# Provably Protected Nested One-Time Secret Mechanisms for Rapid Mutual Certification and Key Swap in Mobile Interactions

**N.Mahesh[1], K.Subba Reddy[2], P.V.Ravikanth[3]**
M.Tech Student[1], Professor[2], Asst. Professor[3]
Prakasam Engineering College[#1 #2], Malineni Engineering College[#3]
Andhra Pradesh, India.

## Abstract
Many security mechanisms for mobile interactions have been introduced in the literature. Among these mechanisms, certification plays a quite important role in the entire mobile network system and acts as the first defense against attackers since it ensures the correctness of the identities of distributed interaction entities before they engage in any other interaction activity. Therefore, in order to guarantee the quality of this advanced service, an efficient (especially user-efficient) and protected certification scheme is urgently desired. In this paper, we come up with a novel certification mechanism, called the nested one-time secret mechanism, tailored for mobile interaction 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 certification, but it also greatly reduces the computation and interaction cost of the mobile users as compared to the existing certification schemes. Finally, the security of the Proposed scheme will be demonstrated by formal proofs.

**Index Terms**—Information security, mutual certification, one time secrets, protected mobile interaction.

## I. Introduction
DUE to the Rapid progress of interaction technologies, many popular services have been developed to take advantage of the advanced technologies. One of these popular services is wireless interaction. Ubiquitous wireless networks make it possible for distributed entities to remotely and efficiently communicate with each other anytime and anywhere, even in mobile status. Furthermore, tiny and exquisite handsets greatly raise the portability of mobile devices. Owing to the features of Raapid mobility and high portability, wireless interaction has played an extremely important role in personal interaction activities.

Most of the current mobile interaction services are based on the Global System for Mobile Interactions (GSM) architecture, and some novel applications based on the third generation (3G) of mobile interaction systems have also been deployed. However, the messages transmitted in wireless com-munication networks are exposed in the air, so malicious parties in wireless environments have more opportunities than those in wire-line environments to eavesdrop or intercept these trans-mitted messages [1], [2]. It will seriously threaten the security of wireless interaction systems if no protection mechanism is considered. Although some security aspects of current mo-bile interaction systems have been concerned, there still exist security problems in some GSM-based systems for ex-ample, the impersonating attack works because of the lack of mutual certification in the GSM system. Mutual authentication and other related security issues have been considered in the GSM-based certification protocols proposed in the literature [3] but their performance should be improved as much as possible to further meet the low-computation requirement for mobile users and guarantee the quality of the interaction services.

TABLE I
NOTATION USED IN HWANG AND CHANG'S SCHEME

| Notation | Definition |
|---|---|
| $U_i$ | the identity of user $i$ |
| $V$ | the identity of some VLR |
| $H$ | the identity of the HLR |
| $K_{uh}$ | a common secret key kept by $U_i$ and $H$ |
| $K_{vh}$ | a common secret key kept by $V$ and $H$ |
| $K_{auth}$ | an authentication key kept by $U_i$ and $V$ |
| $E_{K_x}$ | a symmetric encryption function with a secret key $K_x$ |
| \| | the concatenation operator |

The rest of this paper is organized as follows. Hwang and Chang's scheme of [10] is briefly described in Section II. Our basic idea is illustrated in Section III. In Section IV, we present an efficient mutual certification scheme for mobile interactions.

## Ii. Review of Hwang Andchang'S Scheme

In 2003, Hwang and Chang proposed a mutual certification scheme for mobile interactions [10], which is briefly described below. First, the notation used in the scheme is defined in Table I. Hwang and Chang's scheme is quite efficient for mobile users without impractical assumptions. In the following, we will present a novel practical mobile certification scheme that is much more efficient than Hwang and Chang's scheme [10] in both computation and interaction under the same assumption of [10].

## Iii. Our Idea

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

A. An Efficient Hybrid Mechanism for Mutual Certification With a preshared secret key , there are two basic approaches to achieve mutual certification between two entities, say Alice and Bob. One is the timestamp-based approach, and the other is the nonce-based approach.

The assumptions of a timestamp-based certification scheme:

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

The advantages of a timestamp-based certification scheme:

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

Although timestamp-based certification 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.

The advantages of a nonce-based certification scheme:

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

The drawbacks of a nonce-based certification scheme:

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

The assumption of an certification scheme based on one time secrets:

- Alice and Bob cannot perform the first time of mutual certification via the protocol since there is no one-time secret shared by them before the first certification.

The advantages of an certification scheme based on one time secrets:

- The protocol only requires two rounds of transmission to reach the goal of mutual certification.
- It is more efficient than a nonce-based certification scheme in computation and interaction.

The drawback of an certification scheme based on one- time secrets:

- Alice and Bob must store an extra string, i.e., the one-time secret, in their devices or computers.

The comparisons of the three certification mechanisms (i.e., timestamps, one-time secrets, and nonces) are summarized in Table II.

TABLE II
COMPARISONS OF THE THREE AUTHENTICATION MECHANISMS

| | Timestamps | One-Time Secrets | Nonces |
|---|---|---|---|
| **Assumptions:** | 1. Clock synchronization<br>2. Stable transmission time | The previous authentication must be successfully finished | None |
| **Performance:** | The most efficient solution | Slightly less efficient | Much less efficient |
| **Suitable for:** | The authentication between VLR and HLR | The authentication between a user and the system for the authentication processes after the initial one | The initial authentication between a user and the system |

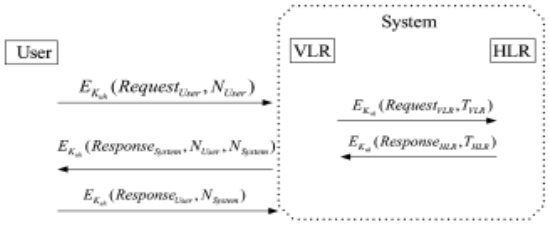



Fig. 1. Our idea for the initial authentication between a mobile user and the system (VLR and HLR).

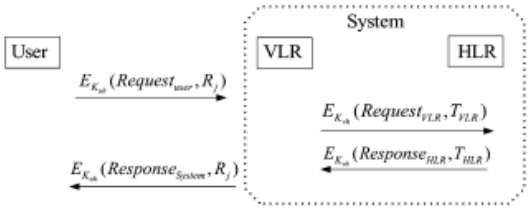



Fig. 2. Our idea for the $j$th authentication between a mobile user and the system (VLR and HLR) after the initial one, where $j \geq 1$.

## B. Nested One-Time Secret Mechanisms

Consider a sequence of mutual certification processes based on our proposed hybrid mechanism between mobile user and the system (a VLR and the HLR). In the initial certification, the user and the system authenticate each other by performing a nonce-based certification 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 certification processes.

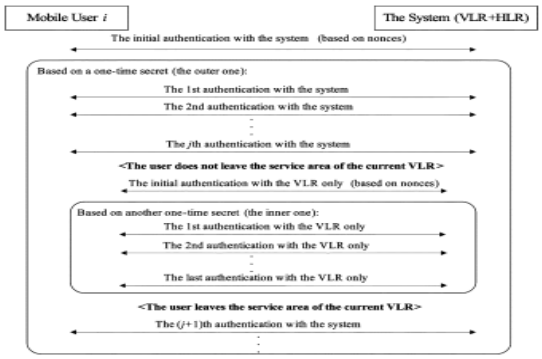



Fig. 3. The proposed nested one-time secret mechanism.

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, which is illustrated in Fig. 3.

## Iv. the proposed Scheme

Based on the ideas introduced in Section III, we propose a Rapid mutual certification and key swap scheme for mobile interactions. 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 certification between a mobile user and the system (a VLR and the HLR) where it includes two protocols: 1) an initial certification protocol for mutual certification and the initialization or reinitialization of the outer one-time secret (described in Section IV-A); and 2) an certification protocol based on the outer one-time secret for the $j^{th}$ certification after the most recent performance of the initial certification protocol in Section IV-A between the user and the system where is a positive integer (described in Section IV-B).

The second part of the scheme is tailored for mutual certification 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 certification protocol for mutual certification and the initialization or reinitialization of the inner one-time secret (described in Section IV-C); and 2) an certification protocol based on the inner one-time secret for the th certification after the most recent performance of the initial certification protocol in Section IV-C between the user and the VLR where is a positive integer.

Besides, according to the specification of Advanced Encryption Standard (AES), 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.

- The Initial Certification Protocol for Mobile User $U_i$ and the System
- The J th Certification Protocol for Mobile User and the System
- The Initial Certification Protocol for User and the Current VLR
- The th Certification Protocol for User and the Current VLR

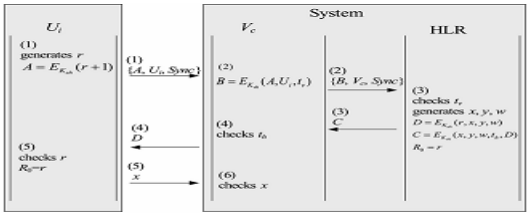



Fig. 4. The initial authentication protocol for a user and the system.

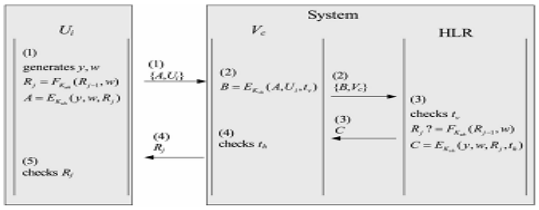



Fig. 5. The $j$th authentication protocol for a user and the system (VLR and HLR) after the most recent initialization.

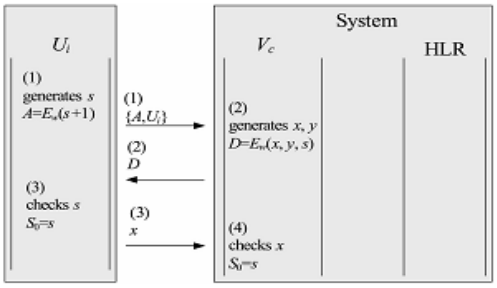



Fig. 6. The initial authentication protocol for a user and a VLR.

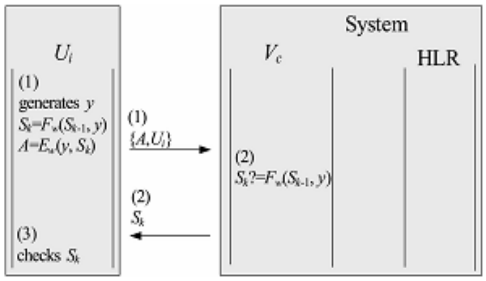



Fig. 7. The $k$th authentication protocol for a user and the current VLR after the most recent initialization.

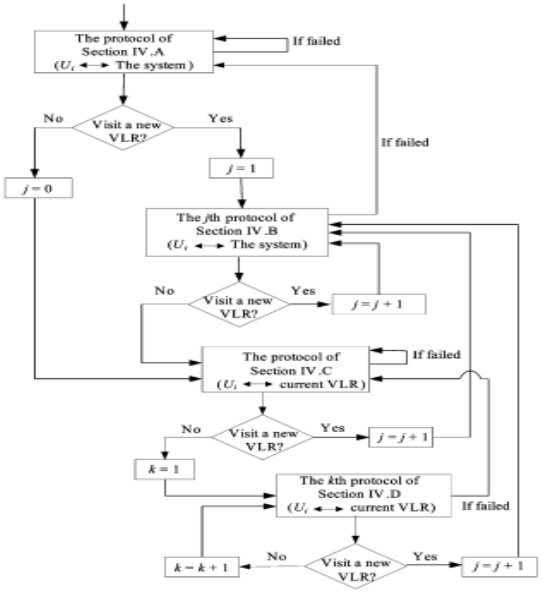
Finally, the four protocols of the two parts proposed in Sections IV-A –D, respectively, are integrated into a complete and Raapid certification scheme for mobile interaction. Fig. 8 illustrates the execution order and the relationship of the four proposed protocols in the proposed scheme.

## V. Security Models and Proofs

A. Security Models and Definitions Our interaction model and security notions are based on. A simulator simulates an environment such that an adversary can execute the proposed protocols with .If breaks one of the proposed protocols, can use the output from to solve a hard problem.

In our model, oracle models a player attempting to authenticate a player in session of the protocol , where being the set of the identities of the players who can participate in the protocol, and being the set of positive integers. The adversary is not a player in our model. Let us define the capability of , which can be captured by the following queries:

- Execute
- Send
- Reveal




- Test Fig. 8. The execution order and the relationship of the four proposed protocols.

### B. Security Proofs

In this subsection, we prove that the proposed protocols are protected mutual certification and key swap protocols under the assumption that the adopted underlying symmetric cryptosystem is with the IND-CCA security and the adopted pseudorandom permutation and the pseudorandom function are protected.

## Vi. C Onclusion

We have proposed a protected mutual certification and key swap scheme for mobile interactions 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 interactions and speed up certification.

## References

[1] D. Brown, "Techniques for privacy and certification in personal interaction systems,"IEEE Personal Commun. , vol. 2, no. 4, pp. 6–10, Aug. 1995.

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

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

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

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

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

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

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

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

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