Wireless Pers Commun (2009) 51:95–107
DOI 10.1007/s11277-008-9603-1

Reducing Signaling Traffic for the Authentication and Key Agreement Procedure in an IP Multimedia Subsystem

Chung-Ming Huang · Jian-Wei Li

Published online: 10 October 2008

Abstract In the IP multimedia subsystem (IMS) of UMTS, two authentication procedures are necessary for IMS subscribers before accessing IMS services: (i) packet-switch domain authentication using the authentication and key agreement of the 3rd Generation Partnership Projects (3GPP AKA), and (ii) IMS authentication using IMS AKA. However, since IMS AKA is based on 3GPP AKA, almost all of the operations are the same. Besides, IMS AKA needs two round-trips to carry out. Therefore, it is inefficient that almost all involved steps in IMS AKA are duplicated. Therefore, we propose a one-pass IMS AKA instead of IMS AKA. The one-pass IMS AKA can keep the security properties of IMS AKA, such as mutual authentication and key agreement. Furthermore, the one-pass IMS AKA not only has at least 45% improvement over IMS AKA in terms of authentication signaling, but also has 76.5% improvement over IMS AKA in terms of storage space.

Keywords 3GPP AKA · Authentication · IMS · IMS AKA · SIP

1 Introduction

IP multimedia subsystem (IMS) defined the Third Generation Partnership Projects (3GPP) release 5 is an overlay architecture that is over the packet-switched domain in the core network. The purpose of IMS is to provide IP-based multimedia services, such as voice telephony, messaging and multimedia conferencing[1,7]. Multimedia sessions are controlled by Call Server Control Function (CSCF) on which the Session Initiation Protocol (SIP) function works [1,14].

C.-M. Huang (✉) · J.-W. Li
Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan, ROC
e-mail: huangcm@locust.csie.ncku.edu.tw

J.-W. Li
e-mail: lijw@locust.csie.ncku.edu.tw

In addition to International Mobile Subscriber Identity (IMSI) in UMTS Subscriber Identity Module (USIM) of user equipment (UE), IMS subscriber has IP Multimedia Privacy Identity (IMPI) in UE's IMS Subscriber Identity Module (ISIM). In IMS, two authentication procedures are necessary for IMS subscriber before accessing IMS services: (i) packet-switch domain authentication: when UE sends an attach request to Serving GPRS Support Node (SGSN) in the packet-switch domain for accessing packet data services, SGSN is triggered to authenticate UE via HSS using the 3GPP authentication and key agreement (3GPP AKA) protocol, called the packet-switch domain authentication [6,9]. (ii) IMS authentication: UE must be authenticated again using IMS AKA before it can access IMS services [4]. IMS AKA reuses the same concept and principles of 3GPP AKA. Both the packet-switch domain and the IMS authentications are necessary for IMS subscriber, so-called a two-pass authentication. If only the packet-switch domain authentication, an adversary can impersonate other IMS subscribers in IMS, so-called fraudulent IMS usage [12].

Since IMS AKA is based on 3GPP AKA, the operations in IMS AKA are almost the same as that in 3GPP AKA. It is inefficient that almost all involved steps in the two-pass authentication are duplicated. Therefore, Lin et al. proposed a simple IMS authentication scheme instead of IMS AKA, which is called one-pass authentication. However, Huang and Li founds that Lin et al.'s one-pass authentication is vulnerable to (i) the fake attack on IMS subscriber and (ii) the temporary cheat attack [10]. Furthermore, Lin et al.'s one-pass authentication loses mutual authentication and key agreement capabilities [4]. It results in the lack of the confidentiality and integrity protection support between UE and CSCF. Therefore, Huang and Li proposed the evolutionary IMS AKA (E-IMS AKA) instead of IMS AKA to solve the aforementioned problems. However, the E-IMS AKA does not have the properties of forward and backward secrecy once the IMS temporary key in the E-IMS AKA is compromised.

This paper proposes an enhanced one-pass IMS AKA instead of IMS AKA in the IMS authentication, which has the following properties: (i) The one-pass IMS AKA does not need the duplicated AKA operations to keep the efficient property of Lin et al.'s one-pass authentication. (ii) The one-pass IMS AKA can withstand the aforementioned security attacks, and keep the mutual authentication and key agreement capabilities. (iii) The one-pass IMS AKA only uses the specified cryptography functions in the IMS AKA to carry out the aforementioned functions and does not modify the corresponding system architecture [4]. (iv) The one-pass IMS AKA can withstand the replay attack when timestamp falls into the timestamp acceptance window. (v) The one-pass IMS AKA has the properties of forward and backward secrecy. Furthermore, we model the signaling traffic of IMS AKA and the one-pass IMS AKA. Then, we use the signaling traffic model to compare the performance between IMS AKA and the one-pass IMS AKA.

2 Preliminary

Figure 1 illustrates a simple IMS architecture in 3GPP [1]. The IMS singling is achieved by three types of CSCF: (i) Proxy-CSCF (P-CSCF), (ii) Interrogating CSCF (I-CSCF) and (iii) Serving-CSCF (S-CSCF). P-CSCF is responsible for redirecting the SIP messages to home network. Besides, P-CSCF may be located either in the visited network or in UE's home network. I-CSCF is responsible for selecting a S-CSCF for UE. S-CSCF is responsible for authenticating UE and providing session control of multimedia services. Besides, I-CSCF and S-CSCF are located in UE's home network. Furthermore, the other important entity is Home Subscriber Server (HSS), which contains subscriber databases, e.g., user identity

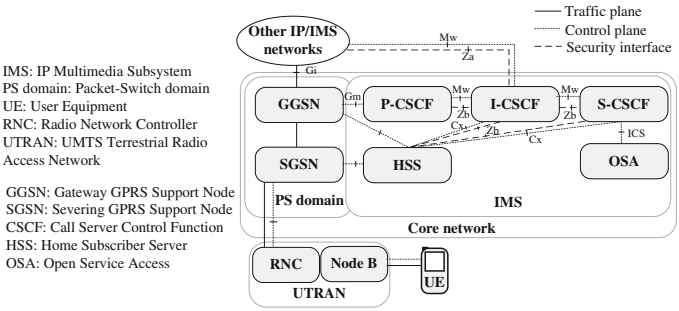

Fig. 1 The simple IMS architecture

and registration information. HSS is used by S-CSCF in IMS for acquiring subscription information.

In IMS, three important reference points are as follows: (i) Mw is a SIP-based reference point between different CSCFs. (ii) Cx is a reference point for S-CSCF and I-CSCF to acquire subscriber information from HSS, in which the adopted protocol is the diameter protocol [2,3]. (iii) Za/Zb is the security interface, which is defined in 3GPP network domain security, providing confidentiality and data integrity between different components within the core network (Zb) and toward other networks (Za) [5].

2.1 IMS Authentication in 3GPP

Assuming that UE has passed the packet-switch domain authentication. After the packet data protocol (PDP) context activation, UE can request IMS services through the IMS registration/authentication procedure using IMS AKA [4]. Note that, IMS AKA needs to protect SIP messages in addition to raise mutual authentication and key agreement. As a result, RES in IMS AKA must be the role of one-time-password to derive the HTTP digest for confirming the identity of UE and protecting SIP messages [13]. In contrast with 3GPP AKA, UE must keep RES secret in IMS AKA. The IMS AKA illustrated in Fig. 2 can be decomposed in the following steps:

Step I1. UE sends a SIP Register message with $IMPI$ to P-CSCF through SGSN. Then, P-CSCF forwards the request to I-CSCF. I-CSCF exchanges the User Authorization Request (UAR) and User Authorization Answer (UAA) pair with HSS over Cx reference to obtain the name of the S-CSSF that is serving UE. Then, I-CSCF forwards the Register message to the S-CSCF.

Step I2. If S-CSCF does not have a valid authentication vector (AV) array for UE, S-CSCF sends a Multimedia Authentication Request (MAR) to HSS for obtaining an AV array. Otherwise, this Step and Step **I3** can be skipped. Note that an AV contains (i) a random number $RAND$, (ii) an expected response $XRES$, (iii) a cipher key CK, (iv) an integrity key IK, and (v) an authentication token $AUTH$.

Step I3. HSS generates an ordered array of n AVs. HSS sends the AV array over Cx to S-CSCF through a Multimedia Authentication Answer (MAA) message.

Step I4. and **I5.** S-CSCF selects the $AV[i]$ and sends it to P-CSCF through a SIP 401 Unauthorized message. P-CSCF keeps CK_i and IK_i and sends the parameter $RAND_i||AUTH_i$ to UE through a SIP 401 Unauthorized message.

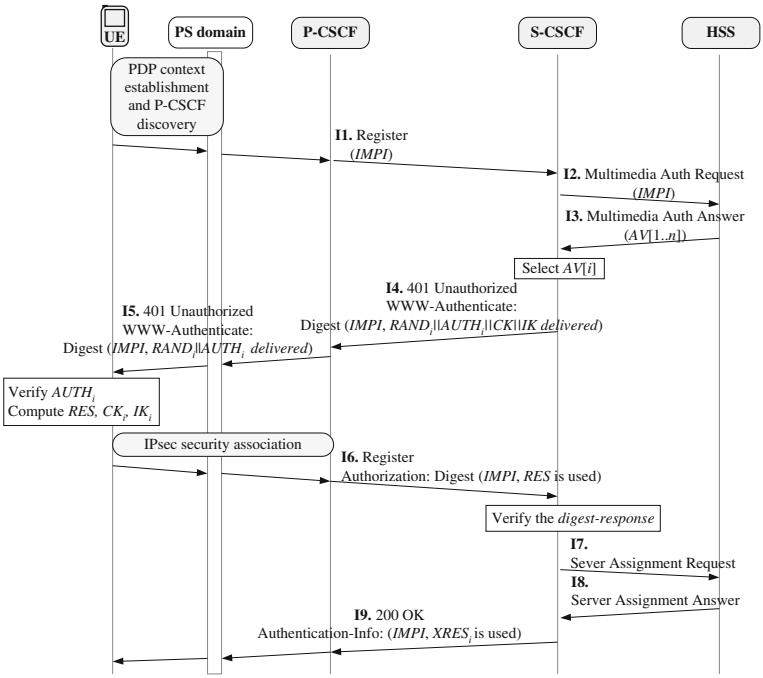

Fig. 2 IMS authentication in 3GPP

Step I6. UE verifies $AUTH_i$. If the result is positive, UE derives RES, CK_i and IK_i. Both IK_i and CK_i are used for IP security (IPsec) security association between UE and P-CSCF. Therefore, subsequent messages between UE and P-CSCF can be protected by IPsec. After that, UE employs RES as the password of HTTP digest to derive the $digest\text{-}response$ of the Authentication request header defined in [8] and sends it to S-CSCF.

Step I7. S-SCSF verifies the *digest-response* using $XRES_i$. If the result is positive, S-CSCF sends a Server Assignment Request (SAR) over Cx reference to HSS for informing which S-CSCF will serve the UE.

Step I8. Upon receipt of SAR, HSS stores the S-CSCF name and replies a Server Assignment Answer (SAA) over Cx reference to S-CSCF.

Step I9. S-CSCF employs $XRES_i$ as the password of HTTP digest to derive the $response\text{-}auth$ of the Authentication-Info header defined in [8]. Then, S-CSCF sends a 200 OK message with the *response-auth* to UE through I-CSCF and P-CSCF.

Step I10. UE verifies the *response-auth* of the Authentication-Info header retrieved from S-CSCF using $XRES_i$. If the result is positive, it means that S-CSCF is a legal S-CSCF. Simultaneously, UE derives CK_i and IK_i.

3 The One-pass IMS AKA

The assumption of the One-Pass IMS AKA is same as that of IMS Authentication in 3GPP presented in Sec. 2.1. The proposed AKA depicted in Fig. 3 can be decomposed into the following steps:

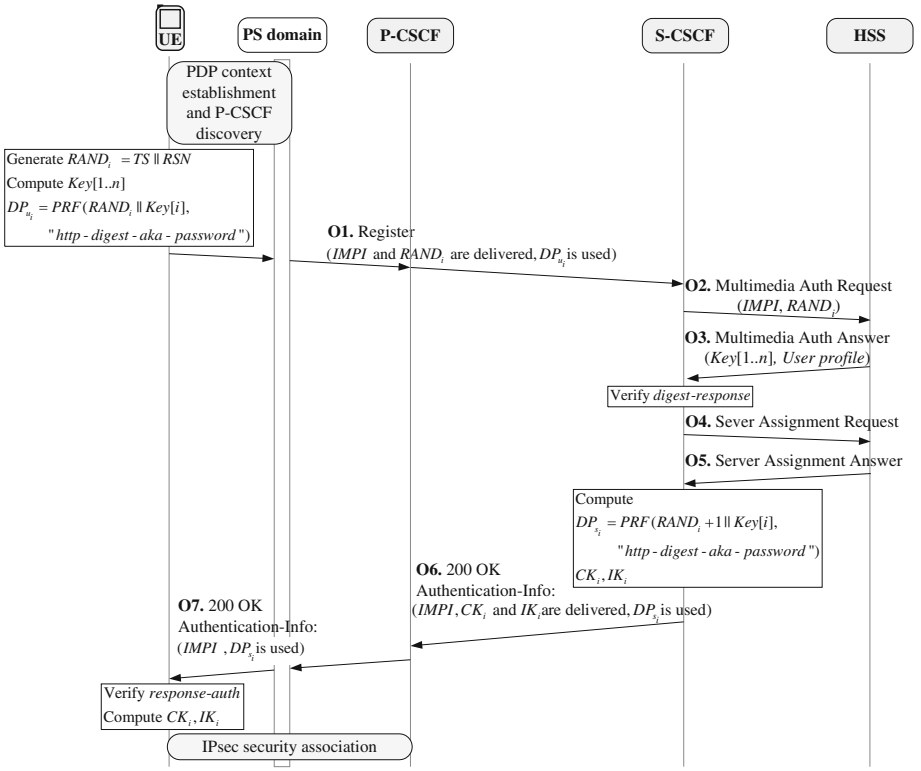

Fig. 3 The one-pass IMS AKA

Step 1. In the ith one-pass IMS AKA procedure, the UE forms a timestamp TS based on the universal time and then concatenates it with the random sequence number RSN to derive $RANDi$, which can be written as

$$RANDi = TSi||RSNi, \tag{1}$$

where $RSN_i = RSN_{i-1} + INC$, in which $RSN_0 = 0$ and INC denotes an random increment [10]. If UE does not have a vector of IMS-key $Key[1 \ldots M]$ for S-CSCF, i.e., i = 1, UE needs to derive $Key[1 \ldots M]$ as

$$\begin{aligned} Key[2s-1] &= f3_K(RANDi + (i-1)) \\ Key[2s] &= f4_K(RANDi + (i-1)), \end{aligned} \tag{2}$$

where $s = 1, 2, \ldots, \frac{M}{2}$. $f3(\cdot)$ and $f4(\cdot)$ are 128-bit length. K is the shared secret key between UE and HSS. If UE has $Key[1 \ldots M]$, UE selects the corresponding IMS-key from $Key[1 \ldots M]$. Next, UE can directly perform the subsequent operations: UE computes a digest password DP_{u_i} as

$$DP_{u_i} = PRF(RANDi||Key[i], String_1), \tag{3}$$

where $PRF(\cdot)$ is a pseudo-random function [15] and $String_1$ denotes "http-digest-aka-password". Then, UE calculates the "$digest\text{-}response$" of the Authentication

request header defined in [8] using DP_{u_i}. After that, UE sends a SIP Register message with $IMPI$, $RAND_i$ and the $digest\text{-}response$ to S-CSCF via P-CSCF.

Step 2. Upon receipt of the message of Step **1**, S-CSCF needs to verify $RAND_i$ using the two-step checks: (i) confirming whether TS_i in $RAND_i$ falls into the acceptance window or not, then (ii) confirming whether RSN_i in $RAND_i$ is larger than RSN_{i-1} in $RAND_{i-1}$ or not. After that, S-CSCF sends a MAR message with $IMPI$ and $RAND_i$ over Cx reference to HSS. If S-CSCF has $Key[1 \ldots M]$ for UE, MAR in this step and MAA in Step **3** can be skipped. Note that since $f3(\cdot)$ and $f4(\cdot)$ are located in UE and HSS, S-CSCF needs to retrieve $Key[1 \ldots M]$ from HSS.

Step 3. HSS uses $RAND_i$ to derive $Key[1 \ldots M]$ as Eq .2. Then, HSS sends a MAA message with $Key[1 \ldots M]$ and user profile over Cx reference to S-CSCF.

Step 4. Upon receipt of the message of Step **3**, S-CSCF keeps $Key[1 \ldots M]$ for UE and derives DP'_{u_i} using Eq. (3). Then, S-CSCF verifies the $digest\text{-}response$ retrieved from Step 1 using DP'_{u_i}. If the result is positive, it means that UE is a legal user. S-CSCF sends a SAR message over Cx reference to HSS. Note that DP'_{u_i} should equal DP_{u_i} if the used $RAND_i$ and $Key[i]$ are the same.

Step 5. HSS stores the name of S-CSCF and sends a SAA message over Cx to S-CSCF.

Step 6. and **7.** S-CSCF derives DP_{s_i} as

$$DP_{s_i} = PRF(RAND_i + 1 || Key[i], String_1) \tag{4}$$

and derives CK_i and IK_i as

$$\begin{aligned} CK_i &= PRF(DP_{u_i} || DP_{s_i} || Key[i], String_2) \\ IK_i &= PRF(DP_{u_i} || DP_{s_i} || Key[i], String_3), \end{aligned} \tag{5}$$

where $String_2$ and $String_3$ denote "http-digest-aka-cipherkey" and "http-digest-aka-integritykey", respectively. Then, S-CSCF calculates the $response\text{-}auth$ of the Authentication-Info header using DP_{s_i}. After that, S-CSCF sends a SIP 200 OK message together with $IMPI$, CK_i, IK_i and the $response\text{-}auth$ to P-CSCF. P-CSCF stores CK_i and IK_i, and sends the SIP OK message with $IMPI$ and the $response\text{-}auth$ to UE.

Step 8. UE derives DP'_{s_i} using Eq. 4. Then, UE verifies the $response\text{-}auth$ retrieved from Step **7** using DP'_{s_i}. If the result is positive, it means that S-CSCF is a legal S-CSCF. Simultaneously, UE derives CK_i and IK_i as Eq. 5. Both IK_i and CK_i are used for IPsec security association between UE and P-CSCF. So, subsequent messages between UE and P-CSCF can be protected by IPsec.

4 Security Analysis

The security properties in the proposed mechanism are demonstrated as follows:

S1 *Mutual authentication between UE and S-CSCF*:

In the one-pass IMS AKA, UE and S-CSCF need to mutually authenticate with each other. S-CSCF can retrieve $Key[1..M]$ from HSS to confirm the identity of UE by means of verifying the $digest\text{-}response$ sent by UE. On the other hand, UE can confirm the identity of S-CSCF by means of verifying the $response\text{-}auth$ sent by S-CSCF. If faking either one of UE and S-CSCF, an adversary needs $Key[1..M]$ to derive $RAND$ and DP_s or DP_u. However, although $RAND$ is publicly available, it is infeasible to derive $Key[1..M]$ using Eq. 2 without the K shared between UE and HSS.

S2 *Key agreement and its freshness:*

In the one-pass IMS AKA, UE and S-CSCF need to agree CK and IK using Eq. 5 and $Key[1..M]$ after mutual authentication. Similarly, it is infeasible to derive CK and IK using Eq. 5 without the $Key[1..M]$, DP_s and DP_u.

As Eq. 5 presented, CK and IK are derived by (i) a pseudo random function $PRF(.)$ that is unpredictable, (ii) $Key[1 \ldots M]$, and (iii) DP_s and DP_u that vary on each session. Even if an adversary is eventually able to derive the CK and IK for one session, the CK and IK for future or past sessions are not comprised since the adversary does not learn the knowledge of $Key[1 \ldots M]$.

S3 *Forward and backward secrecy*:

In the one-pass IMS AKA, S-CSCF obtains IMS-key $Key[1 \ldots M]$ from HSS and employs the IMS-key as the role of shared secret key between S-CSCF and UE. Besides, each authentication event uses different IMS-keys to perform mutual authentication and key agreement. Even if an adversary compromised one IMS-key, such condition does not cause the compromise of any earlier session or subsequent session.

S4 *Temporary cheat attack*:

In Lin et al.'s one-pass authentication, the SAR message is sent to HSS before S-CSCF has verified the identity of UE. If an adversary sends an incorrect Register message to S-CSCF for de-registering the already registered $IMPI$ or other operations, S-CSCF sends the SAR message to HSS, and HSS performs the requested operations. However, once S-CSCF learns the Register message is incorrect, then another SAR message is sent to HSS for recovering to the UE's previous status. As a result, the adversary succeeds in its malicious purpose during a short period. On the contrary, in the proposed one-pass AKA, S-CSCF needs to authenticate UE before sending the SAR message to HSS.

S5 *Replay attack*:

In order to prevent the replay attack, the one-pass IMS AKA has employed the mix of the timestamp TS and the random sequence number RSN shown in Eq. (1) [10]. Although $RAND$, the $digest\text{-}response$ and the $response\text{-}auth$ are publicly available, S-CSCF can check whether or not TS is within the timestamp acceptance window and whether or not the received RSN is larger than the previous RSN. $RAND$ can be selected uniquely in each authentication and the newly selected $RAND$ is certainly greater than the past $RAND$. If the replay attack is raised, S-CSCF can learn the past $RAND$ even when TS is within the acceptance window.

5 Performance Analysis

Referring to Figs. 2 and 3, the time diagrams of IMS AKA and the one-pass IMS AKA are depicted in Fig. 4. For convenient expression in Fig. 4, the message pair MAR and MAA are shorten as MAR/A. The message pair SAR and SAA are shorten as SAR/A, and the messages between S-CSCF and MS for IMS registration/authentication procedure are denoted as SIP-R messages. Let the total number of MARs that are involved when UE resides in S-CSCF service be N and M be the number of authentication information array, such as M AVs, M IMS-keys $Key[1..M]$. As Fig. 4 depicts, UE registered a new S-CSCF by sending the SIP-R message at time $T_{1,1}$. Since S-CSCF does not have AV or IMS-key, S-CSCF needs to send MAR/A to HSS for obtaining M AVs or $Key[1 \ldots M]$. At time $T_{1,M}$, the Mth AV or $Key[M]$ is used for the Mth authentication event. Then, at time $T_{2,1}$, S-CSCF needs to

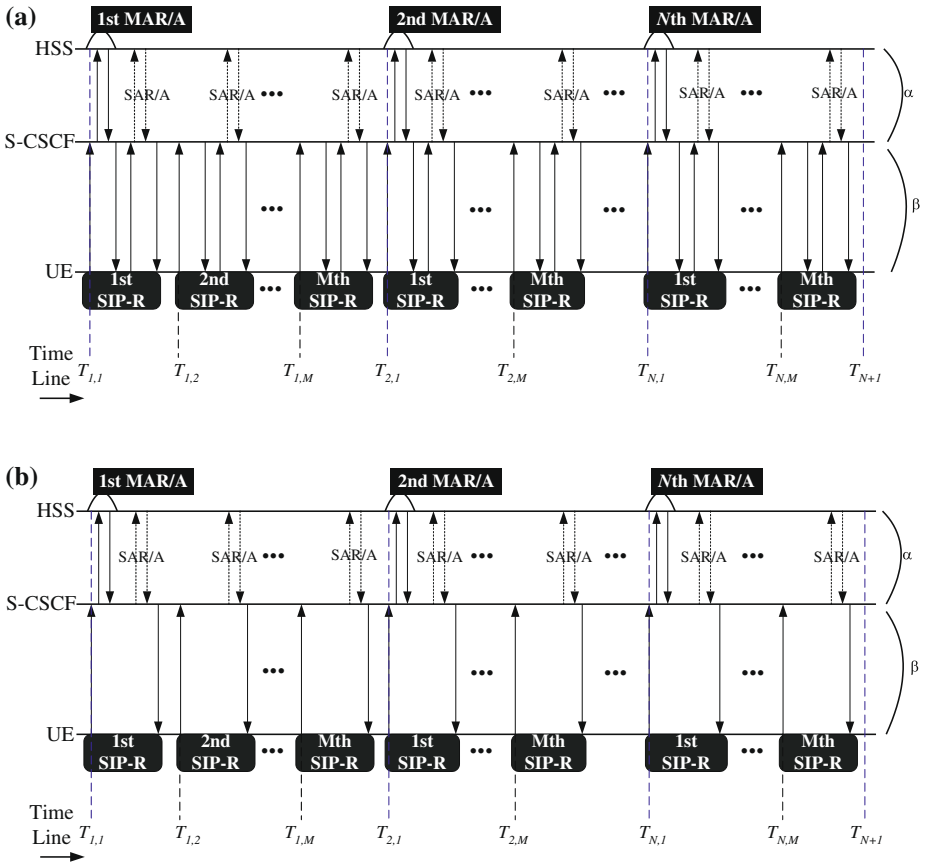

Fig. 4 The timing diagram (**a**) IMS AKA, (**b**) The one-pass IMS AKA

obtain AV or IMS-key for UE. Finally, at time T_{N+1}, UE leaves S-CSCF service. Therefore, $(N-1)M+m$ SIP-Rs and N MAR/As are involved during the period from T_{N+1} to $T_{1,1}$, where $1 \leq m \leq M$.

5.1 Expectation of N

Since [11] considers the authentication signaling traffic of 3GPP AKA, which is similar to that of IMS AKA and the one-pass IMS AKA, we can consider to use the authentication signaling traffic model adopted in [11]. According to the Poisson distribution with arrival rate λ, $\Pr(N, M, T)$ denoting the probability in which n MAR/As are involved to HSS can be derive as

$$\Pr(N, M, T) = \sum_{m=1}^{M} \left\{ \frac{(\lambda T)^{(N-1)M+m}}{[(N-1)M+m]!} \right\} e^{-\lambda T}. \tag{6}$$

The probability that there are n MAR/As during the MS residence in the S-CSCF is

$$\Pr(N, M) = \int_{t=0}^{\infty} b(N, M, t) f(t) \mathrm{d}t, \tag{7}$$

where $t = T_{N+1} - T_{1,1}$, i.e., UE resides in S-CSCF service for period t. t has the general distribution with the density function $f(t)$ with mean $1/\mu$.

$$\begin{aligned} \Pr(N, M) &= \sum_{m=1}^{M} \int_{t=0}^{\infty} \left\{ \frac{(\lambda t)^{(N-1)M+m}}{[(N-1)M+m]!} \right\} e^{-\lambda t} f(t) \mathrm{d}t \\ &= \sum_{m=1}^{M} \left\{ \frac{(\lambda)^{(N-1)M+m}}{[(N-1)M+m]!} \right\} \int_{t=0}^{\infty} t^{(N-1)M+m} \times f(t) e^{-\lambda t} \mathrm{d}t \end{aligned} \tag{8}$$

The Laplace transform of $f(t)$ is

$$F(s) = \int_{t=0}^{\infty} f(t) e^{-st} \mathrm{d}t, \tag{9}$$

where s is a real number. According to Eqs. 8 and 9, the equation can be rewritten as

$$\Pr(N, M) = \sum_{m=1}^{M} \left\{ \frac{(\lambda)^{(N-1)M+m}}{[(N-1)M+m]!} \right\} (-1)^{(N-1)M+m} \times \left[\frac{d^{(N-1)M+m} F(s)}{ds^{(N-1)M+m}} \right] \Bigg|_{s=\lambda} \tag{10}$$

Let $f(t)$ be a gamma density function with mean $1/\mu$ and variance v. Besides, let $\mu v^2 = 1$, i.e., t is exponential distribution. Then,

$$\Pr(N, M) = \left(\frac{\lambda}{\lambda + \mu} \right)^{(N-1)M} \left[1 - \left(\frac{\lambda}{\lambda + \mu} \right)^{M} \right] \tag{11}$$

The expected number of MAR/As when the UE resides in S-CSCF service is

$$E[N] = \sum_{N=1}^{\infty} N \times \Pr(N, M) = \frac{1}{1 - \left(\frac{\lambda}{\lambda+\mu} \right)^{M}} \tag{12}$$

5.2 The Total Authentication Signaling Cost

Let $C_I(M)$ be the total authentication signaling cost of IMS AKA when an UE resides in S-CSCF service. Then, we can derive $C_I(M)$ as

$$C_I(M) = E[N] \times [2(M+1)\alpha + 4M\beta] = \frac{2(M+1)\alpha + 4M\beta}{1 - \left(\frac{\lambda}{\lambda+\mu} \right)^{M}}, \tag{13}$$

where α denotes the cost for Cx reference point and β denotes the cost for the SIP registration/authentication messages between UE and S-CSCF. Let $C_O(M)$ be the total authentication signaling cost of the one-pass IMS AKA when an UE resides in S-CSCF service. Then, we can derive $C_O(M)$ as

$$C_O(M) = E[N] \times [2(M+1)\alpha + 2M\beta] = \frac{2(M+1)\alpha + 2M\beta}{1 - \left(\frac{\lambda}{\lambda+\mu} \right)^{M}}. \tag{14}$$

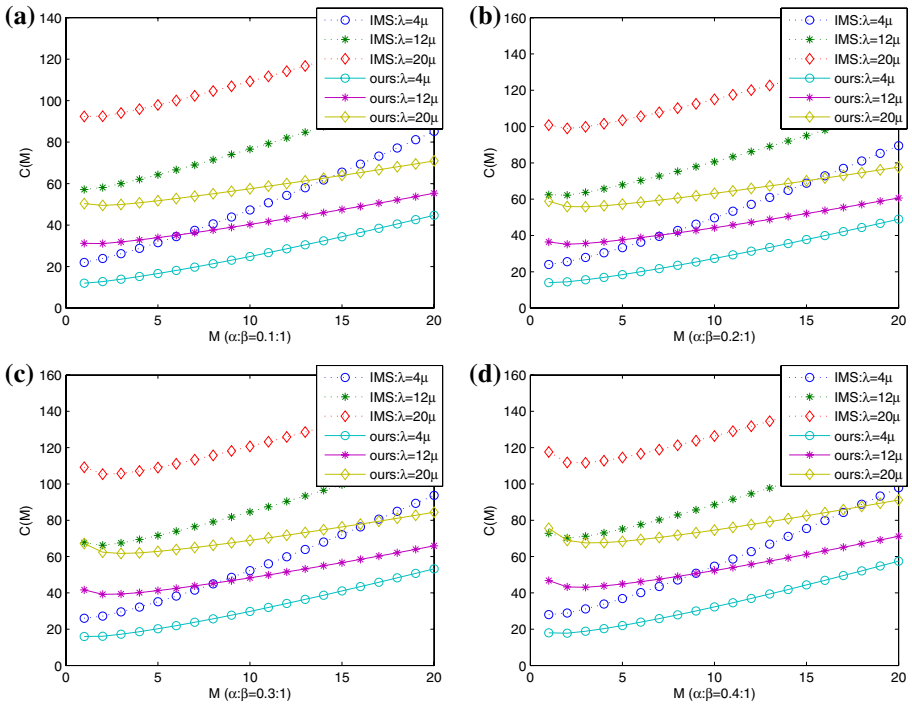

Fig. 5 The comparison of authentication signaling cost between IMS AKA and the one-pass IMS AKA, (**a**) $\alpha = 0.1$ and $\beta = 1$, (**b**) $\alpha = 0.2$ and $\beta = 1$, (**c**) $\alpha = 0.3$ and $\beta = 1$, (**d**) $\alpha = 0.4$ and $\beta = 1$

The signaling cost contains the delivery cost of SIP-R and Cx messages. Let the delivery cost of each SIP-R message between the UE and S-CSCF be one unit, i.e., $\beta = 1$, and the delivery cost of a Cx message between S-CSCF and HSS be α unit, where $\alpha \leq 1$. Reasons for these assumptions are as follows: (i) CSCF and HSS exchange the Cx message through the IP network. However, in addition to the IP network overhead, the delivery cost of the SIP-R messages also involves the packet-switch domain overhead and the UTRAN radio network overhead. (ii) S-CSCF and HSS are typically located at the same network, while the UE may reside in a remote network. (iii) Even when the UE resides in its home network, the SIP-R message needs to travel at least three hops between the UE and S-CSCF, such as P-CSCF, I-CSCF and then S-CSCF. Meanwhile the Cx message travels only one hop between S-CSCF and HSS. Therefore, when the UE resides in its home network, the delivery cost of the SIP message between the UE and S-CSCF needs triple the delivery cost of Cx message, i.e., $\alpha < \frac{1}{3}$.

According to the aforementioned assumption, set $\alpha = 0.1, 0.2, 0.3, 0.4$ and $\beta = 1$ in Eqs. 13 and 14. Figure 5 plots $C(M)$ against M with various SIP-R arrival rates λ. Figure 5 contains concave curves, i.e., $C(M)$ decreases and then increases as M increases. Obviously, the authentication cost of the one-pass IMS AKA in Fig. 5 under different parameters is lower than that of IMS AKA. Furthermore, we define the improvement of authentication signaling cost over IMS AKA as

$$C_{Improvement} = \frac{C_I(M) - C_O(M)}{C_I(M)} \tag{15}$$

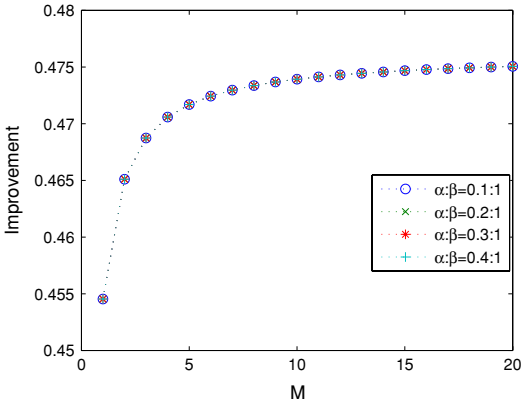

Fig. 6 The improvement of authentication signaling cost over IMS AKA

Table 1 Authentication parameters

Parameter	Length (bits)	Parameter	Length (bits)
RAND	128	*CK*	128
MAC	64	*IK*	128
AUTH	128	IMS-key	128

and depicts it in Fig. 6. Figure 6 depicts that the one-pass IMS AKA has at least 45% improvement over IMS AKA.

5.3 The Total Cost of the Authentication Parameters

The total cost of authentication parameters in IMS AKA is

$$S_I = E[N] \times M \times L_{AV}, \tag{16}$$

where L_{AV} is the length of each AV. Since each AV contains $RAND$, $XRES$, CK, IK and $AUTH$, whose length are depicted in Table 1, L_{AV} can be derived as

$$L_{AV} = L_{RAND} + L_{XRES} + L_{CK} + L_{IK} + L_{AUTH} = 544 \text{ bits} \tag{17}$$

The total cost of authentication parameters in IMS AKA is

$$S_O = E[N] \times M \times L_{IMS-key} = 128ME[N] \text{ bits} \tag{18}$$

Then, according to Eqs. 16, 18 and 17, we define the improvement of total cost of authentication parameters over IMS AKA as

$$S_{Improvement} = \frac{S_I - S_O}{S_I} = 76.5\%. \tag{19}$$

The advantages of the improvement of authentication parameter cost over IMS AKA are (i) reducing the computation cost of authentication parameters and (ii) reducing the storage space for S-CSCF.

6 Conclusion

This paper has proposed the one-pass IMS AKA instead of IMS AKA in the IMS authentication. The one-pass IMS AKA does not need the duplicated AKA operations and only needs one round-trip to carry out the IMS authentication. Besides, the one-pass IMS AKA can keep the security properties as IMS AKA and withstand some security attacks demonstrated in Sect. 4. Since the one-pass IMS AKA only needs one round-trip to carry the purpose of IMS authentication, Sect. 5 demonstrates that the one-pass IMS AKA can save at least 45% authentication signaling comparing with IMS AKA. Besides, the one-pass IMS AKA can save 76.5% storage space to store authentication parameters.

Acknowledgements The research is supported by the National Science Council of the Republic of China under the grant number NSC 96-2219-E-006-008 and the Program of Top 100 Universities Advancement, Ministry of Education, Taiwan, Republic of China.

References

1. 3GPP TS 23.228: Technical Specification Group Services and Systems Aspects; IP Multimedia Subsystem Stage 2.
2. 3GPP TS 29.228: Technical Specification Core Network; IP Multimedia Subsystem Cx and Dx Interfaces; Signaling Flows and Message Contents (Release 5).
3. 3GPP TS 29.229: Technical Specification Core Network;Cx and Dx Interfaces Based on the Diameter Protocol; Protocol Details.
4. 3GPP TS 33.203: Technical Specification Group Services and Systems Aspects; 3G Security; Access security for IP-based services (Release 6).
5. 3GPP TS 33.210: Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security (Release 7).
6. 3GPP TS33.102: Technical Specification Group Services and System Aspects; 3G Security; Security Architecture.
7. Camarillo, G., Kauppinen, T., Kuparinen, M., & Ivars, I. (2007). Towards an innovation oriented ip multimedia subsystem. *IEEE Communications Magazine, 45*(3), 130–136.
8. Franks, J., Hallam-Baker, P. M., Hostetler, J. L., Lawrence, S. D., & Leach, P. J. (1999).HTTP authentication: Basic and digest access authentication, RFC 2617, IETF.
9. Huang, C. M., & Li, J. W. (2005). Authentication and key agreement protocol for UMTS with low bandwidth consumption. *Proc International Conference on advanced Information Networking and Applications (AINA), 1*, 392–397.
10. Huang, C. M., & Li, J. W. (2007). Efficient and provably secure ip multimedia subsystem authentication for umts. *The Computer Journal, 50*(6), 739–757.
11. Lin, Y., & Chen, Y. (2004). Reducing authentication signaling traffic in third generation mobile network. *IEEE Transactions on Wireless Communications, 2*(3), 493–501.
12. Lin, Y. B., Chang, M. F., Hsu, M. T., & Wu, L. Y. (2005). One-pass GPRS and IMS authentication procedure for UMTS. *IEEE Journal on Selected Areas in Communications, 23*(6), 1233–1239.
13. Niemi, A., Arkko, J., & Torvinen, V. (2002). Hypertext Transfer Protocol (HTTP) digest Authentication Using Authentication and Key Agreement (AKA).RFC 3310.
14. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., & Peterson, J., Sparks, R., Handley, M., & Schooler, E. (2002). SIP Session Initiation Protocol.RFC 3261, IETF.
15. Torvinen, V., Arkko, J., & Naeslund, M. (2005). Hypertext Transfer Protocol Digest Authentication Using Authentication and Key Agreement Version-2.RFC 4169.

Author Biographies

Chung-Ming Huang received the BS degree in electrical engineering from National Taiwan University, and the MS and PhD degrees in computer and information science from The Ohio State University. Currently, he is a Distinguished Professor, Chairman of Dept. of Computer Science and Information Engineering, and Director of Institute of Medical Informatics, National Cheng Kung University, Taiwan, ROC He has published more than 200 referred journal and conference papers in wireless and mobile communication protocols, interactive multimedia systems, audio and video streaming and formal modeling of communication protocols. His research interests include wireless and mobile network protocols design and analysis, multimedia processing and streaming, web technologies, and network applications and services.

Jian-Wei Li received the BS degree in Information Engineering and Computer Science from Feng Chia University, Taichung, Taiwan, ROC, in 2001 and the MS degree in Computer Science and Information and Engineering from Chaoyang University of Technology, Taichung, Taiwan, ROC, in 2003. He is currently a PhD candidate in Dept. of Computer Science and Information and Engineering, National Cheng Kung University, Tainan, Taiwan, ROC. He is a member of the Phi Tau Phi Society. His research interests include wireless and mobile networks, network security, information security and cryptography.