Tenable Mutual Authentication and Key Exchange Using Cryptography

Thirupurasundari D R[1] and Dr.A.Sivabalan[2]

[1,2]*Computer Science and Engineering, Anna University*
[1,2]*S.M.K Fomra Institute of Technology, Chennai, India*
[1]*tpsdr@yahoo.com* [2]*sivabalan.a@gmail.com*

***Abstract*— Most of current authentication schemes for mobile systems have some weaknesses. This paper proposes a secure authentication mechanism for mobile communication. There are many security mechanisms for mobile communications. Among these mechanisms, authentication plays a quite important role in the entire mobile network system and acts as the first defence against attackers. In this paper, we come up with a novel authentication mechanism, called the *nested one-time secret* mechanism, tailored for mobile communication environments. Through maintaining inner and outer synchronously changeable common secrets, respectively, every mobile user can be rapidly authenticated by visited location register (VLR) and home location register (HLR), respectively, in the proposed scheme. Not only does the proposed solution achieve mutual authentication, but it also greatly reduces the computation and communication cost of the mobile users as compared to the existing authentication schemes. Therefore, in order to guarantee the quality of this advanced service, an efficient and secure authentication scheme is urgently desired.**

***Keywords*—** Authentication**, mutual authentication, nested onetime secrets, secure mobile communication**

I. INTRODUCTION

In recent years, due to technology advances, we have seen a phenomenal increase in the number of cellular users. As the demand increases, so does the importance of security in the cellular systems. To provide protection, many different security areas are addressed, e.g., network access security provides users with secure access to the mobile services, network domain security provides secure exchanges of signaling data in the core network, application domain security provides users and providers with secure exchanges of application data, etc. Our emphasis in this paper is in the area of network access security.

Seamless inter-network operation is highly desirable to mobile users, and security such as authentication of mobile stations is challenging in this type of networks. A mobile station (MS) out of its home network needs to be authenticated to be allowed to access a visited network; however, in general there is no trusted authentication server available to the MS out of its home network.

Security, Authentication, Encryption and Access Control are vital features that must be presented in any communication network. One of the principal reasons that security is such a significant issue in cellular system because they rely on radio waves to carry communications. These radio waves are not restricted by walls or physical boundaries, but rather they are designed to cover, as large as possible wireless cell. However, because the radio waves are so exposed and available, they can be intercepted or jammed by anyone who is within range. Security has always been an issue for mobile communication networks. First generation analogue phones were susceptible to user traffic eavesdropping and cloning whereby fraudsters were able to change the identity of mobiles so that calls could be charged to another customer’s account.

Against this background, second generation system such as General system for Mobile communications (GSM) were developed. GSM was the first public telephone system to introduce integrated cryptographic mechanisms for authentication and confidentially. These mechanisms have been extremely effective in eliminating technical fraud due to cloning and have provided good protection against user traffic eavesdropping. GSM implements security features, which ensure physical security, data security, user authentication, and user anonymity. However, GSM suffers from security problems such as weak authentication and encryption algorithms, short secret key length (only 32 bits) with no network authentication.

This has lead to false base station attack and lack of data integrity, allowing denial of service attacks, limited encryption scope and insecure key transmission.

All security mechanisms in the GSM-based systems, authentication schemes are key techniques to ensure the correctness of the identities of all communication entities before they are about to perform other communication activities. These schemes form robust defenses to withstand the replay attack and the impersonating attack in the GSM system. Several authentication protocols have been introduced in the literature. In 1997, Suzuki and Nakada [7] proposed an authentication protocol for the global mobility network.

However, Buttyan *et al.* [9] pointed out that Suzuki and Nakada's protocol has some weaknesses, and they proposed an improved scheme based on Suzuki and Nakada's protocol to eliminate the weaknesses.

In 2003, Hwang and Chang [10] proposed a mutual authentication mechanism for mobile communications, which is more efficient than the previous scheme of [9]. In 2005, Chang *et al.* [14] proposed an efficient GSM authentication protocol. In 2006, the protocols [18], [19] based on elliptic curve cryptography were proposed. These protocols [14], [18], [19] are based on timestamps, so they are more efficient than Hwang and Chang's scheme [10]. However, the protocols of [14], [18], and [19] must be under the assumption that the clocks of each mobile user and the system are synchronized and the transmission time between them is stable. In fact, it is difficult to satisfy the above assumption in current mobile communication environments. In 2007 and 2008, some schemes [15]–[17] were proposed. They are all based on asymmetric cryptosystems, which are less efficient than symmetric ones, where the scheme of [15] also requires the above assumption, i.e., clock synchronization and stable transmission time.

In the 3rd Generation Partnership Project (3GPP) authentication and key agreement protocol [20], it has to be assumed that there exists a secure channel between each visited location register (VLR) and home location register (HLR). Besides, in the protocol of [20], HLR transfers a long sequence of authentication vectors to a VLR in the first round of authentication for each mobile user, where the VLR must store these vectors. The vectors will be discarded whenever the corresponding mobile user visits a new VLR, which will waste the resources and increase the computation and communication cost for the system. Accordingly, among these proposed authentication protocols [7], [9], [10], [14]–[20], the scheme of [10] is the most efficient and practical one for GSM-based systems.

We make deep research on the performance of secure mutual authentication schemes and come up with an efficient solution to further simplify and speed up the authentication processes through synchronously changeable secrets, which form a nested structure (containing an outer one-time secret and an inner one), shared by each mobile user and the system. The outer one-time secret is a temporal common key of the user and the HLR for initial authentication or authentication when the user roams around the service area of a new VLR. The inner one-time secret is shared by the user and some VLR for mutual authentication between the user and the same VLR. Compared to Hwang and Chang's scheme of [10], the proposed scheme greatly reduces the computation cost required for each mobile user

II RELATED WORK

Extension of Authentication and Key Agreement Protocol (AKA) for Universal Mobile Telecommunication System (UMTS):

The current 3GPP authentication and key agreement protocol (AKA) has some shortcomings such as the bandwidth consumption between visitor serving network and home network, the delay time that incurred from generated authentication vector in home network, waste of storage space in VLR to store authentication vectors and the management of sequence number which needed for synchronization between mobile station and its home network. This paper proposes a new protocol as an extension for the 3GPP AKA to eliminate the 3GPP AKA shortcomings by using temporary security key

An Efficient Mobile Authentication Scheme for Wireless Networks

In this paper, an efficient authentication scheme is proposed which is suitable for low-power mobile devices. It uses an elliptic-curve-cryptosystem based trust delegation mechanism to generate a delegation passcode for mobile station authentication, and it can effectively defend all known attacks to mobile networks including the denial-of-service attack. Moreover, the mobile station only needs to receive one message and send one message to authenticate itself to a visitor's location register, and the scheme only requires a single elliptic-curve scalar point multiplication on a mobile device. Therefore, this scheme enjoys both computation efficiency and communication efficiency as compared to known mobile authentication schemes.

On the Security of Wireless Network Access with Enhancements

The security of the current 3G wireless protocols addresses the problems faced by the 2G systems, in addition to fulfilling the higher 3G security requirements mandated from operating in IP networks as well as voice networks. However, the approach adopted by the two most popular 3G mobile system forerunners, UMTS and cdma2000, leaves many areas for improvement. In this paper, the authors Lein Harn and Wen-Jung Hsin provide algorithms to 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.

A New Hybrid Approach of Symmetric/ Asymmetric Authentication Protocol for Future Mobile Networks

Most of current authentication schemes for mobile systems have some weaknesses; such as leakage of UE identities and high update overhead of temporary identities. This paper proposes a secure authentication mechanism for mobile communication systems that satisfies the security requirements of the third generation mobile systems. In this proposed protocol, the number of messages between authentication entities of the network is reduced to four messages instead of five in initial authentication procedure. The subsequent authentication procedure only contains two message exchanges. Therefore, the bottleneck at authentication center is avoided by reducing the number of messages between mobile and authentication center. The authentication time delay, call setup time and signaling traffic are minimized. Also, this proposed protocol is designed to be secure against network attacks, such as replay attacks and Guessing attacks and others attacks. Consequently, this approach is secure and practical as it can satisfy the security requirements of the third generation mobile communication systems based on hybrid asymmetric and symmetric cryptosystem, and can save up to 20% of the authentication traffic delay time.

III. OUR IDEA

In this section, we will introduce our basic idea that is the underlying foundation for the construction of the proposed authentication scheme in mobile environments.

A. An Efficient Hybrid Mechanism for Mutual Authentication

With a pre shared secret key, there are two basic approaches to achieve mutual authentication between two entities, say Alice and Bob. One is the timestamp-based approach, and the other is the nonce-based approach.

Time stamp based Approach

In this approach, Alice prepares a request message Request with the current timestamp TA and sends to Bob, where Ek(Request, timestamp) is a symmetric encryption algorithm with key K . After receiving Ek(Request, timestamp), Bob decrypts it and then Obtains (Request, timestamp). If the difference between the current time in Bob's computer and TA is not greater than the maximal transmission time from Alice to Bob, i.e., is still fresh, then Bob believes that Ek (Request, timestamp) is produced by Alice in this session, and thus Bob authenticates Alice. Similarly, Bob can be authenticated by Alice as long as he can send a correct and fresh to Alice.

The assumptions of a timestamp-based authentication scheme:

- ➢ The clocks of Alice and Bob must be synchronous.
- ➢ The transmission time for the authentication message transmitted from Alice to Bob (or from Bob to Alice) must be stable.

The advantages of a timestamp-based authentication scheme:

- ➢ The protocol only requires two rounds of transmission to reach the goal of mutual authentication.
- ➢ It is efficient in computation and communication.

Demerits of Timestamp Approach:

Although timestamp-based authentication schemes are simple and efficient, the above two constraints make them impractical in the Internet and mobile environments since most of the users' clocks are not synchronous with the server's or system's clocks and the transmission time is usually not stable.

NONCE based Mutual Authentication Scheme:

In a nonce-based mutual authentication scheme, Alice prepares a request message Request and a randomly chosen string Na, and then sends to Bob Ek (Request, Na), where Na is called a nonce produced by Alice.

After receiving Ek (Request, Na), Bob decrypts it to obtain (Request, Na). Bob prepares a response message ResponseB and a randomly chosen string Nb, and then sends to Alice Ek(ResponseB, Nb) , where Nb is said to be a nonce produced by Bob. Alice decrypts Ek (ResponseB, Nb) to obtain (ResponseB, Nb) and checks if is identical to the one she chosen before. If true, Alice believes that is produced by Bob in this session, and thus Alice authenticates Bob. Similarly, Alice forms a response message and then sends to Bob. Bob decrypts to obtain and verifies if is equal to the one he chose before. If true, Bob believes that is produced by Alice in this session, and thus Bob authenticates Alice.

A nonce-based authentication scheme is free from the two constraints required in a timestamp-based authentication scheme, but the performance may be a problem in the nonce-based scheme as compared to the timestamp-based one.

The advantages of a nonce-based authentication scheme:

- ➢ It is not necessary to synchronize the clocks of Alice and Bob.
- ➢ The transmission time for the authentication message transmitted from Alice to Bob (or from Bob to Alice) can be unstable.

Demerits of Nonce-based authentication scheme:

- The protocol requires three rounds of transmission to reach the goal of mutual authentication.
- The scheme is less efficient than a timestamp-based authentication scheme in computation and communication.

In the GSM system, two authentication actions must be performed, i.e., the mutual authentication between a VLR and the HLR and the mutual authentication between the system (VLR and HLR) and each user. In order to guarantee the quality of mobile communication, the authentication mechanisms I adopt should be as efficient as possible.

Each VLR and the HLR are both located in the interior wired network of the GSM system, so they can authenticate each other through the timestamp-based authentication mechanism without suffering from the problem of clock synchronization. Since the clocks of each VLR and the HLR can be easily synchronized and the time consumed by transmitting a message between them is stable, I can make use of the timestamp-based solution to build up the mutual authentication protocol between each VLR and the HLR. It is also shown in the system part of Figs. 1 or 2. On the other hand, it is difficult to synchronize the clocks of the system (VLRs and the HLR) and all mobile users.

Hence, I cannot utilize the timestamp-based solution to construct the authentication protocol between the system and every mobile user even though the solution is the most efficient one among the three authentication mechanisms. Owing to the assumption of the mechanism based on one-time secrets, it cannot form the authentication protocol for the initial authentication between the system and each mobile user. Thus, I adopt the nonce-based mechanism to establish the authentication protocol for the initial authentication between the system and every user (shown in Fig. 1), and the following authentication processes will be accomplished through the technique of one-time secrets (shown in Fig. 2)

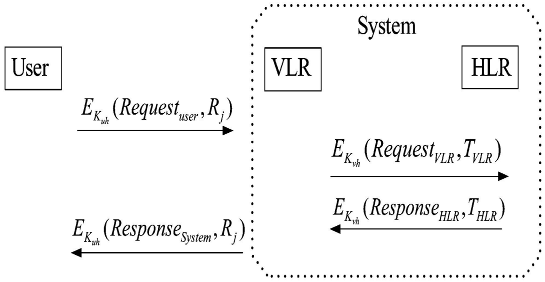
System
User
VLR
HLR
$E_{K_{uh}}(Request_{user}, R_j)$
$E_{K_{vh}}(Request_{VLR}, T_{VLR})$
$E_{K_{vh}}(Response_{HLR}, T_{HLR})$
$E_{K_{uh}}(Response_{System}, R_j)$

Fig.1. Idea for the initial authentication between a mobile user and the system (VLR and HLR).

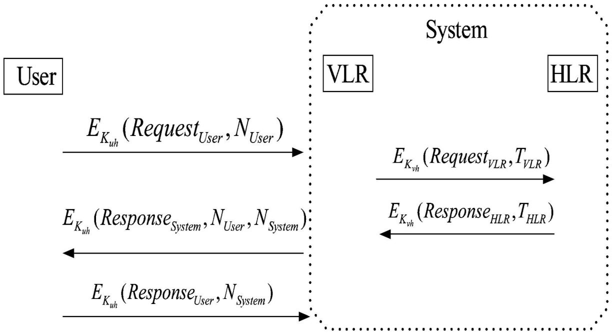
System
User
VLR
HLR
$E_{K_{uh}}(Request_{User}, N_{User})$
$E_{K_{vh}}(Request_{VLR}, T_{VLR})$
$E_{K_{uh}}(Response_{System}, N_{User}, N_{System})$
$E_{K_{vh}}(Response_{HLR}, T_{HLR})$
$E_{K_{uh}}(Response_{User}, N_{System})$

Fig. 2. Idea for the jth authentication between a mobile user and the system (VLR and HLR) after the initial one, where j>1.

B. Nested One-Time Secret Mechanisms

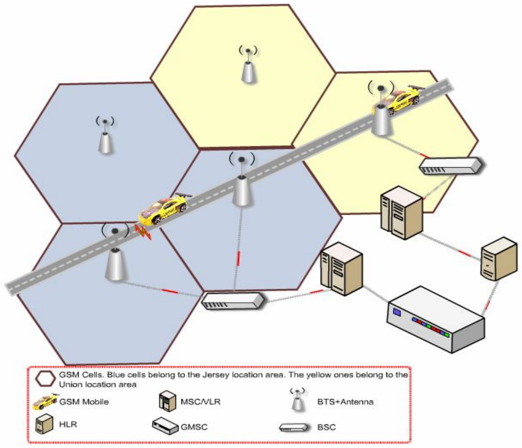
GSM Cells. Blue cells belong to the Jersey location area. The yellow ones belong to the Union location area
GSM Mobile
MSC/VLR
BTS+Antenna
HLR
GMSC
BSC

Fig 3 System Architecture

Consider a sequence of mutual authentication processes based on our proposed hybrid mechanism between mobile user and the system (a VLR and the HLR). In the initial authentication, the user and the system authenticate each other by performing a nonce-based authentication protocol, and then they negotiate an initial value of a one-time secret. Thus, they make use of the one-time secret, called the *outer* one-time secret, to complete the following authentication processes.

In fact, the cost of the authentication can be further reduced again if the user does not leave the service area of the current VLR. In this case, the user performs an initial mutual authentication protocol with the VLR only, and they set an initial value of another one-time secret, called the *inner* one-time secret, shared by them. They can perform the following authentication actions via the inner one-time secret until the user leaves the service area of the VLR. Once the user enters the service area of another VLR, the outer one-time secret will be resumed to serve as the key parameter for the next round of authentication between the user and the system.

In the proposed idea, mobile user shares the outer one-time secret with the HLR and shares the inner one-time secret with the current VLR. This is referred to as the *nested* one-time secret mechanism.

IV PROPOSED SYSTEM

Based on the ideas introduced, 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 or re- initialization of the outer one-time secret; and 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 between the user and the system where j is a positive integer. The second part of the scheme is tailored for mutual authentication between a mobile user and a VLR when the user does not leave the service area of the VLR. Similarly, the second part contains two protocols: 1) an initial authentication protocol for mutual authentication and the initialization or reinitialization of the inner one-time secret; and 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 in between the user and the VLR where $k$is a positive integer

The initial authentication protocol for the user and the system is based on nonces. In addition to the functionality of mutual authentication, the initial authentication protocol can initialize or reinitialize a new value of a common one-time secret, i.e., the outer one-time secret, between the user and the system for the next authentication.

Once the outer one-time secret has been shared by the system and the mobile user, they can perform the first mutual authentication based on the secret and also negotiate a new value of the secret for the next authentication. The jth authentication based on the outer one-time secret can be performed as long as the (j – 1)th authentication is successfully finished, where (j $\geq$ 2). Especially, if the user stays in the same service area of the same VLR, the following authentication processes can be simplified as an initial authentication process and a sequence of authentication processes based on the inner one-time secret between the user and the VLR only. The details of the four protocols are described in the following four subsections, respectively. First, we define some notation in Table I.

Besides, according to the specification of Advanced Encryption Standard (AES) [21], which is the current standard of symmetric cryptosystems, we define that the key length of every encryption/decryption key in the proposed scheme is 256 bits, which will generate a large enough key space containing 2^{256} possible key values.

TABLE I - DEFINITION OF NOTATION IN THE PROPOSED SYSTEM

Notation	Definition
U_i	the identity of user i
V_c	the identity of some VLR c
K_{uh}	a common secret key kept by U_i and the HLR
K_{vh}	a common secret key kept by V_c and the HLR
E_{K_x}	a symmetric encryption function with a secret key K_x
F_K	a one-way function with key K
Sync	the signal for the request of synchronization with authentication produced by U_i

V MODULE DESCRIPTION

A. The Initial Authentication Protocol for Mobile User and the System

B. The jth Authentication Protocol for Mobile User and the System

C. The Initial Authentication Protocol for User and the Current VLR

D. The kth Authentication Protocol for User and the Current VLR

The Initial Authentication Protocol for Mobile User and the System

User Ui must perform the initial authentication protocol for authentication and initializing the outer one-time secret if one of the following two conditions occurs:

- ➢ Ui requests to be authenticated by the system at the first time.
- ➢ The initial authentication protocol for mobile user Ui and the system are the jth authentication protocol for mobile user Ui and the system is not successfully finished.

The jth authentication protocol for a user Ui and the system

User Ui performs the protocol based on the outer one-time secret for authentication as long as Ui 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 the initial authentication protocol for mobile user and the system are 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 the initial authentication protocol for mobile user Ui and the system.

The Initial Authentication protocol for User Ui and the Current VLR

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

- ➢ The most recent authentication is successfully finished by performing the protocol of the initial authentication protocol for mobile user and the system or the jth authentication protocol for mobile user and the system, and user does not leave the service area of the current VLR.
- ➢ The protocol of the initial authentication protocol for user and the current VLR or The jth authentication protocol for user and the current VLR is not successfully finished, and does not leave the service area of the current VLR.

The kth Authentication Protocol for User and the Current VLR

User Ui performs the protocol based on the inner one-time secret for mutual authentication as long as Ui does not leave the service area of the current VLR and the most recent authentication was successfully finished via the protocol of the initial authentication protocol for user and the current VLR or the jth authentication protocol for the user and the current VLR.

The kth mutual authentication protocol for the user and the current VLR after the successful execution of the protocol in the initial authentication protocol for user and the current VLR, where k is a positive integer. The initial value k of is reset to 1 whenever the most recent authentication was successfully completed through performing the protocol of the initial authentication protocol for user Ui and the current VLR.

ALGORITHM FOR USER*:*

```
Step1 : Start
Step 2 : Generate a string
Step 3 : Encrypt the string
Step 4 : Send(encrypted data, My id,current time) to VLR
Step 5 : Wait for response
Step 6 : If response received goto step 7 Else goto step 5:
Step 7 : Decrypt data check string value if equal go to step 8: Else goto step2 :
Step 8 : Send decrypted (x) to VLR set R0= r
Step 9 : Wait for authentication
Step 10 :If authentication = true  decrypted w  is mutual authentication key  Else goto step 2:
```

ALGORITHM FOR VLR

```
Step1 : Start
Step2 : Wait for Request signal  or authenticate signal
Step3 : If request received  goto step 4 else if authenticate received goto step7 else if Authentication key received from user goto step 5 else goto step2
Step4 : Check time stamp If time stamp=equal go to step5 : Else goto step 1
Step5:  encrypt request data
Step 6: send (encrypted request,VLR id,time stamp) Goto step 2
Step 7: Decrypt data obtain x,y,w ,timestamp ,d check time  stamp If time stamp=equal go to step 8  Else goto step 1
Step8 : Send data to mobile user
Step9 : Check x with decrypted x value from HLR If (equal ) send authentication to user Else Discard user and gotostep 2
```

ALGORITHM OF HLR:

```
Step1: Start
Step2: wait for request
Step3: decrypt data
Step4: check for time stamp & VLR ID
Step 5: if true goto step 6 Else goto step 2
Step 6:Decrypt user data check user ID
Step 7:if true goto step 8:Else goto step2 Choose
    x,y,w Encrypt (user string-1,x,y,w)
    Encrypt(x,y,w,timestamp,(Encrypt (user
    string-1,x,y,w))
Step8: Encrypt(x,y,w,timestamp,(Encrypt (user string-
     1,x,y,w))) to Corresponding VLR Goto Step2
```

The four protocols of the two parts proposed in, respectively, are integrated into a complete and fast authentication scheme for mobile communication. Fig. 4 illustrates the execution order and the relationship of the four proposed protocols in the proposed scheme.

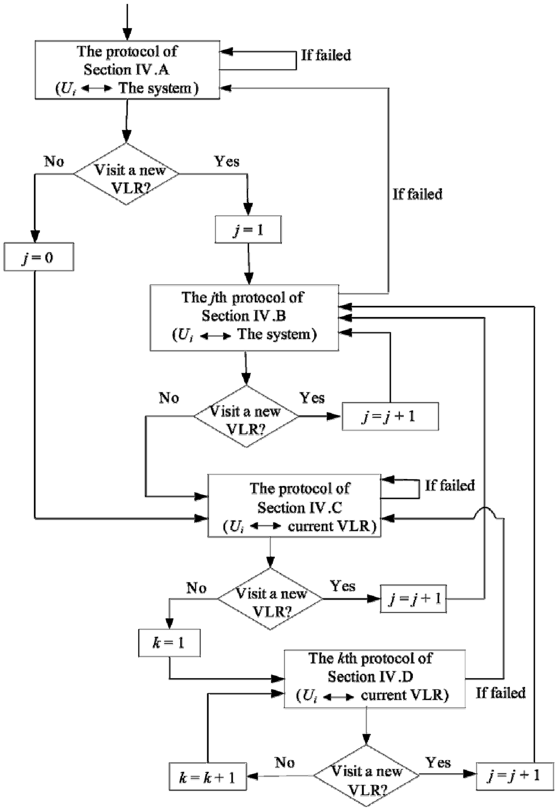
The protocol of Section IV.A (U_i ↔ The system)
If failed
No
Visit a new VLR?
Yes
If failed
$j = 1$
$j = 0$
The jth protocol of Section IV.B (U_i ↔ The system)
No
Visit a new VLR?
Yes
$j = j + 1$
The protocol of Section IV.C (U_i ↔ current VLR)
If failed
No
Visit a new VLR?
Yes
$j = j + 1$
$k = 1$
The kth protocol of Section IV.D (U_i ↔ current VLR)
If failed
$k = k + 1$
No
Visit a new VLR?
Yes
$j = j + 1$

Fig . 4 The execution order and the relationship of the four proposed protocols

VI CONCLUSIONS

We have proposed a secure mutual authentication and key ex- change scheme for mobile communications based on a novel mechanism, i.e., nested one-time secrets. The proposed scheme can withstand the replay attack and the impersonating attack on mobile communications and speed up authentication. Compared to Hwang and Chang's scheme, proposed protocol fulfils the security requirements of the third generation mobile systems and improves the performance by reducing the communication times, and by creating fewer authentication messages and data sizes during the process of authentication. Analysis of our protocol showed that it can not only overcome the security flaws existing in some recently proposed protocols, but also satisfy the asymmetric wireless computing conditions.

In addition, this proposed authentication scheme does not only protect user data, but also it prevents many kinds of attacks such as the replay attacks and Guessing attacks. In short, the proposed authentication protocol satisfies the security requirements of the third generation mobile communication systems. Moreover, testing has proven that this protocol is efficient and robust.

REFERENCES

[1]. Chun-I Fan, Pei-Hsiu Ho, and Ruei-Hau Hsu, " Provably Secure Nested One Time Secret Mechanism for Fast Mutual Authentication and Key Exchange in Mobile Communications" in IEEE/ACM Transactions on Networking, Vol.18,NO.3,JUNE 2010

[2]. Brown, "Techniques for privacy and authentication impersonal communication systems," IEEE Personal Commun., vol. 2, no. 4, pp. 6–10, Aug. 1995.

[3]. N. Jefferies, "Security in third-generation mobile systems," *IEE Coll. Security Netw.*, pp. 8/1–8/5, 1995.

[4]. M. Rahnema, "Overview of the GSM system and protocol architecture," *IEEE Commun. Mag.*, vol. 31, no. 4, pp. 92–100, Apr. 1993.

[5]. B. Mallinder, "An overview of the GSM system," in *Proc. 3rd Nordic Seminar Digital Land Mobile Radio Commun.*, Copenhagen, Denmark, 1998, pp. 12–15.

[6]. A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," *IEEE Personal Commun.*, vol. 1, no. 1, pp. 24–31, 1993.

[7]. M. S. Hwang, Y. L. Tang, and C. C. Lee, "An efficient authentication protocol for GSM networks," in *Proc. AFCEA/IEEE Euro-Comm*,2000, pp. 326–329.

[8]. S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," *IEEEJ. Sel. Areas Commun*, vol. 15, no. 8, pp. 1608–1617, Oct. 1997.

[9]. C. H. Lee, M. S. Hwang, and W. P. Yang, "Enhanced privacy and authentication for the global system for mobile communications," *Wireless Netw.*, vol. 5, no. 4, pp. 231–243, 1999.

[10]. L. Buttyan, C. Gbaguidi, S. Staamann, and U. Wilhelm, "Extensions to an authentication technique proposed for the global mobility network,"*IEEE Trans. Commun.*, vol. 48, no. 3, pp. 373–376, Mar., 2000.

[11]. K. F. Hwang and C. C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," *IEEE Trans.Wireless Commun.*, vol. 2, no. 2, pp. 400–407, Mar. 2003.

[12]. C. C. Lee, M. S. Hwang, and W. P. Yang, "Extension of authentication protocol for GSM," *IEE Proc., Commun*, vol. 150, no. 2, pp. 91–95, 2003.

[13]. L. Harn and W. J. Hsin, "On the security of wireless network access with enhancements," in *Proc. ACM Workshop Wireless Security*, 2003, pp. 88–95.

[14]. Peinado, "Privacy and authentication protocol providing anonymous channels in GSM," *Comput. Commun.*, vol. 27, no. 17, pp. 1709–1715, 2004.

[15]. C. Chang, J. S. Lee, and Y. F. Chang, "Efficient authentication protocol of GSM," *Comput. Commun.*, vol. 28, no. 8, pp. 921–928, 2005.

[16]. Tang and D. O. Wu, "An efficient mobile authentication scheme for wireless networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1408–1416, Apr. 2008.

[17]. M. Al-Fayoumi, S. Nashwan, S. Yousef, and A. R. Alzoubaidi, "A new hybrid approach of symmetric/asymmetric authentication protocol for future mobile networks," in *Proc. Wireless Mobile Comput, Netw. Commun*, 2007, pp. 29–29.