One-Pass GPRS and IMS Authentication Procedure for UMTS

Yi-Bing Lin, *Fellow, IEEE*, Ming-Feng Chang, Meng-Ta Hsu, and Lin-Yi Wu

***Abstract*—Universal Mobile Telecommunications System (UMTS) supports Internet protocol (IP) multimedia services through IP multimedia core network subsystem (IMS). Since the IMS information is delivered through the general packet radio service (GPRS) transport network, a UMTS mobile station (MS) must activate GPRS packet data protocol (PDP) context before it can register to the IMS network. In the Third-Generation Partnership Project (3GPP) specifications, authentication is performed at both the GPRS and the IMS networks before an MS can access the IMS services. We observe that many steps in this 3GPP "two-pass" authentication procedure are identical. Based on our observation, this paper proposes an one-pass authentication procedure that only needs to perform GPRS authentication. At the IMS level, authentication is implicitly performed in IMS registration. Our approach may save up to 50% of the IMS registration/authentication traffic, as compared with the 3GPP two-pass procedure. We formally prove that the one-pass procedure correctly authenticate the IMS users.**

***Index Terms*—Authentication, call session control function (CSCF), general packet radio service (GPRS), IP multimedia core network subsystem (IMS), session initiation protocol (SIP), universal mobile telecommunications system (UMTS).**

I. Introduction

UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM (UMTS) proposed by the Third-Generation Partnership Project (3GPP) is a third-generation (3G) mobile telecommunications technology evolved from general packet radio service (GPRS) [2]. Fig. 1 illustrates the UMTS packet switched (PS) core network (CN), where the packet data services of a mobile station (MS) are provided by the serving GPRS support node (SGSN) via UMTS terrestrial radio access network (UTRAN). The SGSN connects to the external data network through the gateway GPRS support node (GGSN). Furthermore, the SGSN communicates with the home subscriber server (HSS) and the authentication center (AuC) to retrieve subscriber data and authentication information of an MS. The AuC, which may be collocated with the HSS, is responsible for security management of subscribers. UMTS supports voice and multimedia services through the PS CN based on the Internet protocol (IP) technology. Specifically, the 3GPP defines IP multimedia core network subsystem (IMS) to support multimedia services such as voice telephony, video, real-time interactive games, messaging, and multimedia conferencing [7]. In IMS, multimedia services are provided by call session control function (CSCF) utilizing session initiation protocol (SIP) [5], [16]. Three types of CSCFs are defined in IMS: A proxy-CSCF (P-CSCF) located in the visited network of an MS is responsible for redirecting the SIP messages of an MS to the home network (where the HSS/AuC resides). A serving-CSCF (S-CSCF) is located in the home network of the MS to provide session control of multimedia services. The S-CSCF interacts with the application servers to obtain value added services. Furthermore, the S-CSCF communicates with the HSS and the AuC to receive IMS-related subscriber data and authentication information of the MS. An interrogating-CSCF (I-CSCF) is a firewall for the SIP messages toward the home network, and is responsible for selecting an S-CSCF for the MS.

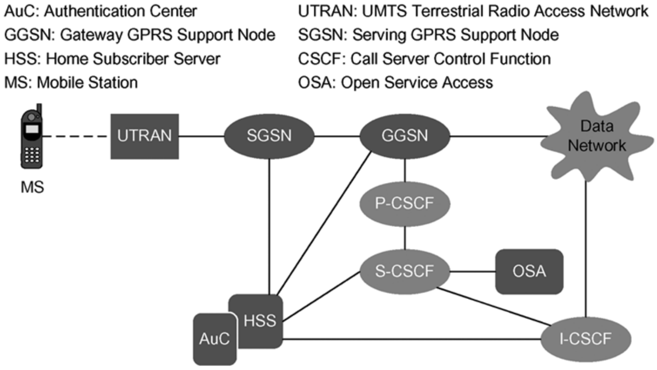

AuC: Authentication Center
GGSN: Gateway GPRS Support Node
HSS: Home Subscriber Server
MS: Mobile Station
UTRAN: UMTS Terrestrial Radio Access Network
SGSN: Serving GPRS Support Node
CSCF: Call Server Control Function
OSA: Open Service Access
UTRAN
SGSN
GGSN
Data Network
MS
P-CSCF
S-CSCF
OSA
HSS
AuC
I-CSCF

Fig. 1. UMTS architecture for packet switched service domain.

In UMTS, when an MS sends an "Initial L3 message" (e.g., location update request, connection management service request, routing area update request, attach request, paging response, etc.) to the SGSN, the SGSN may be triggered to authenticate the user. The authenticating parties are HSS/AuC in the home network and the universal subscriber identity module (USIM) in the MS. GPRS authentication consists of two major procedures [1], [10].

- **Distribution of authentication information from the AuC to the SGSN**: The SGSN sends an authentication data request to the HSS/AuC with the parameter international mobile subscriber identity (IMSI) of the MS, and receives a response with an array of authentication vectors (AVs) from the AuC. An authentication vector consists of a random number **RAND**, an expected response **XRES**, a cipher key **CK**, an integrity key **IK**, and an authentication

Manuscript received January 15, 2004; revised December 1, 2004. This work was supported in part by the National Science Council under Contract NSC 92-2219-E-009-032, in part by IIS/Academia Sinica, in part by CCL/ITRI and NCTU Joint Research Center under Contract NSC 93-2213E009026, in part by the NSC Excellence Project under Contract NSC93-2752-E-0 090 005-PAE, and in part by the National Science and Technology Program on Telecommunication (NTP).

The authors are with the Department of Computer Science and Information Engineering, National Chiao-Tung University, Hsinchu 30010, Taiwan (e-mail: liny@csie.nctu.edu.tw).

Digital Object Identifier 10.1109/JSAC.2005.845631

token **AUTN**. Each AV is good for one authentication and key agreement between the SGSN and the MS.

- **Authentication and key agreement between the SGSN and the MS**: This procedure performs authentication between an MS and the network by showing knowledge of a preshared secret key **K** that is only available in the USIM of the MS and the AuC. The SGSN invokes the authentication procedure with an authentication vector. This procedure supports mutual authentication between the MS and the network. Specifically, the **AUTN** is used by the MS to authenticate the network, and the **RES/XRES** pair is used by the SGSN to authenticate the MS (where the **RES** is generated by the MS). Details of the procedure will be given in Section II-A. The MS also computes two keys **CK** and **IK** using the received **RAND** and the preshared secret key **K** stored in the USIM. On the network side, the SGSN passes **CK** and **IK** to the UTRAN. During data transmission, **CK** and **IK** are used for ciphering and integrity between the MS and the UTRAN. Data ciphering and integrity is out of the scope of this paper, and will not be discussed further.

In addition to GPRS authentication, it is necessary to authenticate the MS before it can access IMS services. Without IMS authentication, a mobile user who passes the GPRS authentication can easily fake being another IMS user. Details of the fake procedure will be elaborated in Section II-C. IMS authentication is performed between the IMS subscriber identity module (ISIM) in the MS and the AuC in the home network [6]. This procedure is basically the same as the GPRS authentication. In this procedure, the CSCF first sends a multimedia authentication request to the HSS/AuC with the IP multimedia private identity (IMPI) of the MS, and receives a response with an array of AVs. (This step is skipped if the CSCF already has the AV array.) The CSCF then invokes the IMS authentication and key agreement procedure with an authentication vector. The MS authenticates the network through the received **AUTN** and the CSCF authenticates the MS using the **RES/XRES** pair. Detailed message flow of this procedure will be given in Section II-B.

Although both GPRS and IMS authentications are necessary, most steps in these two "authentication passes" are duplicated. In other words, the two-pass authentication proposed in 3GPP 33.203 [6] is not efficient. In this paper, we propose an one-pass authentication procedure that effectively combines both the GPRS and the IMS authentications. We prove that this simplified one-pass authentication procedure correctly authenticate the IMS users.

II. 3GPP Two-Pass Authentication

This section describes the 3GPP two-pass authentication procedure. We first describe GPRS authentication in Section II-A, and then we elaborate more on IMS authentication in Section II-B. In Section II-C, we explain why authentication must be performed in both the GPRS and the IMS levels.

A. GPRS Authentication

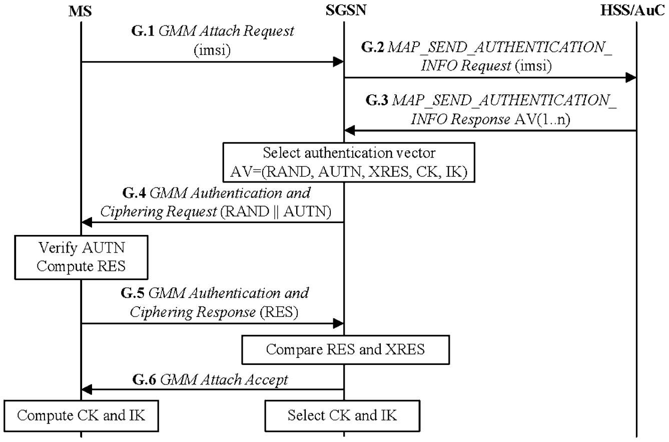

MS
SGSN
HSS/AuC
G.1 GMM Attach Request (imsi)
G.2 MAP_SEND_AUTHENTICATION_INFO Request (imsi)
G.3 MAP_SEND_AUTHENTICATION_INFO Response AV(1..n)
Select authentication vector AV=(RAND, AUTN, XRES, CK, IK)
G.4 GMM Authentication and Ciphering Request (RAND || AUTN)
Verify AUTN Compute RES
G.5 GMM Authentication and Ciphering Response (RES)
Compare RES and XRES
G.6 GMM Attach Accept
Compute CK and IK
Select CK and IK

Fig. 2. Message flow for 3GPP GPRS authentication.

When an MS invokes the GPRS access (e.g., turns on its power), the MS sends an attach request to the SGSN. This message will trigger the GPRS authentication [2], which is implemented by GPRS mobility management (GMM) between the MS and the SGSN, and signaling system number 7 (SS7) mobile application part (MAP) between the SGSN and the HSS/AuC [11]. This procedure consists of the following steps (see Fig. 2).

Step G.1) Consider an MS with the IMSI value *imsi* and the IMPI value *impi*. To access the GPRS services, the MS sends a GMM Attach Request (with the parameter $\mathrm{IMSI} = imsi$) to the SGSN.

Step G.2) If the SGSN has the AVs of the MS, then Steps G.2 and G.3 are skipped. Otherwise, the SGSN must obtain the AV's from the HSS/AuC. That is, the SGSN invokes the authentication vector distribution procedure by sending a MAP_SEND_AUTHENTICATION_INFO Request message to the HSS/AuC (with the parameter $\mathrm{IMSI} = imsi$).

Step G.3) The HSS/AuC uses *imsi* to retrieve the record of the MS, and generates an ordered array of AVs (based on the preshared secret key **K** in the MS record). The generated AV array is sent to the SGSN through a MAP_SEND_AUTHENTICATION_INFO Response message.

Step G.4) The SGSN selects the next unused authentication vector in the ordered AV array and sends the parameters **RAND** and **AUTN** (from the selected authentication vector) to the MS through a GMM Authentication and Ciphering Request message.

Step G.5) The MS checks whether the received **AUTN** can be accepted. If so, it produces a response **RES** that is sent back to the SGSN through a GMM Authentication and Ciphering Response message. The SGSN compares the received **RES** with the **XRES**. If they match, then the authentication and key agreement exchange is successfully completed.

Step G.6) The SGSN sends a GMM Attach Accept message to the MS, and the attach procedure is completed.

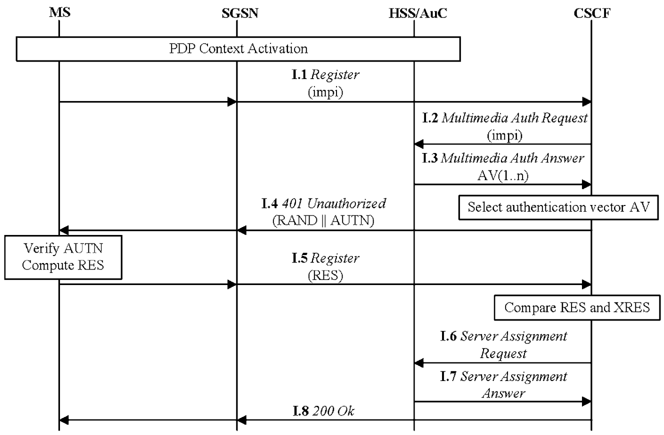

MS
SGSN
HSS/AuC
CSCF
PDP Context Activation
I.1 Register (impi)
I.2 Multimedia Auth Request (impi)
I.3 Multimedia Auth Answer AV(1..n)
Select authentication vector AV
I.4 401 Unauthorized (RAND || AUTN)
Verify AUTN Compute RES
I.5 Register (RES)
Compare RES and XRES
I.6 Server Assignment Request
I.7 Server Assignment Answer
I.8 200 Ok

Fig. 3. Message flow for 3GPP IMS authentication.

After GPRS authentication, GPRS registration follows (details of GPRS registration can be found in [13]). Then, the MS performs packet data protocol (PDP) context activation to obtain access to the GPRS network. The PDP context specifies the application-layer packet data protocol and the routing information used for the GPRS communication session (see [12] for the details).

B. IMS Authentication

After PDP context activation, the MS can request the IMS services through the registration procedure illustrated in Fig. 3. In this procedure, the MS interacts with the S-CSCF possibly through P-CSCF and I-CSCF. To simplify our discussion, Fig. 3 uses the term "CSCF" to represent the proxy, interrogating, and service functions of CSCF. Details of message exchanges among these CSCFs are given in [12]. IMS authentication/registration is implemented by SIP and Cx protocols [3], [4], which consists of the following steps.

Step I.1) The MS sends a SIP Register message to the CSCF (with the parameter $\text{IMPI} = impi$) through the SGSN.

Step I.2) Assume that the CSCF does not have the AVs for the MS. The CSCF invokes the authentication vector distribution procedure by sending a Cx Multimedia Authentication Request message to the HSS/AuC (with the parameter $\text{IMPI} = impi$).

Step I.3) The HSS/AuC uses *impi* to retrieve the record of the MS, and generate an ordered array of AVs. The HSS/AuC sends the AV array to the CSCF through a Cx Multimedia Authentication Answer message.

Step I.4) The CSCF selects the next unused authentication vector from the ordered AV array and sends the parameters **RAND** and **AUTN** (from the selected authentication vector) to the MS through a SIP 401 Unauthorized message.

Step I.5) The MS checks whether the received **AUTN** can be accepted. If so, it produces a response **RES**. The MS sends this response back to the CSCF through a SIP Register message. The CSCF compares the received **RES** with the **XRES**. If they match, then the authentication and key agreement exchange is successfully completed.

TABLE I
IDENTICAL STEPS IN GPRS AND IMS AUTHENTICATIONS

GPRS authentication (SS7 MAP)	IMS authentication (SIP/Cx)
G.2: MAP_SEND_AUTHENTICATION_INFO Request Parameter: IMSI	**I.2:** Multimedia Authentication Request Parameter: IMPI
G.3: MAP_SEND_AUTHENTICATION_INFO Response Parameter: AV[1..n]	**I.3:** Multimedia Authentication Answer Parameter: AV[1..n]
G.4: User Authentication Request Parameter: **RAND**||**AUTN**	**I.4:** 401 Unauthorized Parameter: **RAND**||**AUTN**
G.5: User Authentication Response Parameter: **RES**	**I.5:** Register Parameter: **RES**
G.6: GMM Attach Accept	**I.8:** 200 Ok

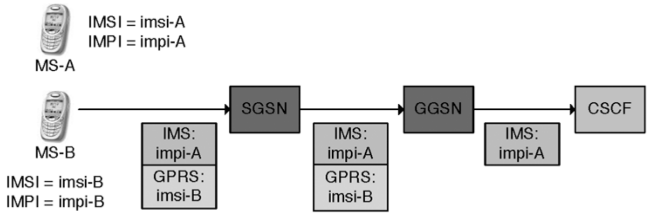


Fig. 4. Illegal IMS registration.

Step I.6) The CSCF sends a Cx Server Assignment Request message to the HSS/AuC.

Step I.7) Upon receipt of the Server Assignment Request, the HSS/AuC stores the CSCF name and replies a Cx Server Assignment Answer message to the CSCF.

Step I.8) The CSCF sends a 200 ok message to the MS through the SGSN, and the IMS registration procedure is completed.

In the above procedure, Steps I.1–I.5 exercise authentication, and Steps I.6–I.8 perform registration.

C. Fraudulent IMS Usage

Although GPRS authentication is implemented by GMM and SS7 MAP, and IMS authentication is implemented by SIP and Cx, many steps of these two authentication procedures are duplicated (see Table I). Unfortunately, these redundant steps are required. That is, after GPRS authentication, it is necessary to authenticate the MSs again at the IMS level. Without IMS authentication, an IMS user may pretend to be another IMS user. Consider the example in Fig. 4, where there are two MSs. MS-A has the IMSI value *imsi-A* and the IMPI value *impi-A*. MS-B has the IMSI value *imsi-B* and the IMPI value *impi-B*. Suppose that MS-B is a legal GPRS user and has passed the GPRS authentication (by using *imsi-B*) to obtain GPRS network access. If no IMS authentication is required, MS-B may perform IMS registration by sending the CSCF a Register request that includes the MS-A's IMPI value *impi-A* as a parameter. The CSCF will consider this IMS registration as a legal action activated by MS-A. Therefore, MS-B can illegally access the IMS services

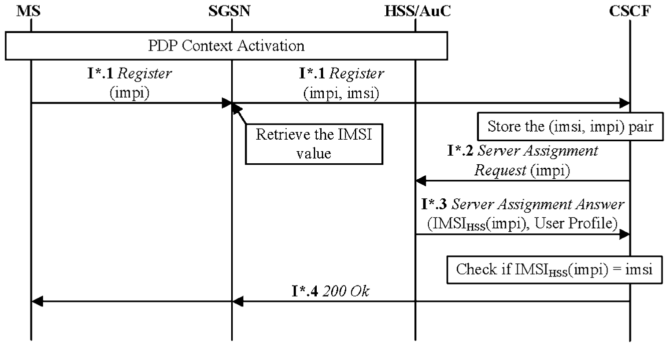

MS
SGSN
HSS/AuC
CSCF
PDP Context Activation
I*.1 Register (impi)
I*.1 Register (impi, imsi)
Retrieve the IMSI value
Store the (imsi, impi) pair
I*.2 Server Assignment Request (impi)
I*.3 Server Assignment Answer (IMSI_HSS(impi), User Profile)
Check if IMSI_HSS(impi) = imsi
I*.4 200 Ok

Fig. 5. IMS registration (one-pass authentication).

of MS-A. The above example shows that IMS-level authentication is required to prevent illegal access to the IMS services. In the next section, we describe an one-pass authentication procedure for both GPRS and IMS authentications. Our approach significantly reduces the number of accesses to the HSS/AuC.

III. One-Pass Authentication Procedure

This section proposes an one-pass authentication (performed at the GPRS level) that can authenticate an IMS user without explicitly performing the IMS-level authentication. In our approach, the SGSN implements a SIP application level gateway (ALG) [8] that modifies the format of SIP messages (to be elaborated). We first describe the SIP message flow of the one-pass procedure. Then, we provide a brief cost comparison between the one-pass and the two-pass procedures.

A. SIP Message Flow

After GPRS authentication (Steps G.1–G.6 in Fig. 2) the MS performs PDP context activation to obtain GPRS access. Then, the MS registers to the IMS through Steps I*.1–I*.4 illustrated in Fig. 5.

Step I*.1) The MS sends a SIP Register message to the SGSN with the parameter $\mathrm{IMPI} = impi$. Note that after PDP context activation, the SGSN can identify the IMSI of the MS that transmits the GPRS packets [2]. The SIP ALG in the SGSN adds the IMSI value (i.e., *imsi*) of the MS in the Register message and forward it to the CSCF. Details of a possible SIP ALG implementation can be found in [8].

Step I*.2) The CSCF stores the (*imsi*, *impi*) pair in the MS record, and sends a Cx Server Assignment Request message to the HSS/AuC with the parameter $\mathrm{IMPI} = impi$. We note that if the CSCF has stored the (*imsi*, *impi*) pair before, then **Steps I*.2** and **I*.3** are skipped.

Step I*.3) The HSS/AuC uses the received IMPI value *impi* as an index to retrieve the IMSI and the user profile of the MS. We denote $\mathrm{IMSI}_{\mathrm{HSS}}(impi)$ as the IMSI value retrieved from the HSS/AuC. The HSS/AuC stores the CSCF name and sends a Cx Server Assignment Answer to the CSCF (with the parameters $\mathrm{IMSI}_{\mathrm{HSS}}(impi)$ and user profile).

TABLE II
Comparing the One-Pass and the Two-Pass Authentication Procedures in IMS Registration

One-Pass Procedure	Two-Pass Procedure
I*.1: Register Parameters: $impi$ and $imsi$	**I.1:** Register Parameter: $impi$
-	**I.2:** Multimedia Authentication Request Parameter: $impi$
-	**I.3:** Multimedia Authentication Answer Parameter: AV[1..n]
-	**I.4:** 401 Unauthorized Parameter: **RAND**||**AUTN**
-	**I.5:** Register Parameter: **RES**
I*.2: Server Assignment Request	**I.6:** Server Assignment Request
I*.3: Server Assignment Response	**I.7:** Server Assignment Response
I*.4: 200 Ok	**I.8:** 200 Ok

Step I*.4) The CSCF checks whether the value *imsi* and $\mathrm{IMSI}_{\mathrm{HSS}}(impi)$ are the same. If so, the CSCF sends a SIP 200 Ok message to the SGSN and the authentication is considered successful. If $\mathrm{IMSI}_{\mathrm{HSS}}(impi) \neq imsi$, then it implies that the registration is illegal (i.e., the scenario illustrated in Fig. 4 occurs). Suppose that $\mathrm{IMSI}_{\mathrm{HSS}}(impi) = imsi$. The SGSN forward the 200 Ok message to the MS, and the IMS registration procedure is successfully completed.

B. Cost Analysis

Table II compares the steps executed in the one-pass and the two-pass authentication procedures. Suppose that the expected SIP message delivery cost between an MS and the CSCF is one unit, and the expected Cx message delivery cost between the CSCF and the HSS/AuC is α units. It is anticipated that $\alpha < 1$ for the following two reasons.

- The CSCF and the HSS/AuC exchange the Cx messages through IP network. On the other hand, besides the IP network overhead, SIP communications between the MS and the CSCF involves GPRS core network and UTRAN radio network.
- The CSCF and the AuC/HSS are typically located at the same location, while the MS is likely to reside at a remote location.

It is clear that the expected IMS registration C_1 for the one-pass procedure (see Fig. 5) is

$$C_1 = 2 + 2\alpha. \tag{1}$$

Note that Step I*.1 needs to trigger SIP ALG for SIP message analysis. Since this action is executed in micro kernel of the SGSN, the overhead can be ignored as compared with SIP message exchange. Similarly, the extra cost of $\mathrm{IMSI}_{\mathrm{HSS}}(impi)$ and $imsi$ comparison at Step I*.4 can be ignored. Our analysis assumes that the (*imsi*, *impi*) pair does not exist at Step I*.1. Therefore Steps I*.2 and I*.3 are always executed. This assumption favors the two-pass procedure.

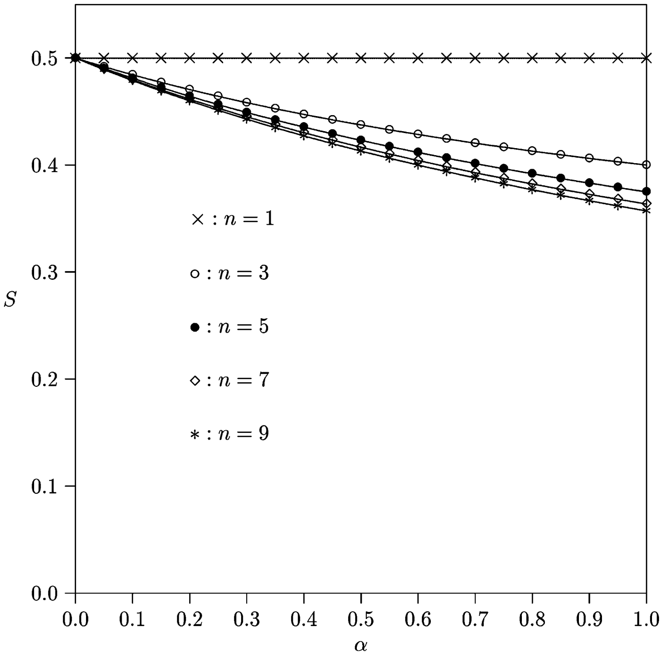


Fig. 6. Improvement S of the one-pass procedure over the two-pass procedure.

In the two-pass procedure, if the distribution of authentication vectors from the HSS/AuC to the SGSN (Steps I.1–I.4 in Fig. 3) is performed, then the expected IMS registration cost $C_{2,1}$ is expressed as

$$C_{2,1} = 4 + 4\alpha. \quad (2)$$

If the authentication vector distribution is not executed in the two-pass procedure, then the expected IMS registration cost $C_{2,2}$ is expressed as

$$C_{2,2} = 4 + 2\alpha. \quad (3)$$

Like periodic location update in UMTS [14], IMS registration is periodically performed. In Steps I.2 and I.3 of the two-pass procedure, an AV array of size n (where $n \geq 1$) is sent from the HSS/AuC to the CSCF. Therefore, one out of the n IMS registrations incurs execution of Steps I.2 and I.3. Therefore, from (2) and (3), the expected IMS registration cost C_2 for the two-pass procedure is

$$C_2 = \left(\frac{1}{n}\right) C_{2,1} + \left(\frac{n-1}{n}\right) \quad C_{2,2} = 4 + \left(\frac{n+1}{n}\right) 2\alpha. \quad (4)$$

From (1) and (4), the improvement S of the one-pass procedure over the two-pass procedure is

$$S = \frac{C_2 - C_1}{C_2} = \frac{n + \alpha}{2n + (n+1)\alpha}. \quad (5)$$

Fig. 6 plots S as a function of n and α. The figure indicates that the one-pass procedure can save up to 50% of the SIP/Cx traffic for IMS registration/authentication, as compared with the two-pass procedure. Another significant advantage of the one-pass procedure is that it consumes much less AVs (about 50% less) than the two-pass procedure.

One may argue that implementation of a SIP ALG is required in the one-pass procedure. Since IMS is based on SIP, a SIP ALG is required for other purposes (see an example in [9]). Therefore, the one-pass procedure will not incur extra cost for implementing SIP ALG.

IV. Correctness of the One-Pass Procedure

In this section, we prove that the one-pass authentication procedure correctly authenticates the IMS users. In UMTS, every MS maintains the attributes IMSI, IMPI, and the preshared secret key $\mathbf{K}$ in its SIM card. Consider an MS with $\text{IMSI} = \mathit{imsi}, \text{IMPI} = \mathit{impi}$, and $\mathbf{K} = k$. To simplify our discussion, we assume that these parameters are grouped into a set $R_{\text{MS}} = \{\mathit{imsi}, \mathit{impi}, k\}$ in the SIM card of the MS. Define functions $\text{IMSI}_{\text{MS}}, \text{IMPI}_{\text{MS}}$, and K_{MS} such that for any $x \in R_{\text{MS}}$

$$\text{IMSI}_{\text{MS}}(x) = \mathit{imsi}, \text{where } \mathit{imsi} \text{ is the IMSI value in } R_{\text{MS}} \quad (6)$$

$$\text{IMPI}_{\text{MS}}(x) = \mathit{impi}, \text{where } \mathit{impi} \text{ is the IMPI value in } R_{\text{MS}} \quad (7)$$

$$K_{\text{MS}}(x) = k, \text{where } k \text{ is the } \mathbf{K} \text{ value in } R_{\text{MS}}. \quad (8)$$

Based on the above definitions, it is clear that, for example

$$\text{IMSI}_{\text{MS}}(\mathit{impi}) = \text{IMSI}_{\text{MS}}(k) = \mathit{imsi}.$$

Similarly, for every MS, the HSS/AuC maintains a record R_{HSS} that consists of attributes IMSI, IMPI, and $\mathbf{K}$. That is, for an MS who has legal GPRS and IMS accesses

$$R_{\text{HSS}} = \{\mathit{imsi}, \mathit{impi}, k\} = R_{\text{MS}}.$$

Like (6)–(8), we define functions $\text{IMSI}_{\text{HSS}}, \text{IMPI}_{\text{HSS}}, K_{\text{HSS}}$ such that for $x \in R_{\text{HSS}}$,

$$\text{IMSI}_{\text{HSS}}(x) = \mathit{imsi}, \text{where } \mathit{imsi} \text{ is the IMSI value in } R_{\text{HSS}} \quad (9)$$

$$\text{IMPI}_{\text{HSS}}(x) = \mathit{impi}, \text{where } \mathit{impi} \text{ is the IMPI value in } R_{\text{HSS}} \quad (10)$$

$$K_{\text{HSS}}(x) = k, \text{where } k \text{ is the } \mathbf{K} \text{ value in } R_{\text{HSS}}. \quad (11)$$

In 3G 23.060 [2] and 3G 33.203 [6], MS authentication at the GPRS and the IMS levels are based on the following Theorem.

Theorem 1: Suppose that an MS claims that it has the IMSI value *imsi* and the IMPI value *impi*. Then, the following.

a) The MS is a legal GPRS user if $K_{\text{MS}}(\mathit{imsi}) = K_{\text{HSS}}(\mathit{imsi})$.

b) The MS is a legal IMS user if $K_{\text{MS}}(\mathit{impi}) = K_{\text{HSS}}(\mathit{impi})$.

Note that Theorem 1 does not hold if an illegal user already possesses the SIM information of a legal user (e.g., by duplicating the SIM card through the SIM card reader [9]). This issue was addressed in [15]. In this paper, we assume that such fraudulent usage does not occur. 3GPP GPRS authentication procedure (i.e., Steps G.1–G.6) checks if both a GPRS user and the HSS/AuC have the same preshared secret key $\mathbf{K}$ using Theorem 1 and Fact 1a below. Similarly, 3GPP IMS authentication procedure (i.e., Steps I.1–I.8) checks if both an IMS user and the HSS/AuC have the same preshared secret key using Theorem 1 and Fact 1b.

Fact 1:

a) For an MS claiming $\mathrm{IMSI} = imsi$, if $\mathbf{XRES} = \mathbf{RES}$, then $K_{\mathrm{MS}}(imsi) = K_{\mathrm{HSS}}(imsi)$.

b) For an MS claiming $\mathrm{IMPI} = impi$, if $\mathbf{RES} = \mathbf{XRES}$, then $K_{\mathrm{MS}}(impi) = K_{\mathrm{HSS}}(impi)$.

Now, we prove that the one-pass authentication correctly authenticates the IMS users (i.e., the one-pass procedure checks if $K_{\mathrm{MS}}(impi) = K_{\mathrm{HSS}}(impi)$). From the definitions of the $\mathrm{IMSI}_{\mathrm{HSS}}$ and K_{HSS} functions [i.e., (9) and (11)], it is trivial to have the following fact.

Fact 2: For any IMPI value *impi*, if $\mathrm{IMSI}_{\mathrm{HSS}}(impi) = imsi$, then $K_{\mathrm{HSS}}(impi) = K_{\mathrm{HSS}}(imsi)$.

With Fact 2, correctness of the one-pass authentication procedure is guaranteed according to the following two theorems.

Theorem 2: Suppose that

a) an MS with the IMSI value *imsi* has passed the GPRS authentication; that is

$$K_{\mathrm{MS}}(imsi) = K_{\mathrm{HSS}}(imsi). \tag{12}$$

b) The MS claims that its IMPI value is *impi*.

c) The network maps *impi* to the IMSI value *imsi*; that is

$$\mathrm{IMSI}_{\mathrm{HSS}}(impi) = imsi. \tag{13}$$

Then, the MS is a legal IMS user. In other words

$$K_{\mathrm{MS}}(impi) = K_{\mathrm{HSS}}(impi). \tag{14}$$

Proof: From hypothesis a, $imsi \in R_{\mathrm{MS}}$. In hypothesis b, the MS claims that it has the IMPI value *impi*, which implies that $impi \in R_{\mathrm{MS}}$. From (8)

$$K_{\mathrm{MS}}(imsi) = K_{\mathrm{MS}}(impi). \tag{15}$$

From Fact 2 and (13) in hypothesis c, we have

$$K_{\mathrm{HSS}}(impi) = K_{\mathrm{HSS}}(imsi). \tag{16}$$

From (12) in hypothesis a and (16), we have

$$K_{\mathrm{MS}}(imsi) = K_{\mathrm{HSS}}(impi). \tag{17}$$

From (15) and (17), we have

$$K_{\mathrm{MS}}(impi) = K_{\mathrm{HSS}}(impi).$$

In other words, if hypotheses a–c hold, an MS is a legal IMS user with $\mathrm{IMPI} = impi$. Q.E.D.

Theorem 3: The one-pass authentication procedure correctly authenticates the IMS users; that is, for an MS claiming the IMPI value *impi*, the one-pass procedure recognizes the MS as a legal IMS user if $K_{\mathrm{MS}}(impi) = K_{\mathrm{HSS}}(impi)$.

Proof: After Steps G.1–G.6 have been executed, the network verifies that $K_{\mathrm{MS}}(imsi) = K_{\mathrm{HSS}}(imsi)$; i.e., (12) in Theorem 2 is satisfied.

At Step I*.1, the MS claims that its IMPI value is *impi* and, therefore, the network assumes that $K_{\mathrm{MS}}(imsi) = K_{\mathrm{MS}}(impi)$; i.e., (15) in Theorem 2 is satisfied.

At Step I*.4, the one-pass authentication checks if $\mathrm{IMSI}_{\mathrm{HSS}}(impi) = imsi$ [i.e., (13) in Theorem 2 is checked]. If so, $K_{\mathrm{MS}}(impi) = K_{\mathrm{HSS}}(impi)$ as a direct consequence of Theorem 2, and the authentication procedure recognizes the MS as a legal user (according to Theorem 1). Otherwise, the authentication fails.

In other words, the one-pass procedure follows Theorem 1 to authenticate an MS. Q.E.D.

V. Conclusion

This paper proposed an efficient IMS registration procedure without explicitly performing tedious authentication steps. As specified by the 3GPP, after a UMTS mobile user has obtained GPRS network access through GPRS authentication, the "same" authentication procedure must be executed again at the IMS level (during IMS registration) before it can receive the IP multimedia services. This paper described an one-pass authentication procedure, which only needs to perform GPRS authentication. At the IMS registration, the one-pass procedure performs several simple operations to verify if a user is legal. We prove that the one-pass procedure correctly authenticates the IMS users. Compared with the eight-step two-pass authentication, the four-step one-pass authentication saves two to four SIP/Cx message exchanges among the MS, the SGSN, the CSCF, and the HSS/AuC. Our study indicates that this new approach can save up to 50% of the network traffic generated by the IMS registration. This approach also saves 50% of the storage for buffering the authentication vectors. The one-pass authentication procedure is pending ROC and US patents.

References

[1] 3GPP, 3rd generation partnership project; technical specification group services and systems aspects; 3G security; security architecture, Tech. Spec. 3G TS 33.102 V3.7.0 (2000–12), 2000.

[2] 3GPP, 3rd generation partnership project; Technical specification group services and systems aspects; General packet radio service (GPRS); Service description; Stage 2, Tech. Spec. 3G TS 23.060 version 4.1.0 (2001–06), 2001.

[3] 3GPP, 3rd generation partnership project; Technical specification core network; Cx and Dx interfaces based on the diameter protocol; Protocol details, Tech. Spec. 3G TS 29.229 V5.3.0 (2003–03), 2003.

[4] 3GPP, 3rd generation partnership project; Technical specification core network; IP multimedia subsystem Cx and Dx interfaces; Signaling flows and message contents (Release 5), Tech. Spec. 3G TS 29.228 V5.4.0 (2003–06), 2003.

[5] 3GPP, 3rd generation partnership project; Technical specification group core network; Signaling flows for the IP multimedia call control based on SIP and SDP; Stage 3, version 5.5.0 (2003–06). 3GPP TS 24.228, 2003.

[6] 3GPP, 3rd generation partnership project; Technical specification group services and systems aspects; 3G security; Access security for IP-based services, Tech. Spec. 3G TS 33.203 V5.5.0 (2003–03), 2003.

[7] 3GPP, 3rd generation partnership project; Technical specification group services and systems aspects; IP Multimedia subsystem stage 2, Tech. Spec. 3G TS 23.228 version 6.2.0 (2003–06), 2003.

[8] W. E. Chen, Q. Wu, A.-C. Pang, and Y.-B. Lin, "Design of SIP application level gateway for UMTS," in *Design and Analysis of Wireless Networks*, Y. Pan and Y. Xiao, Eds. Commack, NY: Nova, 2004.

[9] V. W.-S. Feng, L.-Y. Wu, Y.-B. Lin, and W. E. Chen, "WGSN: WLAN-based GPRS environment support node with push mechanism," *Comput. J.*, vol. 47, no. 4, pp. 405–417, 2004.

[10] Y.-B. Lin and Y.-K. Chen, "Reducing authentication signaling traffic in third generation mobile network," *IEEE Trans. Wireless Commun.*, vol. 2, no. 3, pp. 493–501, 2003.

[11] Y.-B. Lin and I. Chlamtac, *Wireless and Mobile Network Architectures*. New York: Wiley, 2001.

[12] Y.-B. Lin, Y.-R. Hanug, A.-C. Pang, and I. Chlamtac, "All-IP approach for UMTS third generation mobile networks," *IEEE Netw.*, vol. 16, no. 5, pp. 8–19, 2002.

[13] Y.-B. Lin, Y.-R. Huang, Y.-K. Chen, and I. Chlamtac, "Mobility management: From GPRS to UMTS," *Wireless Commun. Mobile Comput.*, vol. 1, no. 4, pp. 339–360, 2001.

[14] Y.-B. Lin, P.-J. Lee, and I. Chlamtac, "Dynamic periodic location area update in mobile networks," *IEEE Trans. Veh. Technol.*, vol. 51, no. 6, pp. 1494–1501, 2002.

[15] Y.-B. Lin, M.-F. Chen, and H. C.-H. Rao, "Potential fraudulent usage in mobile telecommunications networks," *IEEE Trans. Mobile Comput.*, vol. 1, no. 2, 2002.

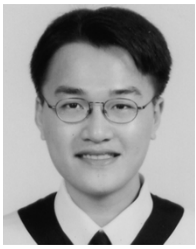
[16] J. Rosenberg *et al.*, "SIP: Session initiation protocol," IETF, RFC 3261, 2002.

Yi-Bing Lin (M'96–SM'96–F'04) is Chair Professor of Computer Science and Information Engineering, National Chiao-Tung University (NCTU), Hsinchu, Taiwan. He also serves as Vice President of the Office of Research and Development, NCTU. He is an Adjunct Research Fellow of Academia Sinica and is an Adjunct Chair Professor of Providence University. He is coauthor of *Wireless and Mobile Network Architecture* (New York: Wiley, 2001), with I. Chlamtac. He has published over 190 journal articles and more than 200 conference papers. His current research interests include wireless communications and mobile computing.

Dr. Lin is a Fellow of ACM, a Fellow of AAAS, and a Fellow of IEE. He received the 1998, 2000, and 2002 Outstanding Research Awards from the National Science Council, R.O.C., the 1998 Outstanding Youth Electrical Engineer Award from CIEE, R.O.C., and the NCTU Outstanding Teaching Award in 2002. He is a Senior Technical Editor of the *IEEE Network*, an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, an Associate Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, an Editor of the *IEEE Wireless Communications Magazine* and *ACM/Baltzer Wireless Networks*. He is Guest Editor of the *ACM/Baltzer MONET* (Special Issue on Personal Communications), the IEEE TRANSACTIONS ON COMPUTERS (Special Issue on Mobile Computing), the IEEE TRANSACTIONS ON COMPUTERS (Special Issue on Wireless Internet), and the *IEEE Communications Magazine* (Special Issue on Active, Programmable, and Mobile Code Networking). He is Program Chair for the 8th Workshop on Distributed and Parallel Simulation, General Chair for the 9th Workshop on Distributed and Parallel Simulation, and Program Chair for the 2nd International Mobile Computing Conference.

Ming-Feng Chang received the Ph.D. degree in computer science from the University of Illinois at Urbana–Champaign, Urbana, in 1991.

He is currently a Professor and the Chairman of the Department of Computer Science and Information Engineering, National Chiao-Tung University, Hsinchu, Taiwan. His current research interests include design and analysis of Internet communications, personal communications network, mobile payment, and performance modeling.



Meng-Ta Hsu received the B.S. degree in computer science and information engineering from National Taiwan University, Taipei, Taiwan, in 2000. He is currently working towards the Ph.D. degree in computer science and information engineering from the National Chiao-Tung University, Hsinchu, Taiwan.

His current research interests include Internet communications, intelligent transportation systems, mobile computing, and performance modeling.

Lin-Yi Wu received the B.S. and M.S. degrees from National Chiao-Tung University, Hsinchu, Taiwan, in 1999 and 2001 respectively. She is currently working towards the Ph.D. degree in computer science and information engineering, National Chiao-Tung University.

Her current research interests include heterogeneous network integration, personal communications services, and mobile computing.