# INCREASED MOBILE COMMUNICATION ENVIRONMENTS FOR GLOBAL MOBILE NETWORKS

**G.SREELAKSHMI & G. VENKATESAN**
**BHARATH UNIVERSITY, CSE DEPT, CHENNAI**
**e.sreelakshmi08@gmail.com,venkatesh.kgs@gmail.com**

**Abstract:** Many security mechanisms for mobile communications have been introduced in the literature. Among these mechanisms, a simple authentication technique for use in the global mobility network (GLOMONET) is proposed. Specifically, the wireless medium introduces new opportunities for eavesdropping of wireless data communications. Anyone with the appropriate wireless receiver can eavesdrop and this kind of eavesdropping is virtually undetectable. Global System for Mobile Communications (GSM) is a digital wireless network standard designed by standardization committees from major European telecommunications operators and manufacturers. We improve the security of the 3G protocols in network access by providing strong periodically mutual authentication, strong key agreement, and non-repudiation service in a simple and elegant way. This paper provides the first treatment of these problems in the complexity-theoretic framework of modern cryptography. Addressed in detail are two problems of the symmetric, two-party setting: mutual authentication and authenticated key exchange.

**Index Terms—Authentication, Security, cryptographic protocols, global mobility network secure mobile communication.**

## Introduction

**D**UE to the fast progress of communication technologies,many popular services have been developed to take advantage of the advanced technologies. One of these popular services is wireless communication. Ubiquitous wireless networks make it possible for distributed entities to remotely and efficiently communicate with each other anytime and anywhere, even in mobile status. The mobility network provides service for a user to communicate with other users by moving inside and around networks. In other words, the user has the capability of mobility. Here, "user" is a general term representing a human being, a terminal, a mobile equipment, and so on. There are many mobility networks that have been developed, e.g., GSM,USDC, and PDC [1]. Furthermore, Suzuki and Nakada [1] pointed out that there were many intelligent network based systems that had also been rapidly developing in order to provide more effective personal communication services, e.g., the universal personal telecommunication (UPT) and the future public land mobile

Manuscript received January 31, 2002; revised August 26, 2002; accepted September 3, 2002. The editor coordinating the review of this paper and approving it for publication is W. W. Lu.

K.-F. Hwang is with the Department of Multimedia Design, National Taichung Institute of Technology, Taichung 404, Taiwan R.O.C. (e-mail: kfhwang@ieee.org). C.-C. Chang is with the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 621, Taiwan R.O.C.(e-mail: ccc@cs.ccu.edu.tw). Digital Object Identifier 10.1109/TWC.2003.809452 telecommunication systems (FPLMTS). Suzuki and Nakada\ referred the mobility network that has the capability of global mobility as global mobility network (GLOMONET).

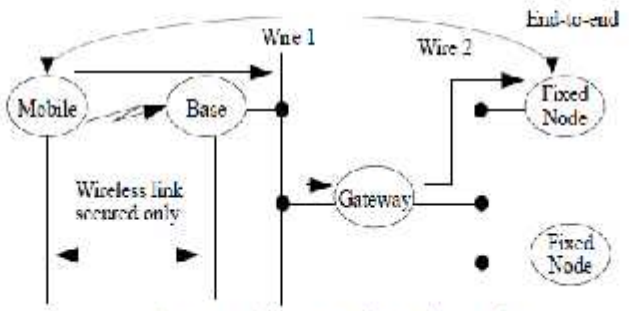


Figure 1: Link vs. End-to-end Security

The link-level security approach adopted in this design obviates the need for upgrading the software in the existing wired network. The wireless link itself is secured and thus the security of the overall network, wired plus wireless, is no less than the security of wired network alone. The link layer involves communication between two machines (or stations). The concept of users at the link layer does not make much sense, since multiple users are typically multiplexed on a
single link layer. The link layer itself is only one hop of many, in a typical wireless plus wired network. (This situation is illustrated in Figure 2).

**Services.**

The system shall provide service portability, i.e., mobile stations (MSs) or mobile phones can be used in all participating countries. The system shall offer services that exist in the wireline network as well as services speciffc to mobile communications. In addition to vehicle- mounted stations, the system shall provide service to MSs used by pedestrians and/or onboard ships.

**Quality of Services and Security.**

The quality for voice telephony of GSM shall be at least as good as the previous analog systems over the practical operating range. The system shall be capable of offering information encryption without significantly affecting the costs to users who do not require such facility.

**Radio Frequency Utilization.**

The system shall permit a high level of spectrum effciency and state-of-the-art subscriber facilities. The system shall be capable of operating in the entire allocated frequency band, and co-exist with the earlier systems in the same frequency band.

**Network.**

The identiffcation and numbering plans shall be based on relevant ITU recommendations. An international standardized signaling system shall be used for switching and mobility management. The existing xed public networks should not be signiffcantly modiffed.

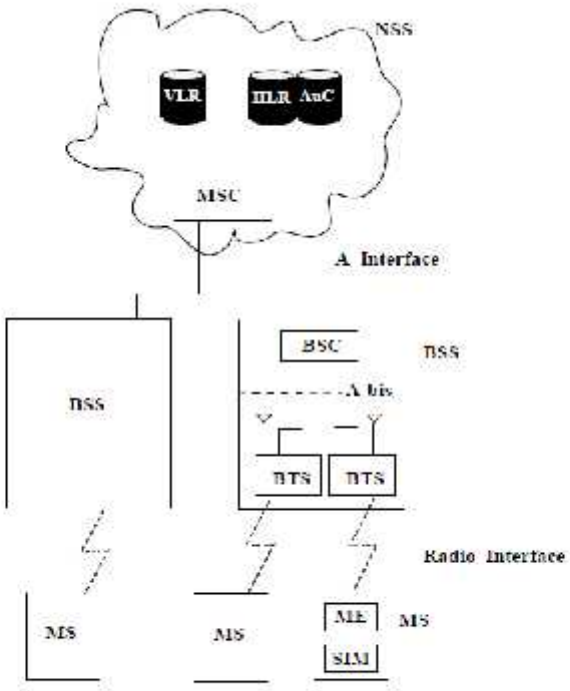


Figure 9.1: GSM Architecture

## II. REVIEW OF HWANG AND CHANG'S SCHEME

In 2003, Hwang and Chang proposed a mutual authentication scheme for mobile communications [2], which is briefly described below. First, the notation used in the scheme is defined in Table I.

The scheme consists of two protocols. The first one is described below.

**Step** (1): First, randomly generates a number , and then sends to .

**Step** (2): generates a number at random and sends and to for authentication. Here, denotes the current date and time, i.e., the timestamp.

**Step** (3): checks and to verify the legality of and Then, sends and back to .

**Step** (4): checks to judge whether is legal or not, and then takes as . sends to .

**Step** (5): checks to examine whether and are both legal or not, and then takes as . Afterward, sends to .

**Step** (6): If then is authenticated by successfully. When does not leave the service area of , it is only required for her/him to perform the second protocol with for authentication by using their common session key , where does not need to participate in the protocol.

The details of the second authentication protocol for and are described in the following.

**Step** (1): randomly generates a string and computes Then, sends to .

**Step** (2): After receiving decrypts and checks whether is a prefix of the result or not. If it is true, randomly generates a string and computes . Then, sends to .

**Step** (3): decrypts and verifies if is equal to the one in If it is true, computes and sends it to.

**Step** (4): decrypts and checks if is equal to the one it chose before. If true, and authenticate each other successfully.

Hwang and Chang's scheme is quite efficient for mobile users without impractical assumptions.

In the following, we will present a novel practical mobile authentication scheme that is much more efficient than Hwang and Chang's scheme [2] in both computation and communication under the same assumption of [2].

**III. OUR IDEA**

In Buttyan *et al.* protocol, two rounds of transmissions are needed between the user and the visited network, as well as between the visited network and the home network. Here, we propose a simpler protocol in order to reduce the number of transmission rounds. In particular, the proposed protocol is not only usable in the roaming environment, but also workable in regular communication. In other words, only one mechanism is needed and, therefore, the complexity of mobile equipment can be simplified. The idea behind the proposed scheme is quite simple. The plaintext involves a secret key, which is used to encrypt the corresponding ciphertext.This mechanism is called "self-encryption."We use this simple mechanism to accomplish our goal of simplifying the authentication protocol. At the end of
this section, we will analyze the security of the proposed scheme and compare it to Buttyan's method.

### *A. Proposed Authentication Protocol*

In the roaming environment, the visited network authenticates a roaming user through the user's home network. After certification, an authentication key is established between the roaming user and the visited network. In later communication, the visited network directly authenticates the user using the authentication key rather than authenticating it through the user's home network. In the proposed protocol, the home network maintains a long-term secret key for his client using a secret one-way function , such as , where denotes the user's
identity. Besides, without loss of generality, denotes the long-term secret key belonging to the visited network and the home network. Note that is acquired when the visited network makes contract with the home network. We describe the proposed authentication protocol for the roaming service as follows

We propose a fast mutual authentication and key exchange scheme for mobile communications. Our scheme consists of two parts and each of the two parts contains two protocols. The first part of the scheme is designed for mutual authentication between a mobile user and the system (a VLR and the HLR) where it includes two protocols. 1) An initial authentication protocol for mutual authentication and the initialization of the outer one-time secret.
2) An authentication protocol based on the outer one-time secret for the jth authentication after the most recent performance of the initial authentication protocol in this section between the user and the system where is a positive integer second part of the scheme is modified for mutual authentication between a mobile user and a VLR when the user does not leave the service area of the VLR.
The second part contains two protocols
1) An initial authentication protocol for mutual authentication and the initialization of the inner one-time secret.
2) An authentication protocol based on the inner one-time secret for the kth authentication after the most recent performance of the initial authentication protocol between the user and the VLR where a positive integer.

#### 4.1 The Initial Authentication Pr otocol for Mobile User and the System

1) Requests to be authenticated by the system at the first time.
2) The protocol of the initial authentication is not successfully finished.
The details of the initial authentication protocol are described as follows:
**Step** (1): Randomly generates a string, and then forms key and sends to VLR.
**Step** (2): After receiving the key by VLR, VLR computes it again with time stamp and sends to
**Step** (3): The HLR decrypts and checks if the key is not expired. If true, the HLR decrypts to obtain and randomly chooses three strings and re computes and then sends to VLR, where is the timestamp made by the HLR, the HLR sets and stores.
**Step** (4): VLR decrypts to obtain the key and checks if key is not expired based on the time stamp of HLR. If true, it will be sent to user.
**Step** (5): User decrypts and checks if identical to the one is produced in step1. If it is true, then it will be sent to VLR. In addition, sets and stores.
**Step** (6): Verifies whether security key identical to the one it obtained in step 4 or not. If true, then the

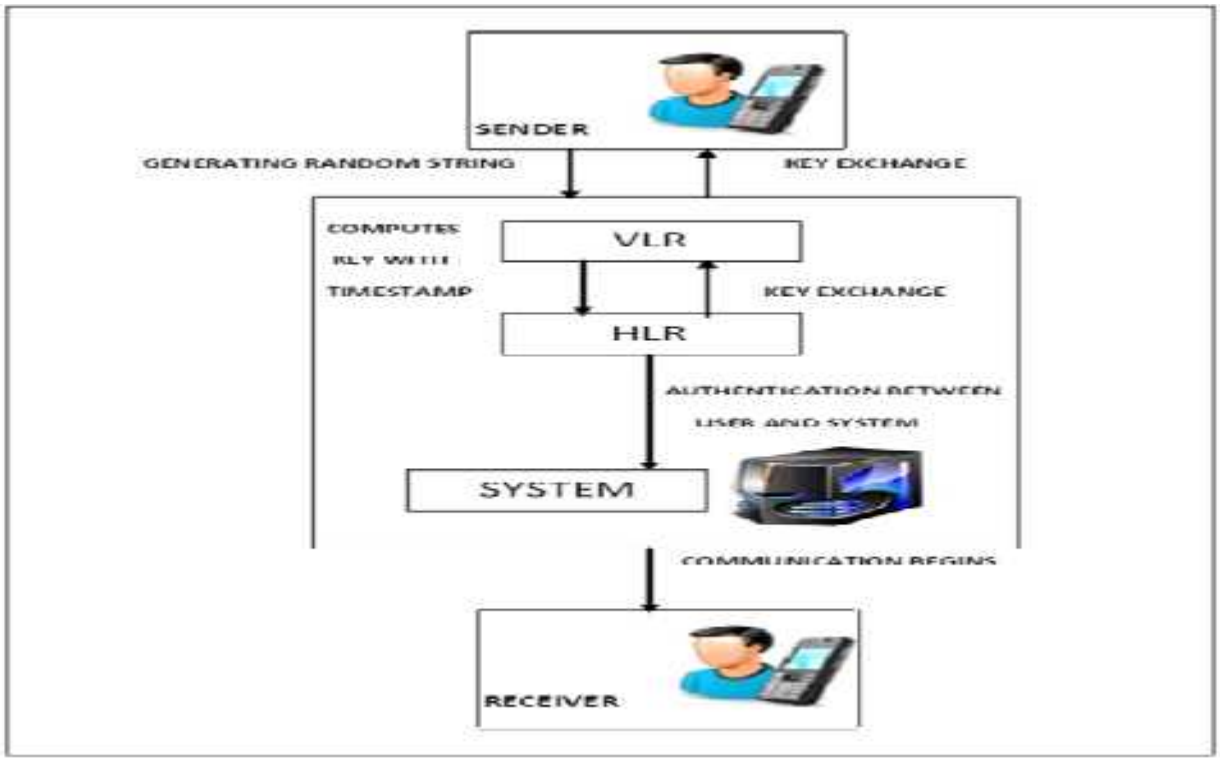


Figure 1 shows the system architecture for one time search key mechanism. The user must perform the initial authentication protocol for authentication and initializing the outer one-time secret if one of the following two conditions occurs: the HLR fails, and HLR will be discarded. The string is used as a common secret key for mutual authentication between and in the next authentication activity if the user still stays in the service area of then.

**4.2 The jth Authentication Protocol for Mobile User and the System**

User performs the protocol based on the outer one-time secret for authentication up to the user visits a new VLR and the most recent authentication between the user and the system was successfully completed. The jth mutual authentication protocol for the user and the system after the successful execution of the protocol in this section is described below, where j is a positive integer. The initial value of j is reset to 1 whenever the previous round of authentication was successfully completed through performing the protocol of this section.

**Step** (0): The jth authentication process begins.

**Step** (1): User randomly generates two strings for example x and y the two strings are computes. Then, sends to VLR which is the current VLR visited by user.

**Step** (2): After receiving the randomly generated key the VLR computes the key along with the timestamp and sends to the HLR, where is the timestamp made by VLR.

**Step** (3): The HLR decrypts and checks if is not expired. The HLR decrypts to obtain the two strings x and y and then HLR retrieves according to where the timestamp made by HLR. HLR deletes and stores.

**Step** (4): VLR decrypts and then checks and sends to user.

**Step** (5): User checks if identical to the one is produced in **Step** (1). If it is true and the system have

mutually authenticated each other successfully deletes and stores, i.e., the new value

of the outer one-time secret. Besides, and take as the session key for secure communication in this session. The string is used as a common secret key for mutual authentication between and in the next authentication activity if still stays in the service area of then.

**Step** (6): The jth authentication process ends. If wants to perform the above protocol for the next round of mutual authentication between the system and user, user again want to set j=j+1 and goes to **Step** (0).

### 4.3 The Initial Authentication Protocol for User and the Current VLR

User performs the protocol for mutual authentication with the current VLR and initializes an inner one-time secret for roaming services with the VLR when one of the following two conditions occurs:

1) The most recent authentication is successfully finished by performing the protocol of this section and user should stay in same service area of the current VLR.

2) The protocol of this section is not successfully finished, and does not leave the service area of the current VLR. The details of the initial authentication protocol for user and the current VLR are described as follows.

**Step** (1): Randomly generates a string she/he computes and sends to VLR.

**Step** (2): VLR decrypts by using the common secret key to get. It randomly chooses two strings
and then computes and sends to HLR.

**Step** (3): After decrypting obtains the key and she/he checks if is equal to the one produced in
step 1. If the key is true, then it will be sent to VLR.

**Step** (4): VLR gets and checks if the key is equal to the one that it has chosen. If true, authentication is successfully made between each other and shares an initial common one-time secret along with a session key successfully.

### 4.4 The kth Authentication Protocol for User and the Current VLR

User performs the protocol based on the inner one-time secret for mutual authentication as long
as does not leave the service area of the current VLR and the most recent authentication was successfully finished via the protocol of this section. The kth mutual authentication protocol for
the user and the current VLR after successful execution of the protocol in this section is described below. The initial value is reset to 1 whenever the most recent authentication was successfully completed through performing the protocol this section.

**Step** (0): The kth authentication process begins.

**Step** (1): Randomly chooses a string and computes and then sends to VLR.

**Step** (2): After decrypting gets and it checks if is equal to VLR timestamp. If it is true, sends to and then deletes and stores.

**Step** (3): HLR gets and checks if it is equal to the one produced in step1. If true, and authenticate each other and share a session key successfully deletes and stores.

**Step** (4): The kth authentication process ends. If user wants to perform the next round of authentication process, she/he sets k=k+1 and goes to **Step** (0).

Finally, the proposed scheme integrated into a complete and fast authentication scheme for mobile communication.

## 5. EXPERIMENTAL RESULT

Mobile subscriber MS is to be authenticated to the HLR via the VLR, using his/her password. KHLR is the public key of the HLR known to all parties, and K VLR is the symmetric encryption key shared between the VLR and HLR. The main difference between the proposed protocol and the current GSM authentication protocol regarding the protocol performance is the use of the public key operations. In the novel authentication mechanism, called the one-time secret key mechanism, the cost of encryption is about 30-33 times less than the cost of existing systems. The current protocol is designed

| | Existed System | Proposed Scheme | Difference |
|---|---|---|---|
| **For Each User** | | | |
| Generating Random Strings | 1280 b | 512 b | 768 b |
| Hashing Process | 0 | 256 b | 256 b |
| Encryption & Decryption | 256 b | 256 b | 0 |
| Communication Cost | 1536 b | 1024 b | Reduced by 512 b |
| **For Entire Protocol** | | | |
| Generating Random Strings | 512 b | 256 b | 256 b |
| Hashing Process | 0 | 512 b | 512 b |
| Encryption & Decryption | 3960 b | 3568 b | 392 b |
| Computational Cost | 4472 b | 4336 b | Reduced by 136 b |

Table.1 Comparisons of Existed System and Proposed Solution Based on Memory Usage.

In the table 1, the usage of the memory for various purposes such as generating random strings, hashing process, encryption and decryption is compared between the existing system and proposed scheme, which describes that the existing system using more memory size for the key exchange process, it leads to high computational and communication cost where as in proposed scheme usage of the memory is minimized and the communication and computational cost reduced. Thus, the proposed scheme is more secure in authentication process and also at very efficient cost.

**CONCLUSION**

In this paper, a simple authentication technique for use in the GLOMONET has been proposed. This technique introduces a quite simple mechanism called "self-encryption" to simplify the authentication protocol. The comparisons show that not only the proposed protocol is simpler than Buttyan *et al.* protocol, but it is also easier to implement. Our main contributions in this paper are the enhancements on the authentication and key agreement protocol in the 3G network access security. To understand the basis of our enhancements, we provide an evolutionary and comparative study of this protocol in two most popular 3G cellular systems, UMTS and cdma2000. The approaches adopted by the two 3G front runners aim to solve the 2G security problems and satisfy the higher 3G security requirements.

Specifically, UMTS uses a sequence number approach to provide network authentication, a feature not in 2G. Cdma 2000 has approved the adoption of the same technique. The sequence number record keeping and management complicate the already complex 3G implementation. In summary, we have achieved the main goal of this work, the fact that a more complex mobile equipment is unnecessary in order to provide both the roaming service and the secure teleconference service. In addition, we believe that the self-encryption mechanism can find a wide application more than roaming and teleconference services.

**REFERENCES**

[1] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," *IEEE J. Select. Areas Commun.*, vol. 15, pp. 1608–1617, Oct. 1997.

[2] T. Pfeifer and R. Popescu-Zeletin, "A modular location-aware service and application platform," in *Proc. IEEE Int. Symp. Computers and Communications*, Sharm El Sheikh, Egypt, 1999, pp. 137–148.

[3] Al-Muhtadi, J., Mickunas, D., and Campbell, R. "A
Lightweight Reconfigurable Security Mechanism for 3G/4G Mobile Devices". IEEE Communications Magazine. vol 40. no. 10. April 2002.

[4] 3GPP TS 21.133. "3GPP: Technical Specification Group services and System Aspects; 3G Security; Security Threats and Requirements".

[5] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22:644-654, 1976

[6] RSA Data Security, Inc. PKCS #1 -- #10, June 1991