Wireless Networks 5 (1999) 231–243

Enhanced privacy and authentication for the global system for mobile communications *

Chii-Hwa Lee [a], Min-Shiang Hwang [b] and Wei-Pang Yang [a]

[a] *Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 30050, ROC*
[b] *Department of Information Management, Chao Yang University of Technology, WuFeng, Taichung, Taiwan, ROC*

The Global System for Mobile Communications (GSM) is widely recognized as the modern digital mobile network architecture. Increasing market demands point toward the relevancy of security-related issues in communications. The security requirements of mobile communications for the mobile users include: (1) the authentication of the mobile user and Visitor Location Register/Home Location Register; (2) the data confidentiality between mobile station and Visitor Location Register, and the data confidentiality between Visitor Location Register and Visitor Location Register/Home Location Register (VLR/HLR); (3) the location privacy of mobile user. However, GSM does not provide enough security functions to meet these requirements. We propose three improved methods to enhance the security, to reduce the storage space, to eliminate the sensitive information stored in VLR, and consequently to improve the performance of the system. Proposed methods include an improved authentication protocol for the mobile station, a data confidentiality protocol, and a location privacy protocol. The merit of the proposed methods is to improve but not to alter the existing architecture of the system. Furthermore, this study also performs computational and capacity analyses to evaluate the original GSM system and proposed approaches on a comparative basis.

1. Introduction

The Global System for Mobile Communications (GSM) is a common standard issued by European Telecommunication Standards Institute (ETSI), and is the first digital mobile network architecture put into practice [21,25]. GSM is undoubtedly a major achievement in modern cellular telephony. The tremendous market growth of GSM systems indicates the growing importance of mobile communications and an eminent need of security in mobile telephones during international communications. The confidentiality of radio transmission, i.e., the privacy, and the authentication of the user are two major issues in the protocols of the wireless communications [5,28]. In some novel applications in modern wireless communications, these two issues are still the major concerns [17,19]. The radio transmission is by nature more susceptible to be eavesdropped and to fraud in use than the wire transmission [14]. The user mobility and universal network access certainly provoke these security threats. Analog systems have indeed suffered from such problems during the 80's [27].

The GSM has been improving in these regards ever since. The protection mechanisms for mobile communications have been examined by many researches [5,12,13]. Most of them offer the authentication mechanisms of portables and the data confidentiality for radio transmission, but not for the wire communications. The comprehensive security requirements for mobile communications, both wireless and wireline, shall include at least the following features [6,16,22]:

- Authentication of Mobile Station (MS) or mobile user.
- Authentication of the location databases, such as Visitor's Location Register/Home Location Register (VLR/HLR).
- Data confidentiality between Mobile Station and Visitor's Location Register or between Visitor's Location Register and the fixed station or the fixed destination.
- Data confidentiality between Visitor's Location Register and Visitor's Location Register/Home Visitor's Location Register.
- Location confidentiality of Mobile Station or mobile user.

The security functions of GSM aim at two goals. One is to protect the network against unauthorized access, and the other one is to protect the privacy of the user [23]. Thus, the security features provided by GSM consist of three aspects as follows [10,11]:

- subscriber identity authentication,
- subscriber identity confidentiality, and
- user data and signaling information confidentiality on radio path.

A user must prove one's identity to access the network. Authentication is to protect against fraudulent uses and to ensure correct billings. The subscriber identity confidentiality deals with the location privacy of mobile users. The confidentiality of user data and signaling information is dependent upon many aspects of the system. Among them the user's subscription data and service profile, user's information sent over open radio links, as well as the security parameters distributed in the network, are considered crucially associated with the confidentiality purpose [29].

* Part of this paper was presented in The 6th National Conference on Information Security, Taiwan, ROC, May 1996.

Since the user mobility and the universal network access are facilitated by present networks, the illegal access and eavesdropping increasingly become imminent threats to the communication security [2].

The authentication protocol (subscriber identity authentication) of the current GSM is defined in GSM recommendation 02.09 [11], and the authentication procedure is always initiated and controlled by the network. A few drawbacks of the current protocol are found, such as the space overhead to store authentication parameters in VLR and the justification of mobile stations via HLR and the bandwidth consumption for transmitting the parameter [15]. Above all, the authentication of VLR/HLR is not designed and implemented in GSM [26]. Moreover, the security designs of GSM are not aimed at the wireline connection, but merely at the radio link. The privacy protection has been introduced only for the radio path. As such, the encryption/decryption mechanisms in GSM provide the confidentiality of user data and signaling information on the radio path, and on the contrary, it lacks the capabilities of supporting the privacy between VLR and VLR/HLR or the privacy between the VLR and other fixed network [24]. The confidentiality of mobile user location implemented by using a Temporary Mobile Subscriber Identity (TMSI) in GSM provides the location privacy of MS. The protocol supports the location privacy of MS on the radio path only. The design of GSM does not provide the privacy protection through the networks.

According to the potential drawbacks mentioned above, we found that the security functions of the current GSM system are not sufficient for the mobile communications. Therefore, this study examines the GSM security protocol design and investigates how well GSM can achieve its security goals. Several inefficient settings and concerned problems embedded in GSM are discussed and remarked. We also propose improved protocols of authentication and privacy for the current GSM system without changing its existing architecture. The improvements are based on the security requirements of mobile communications that reduce the storage space in VLR, eliminate the storage of sensitive information in VLR, and gain better performance in message transmission.

The contents of this paper are divided into four parts. To begin with, we investigate the basic architecture, the authentication and privacy protocols of GSM, where inefficient security mechanisms are discussed. Secondly, we present three improved protocols for the GSM system. The protocols include an improved authentication protocol, a data privacy protocol, and a location privacy protocol. Thirdly, the merits of proposed protocols are presented and a few applications supported by the protocols are illustrated. Finally, we make comparisons, on the basis of computational and capacity analyses, among the original GSM system, Harn and Lin's approach [15] and the proposed approaches.

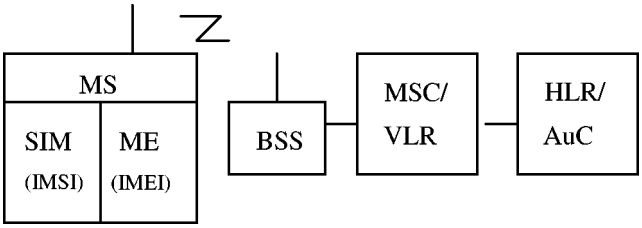

Figure 1. The GSM architecture.

2. The GSM protocols and their weakness

In the GSM architecture, as shown in figure 1 [21,23], the Mobile Stations (MS) communicate through radio link with Base Station Subsystems (BSS) which are connected to Mobile Switching Centers (MSC). The MSC can be regarded as an interface between the radio link and the fixed, or transit, part of the GSM Public Land Mobile Network (PLMN). Associated with each MSC is a VLR. The Authentication Center (AuC) stores subscribers' secret keys and generates security parameters for the authentication protocol on the request of HLRs. AuC would normally be attached to a HLR but located in a secure environment.

The Mobile Station (MS) usually represents the only equipment the user ever sees from the whole system. MS generally includes the Mobile Equipment (ME) and the SIM. Each ME has a valid International Mobile Equipment Identity (IMEI) which references the mobile equipment approval and the final assembly plant. An SIM is a smart card with an integral microprocessor attached to ME, and it contains the Subscriber's Identity Module. The SIM card stores the subscriber's information of International Mobile Subscriber Identity (IMSI), Personal Identity Number (PIN), secret key, *Ki*, and the parameters of security functions as well. Initially, the subscriber is registered in the HLR with a unique identity, IMSI, and obtains one secret key, *Ki*, from the AuC during the registration process. Two location databases play important roles in subscribers' registration and authentication [20]. Home Location Register (HLR) is a database used for mobile information management. All permanent subscriber data are stored in this database. An HLR record consists of three types of information: (a) mobile station information such as IMSI and the mobile station ISDN number (MSISDN) of a mobile station, (b) location information such as the ISDN number (address) of a VLR, and (c) service information such as service subscription, service restriction, and supplementary services. The Visitor Location Register (VLR) is the database of the service area visited by an MS. The VLR contains all subscriber data of an MS required for call handling and other purpose. Similar to the HLR, the VLR information consists of three parts: mobile station information, location information, and service information.

2.1. GSM authentication protocol

Current mobile security implementations in GSM are based on the secrecy of encryption algorithms. The au-

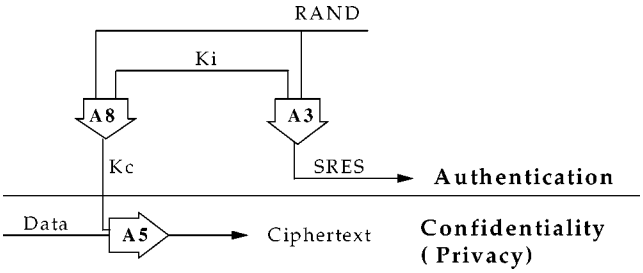

Figure 2. Cryptographic functions in GSM.

thentication and privacy are implemented by one-key cryptographic techniques, as shown in figure 2. A8, A3, and A5 are three special functions in GSM protocols. A8 has a public-known one-way function to generate the secret session key, *Kc*. A3 possesses a one-way function, which is used by the subscriber and AuC to compute Signed Result (*SRES*). As for A5, it is a one-way encryption/decryption algorithm using *Kc* by MS and Base Station.

By using *Ki* and *RAND* as inputs, *SRES* and *Kc* are generated through algorithms A3 and A8, respectively, where

$$SRES = \text{A3}(Ki, RAND), \qquad Kc = \text{A8}(Ki, RAND).$$

The *RAND* shall be a non-predictable outcome of a random number generator. Together with the algorithm A5, the *Kc* is used to encrypt/decrypt speech, data, and signaling information on the radio interface, where

$$Ciphertext = \text{A5}(Kc, Message),$$
$$Message = \text{A5}(Kc, Ciphertext).$$

The current GSM authentication of MS is described in the top portion of figure 3. Each subscriber gets a unique IMSI and one secret key, *Ki*, from AuC during registration. In the authentication process, the AuC/HLR is applied to generate several triplets, $(RAND, SRES, Kc)$, say n copies, for a given IMSI at a time, and passes them back to the visited VLR for storage and subsequent uses. To verify the identity of a subscriber, VLR selects a $(RAND, SRES)$ pair and sends the *RAND* to MS. MS uses this *RAND* and its *Ki* to compute a *SRES*, then sends the result back to the VLR. VLR checks the result with the stored *SRES*. Once a correct match occurs, the subscriber is recognized as an authorized user; otherwise, the VLR will reject the subscriber's access to the system. In this protocol, it is not required for the VLR to recognize the *Ki*, or even the A3 algorithm, to authenticate an MS. By the same token, an AuC must compute n copies of $(RANDi, SRESi, Kci)$ in advance for each subscriber in the HLR, and send them to VLR where the MS is visiting.

There are few existing drawbacks of the current system. First, the space overhead occurs when a set of authentication parameters in the VLR is being stored. Second, the identification of a mobile user is done in VLR and must be aided by the HLR of the mobile user. Third, there is a bandwidth consumption between VLR and HLR, when VLR needs another set of authentication parameters. Fourth, the authentication of VLR/HLR is not instituted in the GSM

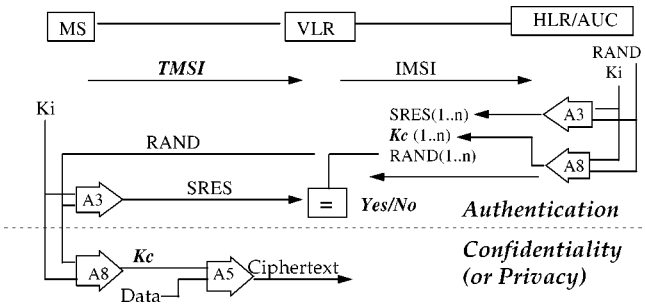

Figure 3. Subscriber identity authentication and user data confidentiality in GSM.

protocol. In fact, a fake VLR/HLR can give incorrect information to the user and cause a leak of confidential data in MSs. Once the sensitive information stored in VLR is intercepted by an unauthorized user, the communication is then eavesdropped.

2.2. GSM data confidentiality protocol

The current GSM carriers base the security on the corresponding ETSI recommendations, which protect information only within the radio domain of that carrier [10]. The protocol in GSM is depicted in the bottom portion of figure 3. The subscriber and BSS communicate with each other in the ciphered mode by using the A5 algorithm with a secret session key, *Kc*, to encrypt the user data. Like the authentication of MS, confidentiality of user data relies upon the security of the internetwork that is traversed by the BSSs communications. According to the existing structure of the GSM, the possible secure communications have two types of architectures. Type 1 is that one of calling and called ends is a mobile station, and the other end is a fixed network station, e.g., mobile station to fixed station. Type 2 is that both calling and called ends are mobile stations, e.g., mobile station to mobile station.

The methods of sensitive data transmissions in the current GSM are shown in figure 4. In the architecture of Type 1, a calling end (MS1) make a secure communication with the called fixed end (FS2), MS1 has to encrypt its segmented message blocks by using A5 algorithm with *Kc*1 before the data is passed over the radio link. The BSS1 nearby the calling end decrypts the received ciphertext. Then it transmits the plaintext of data through the network to the fixed network Switching Center (SC) close to the called end (FS2), then SC transits the message without any protection to FS2. In the reverse direction, the same pattern can be seen while FS2 calls MS1.

In the architecture of Type 2, a calling end (MS1) makes a secure communication with the called end (MS2), MS1 has to encrypt its segmented message blocks by using A5 algorithm with *Kc*1 before the data is passed over the radio link. The BSS1 nearby the calling end decrypts the received ciphertext. Then it transmits the plaintext of data through the network to the remote BSS2 close to the called end (MS2). The receiving BSS2 subsequently encrypts the data

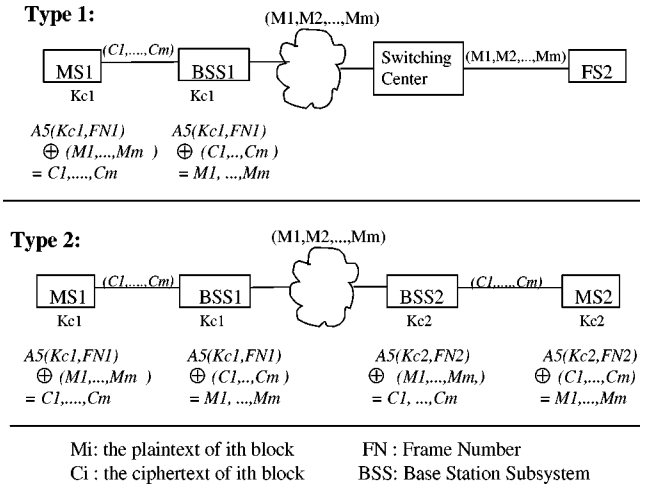

Figure 4. Sensitive data transmission in GSM.

again and sends it to MS2 over the radio link. MS2 then deciphers the encrypted message again.

In the data communication security framework, complete security relies on an implementation of a standard method over the complete path, including wireless and wireline paths. Therefore, an end-to-end security design is still a desired aim of the modern telephony. Notice that for part of the communication path, data information (voice and signaling information) in most cases will not be protected in any existing scenario [24]. Thus, the main drawback of the GSM protocol is that no protection is provided for the transmissions between BSS1 and BSS2/FS2 because the wireless communications are assumed secure in the current system. It also implies that all VLRs/HLRs and SCs are trustworthy under the current system. To assume the VLRs, HLRs and SCs that are either totally reliable or totally unreliable is not justifiable. Each subscriber belongs to only one of the administrative network domains. In a practical sense, the HLR and SC are assumed trustworthy with a reasonable ground because all its subscribers are controlled and managed by them. On the contrary, the VLR, which is either in an adjacent or in a foreign domain, is not of as strong a foundation to be trustworthy as the HLR or SC. Thus, the transmission between VLR and VLR/HLR needs to be protected. Even though the home SC is assumed trustworthy for the fixed station, the transmission on the wireline connection between VLR and the fixed network still needs to be protected from eavesdropping. In addition, the repeated encryption and decryption between VLR and VLR/HLR of Type 2 transmission in the original protocol are very time-consuming processes, and that adds another defect to the system.

2.3. GSM location privacy protocol

The MS roams from one place to another and has access to the network in any place at any time. The location of a particular mobile user is such a valuable information that it needs protection [3]. In the meantime, indiscriminate use

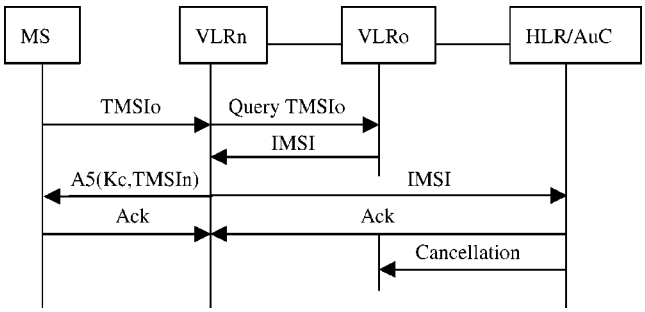

Figure 5. Confidentiality of subscriber identity in GSM.

of location information may result in an invasion of privacy and may be abused by third parties. The Temporary Mobile Subscriber Identity (TMSI) is used to protect user identity from exposing the message of IMSI on the radio path. Whenever a location is updated or registered at a new VLR (denoted as VLRn), the new VLR will provide TMSI in each call set-up. The protocol of updating MS's location with confidentiality is shown in figure 5. When an MS arrives at a new VLR, it sends the old TMSI (TMSIo) to the new VLR to update its location and to register at the new VLR. The new VLR inquires the old VLR (VLRo) about its MS's IMSI and all pertinent security information by passing the old TMSI to the old VLR. After the new VLR authenticates the MS, it transmits the new TMSI (TMSIn) to the MS, and reports the IMSI of the MS to the corresponding HLR. The HLR then stores the current location information of this MS in its database. Finally, the HLR clears all information relevant to the MS in the old VLR.

The design of the location privacy protocol in GSM relies upon the security of wireline connection that is traversed by VLR and HLR communications. The original GSM protocol has three problems. Firstly, when updating the location of an MS, the IMSI will be exposed and delivered throughout the network without any protection. Despite that, secondly, whenever a database failure occurs to the VLR, all the TMSIs stored in the recoverable records may be in a disorder. A problem arises in such a circumstance. When an incoming call arrives, the MSC/VLR pages the Mobile Station throughout its area by using the IMSI instead of TMSI [23]. Thirdly, another problem is that when a user roams to another VLR, the location may be updated by sending its IMSI to the new VLR while the old VLR is not accessible at that moment. It is possible that an unauthorized third party may eavesdrop on the IMSI and identify this mobile user.

3. Enhanced protocols

In this section, we propose three feasible protocols to improve the original GSM system. They are an improved authentication protocol, a data confidentiality protocol, and a location privacy protocol. Moreover, we apply the data confidentiality protocol to mobile teleconferences.

3.1. Improved authentication protocol

We have examined the weakness of GSM protocols in previous sections. Many researches propose solutions to improve the security of the wireless communications. The approach of Harn and Lin's modified protocol [15] is to reduce the amount of information and eliminate the stored sensitive information in VLR for GSM. Some new designed protocols are also proposed for the purpose of security for wireless communications [1,3,4,18]. However, no total solution has been proposed to improve the security functions for GSM. The main concern of the GSM authentication is its reliance on the internetwork security that is traversed by the VLR and HLR communications. In a heterogeneous network environment administrated on a large scale, this authentication assumption is not guaranteed. Therefore, we propose an improved protocol for GSM to achieve the following goals of authentication of mobile users:

(1) To eliminate unnecessary sensitive information stored in VLR.

(2) To reduce the stored space in VLR.

(3) Not to introduce any extra computations in the proposed approach.

(4) Authentication of mobile users is to be done by VLR instead of HLR, even if VLR does not know the subscriber's secret *Ki* and A3 algorithm.

(5) To improve the performance without changing the existing GSM system.

The improved method is depicted in figure 6. During the authentication process of MS, HLR sends only one Temporary *Ki* (TKi) and *RAND* instead of sending a set of triplets ($RAND, SRES, Kc$) to VLR. TKi is generated, with A3 algorithm, by using *Ki* and *RAND* as inputs. The transmission of paired ($RAND, TKi$) is encrypted with the session key (*sk*) of HLR. The generation of *sk* will be discussed later. VLR computes *SRES1*, with A5 algorithm, by using *RAND1* and TKi as inputs. *RAND1* is generated by VLR for the first call of MS. To verify the identity of MS, VLR sends both *RAND* and *RAND1* to MS to check if the subscriber can reply with correct *SRES1*. Once the subscriber is identified, the computations of TKi with *RAND* and *Ki* as well as *SRES1* with TKi and *RAND1* are carried on, and the signed result is sent back to VLR. With the correct *SRES1*, VLR is able to justify the authorization status of a subscriber.

In the subsequent calls, VLR generates different $RANDi$ for each call. No matter how many times the MS calls within a pre-defined period in the coverage of VLR, only one $RANDi$ is needed for each ith call. That is to say, only one copy of authentication parameters is initially transmitted from HLR to VLR. In the meantime, no fraudulent sensitive information or signed result may have access to the services, and no session key (*Kc*) can be used to eavesdrop on the user's data. The parameters are transmitted

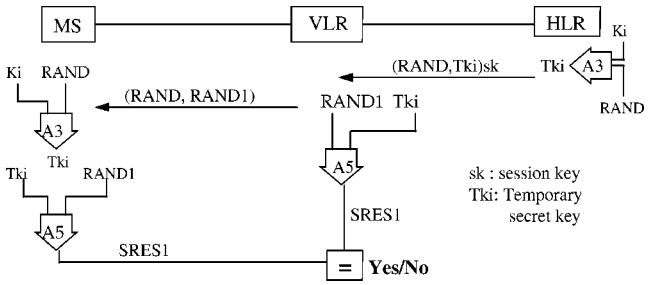

Figure 6. The improved method for MS authentication.

from HLR to VLR in an encrypted mode that protects the signaling data from eavesdropping. Furthermore, the authentication of MS is done by VLR itself, and no more aid from HLR is required. This eliminates the bandwidth consumption for transmitting the authentication parameters.

In the original GSM, AuC generates n copies of authentication parameters at a time for a given IMSI. When VLR or HLR uses up the set of parameters, HLR will inquire another set of parameters from AuC. In our method, there is no limitation for the authentication process to use the $RANDi$ with a specific TKi. Theoretically, as long as the MS stays in the coverage of this VLR, the VLR requests no other *RAND* and TKi from HLR. Periodically refreshed authentication parameters must be better than the information, which has been used for a long time. However, the period of the *RAND* and TKi should be long enough to prevent the benefit loss due to fewer transmissions between VLR and HLR. A period set for the specific *RAND* and TKi is highly recommended.

One point of the proposed protocol that should be noted is the generation of TKi. Despite that the inputs of A5 are made up of 64 bits and 22 bits in the original GSM system, the output of A3 is designed to be 32 bits [23]. The length of TKi should be 64 bits in the modified protocol. Two possible methods can be used to generate a 64-bit TKi. One solution is to expand the result of A3 to 64 bits as the value of TKi when HLR and MS use *RAND* and *Ki* as inputs to run A3 algorithm. This operation will be done only once in the first call of MS. Another solution is to run two times A3 algorithms in HLR and MS to obtain 64 bits of TKi by combining the two 32-bit results. The extra computation in HLR and MS and transmission of two *RAND*s from HLR to VLR, then to MS, will only be done in the first call of MS. Therefore, the computation overhead is negligibly small.

To summarize, this authentication of mobile users is applicable in a practical sense because it takes only one pair of parameters and only one computation for authentication in VLR. The ($RAND, TKi$) which does not contain sensitive information achieves the first goal of authentication. Only one copy of authentication parameters that reduces the stored spaces in VLR achieves the second goal. Only one computation of *SRES* in VLR needed and this accomplishes the third goal. The process of authentication proceeded by VLR instead of by HLR matches the fourth goal. In the meantime, the existing GSM architecture is not changed.

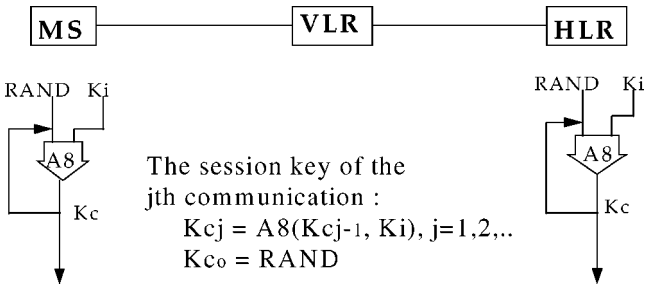

Figure 7. Session key generation for MS.

3.2. Data confidentiality protocol

Just like the authentication of MS, the confidentiality of user data relies upon the security of the network and protection of end-to-end privacy is not undertaken by GSM. For end-to-end privacy, we propose a new method of data confidentiality, which protects both the radio path and the wireline networks. We assume the HLR where MS originally registers is trustworthy under practical administrative consideration. Figure 7 shows how to generate the secret session key for MS. Both MS and HLR use *RAND* and *Ki* of MS as inputs to compute the session key, *Kc*1, for the first call delivery. The *RAND* is generated and forwarded to VLR by HLR when the MS is authenticated. In the following jth call, MS and HLR will take the previous $Kcj-1$ (i.e., the historical Kcj) as an input to re-compute the Kcj, which is used subsequently as the secret session key for data transmission. Due to the output length of A8 being 64 bits, the $Kcj-1$ could be expanded by adding part of *RAND* (i.e., 64 bits of 128 bits) to make it a 128-bit long key.

As mentioned in the previous sections, the secure communications in GSM can be seen as two types of architectures, e.g., mobile station to mobile station or mobile station to fixed station. In the following paragraphs, we propose two approaches to offer secure communications for two mobile ends (MS1 and MS2) and for mobile end to fixed end (MS1 and FS2). One approach has a session key table stored in HLR/SC, and the other one has no key table in HLR/SC.

In end-to-end privacy, the key management and distribution is an important issue to the security and user friendliness of the protocol. However, secret-key cryptosystems demand a serious effort towards key management and distributions [8]. Secret-key cryptosystems require that the mobile users share a common secret-key, and that other users do not have access to this key. Key agreement is the process by which these users agree upon the proper key [17]. In the proposed solutions here for data confidentiality between two end users, the assumptions are that SC and FS also provide the encryption/decryption functions. HLR and SC are always equipped with high power facility, which can support much more data processing or computations. For commercial usage, it is easy to integrate a common microprocessor in the fixed station for the purpose of secure communications. The encryption/decryption

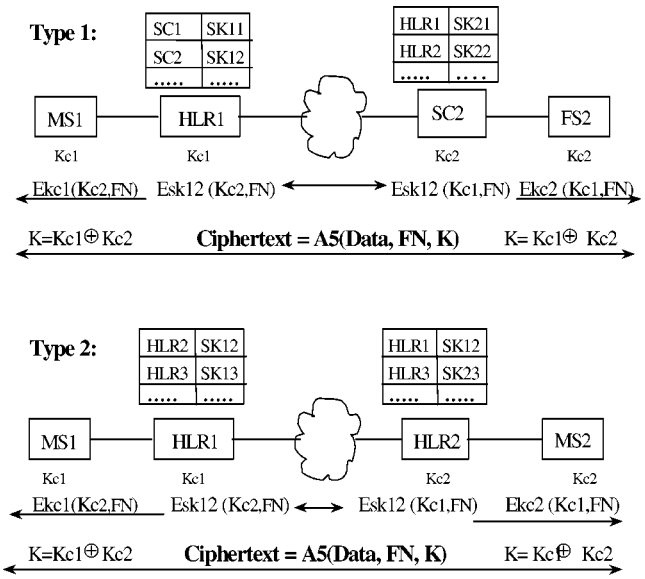

Figure 8. Approach 1 of data confidentiality.

algorithms used in SC and FS can be negotiated beforehand by the GSM system and the fixed network. The algorithms can be adopted either from the security functions in GSM or from some other popular one-way functions. If the algorithms are chosen from GSM, then the whole system can be seen as a full GSM network. Otherwise, the negotiation and management of the algorithms will be a little more complicated than the simple GSM network.

Approach 1 (With a session key table in HLR/SC)

Figure 8 shows the protocol of Approach 1 where HLR1 is the Home Location Register of MS1, HLR2 is the Home Location Register of the remote user MS2 and SC2 is the Switching Center nearby the fixed user FS2 in a fixed network.

The procedures of key distribution and management in Approach 1 are as follows:

Step 1. Maintain a session key table in each HLR/SC.
Type 1: Maintain a session key table in each HLR and SC to keep the session keys between HLR and SC. *SK*11, *SK*12, and *SK*22 are the session keys for HLR1 and SC1, HLR1 and SC2, HLR2 and SC2, respectively.
Type 2: Maintain a session key table in each HLR to keep the session keys between various HLRs. *SK*12, *SK*13, and *SK*23 are the session keys for HLR1 and HLR2, HLR1 and HLR3, and HLR2 and HLR3, respectively.

Step 2. Transmit the *Kc* to the remote user.
Type 1: HLR1 Transmits the session key (*Kc*1) of MS1 to the remote SC2 and then to FS2. FS2 transmits its session key (*Kc*2) to MS1 through SC2 and HLR1.
Type 2: *Kc*1 and *Kc*2 are the session keys for the pairs (MS1, HLR1) and (MS2, HLR2). The HLR transmits the *Kc* of local MS with the encrypted

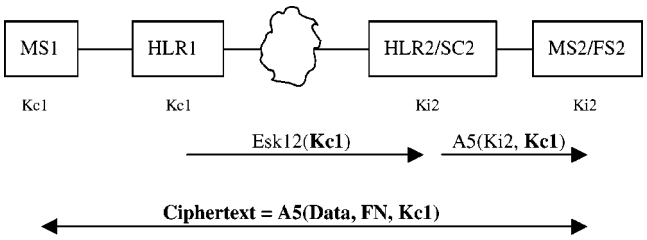

Figure 9. Approach 2 of data confidentiality.

mode (using $SK12$ as key in this case) to the other HLR.

Step 3. Generate the secret key for two end users.
Type 1: At the mobile end user, K is equal to $Kc1 \oplus Kc2$ and can be produced by HLR1 (then forwarded to MS1) or by MS1 itself. At the fixed end user, K is equal to $Kc1 \oplus Kc2$ and is produced by itself.
Type 2: Two alternatives to create the secret key, K, for the two MSs located in different areas. K is equal to $Kc1 \oplus Kc2$ and is produced by HLRs (then forwarded to MSs) or by MSs themselves.

Step 4. Communicate MS1 and MS2/FS2 directly by using K as the secret key and with A5 algorithm or with another encryption algorithm (E) for Type 1.

The session key table in HLR/SC will not take much storage space since the number of HLRs/SCs is kept in a relatively small scale even if the number of subscribers could be large. Key management and distribution and data transmission are in ciphered modes in this approach and provide the confidentiality of data for both the radio path and the wireline connections.

Approach 2 (Without session key table in HLR/SC)

Figure 9 shows the MS secret key management and distribution without maintaining a session key table in each HLR/SC. $Kc1$ is the session key for MS1. And $Ki2$ is the secret key, which is generated by the home SC2 and stored in FS2 in the registration phase, for FS2.

For both types of architectures, when MS2/FS2 is called by MS1, HLR1 has to negotiate with HLR2/SC2 to establish the session key, $SK12$, then it sends the encrypted $Kc1$ with $SK12$ to HLR2/SC2. HLR2/SC2 forwards the $Kc1$ with $Ki2$ to FS2 by using A5 algorithm or any other encryption algorithm (E). MS2/FS2 uses $Ki2$ to decrypt $Kc1$. Finally, $Kc1$ is then used by FS2 as the current secret session key to communicate with MS1. The communication of data can be protected at all VLRs from eavesdropping accordingly. When MS2/FS2 calls MS1, the secret key management and distribution has the same pattern as the former one.

In order to derive the ciphering sequences for each message block in GSM, A5 performs a computation with two inputs: one is the frame number and the other is a key (named Kc) agreed between the mobile station and the network. Applying an "Exclusive-Or" operation between a 114-bit message block and a 114-bit ciphering sequence generated performs both ciphering and deciphering by A5. Therefore, in end-to-end secure communications, both mobile stations have to use the same frame number as a result of applying A5 algorithm. In this proposed protocol of secure communications, including Approaches 1 and 2, MS1 can pick up one random number as the frame number and transmit it with the secret key in the key distribution process. When both mobile stations establish the secret key, the frame number is also set between them. This is the simplest way to deal with the function of A5 and there is no need to change the original structure of the system.

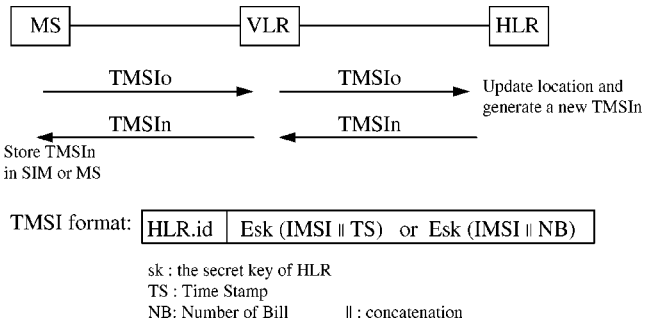

Figure 10. Modified location privacy.

Another defect in the GSM protocol is the repeated encryption and decryption between VLR and VLR/HLR, which are very time-consuming processes. The end-to-end secure communications in this proposed solution decrease the overhead aspects of the data confidentiality. More detailed analysis is shown later in this paper. Another possible contention in these two approaches of data confidentiality is the generation of session key (K, or $Kc1$) to communicate via HLR in each session. We also deal more with the generation of session key and propose an alternative to enhance the performance in generating the key later in this paper.

3.3. Location privacy protocol

In GSM, location updating of MS, in which IMSI is not sent over air, enhances partial security [10]. The problems of the current system have been discussed in the previous sections. In order to support the protections for both the radio path and the wireline connections, the proposed method is shown in figure 10.

The proposed format of TMSI contains MS's HLR identifier and the encrypted IMSI and TS (or NB), where *sk* is the secret key of HLR, TS is the Time Stamp, and NB is the Number of Bills, respectively. When MS roams from one place to another new place, MS sends its old TMSI (TMSIo) to the new VLR. The new VLR is able to recognize the HLR to which MS belongs by reading the TMSIo. The new VLR inquires the signaling information of MS from HLR and, in the meantime, requests to update MS's location. According to the decrypted IMSI, HLR generates a new TMSI (TMSIn) for the real IMSI and sends

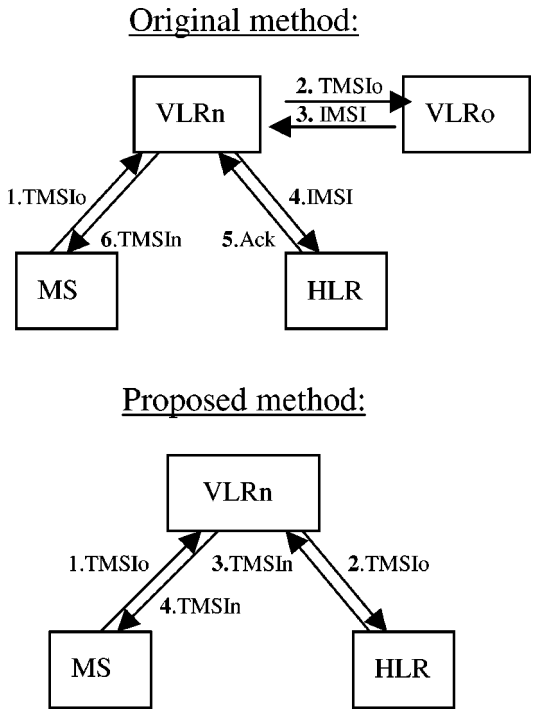

Figure 11. Data flows of location privacy in two methods.

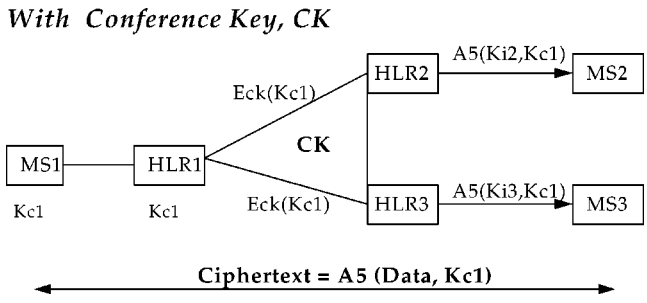

Figure 12. Mobile teleconference with conference key.

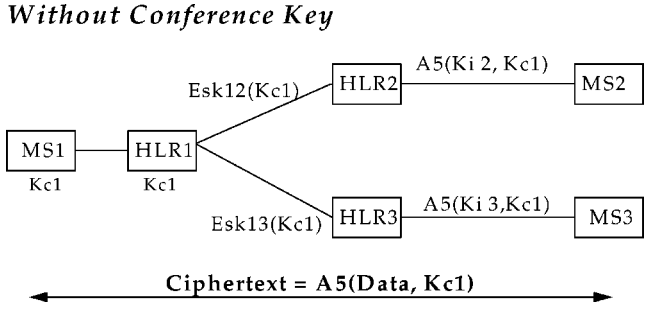

Figure 13. Mobile teleconference without conference key.

it back to the new VLR. VLR passes the TMSIn to MS and the TMSIn is stored in SIM or ME itself. Since VLR does not have the IMSI of MS, it cannot identify the subscriber. Thus, this protocol provides the location confidentiality for both the radio path and the wireline communications.

In this proposed protocol, all the TMSIs of mobile stations are maintained and updated by their HLRs. The proposed solutions enhance the location privacy of the subscriber and solve the three problems. Firstly, IMSI is not sent on both the air and the wireline connection. Secondly, database failure of VLR causes no impact on the TMSIs sent by the mobile stations. Since the VLR does not need to store the location information, the IMSIs are always protected. Furhtermore, when a user roams from one place to another, the location information is updated by passing the previous TMSI to the new VLR and subsequently to the HLR. No damage is done even if the old VLR is no longer accessible for the user.

The bandwidth requirements of the proposed solution are less than those of the original GSM method. The data flows in two methods are depicted in figure 11. In the original method, there are at least six messages transmitted during location update for the MS. There are only four messages needed to protect the current location of the MS in the proposed protocol.

3.4. Mobile teleconferences

The proposed data confidentiality protocol for GSM can also be applied to mobile teleconferences, a new service for digital mobile communication systems. In mobile teleconference, there are more than two users (i.e., MSs $\geqslant$ 3) in the communications instead of only two. The mobile teleconference protocols are similar to the data confidentiality protocol. The requirements of privacy and authentication are also taken into account. Two approaches for mobile teleconferences by using the same protocol of data confidentiality are advocated.

Approach 1 (With a conference key, CK)

The protocol of mobile teleconference with a conference key is shown in figure 12. The conference key, *CK*, shared by HLRs, has to be established before using this protocol [16]. The group of users then generates a common secret key over a public channel so that they may hold a secure conference. If MS1 initiates a conference with MS2 and MS3, it needs to set up the call by distributing the secret session key *Kc*1 to others. HLR1 uses the conference key, *CK*, to pass *Kc*1 to other HLRs and then HLRs pass *Kc*1 by using their own *Ki*'s to MSs. After the keys are distributed, MSs communicate with each other in the encrypted modes by using A5 and *Kc*1.

Approach 2 (Without any conference key)

The protocol of mobile teleconference without any conference key is shown in figure 13. Approach 2 is proposed by maintaining a session key table in each HLR, just like the Approach 1 of data confidentiality to the original GSM. When MS1 initiates a conference, its HLR1 uses these session keys of the remote HLRs to encrypt and pass *Kc*1 to the remote stations so that all MSs during the teleconference can use *Kc*1 as the secret session key.

4. Session key generation and overhead estimation

In the data confidentiality protocol of proposed methods, the possible contention is to generate the session key (K or *Kc*1) of communication via HLRs in each session. It can be solved in the following manner. In fact, a subscriber can choose to communicate in the original GSM mode or a secure mode through the wireline connections. In other words, the session key is only used in a need of sensitive users. In order to obtain a secure communication, it is worthwhile to wait a short moment resulting from the key management and distribution. Comparisons of the communication bandwidth made between the original GSM protocol and the new approach as follows indicate the merits of the proposed improvements.

The overhead of the proposed data confidentiality protocol occurs on the mobile station and fixed station. Both types of stations contain integral microprocessors, which can handle the encrypting/decrypting functions. In the proposed data confidentiality, the bandwidth of communication for both Types 1 and 2 of architectures is

$$2 \cdot \text{A5(114 bits)} + 2 \cdot \text{A5(message length}, m \text{ bits)}. \quad \text{(E.1)}$$

$2 \cdot$ A5(114 bits) means that there are two transmissions of encrypted *Kc*'s from HLR1 and HLR2/SC2 to MS1 and MS2/FS2, respectively, in the key distribution phase. In the data transmission phase, $2 \cdot$ A5(message, m bits) means that MS1 encrypts the message with K or *Kc*1 by using A5 algorithm, transmits it directly to MS2/FS2. MS2/FS2 then decrypts the ciphertext with K or *Kc*1 by using A5 algorithm.

In GSM, the communication bandwidth is

$$4 \cdot \text{A5(message length}, m \text{ bits)}. \quad \text{(E.2)}$$

Each of MS1, BSS1, BSS2 and MS2 has to transmit the m-bit message using A5 algorithm. MS1 encrypts the message, and transmits it to BSS1 on the air. BSS1 decrypts the message, and then transmits it in a plaintext mode to BSS2 through the network. BSS2 encrypts the message again and forwards it to MS2. Finally, MS2 decrypts the ciphertext and gets the message. There are four m-bit bandwidth transmissions in total.

The communication bandwidth of (E.2) is much larger than that of (E.1) when $m \gg 114$ bits. Conceivably, even if the session key has to be established in each session, our method is still more efficient than the original GSM, as long as GSM needs to support secure communication on the wireline connection. An alternative for the secret session key is to concurrently generate the next secret key and to store it in the SIM card (or in MS) in each communication session. That may reduce the setup time of call under such a circumstance.

In the proposed authentication protocol (section 3.1) or Approach 2 of the data confidentiality protocol (section 3.2) of our methods, the session key, *sk*, used to transmit *TKi*, or *Kc*1 between VLR/HLR and HLR, can be generated in one of the following ways:

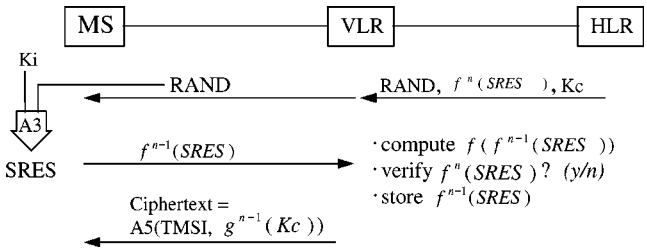

Figure 14. Harn and Lin's approach for authentication of MS.

– The session key is negotiated on-line by using the Diffie and Hellman method or another approach. This task takes place only once and adds negligible overheads of operation-time [9].
– VLR and HLR maintain a session key table in each node.

5. Computational and capacity analyses

In the following sections, we make comparisons among the original GSM system, Harn and Lin's approach and our proposed methods. Harn and Lin's modified protocol of GSM is briefly analyzed. Their approach is sketched in figure 14 [15]. During the authentication of MS, HLR sends only one triplet, (*RAND*, f^n(*SRES*), *Kc*), instead of sending a set of n copies of parameters (*RAND*, *SRES*, *Kc*), to VLR where *RAND*, *SRES*, and *Kc* are the same as defined in the original protocol. In Harn and Lin's approach, it needs to use two more one-way functions, f and g. In order to identify the subscriber, the VLR sends *RAND* to the subscriber to check if the subscriber can reply with f^n(*SRES*). If the subscriber is indeed the IMSI and the corresponding *SRES* is computed with secret *Ki*, then the signed result f^{n-1}(*SRES*) is sent back to the VLR. The VLR computes $f(f^{n-1}$(*SRES*)) and compares it with the stored value f^n(*SRES*). If both values match, the VLR is able to justify the subscriber as an authorized one, and then f^{n-1}(*SRES*) is stored to replace the f^n(*SRES*). The MS communicates with the VLR by using g^{n-1}(*Kc*) as a secret session key, and uses a new TMSI for each call setup.

Harn and Lin's approach has eliminated the stored sensitive information in VLR and only stores the one-way result. This modification also reduces the amount of information to some extents. Nonetheless, the overhead occurs in the computation of f^n(*SRES*) and g^{n-1}(*Kc*) by each subscriber in each session.

5.1. Authentication protocols

The computation analysis and storage space analysis of authentication protocols are compared among the original GSM protocol, Harn and Lin's modified protocol and our proposed method in table 1.

For authentication, only *SRES* used to verify MS is considered as the component of computation and capacity analyses. In the GSM protocol, we may assume that HLR

Table 1
Comparisons of authentication of MS among three methods.

	Original GSM	Harn and Lin	Our method
HLR	A3(*Rand*, *Ki*) = *SRESj* $j = 1, 2, \ldots, n$	A3(*Rand*, *Ki*) = *SRES* Compute f^n(*SRES*)	A3(*Rand*, *Ki*) = *Tki*
MS	A3(*Rand*, *Ki*) = *SRESj* $j = 1, 2, \ldots, n$	A3(*Rand*, *Ki*) = *SRES* Compute f^{n-j}(*SRES*)	A3(*Rand*, *Ki*) = *Tki* A5(*Randj*, *Tki*) = *SRESj* $j = 1, 2, \ldots, n$
Verification (by VLR)	*SRESj*	$f(f^{n-j}$(*SRES*))	A5(*Randj*, *Tki*) = *SRESj*
Total computations	$2nT$(A3)	$\left(n + \sum_{j=1}^{n-1} j\right)T(f)$	$2T$(A3) + $2nT$(A5)
Total storage spaces	nS(*SRES*)	$S(f^{n-j}$(*SRES*))	S(*Tki*)

$T(\cdot)$: computation time, $S(\cdot)$: storage space.

generates n copies of *SRES* and then takes n times of computation of an A3. MS computes the *SRES* in each session, and then there are also n *SRES*'s computed in n sessions. To verify the particular MS, VLR holds at most n copies of *SRES*'s at a time. The total computation is $2nT$(A3) and the total storage space in VLR is nS(*SRES*). T(A3) stands for the computation time for A3 algorithm and S(*SRES*) stands for the storage space for *SRES*, respectively. In Harn and Lin's approach, there are n computations of f function for *SRES* in HLR and $n - j$ computations of f function for each session in MS, where j is the jth call setup. A total of computations for n call setups are

$$\left(n + \sum_{j=1}^{n-1} j\right)T(f) = \left[n(n+1)/2\right]T(f).$$

The storage space needed in VLR is one $S(f^{n-j}$(*SRES*)). In our method, there are one *TKi* computed in HLR, one *TKi* and n A5-function computations in MS, and n A5-function computations in VLR. The total computation is

$$2T(\text{A3}) + 2nT(\text{A5}) \cong 2(n+1)T(\text{A3}).$$

The storage space in VLR is S(*TKi*).

The computational analysis shows that Harn and Lin's approach requires the largest computation among the three methods. The larger the n value is, the more computations will be needed in their approach. For example, in the case of T(A3) $\cong$ T(A5) $\cong$ $T(f)$, and $n = 5$, the computation ratio among GSM, Harn and Lin's approach and our method is 10 : 15 : 12. If $n = 10$, the ratio will then be 20 : 55 : 22. The storage space analysis shows that the original GSM needs much more capacity to store the *SRES*'s in VLR. The relative ratio in GSM, Harn and Lin's approach and our method is n : 1 : 1. The larger the n value is, the larger the space is needed in GSM. Harn and Lin's approach and our method maintain the space, which is proportional to the number of subscribers but not to the n calls. In summary, in the authentication of MS, Harn and Lin's approach takes more computations and the original GSM needs more space.

5.2. Conversation confidentiality protocols

The computational analysis of data confidentiality is shown in table 2 for the GSM protocol and our method.

Table 2
Comparisons of data confidentiality among three methods.

	Original GSM/Harn and Lin	Our method
HLR1, HLR2	A8(*RAND*, $K1$) = *Kc*1	A8(*RAND*, *Ki*) = *Kc*1 A5(*SK*, *Kc*1)
MS1, MS2	A8(*RAND*, $K1$) = *Kc*1 A5(Mj, *Kc*1) = Cj $j = 1, 2, \ldots, m$	A8(*RAND*, $K1$) = *Kc*1 *Kc*1 + *Kc*2 A5(Mj, *Kc*1) = Cj A5(Cj, *Kc*2) = Mj
BSS1, BSS2	A5(Cj, *Kc*) = Mj $j = 1, 2, \ldots, m$	*None*
Total (computations)	$4T$(A8) + $4mT$(A5)	$4T$(A8) + $2T$(XOR) +$2(m+1)T$(A5)

Harn and Lin's method uses the same process to encrypt/decrypt the same data as the GSM system does, except that it uses a different session key, g^{n-1}(*Kc*), as opposed to the *Kc* of GSM. Therefore, we apply the same analysis to GSM and Harn and Lin's methods.

In GSM, the computations in HLR1/MS1, which generate *Kc*1 under A8 algorithm, are $2T$(A8). The computations in HLR2/MS2, which generate *Kc*2 under A8 algorithm, are also $2T$(A8). The total computations for generating *Kc*1 and *Kc*2 are $4T$(A8). In this analysis, the communication message is segmented into m blocks. Thus, encrypting the message with *Kc*1 under A5 algorithm in MS1 takes mT(A5) and decrypting the ciphertext with *Kc*2 under A5 algorithm in MS2 takes $2mT$(A5). In addition to the computations for end-to-end communication, the intermediate BSS1 decrypts the message, and BSS2 encrypts it when they route the message to another node. This transmission takes $4mT$(A5). The total computation is

$$4T(\text{A8}) + 2mT(\text{A5}) + 2mT(\text{A5}) = 4T(\text{A8}) + 4mT(\text{A5}).$$

In our method, since BSS1/BSS2 does not need any computation for encryption/decryption, it just routes the message to the right end. HLR1 and HLR2 generate *Kc1* and *Kc2* by using A8 algorithm and send *Kci* with session key *sk* to their subscribers MS1 and MS2. It takes $2T$(A8) and $2T$(A5) operation-time, respectively. The generation of *Kc1* and *Kc2* in MS1 and MS2 takes $2T$(A8). K from $Kc1 \oplus Kc2$ for each end takes $2T$(XOR) computation-time, respectively. In the communication process, MS1 needs

Table 3
Comparisons of location confidentiality among three methods.

	Original GSM	Harn and Lin	Our method
HLR			*Esk*(IMSI $\|\|$ TS) = TMSIn
VLR	TMSIn	g^{n-1}(*Kc*) A5(TMSI, g^{n-1}(*Kc*))	
MS		g^{n-1}(*Kc*) A5(TMSI, g^{n-1}(*Kc*))	
Computations	nT(Random TMSIn)	$2\left(\sum_{j=1}^{n-1} j\right)T(g) + 2T(\text{A5})$ $= n(n-1)T(g) + 2T(\text{A5})$	$nT(E)$
Storage space	$2S$(TMSIn) + S(IMSI)	$2S$(TMSIn) + S(IMSI)	S(TMSIn) + S(*sk*)

Table 4
Summary of comparisons of the three methods.

				$n = 5$ or $m = 5$			$n = 10$ or $m = 10$		
	GSM	H&L	Improved	GSM	H&L	Improved	GSM	H&L	Improved
Computation									
Authentication	$2n$	$n + \sum_{j=1}^{n-1} j$	$2n + 2$	1	1.5	1.2	1	2.75	1.1
Data confid.	$4(m+1)$	$4(m+1)$	$2(m+3) + C$	1.5	1.5	1	1.7	1.7	1
Location conf.	n	$n(n-1)+2$	n	1	4.4	1	1	9.2	1
Storage									
Authentication	n	1	1	5	1	1	10	1	1
Location	3	2	2	3	2	2	3	2	2

mT(A5) to encrypt the message with K under A5. MS2 needs mT(A5) to decrypt the ciphertext. Combining all those computations, we can calculate the operation-time as

$$2T(\text{A8}) + 2T(\text{A5}) + 2T(\text{A8}) + 2T(\text{XOR}) + 2mT(\text{A5}) = 4T(\text{A8}) + 2T(\text{XOR}) + 2(m+1)T(\text{A5}).$$

Since T(XOR) is a fixed time to compute K and T(A5) $\cong T$(A8) in our method, the computations are actually dependent on the value of m. The performance of the protocol will be dramatically improved when the value of m is very large. In other words, $4mT$(A5) will be greater than $2(m+1)T$(A5) if there is a long secure conversation. Our method demonstrates a better performance in the secure communications.

5.3. Location confidentiality protocols

The computation and capacity analyses for the location confidentiality of the three methods are shown in table 3. In GSM, VLR takes nT(Random TMSIn) to generate n TMSIn for MS in n sessions. VLR stores *one* IMSI and *one* TMSIn for each subscriber at any time whereas MS stores the current TMSIn.

In Harn and Lin's method, both VLR and MS need $\sum_j^{n-1} T(g)$ operation-time to generate g^{n-1}(*Kc*), and require *one* T(A5) operation-time for A5(TMSI, g^{n-1}(*Kc*)). The total operation-time of computation is

$$2\left(\sum_{j}^{n-1} j\right)T(g) + 2T(\text{A5}) = n(n-1)T(g) + 2T(\text{A5}).$$

At the same time, VLR stores *one* TMSIn and *one* IMSI, whereas MS stores *one* TMSIn. The total storage space is $2S$(TMSIn) + S(IMSI).

In our method, the only computation needed in HLR is *Esk*(IMSI $\|$ TS) = TMSIn that takes $nT(E)$ operation-time. VLR stores TMSIn and *sk* of HLR that takes S(TMSIn) + S(*sk*) operation-time.

5.4. Analyses summary of the three methods

We assume that $T(\text{A3}) \cong T(\text{A5}) \cong T(\text{A8}) \cong T(f) \cong T(g) \cong T(E)$, $S(\textit{SRES}) \cong S(f(\textit{SRES})) \cong S(\textit{TKi})$, and S(TMSI) $\cong S$(IMSI) $\cong S$(*sk*). The summary of analytical comparisons for the three methods is shown in table 4, where n is the number of authentication triplet in a set and m is the block number of message transmitted. Harn and Lin's method needs the largest operation-time, and GSM and our method are relatively the same in terms of computations. As for the required storage space, GSM consumes more capacity than that of the two other methods when the authentication process is undertaken.

6. Conclusions

This paper points out the security requirements for mobile communications and the deficiency of security functions in the GSM system. This study thus proposes three improved methods to enhance the security and to improve the protocols for the current GSM system without changing its existing architecture. The assumptions made for this study are that HLR is trusted whereas the VLRs are not.

Both the radio path and the wireline connections are protected from eavesdropping with the improved approaches.

The proposed practical authentication protocol of MS stores no sensitive information in VLRs and decreases the storage spaces in VLRs without introducing more computations. The protocols of data confidentiality and location privacy provide the security functions of user requirements in mobile communication systems and make the GSM system more reliable and accessible. Analyses of computation and capacity indicate that the proposed methods do not add overhead of computation to the existing system on one hand. On the other hand, they effectively reduce overheads on the storage space. Most important of all, the methods give more secure designs to the mobile communications. The improved methods can be applied to other mobile communication systems as well.

References

[1] A. Aziz and W. Diffie, Privacy and authentication for Wireless Local Area Networks, IEEE Personal Communications (First Quarter 1994) 25–31.

[2] J. Beheim, Security first in Europe's mobile communication, Telecom Report International 17(1) (1994) 31–34.

[3] M.J. Beller, L.F. Chang and Y. Yacobi, Privacy and authentication on a portable communications system, IEEE Journal on Selected Areas in Communications 11 (August 1993) 821–829.

[4] V. Bharghavan, Secure wireless LANS, in: *ACM Conference on Computer and Communications Security* (November 1994) pp. 10–17.

[5] D. Brown, Techniques for privacy and authentication in personal communication systems, IEEE Personal Communications (August 1995) 6–10.

[6] U. Carlsen, Optimal privacy and authentication on a portable communications system, ACM Operation System Review (July 1994) 16–23.

[7] C. D'echaux and R. Scheller, What are GSM and DCS, Electrical Communication (2nd Quarter 1993) 118–127.

[8] D.E.R. Denning, *Cryptography and Data Security* (Addison-Wesley, Reading, MA, 1982).

[9] W. Diffie and M.E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (1976) 644–654.

[10] European Telecommunications Standards Institute, GSM 03.20: Security Related Network Functions (June 1993).

[11] European Telecommunications Standards Institute, GSM 02.09: Security Aspects (June 1993).

[12] Y. Frankel et al., Security issues in a CDPD wireless network, IEEE Personal Communications (August 1995) 16–27.

[13] R. Hagen, Security requirements and their realization in mobile networks, in: *Proc. 14th International Switching Symposium '92*, Vol. 1 (October 1992) pp. 127–131.

[14] S.R. Hall and D.P. Maher, Closing in on wireless privacy, AT&T Technology 8(3) (1993) 22–25.

[15] L. Harn and H.Y. Lin, Modification to enhance the security of the GSM protocol, in: *Proc. of the 5th National Conference on Information Security*, ROC (May 1995) pp. 74–76.

[16] M.S. Hwang and W.P. Yang, Conference key distribution schemes for secure digital mobile communications, IEEE Journal on Selected Areas in Communications 13(2) (February 1995) 416–420.

[17] M.S. Hwang and C.H. Lee, Authenticated key-exchange in mobile radio network, European Transactions on Telecommunications 8(3) (May/June 1997) 265–269.

[18] T. Hwang, Scheme for secure digital mobile communications based on symmetric key cryptography, Information Processing Letters (1993) 35–37.

[19] C.H. Lee, M.S. Hwang and W.P. Yang, Phone card application and authentication in wireless communications, in: *Mobile Communications – Technology, Tools, Applications, Authentication and Security* (Chapman and Hall, London, 1996) pp. 323–329.

[20] Y.B. Lin, *Introduction to Mobile Network Management*, National Chiao Tung University Series in Telecommunications, Taiwan, ROC (1997).

[21] B. Mallinder, An overview of the GSM system, in: *Proc. Digital Cellular Radio Conf.* (October 1988).

[22] R. Molva, D. Samfat and G. Tsudik, Authentication of mobile users, IEEE Network (March/April 1994) 26–34.

[23] M. Mouly and M.B. Pautet, *The GSM System for Mobile Communications* (1992).

[24] I. Nurkic, Difficulties in Achieving Security in Mobile Communications, in: *Mobile Communications – Technology, Tools, Applications, Authentication and Security* (Chapman and Hall, London, 1996) pp. 277–284.

[25] M. Rahnema, Overview of the GSM system and protocol architectures, IEEE Communication Magazine 31(4) (April 1993).

[26] S.P. Shieh, C.T. Lin and J.T. Hseuh, Secure communication in global systems for mobile telecommunications, in: *Proc. 1st Workshop on Mobile Computing*, ROC (1995) pp. 136–142.

[27] J.K. Wey, H.C. Chang, L.F. Sun and W.P. Yang, Clone terminator: An authentication service for advanced mobile phone system, in: *Proceedings of 45th IEEE Vehicle Technology Conference*, Chicago (1995) pp. 175–179.

[28] J.E. Wilkes, Privacy and authentication needs of PCS, IEEE Personal Communications (August 1995) 11–15.

[29] E. Zuk, GSM security features, Telecommunication Journal of Australia 43(2) (1993) 26–31.

Chii-Hwa Lee received the B.S. from National Taiwan University, Taiwan, in 1976, and Master of computer science from Texas A&M University, USA, in 1982. She is currently a Ph.D. candidate of computer and information science in National Chiao Tung University, Taiwan. She joined to work on the projects of C3I System in Chung Shang Instiiute of Science and Technology (CSIST) under the Department of Defense, Republic of China, since 1985. She was also the Head of Management Information System of CSIST from 1988 to 1993. Her current work is related to the secure databases for an intelligent system. Her research interests include data security, mobile communications, mobile computing, and database systems.
E-mail: gis81817@cis.nctu.edu.tw

Min-Shiang Hwang received the B.S. in EE from National Taipei Institute of Technology, Taiwan, in 1980; the M.S. in EE from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in computer and information science from National Chiao Tung University, Taiwan, in 1995. He was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications. He was also a project leader for research in computer security at TL since 1990. He has been on the faculty of the Department of Information Management at Chao Yang University of Technology, Taiwan, since 1996. His research interests include cryptography, data security, database systems, and network management. He is a member of IEEE and ACM.
E-mail: mshwang@dec8.cyut.edu.tw

Wei-Pang Yang was born on May 17, 1950, in Hualien, Taiwan, Republic of China. He received a B.S. degree in mathematics from National Taiwan Normal University in 1974, and an M.S. and a Ph.D. from National Chiao Tung University (NCTU) in 1979 and 1984, respectively, both in computer engineering. Since August 1979, he has been on the faculty of the Department of Computer Engineering at NCTU, Hsinchu, Taiwan. In the academic year 1985–1986, he was awarded the National Postdoctoral Research Fellowship and was a visiting scholar at Harvard University. From 1986 to 1987, he was the Director of the Computer Center of NCTU. In August 1988, he joined the Department of Computer and Information Science at NCTU and acted as the Head of the Department for one year. Then he went to the IBM Almaden Research Center in San Jose, California for another year as a visiting scientist. From 1990 to 1992, he was the Head of the Department of Computer and Information Science again. His research interests include database theory, database security, object-oriented database, image database, and Chinese database systems. He was the winner of the 1988 and 1992 Acer Long Term Award for Outstanding M.S. Thesis Supervision, and the winner of 1990 Outstanding Paper Award of the Computer Society of the Republic of China. He also obtained the 1991–1993 Outstanding Research Award of the National Science Council of the Republic of China. Dr. Yang is a member of IEEE, ACM, and the Phi Tau Phi Society.
E-mail: wpyang@cis.nctu.edu.tw