	SQ-I
IMSI	XXX
Integration Key	K_{SIS}
GUTI	XXX

MME		
Parameter	Value	
	Current	Last Time
Pseudonym	SQ_1	SQ_2
GUTI	XXX	

HSS		
Parameter	Value	
	Current	Last Time
Pseudonym	SQ_1	SQ_2
RAND-I	SQ_1-I	SQ_2-I
Status Indicator	0 / 1	
IMSI	XXX	
Integration Key	K_{SIS}	

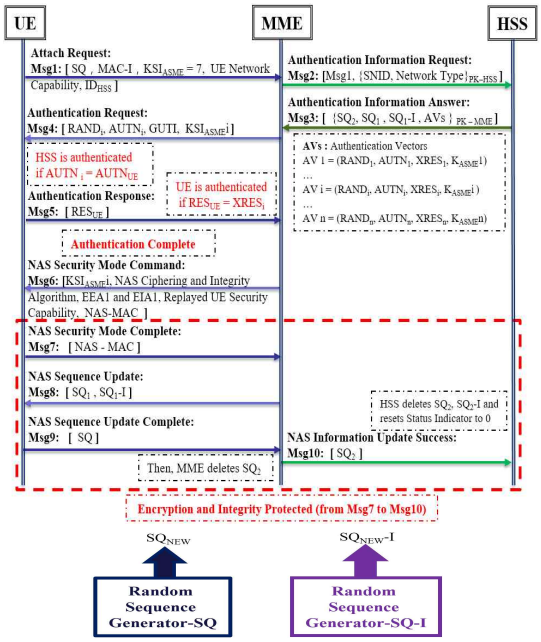

Figure 1. The procedure of ESE-EPS AKA protocol

(1) UE to HSS: Msg1 = [SQ, MAC-I, KSIASME = 7, UE Network Capability, IDHSS];

The user initiates the attach request: Firstly, UE uses the integrity key K_{SIS} which is stored in the USIM card to calculate the integrity code MAC-I of SQ, IMSI and SQ-I, as illustrated in figure 2. Then UE sends Msg1 as attach request message to MME. KSI_{ASME}=7: indicates UE has no authentication key. In addition, MAC-I is sent to MME by UE only when user initiates the attach request. But when MME requests UE to send its Pseudonym, Only SQ will be sent.

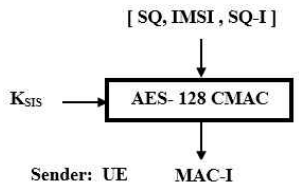

Figure 2. The MAC-I Generation Procedure

(2) MME to HSS: Msg2 = [Msg1, {SNID, Network Type}PK-HSS];

After MME receives the attach request from the user, it encrypts its own network identity SNID and Network Type with the public key PK-HSS and derives the corresponding encrypted information $\{SNID, Network\ Type\}_{PK\text{-}HSS}$. Then MME delivers Msg2 as the authentication information request to HSS.

(3) HSS to MME: Msg3 = [{SQ2, SQ1, SQ1-I, AVs}PK-MME];

After receiving the authentication information data request message from MME, HSS finds the corresponding entry which includes Pseudonym, IMSI, RAND-I, K_{SIS} and Status Indicator via the received SQ. Then HSS calculates the integrity code XMAC-I of SQ, IMSI and SQ-I with K_{SIS} as shown in figure 3, following the same process as performed in UE side in Step 1. (Note: when SQ = SQ_1, SQ-I = SQ_1-I; when SQ = SQ_2, SQ-I = SQ_2-I)

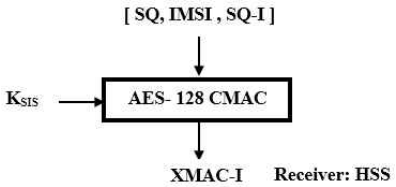

Figure 3. The XMAC-I Generation Procedure

Then HSS compares the derived XMAC-I with the received MAC-I. If XMAC-I and MAC-I are different values, HSS will discard Msg3 and not continue to subsequent process. If XMAC-I equals MAC-I, HSS decrypts the corresponding data to get SNID with its own private key. Then, HSS checks the validation of IMSI and SNID from registration

subscriber list and authentication service network list maintained in the database. If the IMSI or SN identities are invalid, then HSS will discard Msg3 and not continue to subsequent process. If the IMSI and SN identities have been verified, then HSS should check the value of the Status Indicator (VSI). If VSI equals 0 (which means that there is no SQ_2 and the received SQ equals SQ_1), HSS should set the VSI to 1 (which means that SQ_2 and SQ_2-I are not void). And then HSS should replace SQ_2 with SQ_1 and take a new random sequence SQ_{NEW} from the corresponding random sequence generator buffer for updating SQ_1. And also, HSS should replace SQ_2-I with SQ_1-I and take a new random sequence SQ_{NEW}-I from the corresponding random sequence generator buffer for updating SQ_1-I. Finally, HSS will generate the AVs, each of which includes a random number $RAND_i$, authentication token $AUTN_i$, expected response $XRES_i$, and a top-level key of the access network $K_{ASME}i$. The authentication vector generation mechanism is the same as used in the EPS AKA. Then, HSS calculates the cipher-text of SQ_2, SQ_1, SQ_1-I, AVs with the public key PK-MME of MME, and sends it to MME as the authentication information answer.

(4) MME to UE: Msg4 = [RANDi, AUTNi, GUTI, $KSI_{ASME}i$];

After receiving the Authentication Information Answer message, firstly, MME decrypts the corresponding data to derive SQ_2, SQ_1, SQ_1-I and AVs and store AVs in its database. Then MME finds the corresponding entry which includes Pseudonym and GUTI via the received SQ_2. And then MME updates SQ_1 and SQ_2 with the received SQ_1 and SQ_2, respectively. After that, MME selects one authentication vector AV_i which is never used among AVs. Then, MME extracts $RAND_i$, $AUTN_i$ from the selected AV_i, allocates exclusive Key Set Identifier (KSI) $KSI_{ASME}i$ to $K_{ASME}i$ and generates GUTI. Finally, MME sends $RAND_i$, $AUTN_i$, GUTI, $KSI_{ASME}i$ to UE.

(5) UE to MME: Msg5 = [RES_{UE}];

After receiving the Authentication Request message, UE generates the authentication token $AUTN_{UE}$ utilizing the corresponding function and the received parameters $RAND_i$ and $AUTN_i$. If $AUTN_{UE}$ and $AUTN_i$ are not consistent, it means HSS is invalid and the whole AKA procedure should be terminated. Otherwise, UE should derive RES_{UE} as response to authentication request sent to MME. MME should compare the RES_{UE} received from UE with the $XRES_i$. If these two values are not consistent, the whole AKA procedure should be terminated. Otherwise, it indicates that the subscriber is valid. So far, the authentication part of AKA is successfully completed. In the next, the key agreement part will be proceeded to create ciphering key and integrity key for NAS and AS, respectively.

(6) MME to UE: Msg6 = [$KSI_{ASME}i$, NAS Ciphering and Integrity Algorithm, EEA1 and EIA1, Replayed UE Security Capability, NAS-MAC];

(7) UE to MME: Msg7 = [NAS-MAC];

Step 6 and Step 7 are the security key and algorithm negotiation part for NAS and the process is the same as part of EPS AKA. If Step 7 is

successfully completed, all the subsequent NAS messages will be encryption and integrity protected. In the next, the Sequences (Pseudonym and RAND-I) Update part will be proceeded.

(8) MME to UE: Msg8 = [SQ_1, SQ_1-I];

After the security mode of NAS is successfully completed, MME sends the new sequences of SQ_1 and SQ_1-I received from HSS to UE.

(9) UE to MME: Msg9 = [SQ];

After receiving the NAS Sequence Update message, UE replaces SQ and SQ-I with the received new sequences SQ_1 and SQ_1-I, respectively. Then UE send the NAS Sequence Update Complete message including SQ to MME.

(10) MME to HSS: Msg10 = [SQ_2];

After receiving the NAS Sequence Update Complete message, MME finds the corresponding entry via SQ in its database. Then MME sends NAS Information Update Success message including the updated SQ_2 sequence in plain-text to HSS and deletes the SQ2 of Pseudonym. Finally, HSS finds the corresponding entry via the received SQ_2 from MME and reset the value of Status Indicator to 0. Then HSS deletes SQ_2 and SQ_2-I within this entry.

While Step 8 ~ 10 proceeds, the key negotiation of AS and the subsequent processes for the local communication proceed simultaneously. Note that, the message transfer of every message of Step 8 ~ Step 10 may be failure due to the unstable wireless mobile communication environment. But it will not impact the normal operation of the system. According the failure to each step, there should be 3 cases to be analyzed and defined as the following.

(1) Case 1: the message transfer of Step 8 is failure. Hence, the message transfer of Step 9 will not occur. And also, no message will be transferred in Step 10 (Although a message of NAS Information Update Failure is supposed to be sent, it is meaningless except for a waste of communication resources). As a result, SQ_2, SQ_2-I and the value 1 of Status Indicator should be kept until the corresponding response message received by MME and HSS as described above, respectively. Afterwards, when MME requests the UE to send its identity (the corresponding Pseudonym instead of IMSI used in EPS AKA) or UE initiates attach request with its Pseudonym, SQ (equals SQ_2 in this case) will be sent to MME. According to the mapping relationship of Pseudonym and IMSI, the processing procedure is the same as described in Step1 ~ Step10 except that because the new sequences (SQ_1, SQ_1-I) of Pseudonym and RAND-I are not used yet, so HSS will not take the new ones from the corresponding random sequence generator buffers but send the last time obtained SQ_1 and SQ_1-I to MME. And also, HSS will not replace SQ_2 and SQ_2-I with SQ_1 and SQ_1-I, respectively.

(2) Case 2: the message transfer of Step 8 is successful but the message transfer of Step 9 is failure. MME and HSS should keep SQ2, SQ2-I and the value 1 of Status Indicator as described in Case 1 above. Afterwards, when MME requests the UE to send its Pseudonym or UE initiates attach request with its Pseudonym, SQ

(equals SQ_1) will be sent to MME. Then, the remainder operation or processing procedure is the same as described in Step 1 ~ Step 10 above.

(3) Case 3: the message transfer of Step 8 and Step 9 are successful but the message transfer of Step 10 is failure. Then, the processing procedure is the same as described in Case 2 except that MME should delete SQ_2 after receiving the NAS Sequence Update Complete message sent by UE in Step 9.

V. EVALUATION OF ESE-EPS AKA PROTOCOL

The evaluation of ESE-EPS AKA includes performance and security evaluation, respectively.

5.1 Performance Evaluation

In this part, we evaluate the efficiency of ESE-EPS AKA protocol compared with the original EPS AKA and SEPS AKA in[9] which is the most efficient scheme from a survey of the most recent and important works on AKA techniques based on PKI in[2] as mentioned above. Bandwidth consumption and computational cost as the two comparison criteria will be discussed, respectively.

5.1.1 Bandwidth consumption

For measuring the bandwidth consumption, the employed cryptographic algorithm of PKI is supposed to be RSA algorithm with the key size of 2048 bits. Here, we only calculate the additional bandwidth consumption caused by the adoption of encryption protection mechanism compared to the original EPS AKA in which the corresponding information is transferred in plain-text.

According to PKCS#1, the maximum input block size is

$$MIBS = k - hLen - 2 \quad (1)$$

where k is the key size in octet and hLen is the length of the hash function used within OAPE. And the output size (the cipher-text size) is equal to k despite the input size. Hence, for SHA-1 (the default) and a key size of 2048 bits, the MIBS is 2048/8 – 2*20 – 2 = 214 bytes. The output size is 256 bytes.

As shown in table 4, the ESE-EPS AKA scheme consumes a bandwidth less than the SEPS AKA. The main reason contributing to this bandwidth consumption difference is that the DPM mechanism instead of PKI scheme is adopted to prevent the exposure of IMSI. It is expecially beneficial in the point view of UE as mentioned above. Furthermore, the bandwidth consumption difference will be more prominent when MME requests UE to send its Pseudonym (or IMSI). Because in the SEPS AKA scheme, 256 bytes cipher-text should be transferred while only 7 bytes Pseudonym in the ESE-EPS AKA scheme.

Table 4. Additional Bandwidth Consumption

Scheme	Additional Bandwidth Consumption in bytes
ESE-EPS AKA	426
SEPS AKA	646

5.1.2 Computational Cost

To measure the computational cost, we use crypto++ 5.6.5 benchmark which is compiled with Microsoft Visual Studio 2015 using x86 Solution Platform and runs on Intel Core i5-3570 3.40 GHz processor and 16.0GB RAM under Windows 10 Enterprise in 64 bit mode.

The computational costs (more precisely, that is the additional computational costs caused by the security protection schemes compared to the original EPS AKA, which is lack of security protection measures) for the operations employed in both SEPS AKA and ESE-ESP AKA schemes are illustrated in table 5. For the RSA scheme with key size of 2048 bits, there is no obvious running time variation when the plain-text size is within the maximum block size. The plain-text size is set to be 19 bytes because the sum of SQ, IMSI and SQ-I is 19 bytes. Other lightweight operations(e.g., exclusive or – XOR) will be omitted in the following time counting.

Table 5. The Time Cost of Relevant Operations

Operation	Notation	Time Cost (ms)		Plain-Text Size (byte)
		Encryption	Decryption	
RSA-2048	Tr	2.968181	9.378612	1~214
AES-128	Ts	0.000302	0.000229	16
AES-128 CMAC	Tc	0.012600		19
Modular Exponentiation	Td	0.090981		
XOR		0.000012		

From table 6, we can see that the ESE-EPS AKA scheme consumes relatively less time than SEPS AKA. The adoption of DPM instead of PKI to prevent the IMSI leakage accounts for the computational cost difference. In addition, in the case when MME requests UE to send its Pseudonym (or IMSI), the computational cost of SEPS AKA is 12.346793 (Tp – 0)ms more than ESE-EPS AKA scheme. The reason is the same as that in the bandwidth consumption case.

Table 6. The Total Running Time Comparison

Scheme	Relevant Operations	Total Running Time (ms)
ESE-EPS AKA	4*Tc + Ts + 2*Tr	24.693586
SEPS AKA	3*Ts + 2*Td + 3*Tr	37.223250

5.2 Security Evaluation

In this part, we evaluate the security of our protocol to prove that it meets the security requirements of the LTE system. In our protocol, PKI is used to provide entity mutual authentication and protect the transferred information between MME and HSS. Pseudonym is used to conceal the UE's identity (IMSI). MAC-I and Status Indicator are used to make sure that the one to one correspondence relationship between Pseudonym and IMSI cannot be maliciously manipulated. RAND-I is used to increase the randomness and complexity so that even though MAC-I is decrypted, IMSI cannot be intercepted. We should stress that because IMSI only exists in UE and HSS, so it is impossible to capture it from the transferred message among the network entities. This tremendously improves the security strength of the LTE system compared to SEPS-AKA.

Moreover, positive pseudo base station attack or network fraud prevention, man-in-middle attack, replay attack, impersonate attack can be prevented

in our protocol.

(1) Positive pseudo base station attack or fraud network attack: it is caused by SNID leakage. The attackers can induce UE to access the fraud network utilize the captured legal SNID (which lead it is difficult to discover the potential attack). Once the UE has accessed to the fraud network, the attacker may implant virus or steal sensitive user information. These attacks are prevented via the interception protection of SNID utilizing PKI for encryption. In other words, without intercepting the valid SNID, the positive pseudo base station attack or fraud network attack can be easily discovered and prevented by the UE.

(2) Man-in-middle attack : in the mobile communication networks, man-in-middle attack is aimed at intercepting a certain user's communication content via listening the corresponding radio link identified by the UE's identity (IMSI). Concealing the UE's permanent identity via Pseudonym makes it meaningless. That is, without a certain UE's identity, the attacker will lose its target object and the attack can not be performed.

(3) Imxcess to network system use a fake identity but through legitimate access identification. This offers attractive incentives to malicious criminals. The DPM mechanism makes it impossible to impersonate the identity of the UE to access to the network system. Because the adoption of Psudonym prevents the attacker from obtaining the legal UE identity and by checkout of MAC-I, illegal UE can be easily filtered out.

(4) Replay attack: It is a form of impersonation attack. The main threat of repay attack in mobile network is that the attacker can illegally pass through the system security authentication via just resending the intercepted authentication message. In our proposed ESE-EPS AKA scheme, once the Pseudonym sequence SQ has been used, it will be updated before the next authentication process. The replay attack can be discovered and then prevented via checkout the freshness of MAC-I. Even though the SQ update process failure, the attacker, by the replay of last time's messages of authentication procedure, can not access to the system. Because a new authentication procedure with never used AV will always be initiated by MME after receiving the attach request message. For the case that MME requests UE to send its Pseudonym, MME will check out whether the received SQ is equal SQ_1. IF they are not consistent (which means SQ has been used), MME will initiate a AKA procedure to verify validity of the UE's identity. Therefore, the replay attack can be prevented.

Finally, the ESE-EPS AKA protocol attained the security requirements such as confidentiality, authentication and integrity but not well in network availability will be shown.

(1) Confidentiality: The sensitive privacy information, IMSI is concealed and can not be intercepted via the protection of the DPM mechanism as mentioned above. As ESE-EPS AKA scheme follows the EPS-AKA protocol,

the remaining demands, such as encryption algorithm agreement and traffic data protection as mentioned in section III, are successfully satisfied. However, the EPS AKA protocol failed to protect the UE identity, IMSI.

(2) Integrity: Through the checkout of MAC-I, the Psedonym is integrity protected. Thereby, it insures the correctness of the one to one correspondence relationship between Pseudonym and IMSI. But EPS AKA protocol does not provide any verification of IMSI in the authentication part. The remaining demands are attained for both ESE-EPS AKA and ESE AKA protocols, because they experience the same key agreement process and the following procedures.

(3) Authentication: Through the authentication part, after HSS verified the validity of IMSI, UE and HSS can authenticate each other utilizing the uniqueness of the root key K. In the ESE-ESP AKA scheme, for the uniqueness of the one to one correspondence relationship between Pseudonym and IMSI, the authentication strength is increased. Because through MAC-I, an UE is identified mathematically by its IMSI. In the EPS AKA scheme, the transmission of IMSI gains the probability to different previous attacks.

(4) Network Availability: The cost of checking the correctness of the one to one correspondence relationship between Pseudonym and IMSI is very low. That is the cost of calculating MAC-I. Hence, through the checkout of MAC-I, to some extent, the DoS attack, like Authentication Flood Attack can be mitigated. The SEPS AKA scheme can resist DoS attacks more effectively by adopting PKI protection for all the communication entities. However, Both of the two schemes are not strong enough facing so many kinds of DoS attacks.

Table 7 summarizes the results of the above analysis and shows a comparison among ESE-EPS AKA, SEPS-AKA and the original EPS AKA.

Table 7. EPS AKA Security Requirements

	Confidentiality	Integrity	Authentication	Network Availability
ESE-ESP AKA	Yes	Yes	Yes	Medium
SEPS-AKA	Yes	Yes	Yes	High
EPS AKA	No	No	Yes	Low

VI. CONCLUSION

Aiming at addressing some fatal weaknesses such as UE identity exposure, SNID leakage in EPS AKA protocol, we have proposed an efficient and secure EPS AKA protocol, named ESE-EPS AKA, utilizing the combination DPM and PKI. Compared with other PKI based protocols, our scheme is relatively more efficient particularly in terms of UEs which have extremely limited communication resources, while achieving some of the security requirements including confidentiality, authentication and integrity. Furthermore, the ESE-EPS AKA can effectively withstand man-in-middle attack, impersonate attack and replay attack.

ACKNOWLEDGEMENT

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.B0115-16-0001, 5G Communication with a Heterogeneous, Agile Mobile network in the PyeongChang wInter Olympic competioN)

REFERENCES

[1] JM. Zhu, and JF. Ma, "A new authentication scheme with anonymity for wireless environments," IEEE Transactions on Consumer Electronics, Vol.50, No.1, 2004, pp. 231-235.

[2] M. Ramadan, GH. Du, FG. Li, and CX. Xu, "A Survey of Public Key Infrastructure-Based Security for Mobile Communication Systems," Symmetry-Basel, Vol.8, No.9, Article No. 85, 2016.

[3] XH. Li and YJ. Wang, "Security enhanced authentication and key agreement protocol for LTE/SAE network," Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, IEEE.

[4] R. Kreher and K. Gaenger, LTE SIGNALING Troubleshooting and Performance Measurement, John Wiley & Sons Ltd, United Kingdom, 2016, p.36.

[5] P. Mahajan and A. Sachdeva, "A study of Encryption algorithms AES, DES and RSA for security," Global Journal of Computer Science and Technology, Vol.13, No.15, 2013.

[6] B. Padmavathi and S. R. Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique," IJSR, Vol.2, No.4, 2013, pp.170-174.

[7] P. K. Donta, "Performance Analysis of Security Protocols," UNF Theses and Dissertations, 2007.

[8] E. Barker, Recommendation for Key Management- Part 1: General (Revision 4), NIST, U.S., 2016, pp.51-56.

[9] Z. J. Haddad, Sanaa Taha and I. A. S. Ismail, "SEPS-AKA: A Secure EVOLVED PACKET SYSTEM AUTHENTICATION AND KEY AGREEMENT SCHEME FOR LTE-A NETWORKS," The Sixth International Conference on Wireless & Mobile Networks, 2014.

[10] M. Ramadan, F. Li, C. X. Xu, A. Abdalla and H. Abdalla, "An Efficient End-to-End Mutual Authentication Scheme for 2G-GSM System," Big Data Analysis(ICBDA), IEEE International Conference, 2016.

[11] H. C. Poehls, "Security Requirements for Wireless Networks and their Satisfaction in IEEE 802.11b and Buletooth," M.Sc. in Information Security-Information Security Group, Royal Holloway, University of London, 2001.

[12] 장범환, "트래픽 세션의 포트 역할을 이용한 네트워크 공격 시각화," 디지털산업정보학회 논문지, 제11권, 제4호, 2015, pp. 47-60.

[13] 김태경, "위치 기반 관광 정보 서비스 보안 기술

연구," 디지털산업정보학회 논문지, 제12권, 제2호, 2016, pp. 25-29.

■ 저자소개 ■

석 선 우
(Shi Shanyu)

2014년 9월 ~ 현재
한양대학교 전자컴퓨터통신공학과
석사과정
2013년 7월 칭다오과학기술대학교(중국)
정보과학기술학과(공학학사)

관심분야 : LTE-A, WAPA, SDR
E-mail : shishanyu001@dsplab.hanyang.ac.kr

최 승 원
(Choi Seungwon)

2012년 9월~현재
HY-MC 연구센터 센터장
2002년~2011 HY-SDR 연구센터 센터장
1992년~현재 한양대학교 전자전기공학부 교수
1990년~1992년 일본 우정성 통신연구소
선임연구원
1989년~1990년 ETRI 선임연구원
1988년~1989년 미국 Syracuse대학 전지 및
전산과 교수
1988년 12월 미국 Syracuse대학 전기공학
(공학박사)
1985년 12월 미국 Syracuse대학 컴퓨터공학
(공학석사)
1982년 2월 서울대학교 전자공학 (공학석사)
1980년 2월 한양대학교 전자공학 (공학학사)

관심분야 : SDR, 이동통신, 신호처리
E-mai l : choi@dsplab.hanyang.ac.kr

논문접수일 : 2017년 02월 17일
수 정 일 : 2017년 03월 07일
게재확정일 : 2017년 03월 14일