International Journal of Innovative
Computing, Information and Control
Volume **8**, Number **2**, February **2012**

 ISSN 1349-4198
pp. **1385–1396**

EFFICIENT AUTHENTICATION AND KEY AGREEMENT PROCEDURE IN IP MULTIMEDIA SUBSYSTEM FOR UMTS

Hung-Min Sun, Bing-Zhe He, Shih-Ying Chang and Chun-Hua Cho

Department of Computer Science
National Tsing Hua University
No. 101, Sec. 2, Kuang-Fu Road, Hsinchu 30013, Taiwan
hmsun@cs.nthu.edu.tw

Received November 2010; revised May 2011

Abstract. *In a Universal Mobile Telecommunications System (UMTS), a user equipment (UE) can access IP multimedia services through IP Multimedia Subsystems (IMS). In addition to passing IMS authentication, called IMS AKA, this UE also needs to pass General Packet Radio Service (GPRS) authentication, called 3GPP AKA, since the data of the IMS service is transmitted through a GPRS network. Many steps in these two authentication processes are identical and result in inefficiency. Two papers proposed efficient authentication schemes instead of IMS authentication. However, these schemes suffer from security and compatibility problems. In this paper, we design an efficient IMS authentication scheme based on a trust relation between UE and Serving GPRS Support Node (SGSN) established in GPRS authentication. Compared with the conventional IMS authentication, our scheme can save up to 40% transmission and is analyzed as a secure scheme. Moreover, our scheme does not require any modification in the UE's authentication procedures.*
Keywords: 3GPP AKA, IMS AKA, Authentication

1. **Introduction.** To provide different types of services for a user, integration of different heterogeneous wireless network environments is a rising and important issue in recent years. Future telecommunication networks will converge on an All-IP network; that is, users will be able to access data from one or more different wireless network interfaces. Universal Mobile Telecommunications System (UMTS) proposed by the Third-Generation Partnership Project (3GPP) is a third-generation (3G) mobile communication technology. UMTS supports IP-based multimedia services, such as audio, video, text and chat, through IP Multimedia Subsystem (IMS) [1]. Many recent studies have investigated authentication and key agreement for protecting the communications [16-19]. A user can easily establish a session key for encryption and authentication. The authentication mechanism for 3G is called AKA and defined in RFC3310, which is used in GPRS network and IMS.

The UMTS architecture is illustrated in Figure 1. UE accesses the services by Serving GPRS Support Node (SGSN) through UMTS terrestrial radio access network (UTRAN). The SGSN connects to the home subscriber server (HSS) and the authentication center (AuC) to obtain authentication information. In addition, SGSN connects to Call Session Control Functions (CSCFs) and data network via gateway GPRS support node (GGSN) in order to support IP multimedia services and so on.

In UMTS, user equipment (UE) can access services, GPRS services and IMS services. If a UE wants to access GPRS services, the UE and the SGSN must authenticate with each other via GPRS authentication [2]. If the UE wants to use IMS services, besides the GPRS authentication, the UE has to be authenticated by the IMS authentication [3].

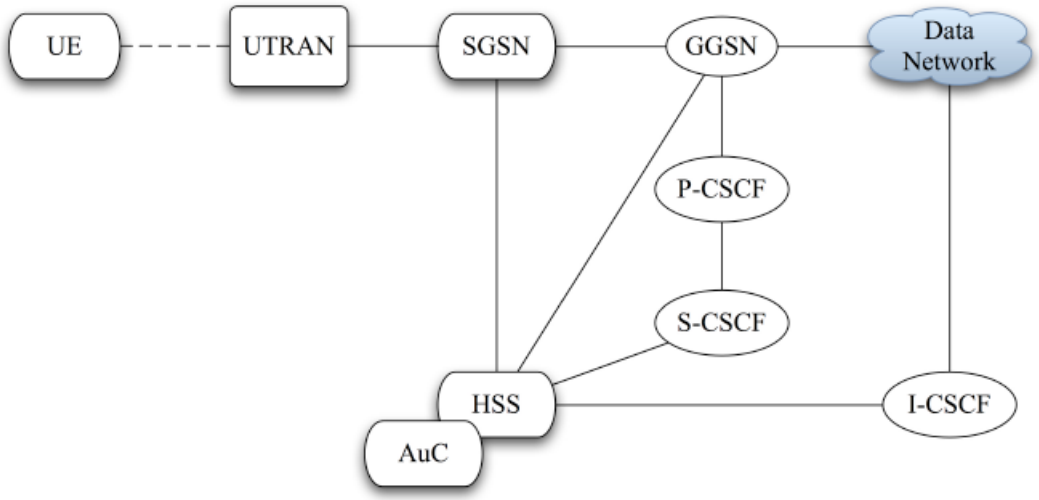

FIGURE 1. The UMTS architecture

If IMS authentication is omitted, a subscriber who only passes the GPRS authentication can impersonate another IMS subscriber and use IMS services.

It is necessary for an IMS subscriber to pass both GPRS authentication and IMS authentication, a two-pass authentication. However, the two-pass authentication is inefficient, since the IMS authentication is based on GPRS authentication so that almost all steps in these two authentications are identical. In GPRS authentication, the parameter used in the first step is the International Mobile Subscriber Identity (IMSI) in the UMTS Subscriber Identity Module (USIM) of the UE [2]. In IMS, authentication is IP Multimedia Privacy Identity (IMPI) in the IMS Subscriber Identity Module (ISIM) of the UE [3]. Besides the differences between these two passes, another difference is that the GPRS authentication is implemented by GMM and the signaling system number 7 (SS7) protocol, while the IMS authentication is implemented by SIP and Cx protocol [4-6,9].

Therefore, instead of IMS authentication, Lin et al. [8] proposed a simple one-pass authentication and key agreement (L-IMS AKA). However, their scheme lacks mutual authentication and key agreement capability [7]. To address above problems, Huang et al. proposed the E-IMS AKA [7,10]. In this scheme, the authentication procedures in UE and CSCF need to be modified, making it prone to the compatibility problem.

Lim et al. [11] also proposed an efficient IMS authentication to address the problem of two-pass authentication. Their new scheme depends on initial authentication in the WiBro-EVO system. Similarly, the new IMS authentication scheme of Veltri et al. [12] depends on initial authentication in Wireless LAN. Their schemes try to solve a similar problem as ours, but the applied scenario of these schemes is different from that of our scheme. Moreover, some papers proposed schemes [13-15] to enhance the performance of 3GPP AKA, but they also have a different applied scenario with that of our scheme. In short, these schemes are unsuitable for the scenario of GPRS to IMS.

In this paper, we propose an efficient and secure IMS authentication protocol based on trust relations between the UE and the SGSN. Since the UE has already passed the GPRS authentication, the UE can trust the SGSN. In order to reduce redundant steps in the IMS authentication protocol, the SGSN can be an agent of the UE for executing the authentication process. Therefore, instead of UE, SGSN authenticates serving call session control function (S-CSCF) mutually to obtain better efficiency. In our protocol, only SGSN, S-CSCF and HSS/Auc need to be modified. During the authentication protocol, the steps the UE executes in our proposed authentication protocol are the same as those

in IMS authentication. In other words, our protocol supports backward compatibility. In short, our proposed scheme is both secure and compatible. To the best of our knowledge, none of the previously proposed schemes can meet these properties simultaneously.

The remainder of this paper is organized as follows: Section 2 briefly reviews the GPRS and IMS authentication protocol. Section 3 presents our proposed protocol in details and Section 4 analyzes the proposed protocol. Finally, we conclude our work and show future direction in Section 5.

2. **Background.**

This section presents the fundamentals of the GPRS and IMS authentication.

2.1. **GPRS authentication.**

When an UE invokes the GPRS access, the UE must pass GPRS authentication. The UE sends a message to trigger 3GPP AKA procedure between the UE and the SGSN [8] (see Figure 2).

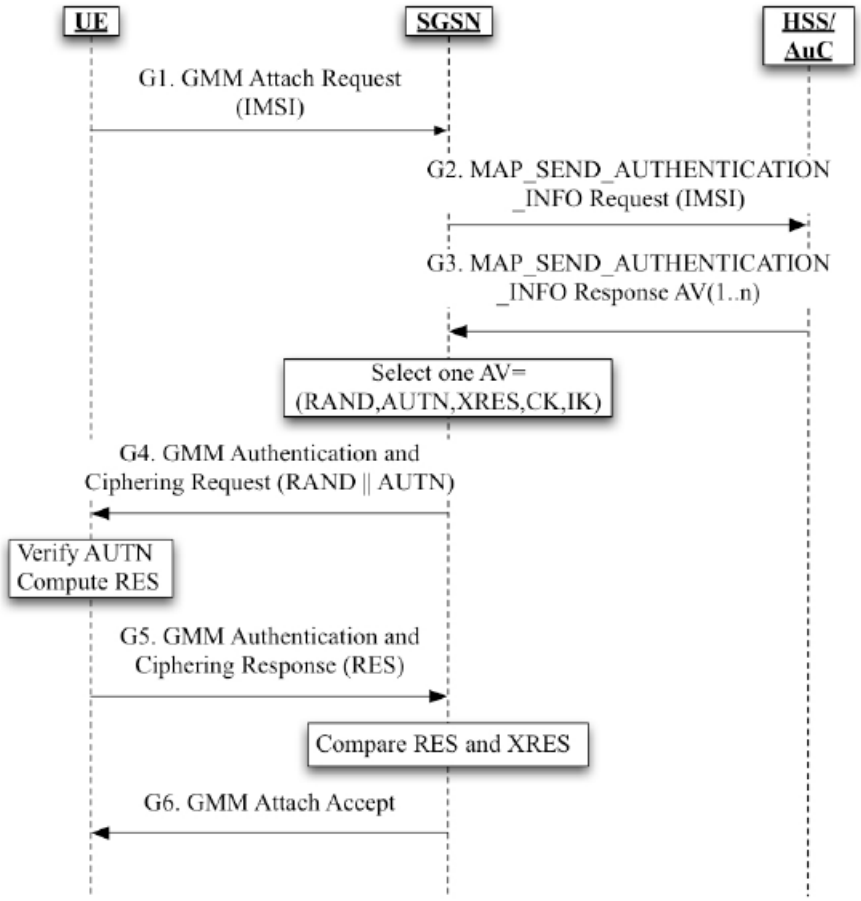

FIGURE 2. Message flow for 3GPP GPRS authentication

Step G1) The UE sends a GMM Attach Request with the parameter IMSI to the SGSN.

Step G2) If SGSN has requested authentication vectors (AVs) of the UE before, this step and step G3 can be skipped. Otherwise, the SGSN obtains these AVs by sending a MAP_SEND_AUTHENTICATION_INFO Request message with the parameter IMSI. An AV consists of a random number (RAND), an expected response (XRES), a cipher key (CK), an integrity key (IK) and an authentication token

(AUTN). The UE and the HSS/AuC share a secret key K and a sequence number SQN. Given input K, SQN and RAND, the UE and HSS/AuC can compute same AUTN, XRES, IK and CK.

Step G3) The HSS/AuC uses the IMSI to generate an ordered array of AVs and sends them to SGSN.

Step G4) The SGSN randomly selects one AV from AVs. Then SGSN sends the parameter RAND and AUTN of AV, to the UE.

Step G5) The UE checks if the received AUTN are valid. If this AV is valid, the UE sends the RES to the SGSN.

Step G6) If the received RES is identical to XRES, the SGSN sends a GMM Attach Accept message to notify the UE that the authentication procedure has been completed.

2.2. **IMS authentication.** In IMS, IP-based multimedia services are provided by CSCF which controls multimedia sessions by means of the Session Initiation Protocol (SIP) [1,4,9]. After passing the GPRS authentication, the UE sends a register message to CSCF in order to obtain IMS service [8] (see Figure 3).

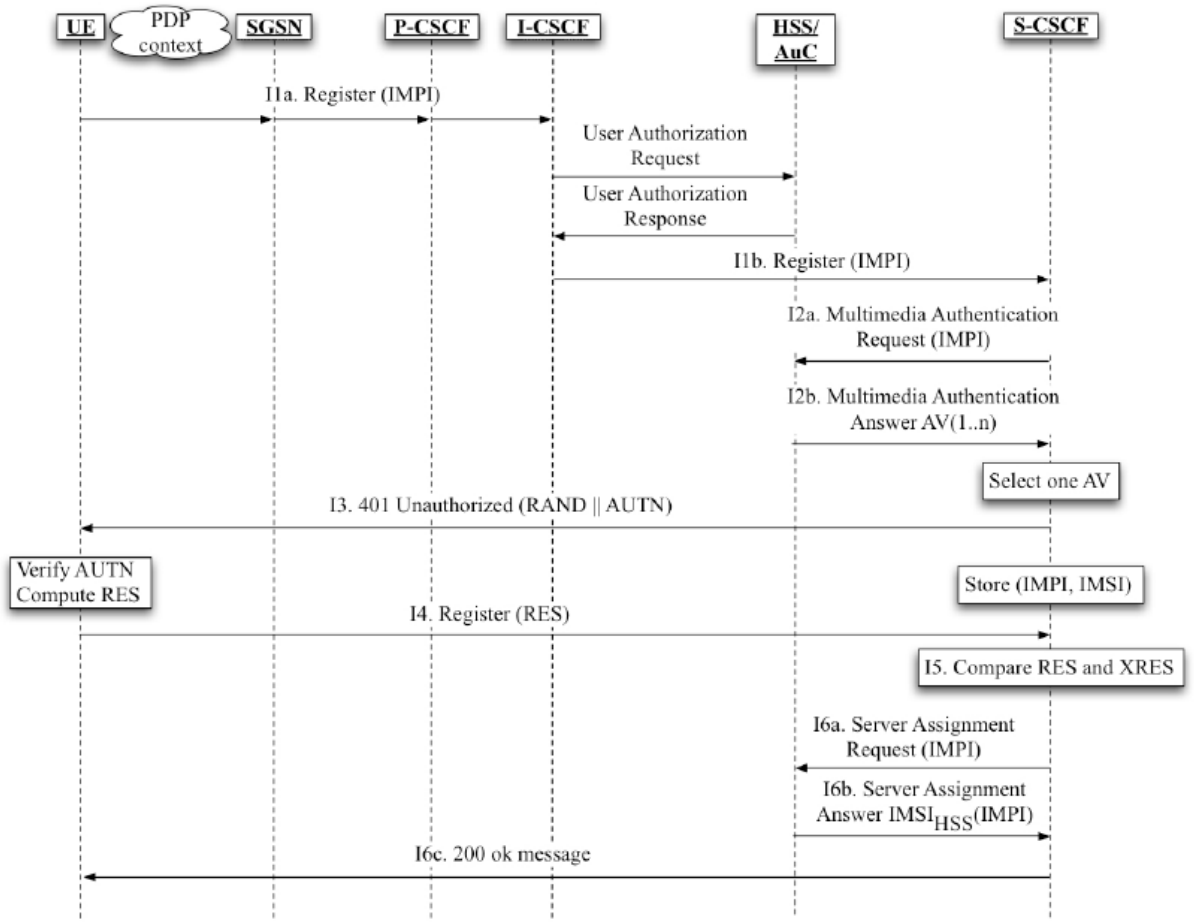

FIGURE 3. Message flows for IMS authentication

Step I1) The UE sends a register message to the Interrogating-CSCF (I-CSCF) with the parameter IMPI through the SGSN. The I-CSCF then exchanges the user authentication request (UAR) and the user authentication answer (UAA) with HSS/AuC to obtain the name of the S-CSCF from the HSS/AuC.

Step I2) If S-CSCF has the AVs of the UE, it skips Steps I2 and I3. Otherwise, the S-CSCF requests these AVs from the HSS/AuC.
Step I3) The S-CSCF selects one AV from requested AVs and sends a message with the parameters RAND and AUTN to the UE.
Step I4) If the UE accepts the AUTN, the UE sends a message with the parameter RES to the S-CSCF.
Step I5) If the parameter RES is identical to the XRES, the authentication procedure is completed.
Step I6) The S-CSCF sends a Cx Server Assignment Request to the HSS/Auc. Upon receiving a Server Assignment Answer message from the HSS/AuC, the S-CSCF sends a 200 message to notify the UE about the completion of IMS authentication.

2.3. **Security requirements of IMS authentication.** After analyzing IMS authentication, we can obtain the security requirements of IMS authentication. In this paper, we modify the message flows of IMS AKA for the sake of better efficiency but our scheme still meets these requirements. These requirements are listed as follows:
R(1). Mutual authentication

UE and S-CSCF can authenticate each other. In IMS AKA, UE authenticates S-CSCF by AUTN and S-CSCF authenticates UE by RES.
R(2). Key agreement

UE and S-CSCF can negotiate two keys, IK and CK, to protect the integrity and confidentiality of the communication between them. In IMS AKA, these keys are generated from successful mutual authentication.
R(3). Replay protection

UE and S-CSCF can avoid accepting replay messages. In IMS AKA, UE and S-CSCF keep a synchronized SQN counter. By this counter, they can check the freshness of the messages.
R(4). Avoiding using reused RAND

The UE and the S-CSCF must avoid reusing RANDs, because reusing RANDs will increase the success probability of replay attacks. An attacker can eavesdrop and record the used pairs of RNAD and XRES. If S-CSCF uses a reused RAND, this attacker can replay the corresponding XRES to impersonate the UE. Note that XRES = $f2_k$(RAND) [2]; that is, the same RAND will generate the same XRES. In IMS AKA, the RAND is determined by HSS/AuC. HSS/AuC records all used RANDs to avoid reusing a used RAND.

3. **The Proposed Scheme.** We propose an authentication protocol that is more efficient than IMS AKA because it reduces the redundant steps in 3GPP AKA. The proposed protocol is also backward compatible with IMS AKA, since the UE does not need any modification in order to execute the proposed protocol. The difference between IMS AKA and our scheme is that the SGSN needs to participate in IMS authentication procedure. After GPRS authentication, the UE and the SGSN can establish a trust relation. Therefore, the UE can delegate the SGSN to execute authentication procedure. When SGSN completes the procedure, the UE can establish session keys with S-CSCF and SGSN does not have these keys. The proposed protocol is also backward compatible to IMS AKA.

In our design, SGSN and S-CSCF will share the same AVs of the UE and use these AVs to complete the authentication procedure. Since HSS/AuC generates these AVs, we can avoid using used RANDs. In addition, in comparison to IMS authentication, we use

AUTN to authenticate S-CSCF and RES to authenticate SGSN. This design can reduce the number of message exchanges. We will describe the analysis in the next section.

Our scheme also supports backward compatibility. This means that the operations the UE performed in the proposed protocol are the same with IMS AKA. In our design, SGSN has the same AVs with S-CSCF. This also means that instead of S-CSCF, SGSN can mutually authenticate with the UE. Therefore, SGSN can simulate the operations that the UE performed in IMS AKA. The messages exchanged by the UE in the proposed protocol (Steps P1, P7b and P8-P10) are the same as those in IMS AKA (Steps I1a, I3, I4 and I6). On the other hand, SGSN and S-CSCF can mutually authenticate each other by using the proposed scheme. Since the UE and SGSN already have a trust relation when they complete GPRS AKA. The real mutual authentication and key agreement needed by IMS service is completed by SGSN and S-CSCF.

The details of the proposed scheme are as follows (see Figure 4).

Step P1) After GPRS authentication, the SGSN can identify the UE and protect the communication between them by using the session key generated in GRPS AKA. The UE then sends IMS register message to start IMS authentication.

Step P2) The SGSN and the UE have a trust relation thus the S-CSCF authenticates the SGSN instead of the UE. If the SGSN does not have AVs of the UE, the SGSN would request AVs from the HSS/AuC in this step. Otherwise, this step should be skipped. Thus, the SGSN and S-CSCF will have the same AV to authenticate each other. Since the HSS/AuC chooses the RANDs, the probability of reusing RAND is small. Note that SGSN only obtain RAND, AUTN and XRES from these AVs. The SGSN cannot use these parameters to compute the session. Since the session keys are used to protect communication between the UE and the S-CSCF, the SGSN does not need to have these keys.

Step P3) The SGSN selects an unused AV from ordered AVs and sends a message with the parameters, (IMPI, IMSI), AUTN and RAND to the I-CSCF. After the I-CSCF receives the register message, the I-CSCF sends the UAR and the UAA to the HSS/AuC in order to obtain the name of the S-CSCF. Finally, the I-CSCF sends (IMPI, IMSI), AUTN and RAND to the S-CSCF.

Step P4) This step is the same as Step P2. If the S-CSCF has AVs of the UE then skip this step. Note that the AVs obtained by S-CSCF are the same as the AVs obtained by the SGSN for authenticating each other.

Step P5) The S-CSCF checks the pair (IMPI, IMSI) through the HSS/AuC.

Step P6) The S-CSCF checks the AUTN from the SGSN. If the AUTN is valid, then the S-CSCF selects an AV according to the receiving RAND and sends the corresponding RES to the SGSN. The S-CSCF can authenticate the SGSN by the AUTN and let the SGSN authenticate the S-CSCF by the RES.

Step P7) If the parameter RES and XRES are identical, then the SGSN authenticates the S-CSCF. After finishing the authentication procedure, the SGSN sends the parameter RAND to the UE. After receiving this RAND, the UE will consider the mutual authentication with S-CSCF to be successfully finished because the UE trusts the SGSN. Then the UE can employ this RAND to generate the same session keys and uses these keys to protect the communication between the UE and S-CSCF. Note that since the session key generated in GPRS AKA protects this RAND, it is hard to modify and eavesdrop on the session generated in the proposed protocol. Thus, the SGSN cannot obtain these keys because the SGSN does not have the keys in its AVs as described in Step P2. If the UE only supports IMS AKA, Steps P8, P9 and P10 are designed for backward

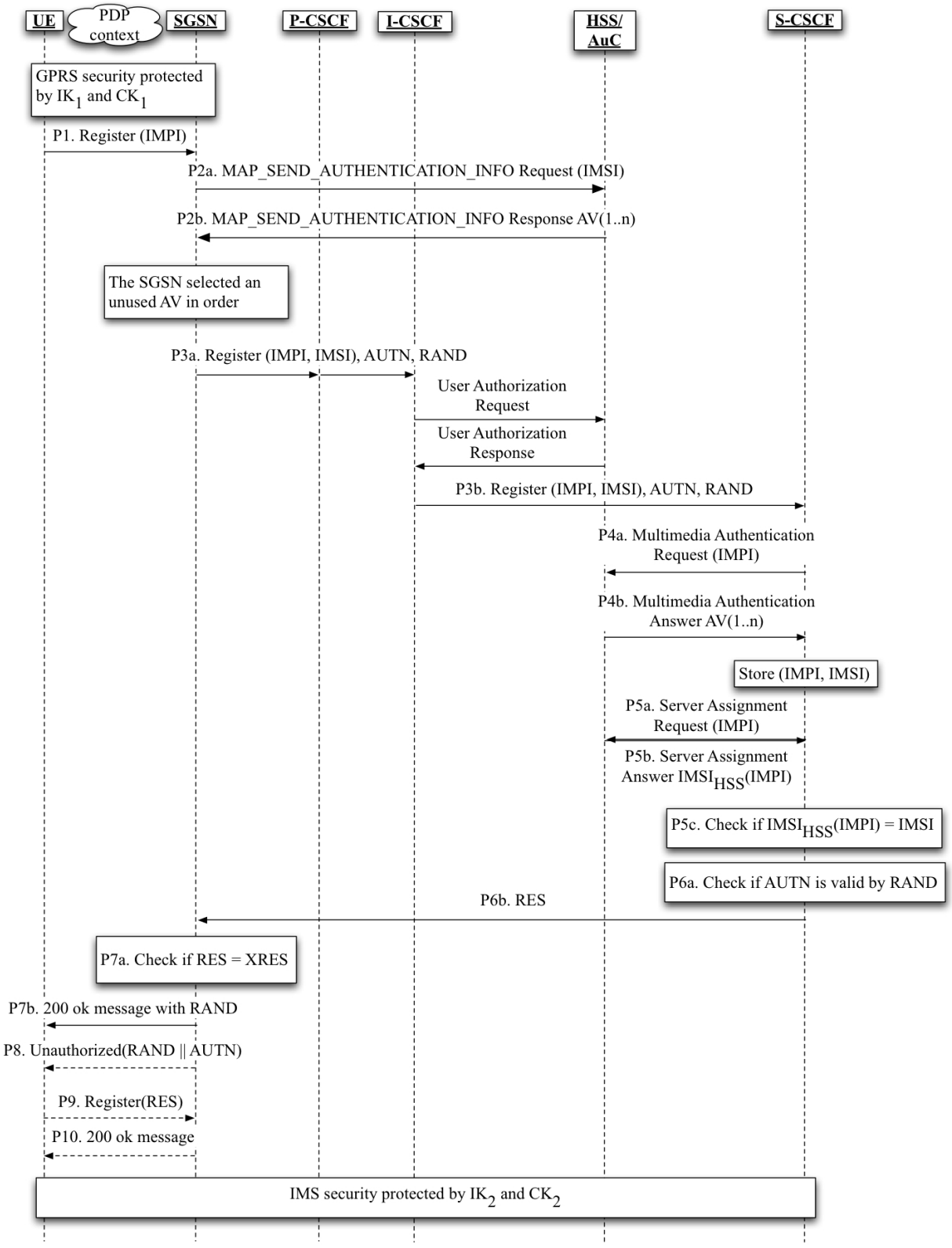

FIGURE 4. The message flow of the proposed one pass authentication

compatibility. In other words, the UE can execute the proposed protocol and IMS AKA without any modification.

Step P8) The SGSN sends RAND and AUTN to the UE. The RAND and AUTN are the same as the ones selected in Step P3.

Step P9) The UE responds associated RES to the SGSN.

Step P10) The SGSN sends 200 OK message to the UE. After receiving this message, the UE completes IMS authentication. By Steps P8, P9 and P10, the UE can generate the same IK2 and CK2 as the SGSN.

4. **Performance and Security Analysis.** In this section, we analyze the performance and security of the proposed protocol.

4.1. **Performance analysis.** In this section, the performance of our scheme is evaluated and compared with the IMS AKA, L-IMS AKA and E-IMS AKA. We use the same definitions and analysis model in [7,8]. We assume that the cost of communication between the UE and the S-CSCF is one unit and is higher than others. The cost between the HSS/AuC and the S-CSCF is α, where $\alpha \ll 1$; the cost between the SGSN and the HSS/AuC is β, where $\beta < 1$.

When registering for IMS service for the first time, the S-CSCF does not have AVs of the UE. Therefore, the S-CSCF must send MAR and MAA message (Step I2 in Figure 3). The cost of initial IMS AKA $C_{I,1}$ is expressed as

$$C_{I,1} = 4 + 6\alpha. \tag{1}$$

Otherwise, the MAR and MAA message can be skipped. In this case, the cost of the IMS AKA $C_{I,2}$ is expressed as

$$C_{I,2} = 4 + 4\alpha. \tag{2}$$

Supposing that the size of AV is n and the authentication procedure run m times, where $m > n$ and $x = \lceil \frac{m}{n} \rceil$. Therefore, the S-CSCF will send MAR and MAA message x times. The average cost of the IMS AKA is expressed as

$$C_I = \left(\frac{x}{m}\right) C_{I,1} + \left(\frac{m-x}{m}\right) C_{I,2} = 4 + \left(\frac{2x}{m} + 4\right) \alpha. \tag{3}$$

In a similar way, the delivery cost of L-IMS AKA is expressed as (4) and the derivation is defined in [7,8].

$$C_L = 2 + 4\alpha \tag{4}$$

Consequently, the average cost of the E-IMS AKA is expressed as

$$C_H = \left(\frac{x}{m}\right) C_{H,1} + \left(\frac{m-x}{m}\right) C_{H,2} = 2 + \left(\frac{2x}{m} + 4\right) \alpha. \tag{5}$$

We assume that the cost between the SGSN and the HSS/AuC is 2β (Step P2 in Figure 4), which is different with the cost between the HSS/AuC and S-CSCF (Step P4 in Figure 4). The Steps P8, P9 and P10 in Figure 4 are for backward compatible. If the UE support our protocol, then the UE can skip these steps for saving delivery cost. In this paper, we suppose that the all UE are modified and we do not consider the cost of these steps. Therefore, the delivery cost of the proposed scheme $C_{P,1}$ is expressed as follows:

$$C_{P,1} = 2 + 6\alpha + 2\beta \tag{6}$$

If the SGSN already has AVs for the UE, then the delivery cost can be expressed as follows:

$$C_{P,2} = 2 + 4\alpha \tag{7}$$

Therefore, the average delivery cost of our scheme can be expressed as follows:

$$C_P = \left(\frac{x}{m}\right) C_{P,1} + \left(\frac{m-x}{m}\right) C_{P,2} = 2 + \left(\frac{2x}{m} + 4\right) \alpha + \left(\frac{2x}{m}\right) \beta \tag{8}$$

From Equations (3) and (4), we can conduct the improvement function for L-IMS AKA over IMS AKA, which represents the ratio of the saving cost.

$$S_L = \frac{C_I - C_L}{C_I} = \frac{m + x\alpha}{2(1+\alpha)m + x\alpha} \tag{9}$$

Likewise, the improvement function of the E-IMS AKA over the IMS AKA, which is obtained from Equations (3) and (5), is as follows:

$$S_H = \frac{C_I - C_H}{C_I} = \frac{m}{2(1+\alpha)m + x\alpha} \tag{10}$$

Likewise, the improvement function of our proposed scheme over the IMS AKA is as follows:

$$S_P = \frac{C_I - C_P}{C_I} = \frac{m - x\beta}{2(1+\alpha)m + x\alpha} \tag{11}$$

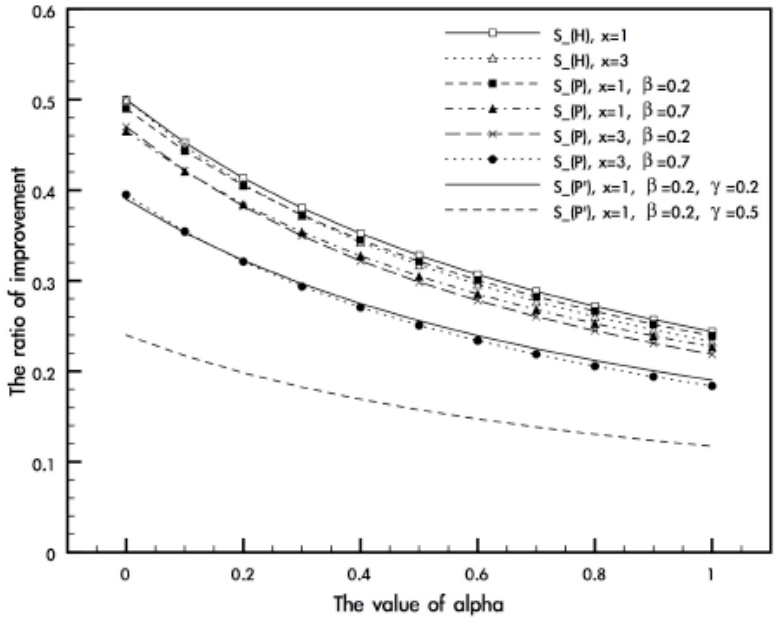

FIGURE 5. The performance evaluation

In Figure 5, the X-axis and Y-axis means that the value of x and the value of saving cost, where $x = \lceil \frac{m}{n} \rceil$ and we assume that m is equal to 10. The definition of γ is the cost of communication between the UE and the SGSN (Steps P8 and P9 in Figure 4). Since the communication distance between the UE and the S-CSCF is longer than others, the value of β and γ are less than 1. In general, we assume that $\beta \in \{0.2, 0.7\}$ and $\gamma \in \{0.2, 0.5\}$. S(H) and S(P) mean that the improvement function of E-IMS AKA and the proposed protocol over IMS AKA, respectively. Although L-IMS AKA is more efficient than others, L-IMS does not meet some security requirements [7,10]. According to Figure 5, both L-IMS AKA, E-IMS AKA and our proposed scheme can save about 40% of the cost over IMS AKA, when $\alpha = 0.3$. If the value of x is larger, which means that the size of AV is larger, the more cost can be saved. When the cost of MAP_SEND_AUTHENTICATION_INFO between the SGSN and the HSS/AuC is approximately equal to α, SP is approximately 10% lower than SH. If the value of x is small, E-IMS AKA is more efficient than ours. Hence, if the size of AVs is large, our protocol is not only more efficient than E-IMS AKA. Better yet, our protocol also meets the security requirement that L-IMS AKA does not

satisfy. Besides, the most important feature is that the proposed scheme is backward compatible with IMS AKA.

4.2. **Security analysis.** In this section, we analyze the security of the proposed protocol according to the security requirements mentioned above.

4.2.1. *Mutual authentication.* In our scheme, the HSS/AuC distributes the same AVs of the UE to the SGSN and S-CS/CF. Therefore, the SGSN and the S-CSCF can use the same AV to authenticate each other. In terms of authenticating the SGSN, the S-CSCF can check if AUTN is valid. Since the UE and the SGSN have authenticated each other through 3GPP AKA and the S-CSCF authenticates the SGSN, the S-CSCF can authenticate the UE indirectly. In terms of authenticating the S-CSCF, the SGSN can check if the RES and the XRES are identical. If the received RES is valid, then the SGSN authenticates the S-CSCF. That is, the UE authenticates the S-CSCF. Consequently, the UE and the S-CSCF achieve mutual authentication.

4.2.2. *Key agreement.* In our scheme, since the UE and the S-CSCF can agree on the same key IK and CK by the RAND, our scheme supports key agreement. Note that it is hard for attackers to generate these two keys.

4.2.3. *Replay protection.* It is also difficult for attackers to impersonate a legal UE even if an attacker can replay IMS register messages to the SGSN. This is because the messages exchanged between the UE and the SGSN are protected by GPRS secure tunnel. In this tunnel, the SGSN can verify the freshness of the messages by checking the parameter FRESH [2].

4.2.4. *Resisting SGSN compromising attack.* In our scheme, each AV that the SGSN obtains from HSS/AuC only has three elements, including RAND, XRES and AUTN. Only the UE and the S-CSCF have the IK and CK of IMS. Since the SGSN cannot generate IK and CK, compromising the SGSN does not compromise IMS communication.

We compare the proposed AKA with IMS AKA, L-IMS AKA and E-IMS AKA and show the results in Table 1 (some results are described in [7,8,10]). L-IMS AKA is the most efficient one, but L-IMS AKA does not meet some security requirements, such as mutual authentication and key agreement [7]. Although E-IMS AKA is more efficient than our scheme, E-IMS AKA is too complicated and is not backward compatible with present architecture. Backward compatibility means that an UE can execute either IMS AKA or our scheme without any modification. The comparisons show that our scheme can achieve both security and compatibility.

Table 1. The comparisons with other schemes

	IMS AKA	Lin et al.'s one-pass auth.	Huang et al.'s one-pass AKA	Our proposed AKA
Unilateral authentication [7]	Yes	Yes	Yes	Yes
Mutual authentication	Yes	No	Yes	Yes
Key agreement	Yes	No	Yes	Yes
One round-trip [7]	No	Yes	Yes	Yes
Additional memory	No	No	Yes	No
Backward compatible	No	No	No	Yes

5. **Conclusions.** Since the UE accesses the IMS through the GPRS network, the UE must pass both 3GPP AKA and IMS AKA. This two-pass authentication results in inefficiency since there are many identical steps in 3GPP AKA and IMS AKA. Hence, we proposed an efficient AKA protocol to reduce the redundant steps. Another important feature is backward compatible. The UE does not need to make any modification. The operations that the UE performed in our proposed protocol are the same as those in IMS AKA. Our scheme also meets the necessary security requirements of IMS authentication.

Acknowledgment. This work was supported in part by the National Science Council, Taiwan, under Contract NSC 100-2218-E-007-006 and NSC100-2628-E-007-018-MY3. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers.

REFERENCES

[1] *3GPP TS 23.228 Technical Specification Group Service and System Aspects; IP Multimedia Subsystem (IMS); Stage 2*, Release 6.

[2] *3GPP TS 33.102 Technical Specification Group Service and System Aspects; 3G Security; Security Architecture*, Release 6.

[3] *3GPP TS 33.203 Technical Specification Group Service and System Aspects; 3G Security; Access Security for IP-based Services*, Release 6.

[4] *3GPP TS 24.228 Technical Specification Core Network and Terminals; Signalling Flows for the IP Multimedia Call Control Based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*, Release 5.

[5] *3GPP TS 29.228 Technical Specification Core Network and Terminals; IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling Flows and Message Contents*, Release 5.

[6] *3GPP TS 29.229 Technical Specification Core Network and Terminals; Cx and Dx Interfaces Based on the Diameter Protocol; Protocol Details*, Release 9.

[7] C. M. Huang and J. W. Li, One-pass authentication and key agreement procedure in IP multimedia subsystem for UMTS, *IEEE the 21st International Conference on Advanced Information Networking and Applications*, pp.482-489, 2007.

[8] Y. B. Lin, M. F. Chang, M. T. Hsu and L. Y. Wu, One-pass GPRS and IMS authentication procedure for UMTS, *IEEE Journal on Selected Areas in Communications*, pp.1233-1239, 2005.

[9] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, SIP: Session initiation protocol (RFC 3261), *IETF*, 2002.

[10] C. M. Huang and J. W. Li, Efficient and provably secure IP multimedia subsystem authentication for UMTS, *The Computer Journal*, pp.739-757, 2007.

[11] S. H. Lim and S. H. Lee, Efficient IMS authentication architecture based on initial access authentication in WiBro-evolution (WiBro-EVO) system, *IEEE the 65th Vehicular Technology Conference*, pp.904-908, 2007.

[12] L. Veltri, S. Salsano and G. Martiniello, Wireless LAN-3G integration: Unified mechanisms for secure authentication based on SIP, *IEEE International Conference on Communications*, pp.2219-2224, 2006.

[13] M. Zhang and Y. Fang, Security analysis and enhancements of 3GPP authentication and key agreement protocol, *IEEE Transactions on Wireless Communications*, pp.734-742, 2005.

[14] J. Al-Saraireh and S. Yousef, A new authentication protocol for UMTS mobile networks, *EURASIP Journal on Wireless Communications and Networking*, pp.1-10, 2006.

[15] C. M. Huang and J. W. Li, Authentication and key agreement protocol for UMTS with low bandwidth consumption, *The 19th International Conference on Advanced Information Networking and Applications*, pp.392-397, 2005.

[16] W.-S. Juang, C.-L. Lei, H.-T. Liaw and W.-K. Nien, Robust and efficient three-party user authentication and key agreement using bilinear pairings, *International Journal of Innovative Computing, Information and Control*, vol.6, no.2, pp.763-772, 2010.

[17] H.-C. Hsiang, A novel dynamic ID-based remote mutual authentication scheme, *International Journal of Innovative Computing, Information and Control*, vol.6, no.6, pp.2407-2415, 2010.

[18] W.-G. Shieh and M.-T. Wang, An improvement on Li and Hwang's biometrics-based remote user authentication scheme, *ICIC Express Letters*, vol.4, no.5(B), pp.2021-2026, 2010.

[19] W.-G. Shieh and W.-B. Horng, Security analysis and improvement of the remote user authentication scheme without using smart cards, *ICIC Express Letters*, vol.4, no.6(B), pp.2431-2436, 2010.