

Secure Communication in Global Systems for Mobile Telecommunications

Shiuh-Pyng Shieh Chern-Tang Lin Jung-Tao Hsueh
Department of Computer Science and Information Engineering
National Chiao Tung University
Hsinchu, Taiwan 30050

Abstract

The digital cellular mobile telecommunication systems have become the trend of future personal communications services (PCS). In order to satisfy the high quality of services, security functions have been embedded into new mobile communication systems. In this paper, we investigate the security issues in the mobile communication systems and focus especially on the security functions of the Global Systems for Mobile Telecommunications (GSM), the first digital mobile network architecture. The analysis of possible weaknesses of these functions in GSM is also presented.

1 Introduction

As the development of communication and computer technologies, people wish all communication services, including audio, video, image, and data, anytime and everywhere to everybody. The Federal Communications Commission (FCC), U. S. A., has defined the personal communications services as "a family of mobile or portable radio communications services which could provide services to individuals and businesses and be integrated with a variety of competing networks. The primary focus of PCS is to meet the communications requirements of people on the move." By the definition, it is apparent that PCS must, at least, have the features of mobility, digitization, and data variability [1].

In the last few years, the analog cellular mobile telephones have supported reliable and ubiquitous communication services to people, and they also provide the idea of the mobility feature in the future PCS. However, in such open environments, all communications are transmitted as cleartext without any protection to prevent security threats, e.g., eavesdropping and illegal access. Therefore, to guarantee the security and satisfy the high quality requirement of more convenient and more various communication services, the so-called second generation digital cellular mobile telecommunications networks have already been developed and rapidly growing, such as, Global Systems for Mobile

* This work was supported by Telecommunication Laboratory under contract number TL-83-3304.

Telecommunications (GSM) [3] and Digital European Cordless Telecommunications (DECT) in several European countries.

Unlike the traditional computer networks, in a mobile communication system, an end user who has subscribed in a home domain may request services after or during moving from a domain to another one. It is necessary for the visited domain, who does not know the user in advance, to immediately identify the user and provide confidential and legal services, then inform the home domain to accumulate user's accounting data. In this paper, we will investigate the security issues of mobile (digital) communication systems and especially aim our focus on the security functions of GSM. GSM is developed by the European Telecommunications Standards Institute and is the first digital mobile network architecture. It supports many security functions to guarantee the confidentiality of transmission and the authentication of registered users. We will introduce these security functions and analyze the security weakness in GSM.

In the section 2, we will describe the general security requirements of mobile communication systems. Then, the security functions and possible weaknesses in GSM are presented in the section 3 and 4, respectively. Finally, we will give the conclusions.

2 Security Requirements of Mobile Communication Systems

To simplify our discussion, we will define a general environment of mobile communication systems as Fig. 1. This environment is based on the architecture of modern cellular mobile telephone systems [7], and is suitable for the future PCS. We use the notations that are similar to the terms used in GSM for the explanation of following sections.

The entire environment consists of two physical components, mobile stations (MS) and management servers. Through MSs, portable equipments, subscribers (end users) of GSM can access all provided services, e.g., calling phones or data transmission. A management server traces and controls all MSs roaming in its administrative domain and provides services for them. From a subscriber's viewpoint, there are two different management servers, home management server and visiting management server. The former is the server that the subscriber subscribed for GSM services, and contains user's all management information, such as authorized services and accounting data. The domain that the subscriber presents now is the administrative domain of the visiting management server. Since, in this paper, we only focus on the security functions of management servers, we denote the home server as HLR (home location register), and the visiting one as VLR (visiting location register). These notations are similar to those in GSM.

In such environment, when MS arrives the domain of a new VLR and signals VLR for a service, VLR must identify the subscriber and justify whether the user has the authority of this service in real-time. Since VLR does not contain the subscriber's information in advance, it must contact with HLR that the subscriber subscribed for help. There exist two possible mechanisms to choose. The first solution is that HLR may directly send the user's information to VLR and VLR decides if the service can be provided or not. Another mechanism is that HLR makes the decision by itself and informs VLR the result.

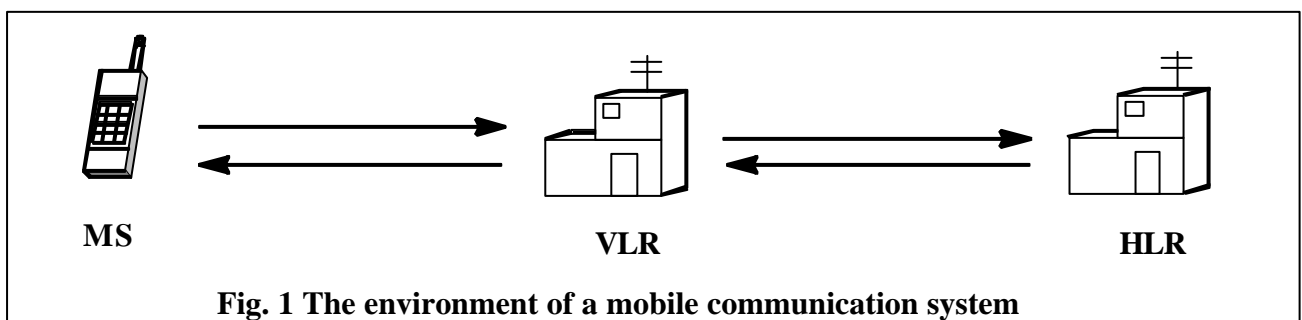
Analyzing the above description, obviously, the mobile communication system is vulnerable to security threats, e.g., impersonating legal subscribers or eavesdropping the communication link between MS and VLR by the third party. To prevent mobile communication systems from hostile attacks, it is necessary to support some protection mechanisms, and we summarize them as the following four security requirements.

Authentication of MS (or Subscriber)

Identifying subscribers is the base of security. Most of modern digital mobile communication systems use a unique identity number for each MS or subscriber to justify the authority. However, the fixed unique ID can be easily faked to access illegal services. Many solutions have been proposed [4, 5] and their design are similar to the traditional computer networks, using a secret information, by a privacy method, to prove the identification is correctly used. The difference is that VLR cannot justify the honesty without the aid of HLR, because the subscriber can travel inter-domain, not as computer users moving within fixed and registered domain. This is also a main challenge of the authentication of MSs in mobile communication systems.

Authentication of VLR/HLR

VLR/HLR can be faked to cheat subscribers and support incorrect services or steal secret data in MSs. A subscriber and a fake HLR can cooperate to obtain all services from VLR that is non-vigilance. Unfortunately, the authentication of VLR/HLR is seldom considered in today's



systems. One of reasons is that the mobile communication systems are homogeneous today, that is, it is more difficult to fake VLR/HLR without being discovered.

Confidentiality of Data between MS and VLR

To prevent private user data or authentication information from eavesdropping, it is necessary to protect the communication channels, radio paths. Although ciphering is the simplest solution to guarantee the confidentiality of messages in digital systems, there are many issues that need be concern, such as which ciphering methods should be applied, and how to set and distribute the session key that is used to encipher/decipher messages. It is a tradeoff between the confidentiality degree and the ciphering overhead. For example, audio communication needs real-time response but some MSs cannot support powerful ciphering computation.

Confidentiality of Data between VLR and HLR

The considerations are similar to what mentioned above. The difference is the communication channels between VLR and HLR may be wireless or wired. And there are a lot of subscribers whose individual data may be transmitted within these channels. By comparison, it needs more protection. Besides, both VLR and HLR can provide more powerful ciphering computations. However, in most systems, they assume that the transmission between VLR and HLR is secure enough.

3 Security Functions of GSM

GSM is the first digital cellular mobile telecommunication system that provides security functions [6, 7] for its subscribers to guarantee the confidentiality of communications and avoid frauds.

The purpose of the security functions in GSM is to prevent:

- ◆ accessing illegal services by intruders who try to impersonate legal and authorized subscribers;
- and
- ◆ eavesdropping of the information which are transmitted on the radio path.

These lead to the need to implement security functions in GSM in order to protect:

- ◆ the access to the mobile services; and
- ◆ the privacy of user-related information on radio paths.

By the above security requirements, GSM considers the following features to guarantee security:

- ◆ subscriber identity (IMSI, international mobile subscriber identity) confidentiality;
- ◆ subscriber identity (IMSI) authentication;
- ◆ user data confidentiality on physical connections, which is to ensure the privacy of all voice and non-voice communication data on the radio path;
- ◆ connectionless user data confidentiality, that is, the user information which is transferred in a connectionless packet mode over a signaling channel is not made available or disclosed;
- ◆ signaling information element confidentiality, that is to ensure the privacy of users related signaling elements which are exchanged between MSs and the network side;

According to the security issues mentioned in section 2, it is obvious that GSM does not cover all requirements of security, since it assumes that all VLRs/HLRs are trustworthy and the transmissions between them are secure. These assumptions are based on GSM is a dedicated and homogeneous systems, which only provides mobile telephone services and can only be accessed by special mobile phones. In other words, GSM's security functions merely include the authentication of subscribers and the confidentiality of data between MS and VLR, where the data involves users' IMSIs, user data on physical connections, connectionless user data, and signaling information elements.

These are the functionality of the security services in GSM. In next section, we will introduce the physical security architecture that GSM adopts.

3.1 GSM Environment

In order to explain the security architecture, we simplify GSM to consist of four parts, MS, VLR_n, VLR_o, and HLR. VLR_n denotes the new VLR where the subscriber is currently visiting, and VLR_o denotes the last VLR he visited. Each subscriber, who identifies himself by a unique IMSI, uses a smart-card (SIM) which contains a secret key K_i known only by HLR, to prove his identity in GSM. We simplify and combine this function to MS.

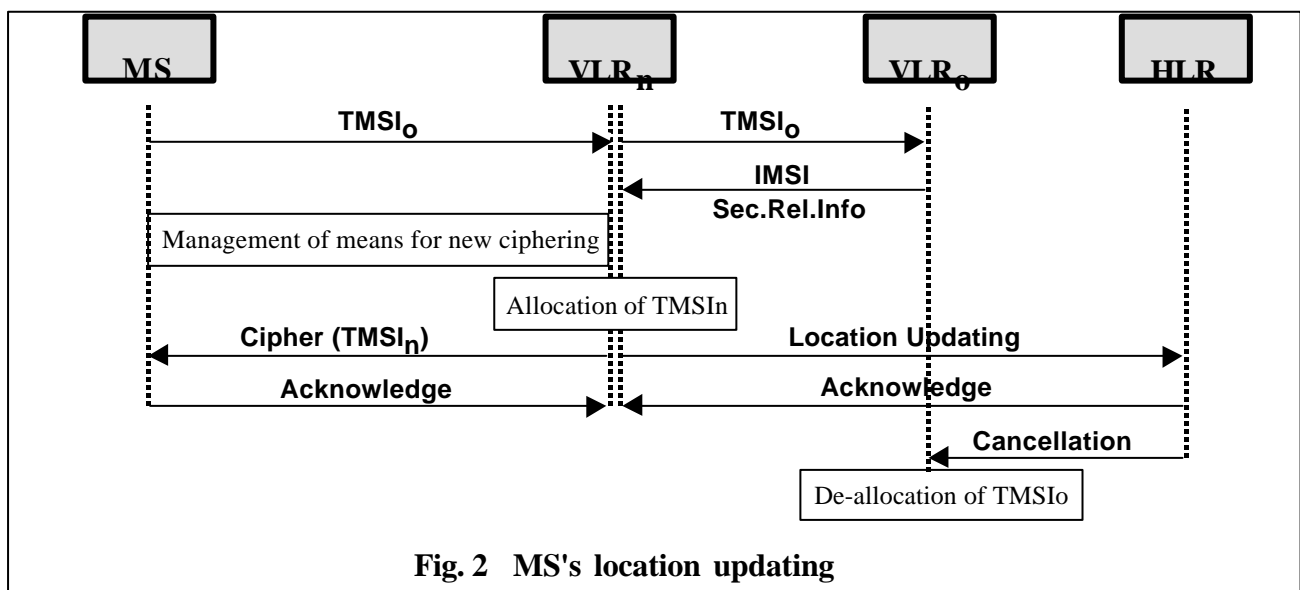
When arriving at a new VLR, MS does not directly send his IMSI to VLR. Instead, MS informs VLR_n who he is by sending TMSI (Temporary Mobile Subscriber Identity), before the MS authentication process. TMSI is a temporary local number and is given in a ciphered mode by VLR_n when MS roams in the area and requests to register and update his location. VLR contains the pair of IMSI and TMSI of each MS in its area and identifies MSs only by their TMSIs. Since TMSI of MS is exchanged as it moves from old VLR to a new one, TMSI must be a variable and be able to protect against tracing the location of a mobile subscriber by listening to the signaling exchanges on the radio path.

We show the GSM environment in Fig. 2, and illustrate how an MS updates its location in a new VLR, where the old VLR is reachable. In the figure, TMSI_o and TMSI_n denote the old and new TMSI getting from VLR_o and VLR_n, respectively. The term Sec.Rel.Info is the security-related information of MS, which is necessary for authentication and ciphering. As an MS arrives at a new VLR, it sends the old TMSI to VLR_n in order to update its location and register to VLR_n. VLR_n bypasses TMSI_o to the original VLR, where the MS comes from, in order to get MS's IMSI and all security-related information. Notice that VLR_n does not know whether the MS is a fraud or not, until it completes the management of means for new ciphering. This part contains the authentication of MS, the decision of ciphering algorithm, and the generation of ciphering key. We will describe them in next subsections. After the location updating procedure, MS uses the new TMSI to access VLR_n until it exchange its location to another VLR area, or until VLR requires to reallocate new TMSI.

Due to the troubles from MS, VLR_o, or anywhere, it is impossible for VLR_n to always get IMSI and Sec.Rel.Info from VLR_o. In this case, VLR_n must request MS sending its IMSI directly with unciphering mode since VLR_n has no Sec.Rel.Info to establish the secret communication channel with MS. Then VLR_n uses IMSI to get message from HLR, and the following procedure is similar to the process done in the previous illustration, except VLR_o. Obviously, this procedure will provide a security hole for hostile attacks.

3.2 Subscriber Identity Authentication

The purpose of the subscriber identity authentication is to confirm that TMSI/IMSI, transferred on the radio path by MS in the identification procedure mentioned above, is the one claimed. This procedure



is based on matching the sensitive information that is known only by the subscriber and HLR. Thus, a physical security mean must be provided to preclude the possibility to obtain sufficient information to impersonate or duplicate a subscriber in GSM, in particular by deriving sensitive information from the mobile station equipment, such as using a smart-card to contain the secret key.

The authentication can be triggered by the system when a subscriber applies to:

- ◆ a change of subscriber-related information element in VLR/HLR, e.g., the location of MS;
- ◆ an access to the service, e.g., call origination;
- ◆ first network access after restart of VLR.

All or some of above events will cause to transfer message between MS and VLR/HLR, that is, the authentication will also be used to set the ciphering key (see next subsection). Therefore, it is performed after TMSI/IMSI is known by the network and before the channel is encrypted.

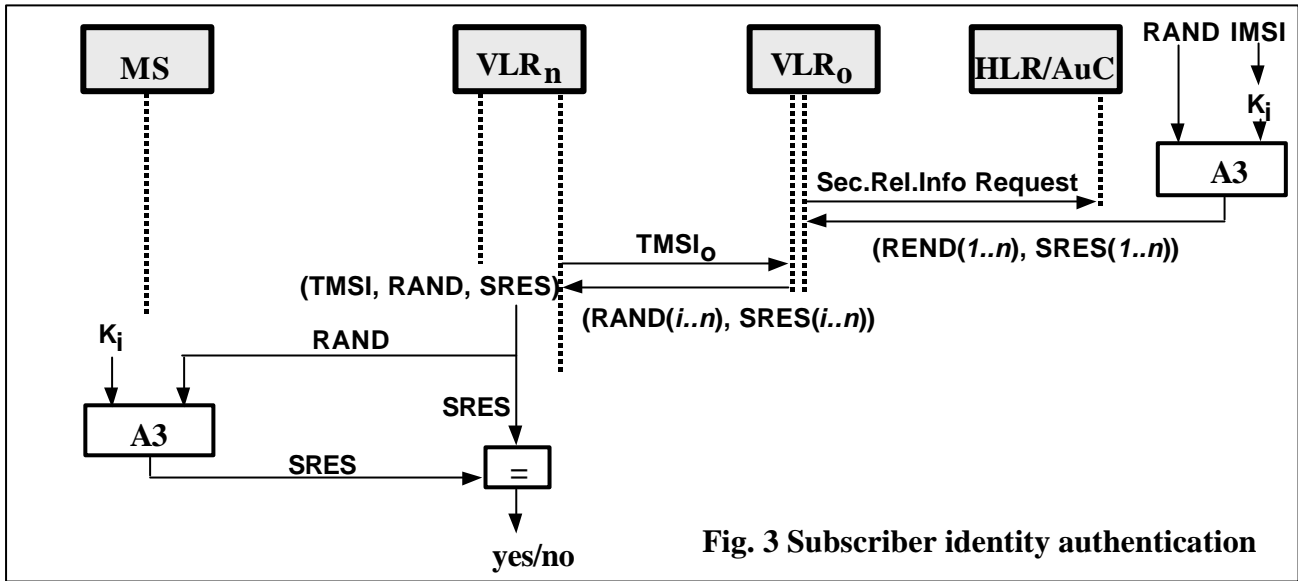
The authentication procedure consists of the following exchanges between VLR and MS.

- ◆ VLR transmits a non-predictable random number $RAND$ to MS.
- ◆ MS computes the signature of $RAND$, say $SRES$, using a one-way function $A3$ with the secret key K_i . That is,
$$SRES = A3 (RAND, K_i).$$
- ◆ MS transmits $SRES$ to VLR.
- ◆ VLR tests $SRES$ for validity.

However, VLR cannot compute $SRES$ using the algorithm $A3$, since MS's secret key K_i is stored within the smart-card and HLR. The solution is VLR requests the pair of $RAND$ and computed $SRES$ from AuC (Authentication Center) in HLR. Thus, AuC must, in advance, compute n ($RAND_i, SRES_i$) pairs for each MS subscribed in this HLR, and send all pairs packed in Sec.Rel.Info to VLR where MS is visiting and registering to. For each authentication, an unused pair is chosen until all pairs have been already used. Then these pairs may be reused again. When MS registers and updates its location with VLR_n, VLR_n gets all unused pairs of $RAND$ and $SRES$ from VLR_o or HLR, if VLR_o is unreachable or there are some troubles. We summarize these processes as Fig. 3 showing.

In commercial products of telecommunications, if any component fails, it is desired to continue serving subscribers' calls if possible. Thus, during a malfunction of the network, GSM follows some principles to handle the requested calls.

In the case that MS requests a call after a successful registration in VLR, since the registration includes the subscriber identity authentication for updating location and setting security related



information, VLR will trust MS and still permit the call, even the reauthentication for the call is unsuccessful due to the network malfunction. On the other hand, if MS requests a call during a malfunction of network and before the registration in VLR, a new registration shall be necessary before the call. But, if MS cannot be successfully authenticated due to the network malfunction, the registration fails and therefore the call is rejected.

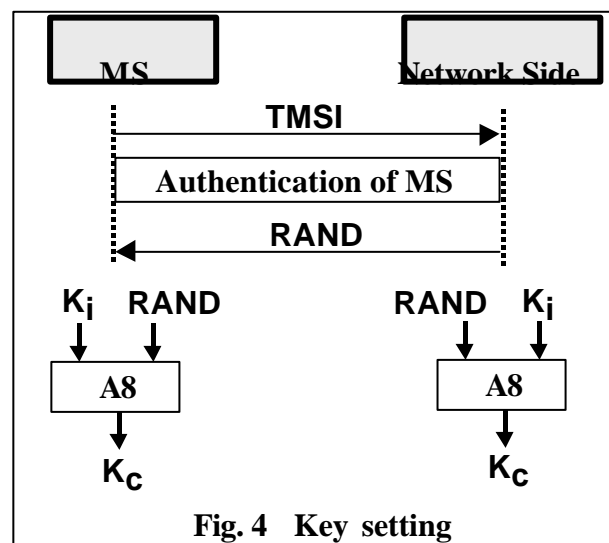
3.3 Confidentiality of Data on Communication Channels

In GSM, some signaling information elements, TMSI, connectionless user data, and user data on physical connections are considered sensitive and must be protected. The confidentiality of these data on communication channels is fulfilled with the same ciphering mechanism. In the mechanism, the algorithm A8 and A5 are used to set the ciphering key, say K_C , and encipher/decipher data with K_C , respectively.

The algorithm A5 is a two-way function which achieves the privacy of data between MS and VLR with the ciphering key K_C .

- ◆ ciphertext = A5 (K_C , cleartext)
- ◆ cleartext = A5 (K_C , ciphertext)

A5 is an unpublished algorithm and has no more than seven versions. As MS wishes to establish a connection with VLR, MS shall indicate which of the seven versions of A5 will be used. And VLR



shall compare its ciphering capabilities and preferences, and any requirement of the subscription of MS to choose a version for the connection or reject it.

The ciphering key K_C used in A5 is generated by AuC of HLR with the algorithm A8 which is a one-way function as A3. The procedure of the key generation is described as Fig. 4.

The generation of K_C is similar to $SRES$ in the authentication procedure. In fact, K_C is computed together with $SRES$, where the same random number $RAND$ is used. Thus, the security related information Sec.Rel.Info consists of $RAND$, $SRES$, and K_C . Therefore, the management of K_C is the same as $SRES$'s mentioned in the above subsection. Notice that, during a service being provided, when a handover occurs, the necessary information, e.g., K_C , is transmitted from the old base station to the new one. That is, K_C remains unchanged at handover.

Finally, we will use the example of updating MS's location to explain how to combine the procedures of identification, authentication, and ciphering. We assume that VLRo is reachable and m couples of $RAND$, $SRES$, and K_C are available for MS. The procedure is schematized in Fig. 5.

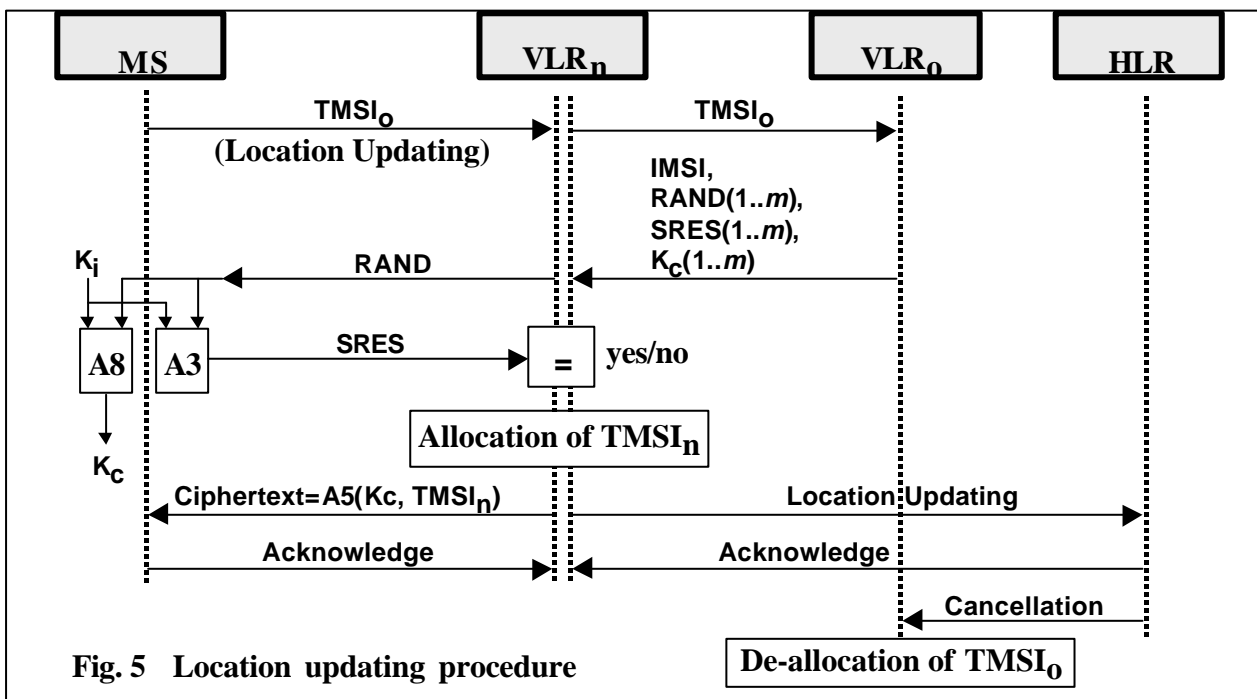


Fig. 5 Location updating procedure

4 Weakness

According to the security requirements presented in the section 2, it is obvious that GSM lacks the capabilities of authenticating VLR/HLR and supporting communication privacy between VLR and VLR/HLR. GSM considers that the network, except the interface of MSs and VLRs, is secure and all

VLRs/HLRs are trustworthy. As we have explained, these are acceptable assumptions in today's mobile telephone systems, which are homogeneous, small and only provide simple services. However, these assumptions cannot be guaranteed in a large scale and heterogeneous communication system.

Since GSM does not adopt ciphering mechanism between VLR and VLR/HLR, a eavesdropper can monitor the physical channel that connects to HLR and eavesdrop MS's location updating information and Sec.Rel.Info which contains MS's IMSI and couples of *RAND*, *SRES*, and K_c . Then, he can trace MS's position, use K_c to eavesdrop MS's communication content, and even impersonate MS to access services without the secret key K_i .

For lack of the authentication of VLR/HLR, an intruder can impersonate a pseudo-VLR. He can send wrong accounting information or wrong location updating message to HLR and confuse the management of the system. In the worst case, the whole system may be crashed. An intruder also can impersonate a pseudo-HLR. He can break all connections to the original HLR and replace his position, and the pseudo-HLR does everything arbitrarily.

Except the two main drawbacks mentioned above, some security functions implemented in GSM are also not suitable and may have potential security problems. For example, when MS wants to update the location in VLRn and VLRo is unreachable at this moment, VLRn will ask MS to directly send its IMSI to VLRn without any protection (see section 2.1). Thus, it is possible to get IMSI and identify MS. The other possible weakness of security is that all algorithms A3, A5, and A8 used in GSM are unpublished. It completely violates the design philosophy of the cryptosystem in open systems. In an open and heterogeneous system, it will be a potential risk to use an unpublished algorithm which is not verified in public.

5 Conclusions

Many security features, e.g., the authentication of end users and data ciphering, have been established in the fixed-topology and static-user computer network. However, these features were absent in traditional mobile communication systems. Since the digital mobile cellular communication systems are the infrastructure of the future personal communication services, the security is essential. In this article, we presented the security requirements of general mobile communication systems and introduced the security features provided by GSM. According the requirements, we indicate that the security functions of GSM are not enough. In order to satisfy the security requirements, today's mobile communication systems, like as GSM, need more upgrading.

References

- [1] Bennett Z. Kobb, "Personal Wireless," IEEE SPECTRUM, Jun. 1993.
- [2] M. Rahnema, "Overview of the GSM System and Protocol Architecture," IEEE Comm. Mag., Vol. 31, No. 4, Apr. 1993.
- [3] M. Mouly, M. B. Pautet, "The GSM System for Mobile Communications," ISBN: 2-9507190-0-7, 1992.
- [4] R. Molva, D. Samfat, G. Tsudik, "Authentication of Mobile Users," IEEE Network, Mar./Apr. 1994.
- [5] M. J. Beller, L. F. Chang, Y. Yacobi, "Privacy and Authentication on a portable Communications System," IEEE Journal on Selected Areas in Comm., Vol. 11, No. 6, Aug. 1993.
- [6] "GSM 03.20: Security Related Network Functions," European Telecommunications Standards Institute, Jun. 1993.
- [7] "GSM 02.09: Security Aspects," European Telecommunications Standards Institute, Jun. 1993.