On the Security of an Enhanced UMTS Authentication and Key Agreement Protocol *

Min-Shiang Hwang† Song-Kong Chong‡ Hsia-Hung Ou§

Department of Management Information Systems†
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw
Fax: 886-4-22857173

Department of Computer Science and Information Engineering‡
National Cheng-Kung University
No. 1, Ta-Hsueh Road, Tainan,Taiwan, ROC.

Department of Computer Science and Information Engineering §
Hwa-Hsia Institute of Technology
111 Gong Jhuan Rd., Chung Ho, Taipei, Taiwan, R.O.C

September 8, 2012

*This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the grants NSC 95-2218-E-001-001, and NSC95-2218-E-011-015.

†Corresponding Author: Prof. Min-Shiang Hwang

On the Security of an Enhanced UMTS Authentication and Key Agreement Protocol

Abstract

In this paper, we propose a practical and secure authentication and key agreement scheme for Universal Mobile Telecommunications System (UMTS). The paper introduces a new requirement, "home network should be partially trusted in an authentication scheme" to the UMTS. The scheme integrates symmetric and public key cryptosystem. Issues such as kinds of "subscriber identity/location confidential" and "non-repudiation services" are solved in the scheme. The paper provides computational analysis, messages transmission length analysis to the proposed scheme. Furthermore, comparisons with other schemes are also given. The results demonstrate that the proposed scheme is practical and secure.

Keywords: 3GPP, authentication, non-repudiation service, privacy, security.

1 Introduction

In the last two decades, due to the advance of technology, we have witnessed that the telecommunication is appearing anytime and anywhere in our daily lives. It greatly simplify the people's life. People are now able to make a contact with others via various ready-made products, e.g. cellular phones, email and miscellaneous communication softwares/apparatus.

1.1 The Security Issue Categories

The tremendous market growth of global mobility communications indicates the growing importance of security in mobile telephones during communications [1, 2, 3, 4, 5]. Since the characteristics of mobile communications, attackers easier disguised themselves o carry on the illegal behaviors. Therefore, the confidentiality of radio transmission, i.e. the *authentication*, and the *privacy* are two major issues in many proposed schemes [6, 7, 8, 9, 10, 11, 12, 13]. Besides, the *subscriber identity/location confidentiality* [14, 15, 16, 17, 18, 19] and *non-repudiation services* [20, 21, 22] become another two critical issues in the mobile communications.

In general, authentication corroborates the identity of an entity. Data confidentiality keeping information secret from all but those who are authorized to read it. Besides, identity/location confidentiality of subscribers highlights that the subscriber's identity and his/her current location are some valuable information to someone, it should be concealed from those potential eavesdroppers when roaming. In addition, non-repudiation service prevents the denial of previous actions or commitments. It protect the subscribers from incorrect bill charging, and also provide the service providers with legal evidences when collecting the bills. Since the resources of a mobile device are limited, therefore, how to minimize the resources utilization becoming another focal point when designing a security scheme.

1.2 The Motivation

So far, the GSM networks still to become the largest personal communication systems (PCS) in the world [23]. With the advent of 3G, we believe this situation will tend to the third generation mobile systems eventually. To run the systems, the UMTS requires that each subscriber shares a secret key K with his/her home network through a User Services Identity Module (USIM) card which is placed in the mobile equipment. There are no secret sharing between a visited network and subscriber in the roaming. Therefore, to obtain the access rights to a visited network, the subscriber needs to authenticate himself/herself to the home network via the assistance of the visited network.

Since "the sole pre-establish secure channel between the visited network goes through the home network" [24], hence the home network should be fully trusted usually becoming a default rule in the current UMTS, as well as in many proposed authentication schemes. Therefore, subscribers are forced to believe that the home network is trusted and would not engaged in any illegal behaviors, e.g. eavesdrops the conversation contents of a subscriber who stays in a visited network. The situation gets worse when government offices intervening in the eavesdropping for some reasons. Moreover, the home network may profit by leaking the authentication key of the subscribers to other illegal users. As a result, those illegal users can make free calls, impersonate a legitimate subscriber to make some illegal actions, or eavesdrops the conversation contents of the subscribers. Since the home network possesses the authentication vectors of the authentication scheme, therefore, it can step in the illegal behaviors as described above.

We consider the security guard should be the home network, but not the visited network (especially for those visited networks overseas). The major cause is all the authentication vectors are going through the home network, if the home network is willing to cooperate with the eavesdroppers, none of the subscribers can resist this attack. On the other hand, since the visited network are not controlled by subscriber's home network, or by subscriber's government offices, we contemplate the eavesdroppers are difficult to do their monitor in the visited network.

Therefore, if a subscriber is able to secret share an authentication key with the visited network, the problems are readily be solved. Since the home network or government offices of the subscriber cannot control the visited network, hence, the conversation eavesdropping or authentication key compromised can be prevented.

For the reasons above, we add another requirement to the mobile communications, *home network should be partially trusted in an authentication scheme.* We consider the home network may betray to its subscriber in some situations. The problems seem can be solved through the utilization of a public key cryptosystem. However, it brings on another problem, the identity/location of a subscriber will be compromised to the potential eavesdroppers when the certificate is transmitted over the radio links. Since subscribers hope to hide their identity/location when roaming, the using of a certificate will divulge their whereabouts. This scenario becomes a predicament in the current system and also in many proposed authentication scheme. In this paper, we shall propose an authentication scheme to solve the problems.

On the other hand, the drawbacks of the current UMTS authentication and key agreement (AKA) protocol are also analyzed in our paper. Although many previous protocols about GSM already show clearly about these similarly drawbacks, however, in order to provide a total solution to the UMTS AKA, the earlier discussed drawbacks are also fixed in this paper. As a result, the proposed UMTS AKA is not only to provide a solution to the problem of *home network should be partially trusted* , the other known drawbacks such as bandwidth consumption between the home network and a visited network, the insecure subscriber identity/location confidentiality protocol in the UMTS also fixed in the paper. Furthermore, the non-repudiation services are also provided in the proposed protocol.

The remainder of this paper is organized as follows. In Section 2, the system architectures of UMTS will be introduced. In Section 3, a new authentication scheme will be proposed to ameliorate the security problems of the UMTS. In Section 4, we will make a detail security analysis of the proposed scheme, and examine how the scheme contents with the security requirement discussed in Section 1. In Section 5, an efficiency analysis shall be given. The analysis will prove that the proposed protocol is very efficient. In Section 6, a comparison with other published protocol will be given. Finally, Section 7 followed by our discussions and conclusions.

2 The Security Schemes of UMTS and Their Drawbacks

In order to demonstrate the security schemes of a UMTS network, we shall introduce its network elements. Figure 1 illustrates the UMTS's architecture. UMTS is divided into three major parts: the air interface, the UMTS Terrestrial Radio Access Network (UTRAN), and the UMTS core network. The base stations and the Radio Network Controllers (RNCs) are collectively known as the UTRAN. From the UTRAN to the core network, the RNC will decide where the traffic will be transmitted to. Packet traffic is sent to a new component, the Serving GPRS Support Node (SGSN), and then to the Gateway GPRS Support Node (GGSN). The functions of the GGSN are very similar to the normal IP gateway, which transfer the receiving packets to the appropriate Internet. On the other hand, if there is a voice call from a subscriber, the RNC will transmit the traffic to the Mobile Switching Center (MSC). If the subscriber is authenticated before, the MSC will switch the phone call to other MSC (if the called end is another mobile subscriber), or the call will be switched to the Gateway MSC (GMSC) (if the called end is in the public fixed phone network).

In the UMTS security schemes, there are three main threats and issues that the UMTS would like to address:

1. Mutual authentication between the subscriber and the connected network.

2. Signalling integrity protection within the Radio Access Network (RAN) and over the radio link.

3. Encryption of user data within the RAN and over the radio link.

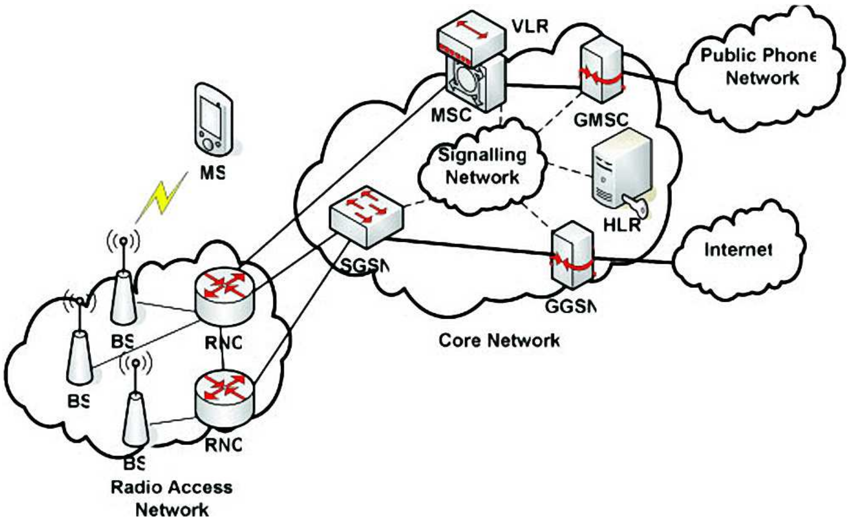

Figure 1: UMTS Architecture

Below, we shall introduce the these security schemes and their drawbacks respectively.

2.1 The Authentication Scheme

UMTS adopts a challenge and response mechanism to achieve the authentication and the key agreement (AKA) among the related parties. Figure 2 illustrates the operation of the authentication scheme.

The AKA procedure is executed in two stages. The first stage (Figure 2, Step (1)∼(4)) is a registration and distribution of authentication vectors. When a subscriber roams into a new network or turn on his/her mobile equipment, he/she needs to identify himself/herself using an old TMSI (TMSIo) that was assigned by the previous visited network (VLRo). The TMSI (Temporary Mobile Subscriber Identity) is the identity between the MS (Mobile Station) and the VLR (Visitor Location Register). TMSI is randomly assigned by the VLR to every MS in the VLR's area, and it has to be updated each time the MS moves to a new VLR's area. VLR is the visitor location register which stores information about all the MSs that are currently under the particular area of the MSC (Mobile Switching Center) which it serves. Af-

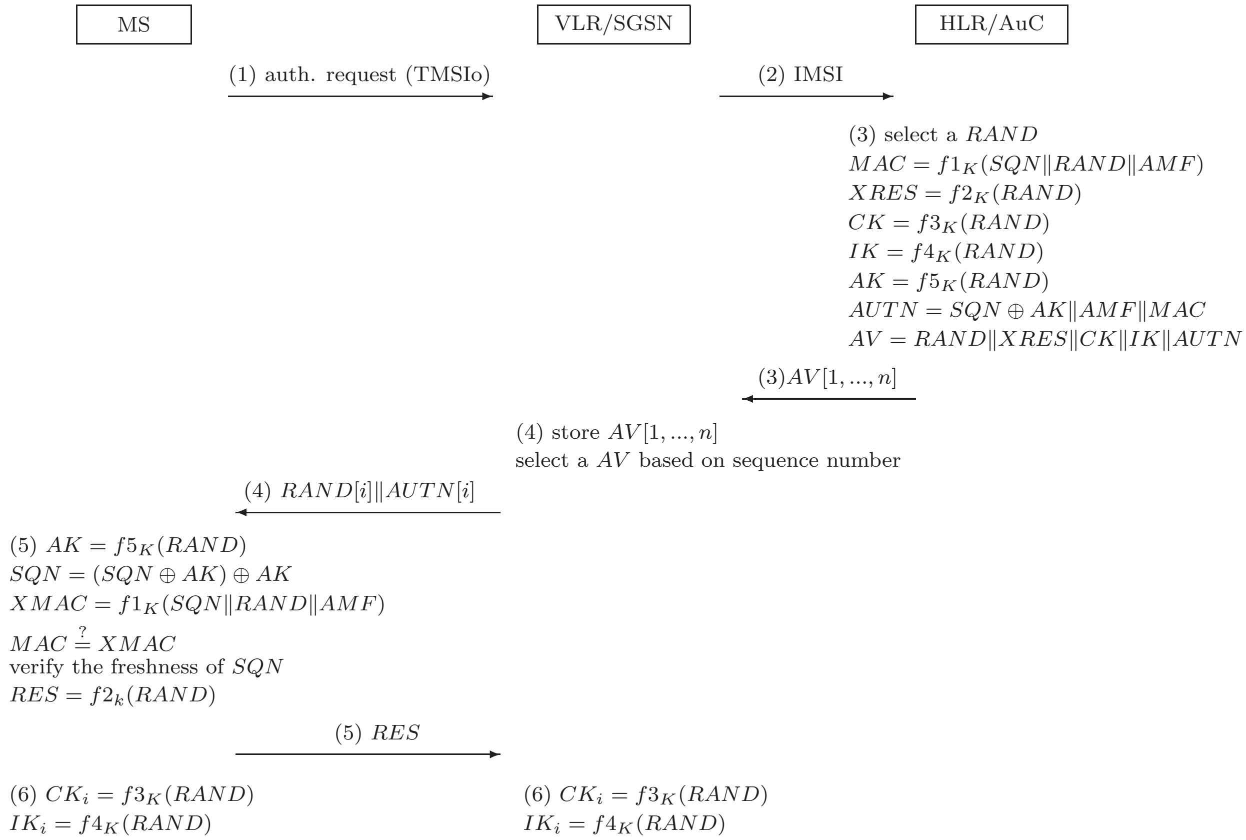

Figure 2: Authentication and Key Agreement (AKA) in UMTS

ter requests the MS's IMSI (International Mobile Subscriber Identity, a unique number associated with MS) from the VLRo, the VLR/SGSN sends a request to the HLR/Auc. The HLR (Home Location Register) is a central database that contains details of each mobile phone subscriber that is authorized to use the network. The AuC generates a list of authentication vectors (AVs) to the VLR/SGSN by using the secret key K which is pre-shared with the subscriber. The AVs are ordered based on sequence number. Each AVs is comprised by a random number $RAND$, an expected response $XRES$, a cipher key CK, an integrity key IK and an authentication token $AUTN$. Each AV is used for one authentication and key agreement between the VLR/SGSN and the MS.

To authenticate the MS, the VLR/SGSN selects the parameters $RAND$ and $AUTN$ on a first-in/first-out (FIFO) basis to the MS. The MS checks whether the $AUTN$ can be accepted or not. If so, the MS sends back a parameter RES to the VLR/SGSN. The VLR/SGSN makes a verification by comparing the received RES with $XRES$. If they match, the mutual authentication and key agreement between the MS and the VLR/SGSN is successful. The established keys CK and IK are stored in the VLR/SGSN and will then be transferred to the RNC when needed. If a VLR/SGSN runs out of AVs, it can request another list of AV from the HLR/AuC.

When the subscriber roams to a newly visited VLRn/SGSNn within one serving network domain, the VLRn/SGSNn will send the $TMSIo$ of the subscriber to its previous visited VLRo/SGSNo. If the subscriber is found, the VLRo/SGSNo will send a response back to the VLRn/SGSNn. The *user identity request* shall include the $IMSI$ of the subscriber, and a number of unused AVs ordered on FIFO basis. The VLRo/SGSNo subsequently deletes the AVs which have been sent. If the VLRo/SGSNo cannot identify the subscriber, it will indicate that the subscriber cannot be retrieved in the user identity request message.

In UMTS, the VLR/SGSN is assumed to be trusted by the subscriber's HLR/AuC to handle the authentication information securely. It is also assumed that the communication links between the VLR/SGSN and the HLR/AuC are adequately secure. Also, it assumed that the subscriber trusts his/her HLR/AuC.

2.2 The Confidentiality Scheme

Confidentiality is normally terminated in the base station. However, in UMTS, the coverage of the data confidentiality is extended to the Radio Network Control (RNC). The main reason is, there is a substantial amount of the connections between base stations and controllers are based on unsecured radio link hops [25]. Therefore, data confidentiality in microwave links between the base stations and the RNC are covered in UMTS.

The authentication vectors (AVs) contain sensitive data, e.g. cryptographic keys and challenge-response authentication data. Therefore, they should be protected against eavesdropping and modification while transferring between the VLR and the HLR/AuC. In the age of GSM, there are no cryptographic security mechanisms available for inter-network communication. The security has been based on the fact that the SS7 network were the provinces of a small number of well established institutions. However, this is no longer the case. The situation now is changing for two main reason. Firstly, there is a trend to replace the SS7 with IP (Internet Protocol) network. Secondly, the number of different operator as well as service providers is increasing. There are many ready-made hacking tools in IP network, and become applicable to the telecommunication networks. For these reasons, the actual mechanism used for the AVs transmission, MAP protocol, is the essential part to be protected. The original MAP (Mobile Application Part) protocol does not contain security functionality, but a security extension to MAP named MAPsec has been developed [26].

The MAP protocol can be run on top of IP, that is, MAP over IP. In this case, there are two alternative methods to protect MAP: either to use MAPsec [26] or IPsec [27]. The later method has more advantage that the protection covers also lower layer headers as it is done in the IP layer.

So far, how to transfer cipher key CK and integrity key IK from the the core network to the RNC is still not standardized. It is imperative that the system operator provides full confidentiality and integrity protection to this communication link (Iu interface). If an operator choose to use IP as the preferred transport protocol over the Iu interface, Network Domain Security for IP (NDS/IP) [27] can be used to solve this problem.

2.3 The Integrity protection

The integrity security service is a new feature in UMTS. It is absence in GSM system. The physical range covered by the integrity protection is same as the confidentiality protection does. However, the integrity service in UMTS is only limited to signalling information between the MS and the RNC, but not the user traffic. The reason to provide the signalling information with a dedicated integrity service in UMTS is because most of these information are considered sensitive and must be integrity protected. For example, the UMTS network must be able to instruct the MS to use an unciphered connection for many reasons. Therefore, the use of ciphering cannot be made mandatory. An attacker can masquerade as a network to establish an unciphered connection with a subscriber. This will result the user communication contents be compromised. In order to prevent such vulnerability, the integrity protection can be made mandatory.

Since the user traffic is not protected by this integrity security service, it represents a problem under certain circumstances. For example, there will be the situation where the data encryption is unavailable. Thus the integrity protection will become the only defense against the insertion, modification, deletion and replay attacks. The absence of user traffic integrity protection may experience the problems above.

2.4 The Subscriber Identity/location Confidentiality

The UMTS provides the security features for Subscriber Identity/location Confidential can be summarized as follow:

- Subscriber identity confidentiality: the IMSI of a subscriber to whom services are delivered cannot be eavesdropped on the radio link.
- Subscriber location confidentiality: The location of a subscriber cannot be determined by eavesdropping on the radio link. Thus, the presence or the arrival of a subscriber in a certain area is safe.
- Subscriber untraceablity: an attacker is unable to determine whether different services are delivered to the same subscriber by eavesdropping

Table 1: Software speeds of RSA by the CryptoLib

RSA Speeds for Different Modulus Lengths with an 8-bit Public Key(on a SPARC II)			
	512 bits	768 bits	1,024 bits
Encrypt	0.03 sec	0.05 sec	0.08 sec
Decrypt	0.16 sec	0.48 sec	0.93 sec
Sign	0.16 sec	0.52 sec	0.97 sec
Verify	0.02 sec	0.07 sec	0.08 sec

on the radio link.

By introducing the concept of Temporary Mobile Subscriber Identity (TMSI), UMTS achieves these objectives. To make subscriber untraceability, the TMSI should not be identified for a long period by means of the same TMSI. These security features are identical to those provided in GSM. Thus, the weaknesses found in GSM (refer to [3] for detail) also inherited by UMTS.

3 The Proposed Scheme

So far, many of the current researches pay their attention on how to provide a secure, robust, efficient security scheme to the existing confidentiality protocol [1, 6, 20, 8, 16, 3, 9, 21, 17, 10, 3, 18, 22][1]. However, none of them achieves the security requirements, *the HLR should be partial trusted in an authentication scheme*.

Buttyan et al. believed that the attack from HLR cannot be avoided since "the sole pre-establish secure channel between the VLR and MS goes through the HLR" [24]. They suggested that did not use the scheme if HLR was dishonest. In order to solve these problems, a new AKA scheme is provided in this paper. Below, we shall describe the proposed scheme in detail.

The proposed scheme involves the using of a public key of VLR, which is used by a legitimate MS to encrypt an authentication key generated by the

[1]Since the UMTS is the descendant of GSM, we consider many of these protocols can be inherited by the UMTS.

HLR.id	$E_{sk}(IMSI\|\|TS)$
sk: the secret key of HLR	TS: timestamp
$\|\|$: concatenation	$IMSI$: International Mobile Subscriber Identity

Figure 3: TMSI format

MS himself/herself and passes it to VLR. To mitigate the computation burden of mobile equipment, the encryption is done in MS side since the public key operation takes $O(K^2)$ complexity but private key operation takes $O(K^3)$ complexity with the typical modular exponentiation algorithms used to implement the RSA algorithm [28], where K is the number of bits in the modulus. Table 1 gives the software speeds of RSA by the CryptoLib [29]. RSA goes much faster if we choose the value of public key e carefully. Therefore, we suggest the exponent value e should be smaller.

In 2003, RSA Laboratories recommends the minimum key length for general data is 1024 bits without any specifying lifetime [30]. NIST (National Institute of Standards and Technology) are recommends 1024 bits for RSA, which is taking into account the lifetime of the data [31]. For security concerns and the execution speeds of the public key encryption, we suggest the value of public key length is optimally 1024 bits.

3.1 The Common Registration Phase

Before we describe the proposed AKA scheme, we assume the following works are done when MS makes a service contract with his/her HLR:

- MS selects a large prime p, and a random number x which is relatively prime to $p-1$. MS generates $y = g^x \bmod p$, and keeps the x secretly. g is a generator of Z_p^* herein.

- MS subscribes (g, y, p) to HLR through a secure channel.

- HLR produces a certificate $cert_{u_i}$ to (g, y, p) and keeps it in its database. HLR writes K_{uh} which is the secret key shared between MS and HLR,

$TMSI$ and $cert_{ui}$ in the USIM of MS. The format of $TMSI$ [3] is illustrated in Table 3.

- Upon receipt the USIM, MS verifies the related values stored in the USIM.

3.2 The Authentication and Key Agreement scheme for UMTS

In UMTS, we assume the communications between VLR and HLR are protected by NDS/IP [27] or MAPsec [26]. The symmetric cryptographic function $E_K(\cdot)$ presented between VLR and HLR denotes that the communication link is not only protected by NDS/IP or MAPSec, but also by other cryptographic system, e.g. AES [32]. The value K presented in $E_K(\cdot)$ means the symmetric cryptographic function is relying on a shared secret key K. Figure 4 illustrates the proposed authentication and key agreement scheme for UMTS. How the proposed AKA scheme running is portrayed as below:

Step 1: MS generates a random number r_0 and computes $h = g^r \bmod p$, where r is a random number, which $0 \leq r < p-1$. Then MS sends his request to VLR, such that $TMSIo, E_{K_{uh}}(V\|TMSIo\|r_0\|h\|T_{u_i})$, where "$\|$" means the concatenation, V is the identity of VLR, T_{u_i} is the current timestamp of MS, and K_{uh} is a secret key shared between the MS and VLR. The old TMSI $TMSIo$, uses the format presented in Figure 3.

Step 2: When VLR receives the authentication request of MS, VLR generates a random number r_1, and sends the $E_{K_{uh}}(V\|TMSIo\|r_0\|h\|T_{u_i})$ and $E_{K_{vh}}(V\|TMSIo\|r_1\|T_v)$ to HLR according to the $HLR.id$ recorded in the $TMSIo$. T_v is the current timestamp of VLR.

Step 3: HLR verifies MS by checking the information stored in TMSIo. If the provided information is validated, then HLR will check to

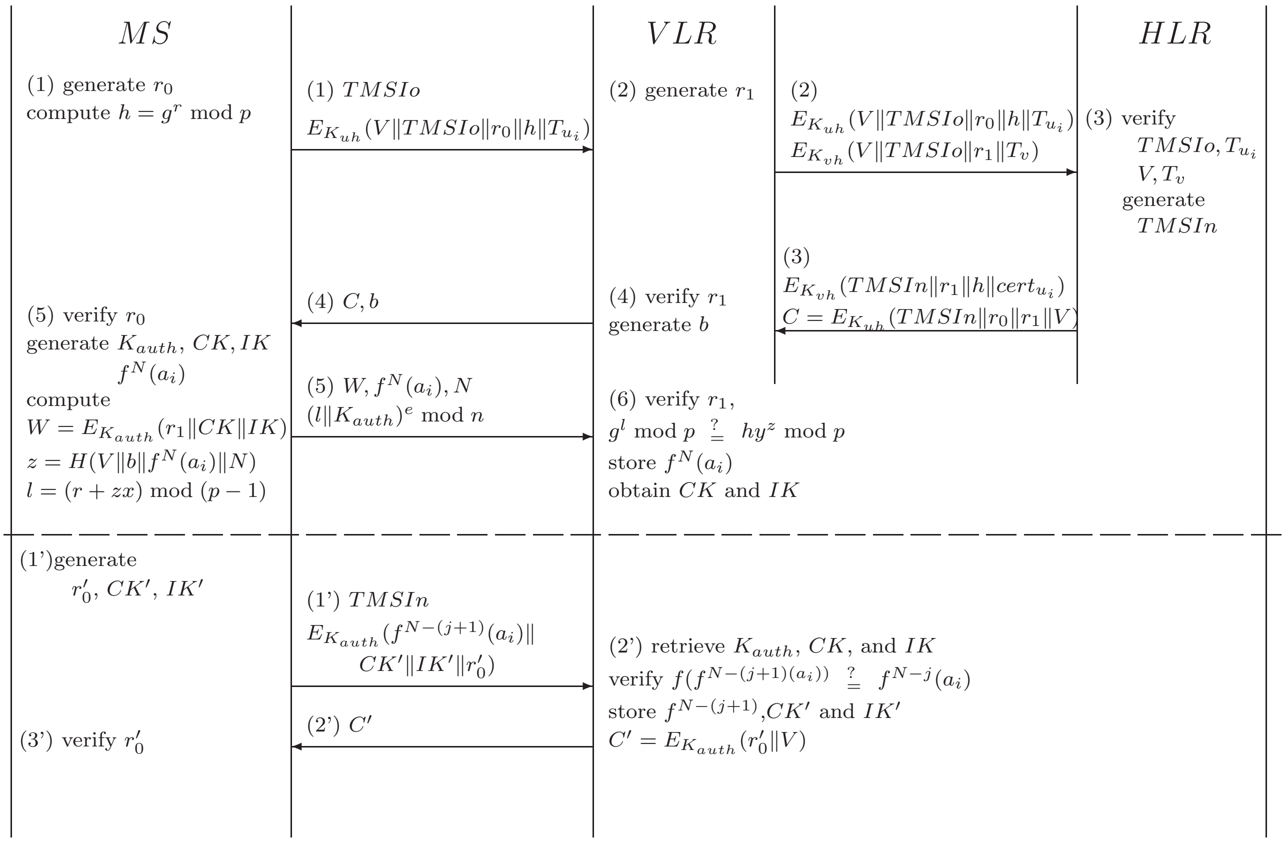

Figure 4: Proposed AKA scheme for UMTS

VLR. Afterward, HLR retrieves the $cert_{u_i}$ of MS from it database. HLR generates a new $TMSIn$. The format of $TMSIn$ is presented in Figure 3. HLR sends $E_{K_{vh}}(TMSIn\|r_1\|h\|cert_{u_i})$ and $C = E_{K_{uh}}(TMSIn\|r_0\|r_1\|V)$ to VLR.

Step 4: Upon receiving the messages, VLR decrypts $E_{K_{vh}}(TMSIn\|r_1\|h\|cert_{u_i})$, if r_1 equals to the previous one, VLR believes that MS is a legitimate subscriber and trusts the $cert_{u_i}$. VLR records the TMSIn as a temporary identity of the particular MS. VLR generates a random numbers b, and transmits with C to MS.

Step 5: Upon receiving the relates messages from VLR, MS checks the value of r_0. Then MS generates an authentication key K_{auth}, a ciphering key CK and an integrity key IK. To achieve non-repudiation services, MS also computes $f^N(a_i)$, where $f(\cdot)$ is a one-way hash function, a_i is a number of random numbers, $0 \le i \le m$. The value

N determines how many times that a MS can use the services of the VLR on each a_i.

To improve the efficiency of a public key encryption (by reducing the messages length), MS extracts some values which should be originally encrypted by the public key scheme. Therefore, MS computes $W = E_{K_{auth}}(r_1 \| CK \| IK)$. Afterwards, MS computes $z = H(V \| b \| f^N(a_i) \| N)$, $l = (r + zx) \bmod (p-1)$ and encrypts $(l \| K_{auth})$ by the VLR's public key e. MS sends the related messages to VLR.

Step 6: VLR gets the k_{auth} by its private key d then decrypt W and verifies r_1, l. If the r_1 is correct and $(g^l \bmod p)$ is equal to $(hy^z \bmod p)$, the VLR establishes CK and IK with the MS. Moreover, the non-repudiation value $f^N(a_i)$ from MS also obtained.

After the first cipher key CK and integrity key IK are established, the MS and VLR can make their communication instantly. However, when the established CK and IK are used up, MS and VLR need to start another mutual authentication procedure again in order to establish another CK and IK. The following steps describe the procedure (see the bottom of Figure 4).

Step 1': MS generates a random number r_0', a new cipher key CK' and a new integrity key IK'. MS selects a pre-determined value a_i and computes $f^{N-(j+1)}(a_i)$, where $0 \le j \le (N-1)$. Afterwards, MS sends $TMSIn$ and $E_{K_{auth}}(f^{N-(j+1)}(a_i) \| CK' \| IK' \| r_0')$ to VLR.

Step 2': Upon receiving the messages from MS, VLR gets the cipher key CK and integer key IK with storage at last. Then decrypts $E_{K_{auth}}(f^{N-(j+1)}(a_i) \| CK' \| IK' \| r_0')$. If $f(f^{N-(j+1))}(a_i) = f^{N-j}(a_i)$, VLR records CK' and IK' as two new shared secret keys on the next time. Finally, VLR computes $C' = E_{K_{auth}}(r_0' \| V)$ to prove itself to MS.

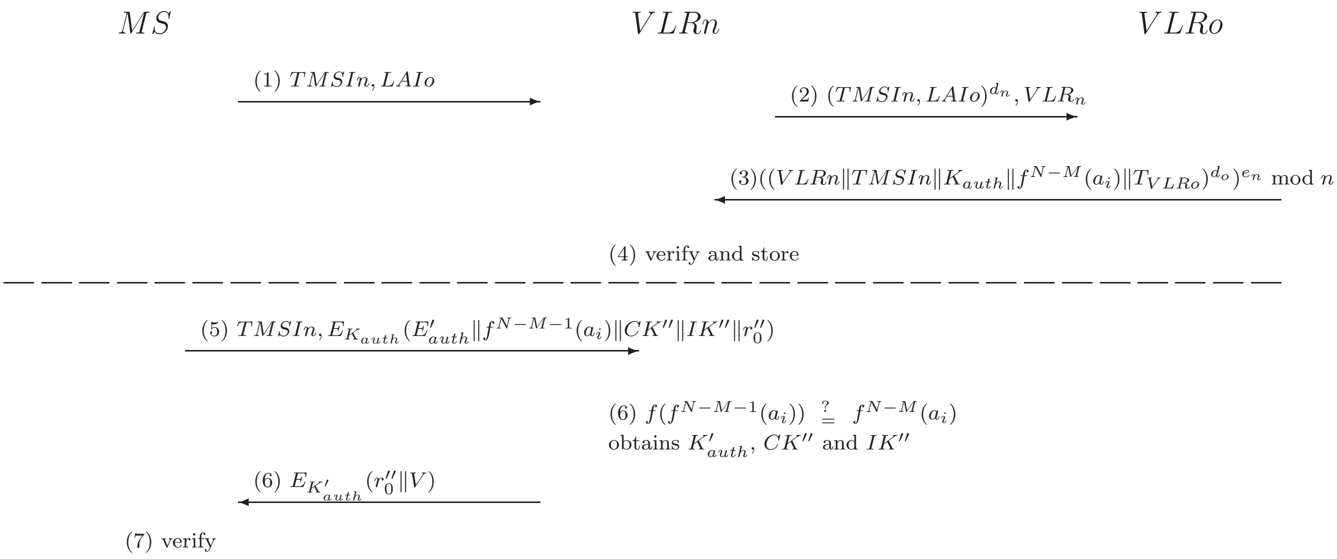

Figure 5: Distribution of authentication vectors within the two UMTS serving network domain

Step 3': As MS receives C', he/she decrypts the message. The correctness of r'_0 signifies that the VLR is authenticated. The new secret keys CK' and IK' are established.

In order to improve the utilization of the authentication vectors, UMTS provides the authentication vectors transferable feature. Figure 5 illustrates the proposed authentication vectors distribution scheme within the two UMTS serving network domain. The detail steps are depicted as below:

Step 1: When MS roams to a new VLRn from the previously visited VLRo, he/she sends $TMSI_n$ and $LAIo$ (old Location Area Identity) to the newly visited VLRn.

Step 2: Upon receiving $TMSI$ and $LAIo$, VLRn signatures it by his private key d_n and queries about the MS to the VLRo.

Step 3: If the subscriber is found, the VLRo shall send a *user identity response* back to the VLRn. The message shall include the VLRo's signature on $(VLRn\|TMSI\|K_{auth}\|f^{N-M}(a_i)\|T_{VLRo})$ and encrypting by VLRn's public key, where $N - M$ is the remaining value on each a_i that can be used by the MS to achieve the non-repudiation services in the new VLRn.

Step 4: After decrypt and verify the correctness of the signature, VLRn stores the signature in its database.

Step 5: The MS sends $TMSIn, E_{K_{auth}}(E'_{auth} \| f^{N-M-1}(a_i) \| CK'' \| IK'' \| r''_0)$ to the VLRn, where CK'' and IK'' is a new ciphering key and integrity key, respectively. K'_{auth} is a new authentication key, r''_0 is a new nonce value.

Step 6: If the verification to $f^{N-M-1}(a_i)$ are passed, CK'' and IK'' becoming the secret key shared with the MS. The VLRn proves itself to MS by sending an encrypted message $E_{K'_{auth}}(r''_0 \| V)$.

Step 7: If the received r''_0 is correct, the VLRn is authenticated by the MS.

In the proposed schemes, K'_{auth} as well as CK and IK are secret keys between MS and VLR, no third party is aware of them unless the RSA scheme is broken. Moreover, an opponent is unable to generate a fake signature in order to deceive the VLR. This is because he/she will face the discrete logarithm problem. Furthermore, if the encryption function $E_x(\cdot)$ is robust also, we believe the proposed scheme is secure against those security issues discussed in Section 4.

4 Security Analysis

In the proposed scheme, we assume a VLR has a powerful computation ability and has no worry about its power supply. Therefore, it can handle more complex calculations. Since we consider the low computation ability and low power of mobile equipments, we make the RSA encryption done in the MS side. Table 1 indicates that the RSA encryption provides a far superior performance than the decryption. Based on the recommendation of RSA Laboratories [30] and NIST [31], the public key length that we use is 1024 bits. For NIST, 1024 bits public key length is appropriate for protecting data through the year 2015 [31], which means it is hardly be broken using today's technology.

Since the security of public-key cryptography depends on the key length and assumes that factoring this large numbers is very hard. From the previous suggestion, we assume the public key pair (e, n) of VLR is secure, and the private key d is safe and known only by VLR. Moreover, we assume the secret key x is kept secretly by MS. Therefore, to pretend to be a valid MS, an intruder needs to compute the correctness of x. Since the security of x is based on the discrete logarithm problem, we believe x is secure and no one can pretend as a legitimate MS to intrude into a VLR.

Furthermore, the authentication key K_{auth} is generated by MS. The VLR will use the key to verify the MS again when he/she requiring a service, for example, make a call etc. We assume that the authentication key K_{auth} is generated through a secure random number generator and kept securely by each related parties. Similarly, the K_{vh} and K_{uh} are supposed to be kept secretly by the HLR.

Base on these hypothesis, we make the following security analysis to prove that our modification is robust and can against the impersonating and replaying attacks. Note that the analysis is based on the UMTS, the same concepts can be applied to the GSM easily.

Impersonating Attack: In this case, an intruder masquerades as a VLR to deceive MS and causes the service to deny MS. To masquerade as a VLR, an intruder needs to convince MS that the encrypted messages which sent in Step 4 is legitimate. However, it fails to achieve this requirement. Since VLR needs to make mutual authentication with HLR in advance, an intruder who does not hold the K_{vh} will fail to complete the mutual authentication in this portion. Therefore, the intruder cannot obtain a legal $C = E_{K_{uh}}(TMSIn \| r_0 \| r_1 \| V)$ from the HLR in Step 3 and transfers it in Step 4 to the MS. This failure will cause the remaining steps fail.

Moreover, if we assume that an intruder obtaining the K_{vh} between VLR and HLR through some illegal methods, and cheat to HLR successfully, it still fail to deceive the MS that it is an authorized VLR in our scheme. This is because the user authentication key K_{auth} is generated by the MS randomly and the related messages are encrypted by the VLR's public key. Therefore, the intruder will fail to decrypt $(l \| K_{auth})^e \bmod n$ in Step 5 because he/she does not hold the valid private key d due to our previous assumption that the private key is secure.

We consider the l is essential to success the proposed scheme. Without l and the related verification, a malicious HLR can forge some ciphertexts[2] to cheat the VLR. In fact, the swindle will usually successful. The main reason is HLR will obtain r_1 in Step 3 easily. Therefore, VLR will believe that the message is coming from a legitimate MS.

Similarly, if an intruder intend to masquerade MS, he/she will be defeated because he/she cannot generate a legitimate $E_{K_{uh}}(V \| TMSIo \| r_0 \| h \| T_{u_i})$ sent in Step 1. Moreover, the authentication key K_{auth} is generated by MS and would not compromised to his/her HLR in the process of authentication. No one can successfully impersonate a legitimate MS and cheat to VLR. However, if an intruder obtains a valid K_{auth} through a cryptanalysis while MS is staying in the VLR, he/she still cannot require a service from the VLR. The main reason is the intruder does not know the value of a_i in Step 5. Therefore, he/she cannot compute a legitimate $f^{N-(j+1)}(a_i)$ in Step 1' to the VLR and consequently the CK and IK generated by the intruder will be rejected.

Since a legitimate MS has no reason to leak out the K_{auth}, a_i and private key x, the responsibility of VLR, MS and HLR is now clear. The proposed scheme employs three authentication values K_{auth}, a_i, x to assure the robustness of the

[2]For example, a malicious HLR can compute $W' = E_{K'_{auth}}(r_1 \| CK' \| IK')$ and $(K'_{auth})^e \bmod n$, where K'_{auth}, CK' and IK' are random generated values. The malicious HLR sends $(K'_{auth})^e \bmod n$ to the VLR.

scheme. As no third party knows the authentication values, the later session key establishment and transmission are believed to be secured.

Eavesdropping Attack: In comparison with the original AKA scheme, the proposed scheme allows a MS to generate his/her cipher key CK and integrity key IK secretly without divulging them to his/her HLR. In order to establish the initial CK and IK with the corresponding VLR, a MS needs to prove that he/she knowing the value of x in Step 5 and 6 of the proposed AKA scheme. In the later key establishment procedure, the MS needs to present his/her knowledge about K_{auth} and a_i to the VLR. Therefore, no one is able to eavesdrop the communication content between the MS and VLR.

Replay Attack: In order to defeat the replay attacks, the proposed scheme employs timestamp or nonce in each transmitted messages. The HLR can verify the freshness of the messages sent in Step 2 by checking timestamp T_{u_i} and T_v. The VLR can timely verify the message $E_{K_{vh}}(TMSIn\|r_1\|h\|cert_{u_i})$ transmitted from HLR is legitimate by checking the r_1. Although the VLR is unable to verify C, however, it can counter the replay attacks by transmitting the message C to the MS. On the other hand, the VLR can verify the legitimate of W by checking the r_1 in Step 6. Since the MS should sign the value b issued by the VLR in Step 4, therefore, the VLR can verify the correctness of the signature in Step 6.

Identity/Location Confidentiality: We extend the idea of Lee-Hwang-Yang's location privacy protocol [3] into the proposed AKA scheme. In the proposed scheme, a TMSI is generated by the MS's HLR, but not a VLR. Although this method may cause a malicious system operator to compromise the location of a MS to someone, however, if the HLR has no idea where the MS is staying, we consider no one can contact with the MS. As a result, the service provided by the original UMTS may get some impacts. In this paper, we emphasis that a HLR is "partially trusted", but not "fully trustless". We consider that if HLR is fully trustless, then its services will become useless. Therefore, a HLR is partially trusted becoming reasonable. Though a HLR may compromise the location of a MS to an attacker, but the attacker still can not eavesdrop the conversation content of the MS, or masquerade as the MS to do some evil.

In the proposed scheme, the IMSI of a MS will never be compromised despite the failure database occurs in the visiting VLR, or the old VLR is not accessible while the MS roaming to another VLR (refer to Figure 5) [3]. If the later situation occurs, the VLRn should send a *old VLR is not accessible* to the MS and notice he/she to restart a full AKA scheme as depict in Figure 4. Although those unused authentication vectors will be wasted, but such design protecting the disclosure of a MS's identity/location from the VLRn.

Non-repudiation services: In the proposed scheme, a MS can not deny that he/she had never using such services if he/she does. At the same time, a HLR also can not falsely incriminate that a MS had using the services if he/she does not. In the scheme, each time a MS needs to use the services of the VLR, the MS should prove that he/she knowing about the value of $f^{N-(j+1)}(a_i)$ (refer to the bottom of Figure 4). Since the value of a hash chain can not be traced back if the a_i is unknown, therefore, the VLR can prove that a particular MS had using a service by showing the $f^{N-(j+1)}(a_i)$. On the other hand, if a MS can not present a legitimate $f^{N-(j+1)}(a_i)$, the new CK' and IK' will be rejected by the VLR. Same situation also occurs when a MS roaming to a new VLR (refer to the Figure 5).

From the above security analysis, we can find that the proposed scheme is secure against impersonating attack and replay attack. Furthermore, the requirements of identity/location confidentiality and non-repudiation services also be considered. Only the legitimate MS will be authorized to login into the VLR. The proposed scheme ensures that no one can harm the rights and interests of the MS unless the authentication values K_{auth}, a_i and x are compromised to an intruder simultaneously by the MS himself/herself.

In this section, only impersonating attack, eavesdropping attack, replay attack, identity/location confidentiality and non-repudiation services are discussed. The other security requirements such as mutual authentication, data confidentiality and etc. will be discussed later in Section 6.

5 Efficiency Analysis

In the previous chapter, we have made a detail analysis to examine how the proposed scheme deters an intruder from various attacks. In this section, two analyses to the proposed scheme shall be given. The first one is the computational analysis. By using a mobile phone simulator, we will show that our schemes are working efficiency in a given circumstance. The second analysis is the messages transmission length analysis, we will demonstrate the bandwidth requirement in each steps.

5.1 Computational Analysis

Since the resources of a MS are limited, therefore, how to mitigate the computational burden on the MS side is very important. On the other hand, we consider the system operators is abundant in capital to enhance their computer hardware resources. Therefore, the computational analysis on the VLR and HLR are given up.

In the proposed AKA scheme, a MS requires to perform its calculation in Step 1 and 5. The predefined variables' value or length for the computational analysis in these two steps is given in Table 2. Note that the variables are defined according to the existing specifications. For example, the value of e is 65537, which is suggested by Annex C to X.509, the use of Fermat's Number F_4 ($F_4 = 2^{2^4} + 1$) [33]. While e is defined to 65537, the transmission capacity and complexity of transformation can be reduced [33]. Although the variable

Table 2: Defined variables' value/length

Item	Variables' Value/Length	Item	Variable's Value/Length
g	17	r, x, y, a_i	512 bits
e	65537	p	768 bits
V	20 bits	$cert_{u_i}$	3072 bits
N	8 bits	K_{uh}, K_{vh}, K_{auth}	128 bits (AES key)
T_{u_i}, T_v, r_0, r_1	48 bits	$E_x()$	128 bits (AES)
CK, IK, b	128 bits	$H(), f^N()$	160 bits (SHA1)
$TMSI_o, TMSI_n$	148 bits	n	1024 bits (RSA)

blocks length in the range of 128 bits, 192 bits and 256 bits were designed by Rijndael scheme, but we will use the 128 bits data block which is defined in the final standard, FIPS 197 published by NIST [32]. In the meanwhile, the AES secret key K_{uh}, K_{auth} are also set to 128 bits according to [32].

Furthermore, in UMTS, the Mobile Country Code (MCC) and Mobile Network Code (MNC) are parts of IMSI and Location Area Identifier (LAI). They are global unique, their combination can be used to identify a particular service operator. Usually, the MMC shall be 3 digits (10 bits), and the MNC shall be either 2 or 3 digits (10 bits) [34, 35]. Therefore, the VLR's identity V is set into 20 bits. Accordingly, the format of $TMSI$ is $HLR.id\|E_{sk}(IMSI||TS)$ (see Figure 3), where the length of $HLR.id$ is same with V, 20 bits. The $IMSI$ is a string of not more than 15 digits, it can be represented by 48 bits. The timestamp TS is 48 bits. If AES is employed, the length of TMSI will totally becomes 148 (=20+128) bits.

Now, a detail computational analysis is given. The operating system that we use is Microsoft Windows XP Professional service pack 1, the programs are written based on Java 2 Platform through Java Development Kit (JDK) 1.4.2 by using the built-in packages. The simulation software is Nokia 6210 simulator. In the hardware environment, the processor is AMD Duron 1.2GHz, the RAM is 512MB. In our simulated processes, we found that given 512 bits data as SHA1's input, per calculation is only needs 0.025587ms. Since the time needed for each SHA1 operation is very trivial, therefore we disregard the time computation of hash chains. The calculations of MS that we sum up in the computational analysis include h and $E_{K_{uh}}(V\|TMSIo\|r_0\|h\|T_{u_i})$ of Step 1, and $W, l, (l\|K_{auth})^e \bmod n$ of Step 5. In our simulation, a MS needs to spend 60ms in order to complete the calculation above. We consider that 60ms do not make sense in human's perception, therefore the proposed authentication schemes are very efficient.

5.2 Messages Transmission Length Analysis

Table 3: The length of messages transmission

Step	The AKA scheme for UMTS
1	1300 bits
2	1536 bits
3	4480 bits
4	512 bits
5	1576 bits
Total	9404 bits

According to the size of each variable given in Table 2, Table 3 shows the length of messages transmission in each step of the AKA scheme. Although the length of messages seem to be higher, however if we consider the proposed scheme is providing a total solution the security requirements described before, these messages' length are tolerable.

Since none of the previous authentication schemes provide a total solution as ours, therefore the comparison with other schemes are omitted. We consider if a scheme is capable of achieving the most security requirements than others, then requiring more messages transmission length are reasonable.

6 Comparisons

In the following, we shall manifest how our scheme achieves the security requirements. Compare greatly part of article [24, 20, 36, 2, 3, 17, 18, 4] concerning the authentication and key agreement protocol in the last years. Our scheme come to the all demands whether MA (Mutual Authentication), DC (Data Confidentiality, both radio and inter-network), ILC (Identity/Location Confidentiality), HTL (HLR is partial Trusted), RBC (Reduction of Bandwidth Consumption), RSV (Reduction of VLR Storage), VSHA (VLR Substitutes as HLR to Authentication MS) and NRS (provide Non-Repudiation Services). Table 4 shows the comparison results. We assume the communications between VLR and HLR are protected by NDS/IP [27] or MAPsec [26].

In the follow, the importance of above-mentioned demand will be mentioned and also included the introduction that our proposed.

- Mutual authentication: The requirement of mutual authentication in this paper indicates that each entities are able to authenticate the other parties in the procedure of the AKA scheme. In other words, the HLR should be able to verify the legitimacy of the VLR and MS, the VLR should be able to verify the HLR and MS, and, the MS is able to verify the HLR and VLR.

  In the proposed schemes, the HLR is able to verify the MS and VLR according to the messages sent in Step 2. The VLR can verify the HLR by checking r_1 in the $E_{K_{vh}}(TMSIn\|r_1\|h\|cert_{u_i})$, and, the MS can be verified through the value l sent in Step5. On the other hand, the MS can confirm the VLR and HLR via message $C = E_{K_{uh}}(TMSIn\|r_0\|r_1\|V)$ by checking the legitimation of r_0 and V.

- Data confidentiality: The purposed schemes should protect all of communication content secretly through the entire networks. This requirement emphasizes if an intruder is able to access the wireline communication networks, he/she will get nothing about the sensitive data (e.g. authentication vectors).

Our scheme achieves this requirement by employing a symmetric encryption algorithm $E_x(\cdot)$ to encrypt all of sensitive data in the entire networks.

- Identity/location confidentiality: In the authentication process, the real identity IMSI of MS should not be compromised despite what the situation is. Most of the existing schemes do not consider this requirement.

  Our scheme achieves this requirement by means of the TMSIo and TMSIn in the entire AKA scheme. Those potential eavesdropper cannot obtain the IMSI of MS and aware of his/her current location when the system of VLR fail. The main reason is the VLR also has no idea about the IMSI of MS. The related discussions can be found in Section 4.

- Home network should be partial trusted: As described in Section 3, a malicious system operator of the HLR may profit by leaking the authentication key K_{auth} of a MS to other MS'. This may result *MS'* can make free calls and eavesdrops all the conversation content of the legitimate MS. If *MS'* masquerades as legitimate MS to do evil, the situation will get worse. However, neither of the purposed schemes think over these problems, except [4]. Unfortunately, Buttyan et al. [24] pointed out that [4] failing to achieve this requirement.

  Our scheme fully consider about this weaknesses. We have demonstrated how the proposed scheme achieves this security requirement in Section 4.

- Reduction of bandwidth consumption: In the original UMTS AKA scheme, new authentication vectors need to transfer to the VLR again by the HLR if the previous authentication vectors are used up. If a scheme allows the VLR unnecessary to go back to HLR to require another set of authentication vectors, we consider it has realized this requirement.

Table 4: Comparisons among the authentication and key agreement schemes

Item	MA	DC	ILC	HTL	RBC	RSV	VHA	NRS
Our Method	yes	yes	yes	yes	yes	yes	yes	yes
UMTS AKA	yes	yes	no	no	no	no	no	no
Harn & Hsia[20]	no	no	no	no	no	no	no	yes
Peinado [18]	no	no	yes	no	yes	yes	yes	no
Hwanf & Chang [36]	yes	yes	no	no	yes	yes	yes	no
Lee et al.'03 [2]	no	no	no	no	yes	yes	yes	no
Lin & Jan [17]	no	yes	yes	no	yes	yes	yes	no
Buttyan et al. [24]	no	yes	no	no	yes	yes	yes	yes
Lee et al.'99 [3]	no	no	no	no	yes	yes	yes	no
Suzuki & Nakada [4]	no	yes	no	no	yes	yes	yes	no
Huang & Lee [37]	yes	yes	yes	no	yes	yes	no	no
Farhat et al. [38]	yes	yes	yes	no	yes	yes	no	no

MA: mutual authentication; DC: data confidentiality, both radio and inter-network;
ILC: identity/location confidentiality; HTL: HLR is partial trusted;
RBC: reduction of bandwidth consumption; RSV: reduction of VLR storage;
VHA: VLR substitutes as HLR to authentication MS; NRS: provide non-repudiation services;

Our scheme accomplishes this requirement by sending VLR an authentication key K_{auth} and $f^N(a_i)$ from MS. Therefore, the VLR is unnecessary to request another set of authentication vectors from HLR.

- Reduction of VLR storage: If a proposed scheme makes a VLR to store some copy of authentication vectors instead of n copies authentication vectors, it has attained this goal.

  In the proposed scheme, it is seen that the VLR only stores K_{auth} and $f^N(a_i)$. Therefore, the proposed scheme can save the storage of VLR.

- VLR substitutes as HLR to authentication MS: In the existing UMTS AKA scheme, the verification of MS is done in the VLR side by the assistance of the HLR. If the authentication vectors are used up, VLR is unable to verify the MS without the support of HLR. If the purposed scheme remedies this weakness, it will be treated as a solution of this drawback.

  In the proposed scheme, authentication of MS is done by VLR alone by means of the authentication key K_{auth} and $f^N(a_i)$. HLR is unnecessary to present if the authentication vectors are exhausted.

- Non-repudiation services: If a proposed scheme can provide service providers legal evidences to collect bill that are denied by subscribers, it has attained this goal.

  In the proposed scheme, we use hash chaining technique to achieve this goal. The detail discussion can be found in Section 4.

It is seen that our scheme accomplishes all the requirements shown above. The comparison results indicate that the purposed scheme is superior than other published schemes.

7 Discussions and Conclusions

Management of secret information such as secret key and private key is one of the most public discussion issues in cryptography. Since these keys have large key sizes, therefore, they are hardly to be remembered by human's memory. Usually, it is necessary to use a device such as a smart card to carry these secret information. In the proposed scheme, a MS's private key x is the case. Since a mobile phone may be equipped with a wiretapping device or might be infected by some computer viruses, therefore, execute all secret computations in a smart card are avoidable.

Unfortunately, most of smart cards are not so powerful to perform public key cryptographic algorithms. Therefore, how a smart card can efficiently execute secret computations using computing power of auxiliary devices (e.g. telephone) which are not necessarily trusted is an important topic.

Recently, Matsumoto, Kato, and Imai proposed the first SASC (Server-Aided Secret Computation) protocols in order to enable a smart card to perform secret computations faster with the aid of a auxiliary device [39]. Later, many related subjects have been discussed [40, 41, 42, 43, 44, 45, 46, 47]. When writing our paper, the center processor power of a mobile phone is up to 600MHz[3]. With the aid of a mobile phone and SASC protocol, we believe the proposed scheme can achieve the performance discussed in Section 5.1 eventually.

In this paper, we have listed out the security requirements for mobile communications. Furthermore, the existing system architectures of UMTS also studied. The paper not only introduces how the UMTS network working, but also study its authentication, data confidentiality, and subscribers identity/location confidentiality schemes.

We have shown that the proposed scheme can satisfy the security requirement, *home network should be partial trusted in the authentication scheme*, which represents a new security requirement for the related researches. We recommend that the security issues which related to UMTS should consider this new requirement in the future. We believe without this new requirement, the existing security schemes may cause the roaming service provided by UMTS become insecure and bring the MS into an unfavorable situation.

References

[1] M. J. Beller, L.-F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," in *IEEE Global Telecommunications Conference (GLOBECOM' 91)*, (Phoenix, Arizona), pp. 1922–1927, Dec. 1991.

[2] C.-C. Lee, M.-S. Hwang, and W.-P. Yang, "Extension of authentication protocol for GSM," *Proceedings of IEE on Communication*, vol. 150, Apr. 2003.

[3] For example, some mobile phones equipped with Intel PXA 270 processor providing processing power at 624MHz

[3] C.-H. Lee, M.-S. Hwang, and W.-P. Yang, "Enhanced privacy and authentication for the global system of mobile communications," *Wireless Networks*, vol. 5, pp. 231–243, July 1999.

[4] S. Suzuki and K. Nakada, "Authentication technique based on distributed security management for the global mobility network," *IEEE Journal on Selected Areas in Communications*, vol. 15, pp. 1608–1617, Oct. 1997.

[5] C. Xenakis, "Security measures and weaknesses of the GPRS security architecture," *International Journal of Network Security*, vol. 6, no. 2, pp. 158–169, 2008.

[6] D. Brown, "Techniques for privacy and authentication in personal communication systems," *IEEE Personal Communications*, vol. 2, pp. 6–10, Aug. 1995.

[7] G. Godor, B. Varadi, and S. Imre, "Novel authentication algorithm of future networks," in *International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 06'.*, pp. 80–86, Apr. 2006.

[8] M.-S. Hwang and C.-H. Lee, "Authenticated key-exchange in a mobile radio network," *European Transactions on Telecommunications*, vol. 8, no. 3, pp. 265–269, 1997.

[9] C.-H. Lee, M.-S. Hwang, and W.-P. Yang, "A novel application of the phone card and its authentication in mobile communications," *Journal of Information Science and Engineering*, vol. 15, no. 4, pp. 471–484, 1999.

[10] J. E. Wilkes, "Privacy and authentication needs of PCS," *IEEE Personal Communications*, vol. 2, pp. 11–15, Aug. 1995.

[11] C.-C. Yang, K.-H. Chu, and Y.-W. Yang, “3G and WLAN interworking security: Current status and key,” *International Journal of Network Security*, vol. 2, no. 1, pp. 1–13, 2006.

[12] K. V. Mangipudi, R. S. Katti, and H. Fu, “Authentication and key agreement protocols preserving anonymity,” *International Journal of Network Security*, vol. 3, no. 3, pp. 259–270, 2006.

[13] W.-S. Juang and J.-L. Wu, “Efficient user authentication and key agreement with user privacy protection,” *International Journal of Network Security*, vol. 7, no. 1, pp. 120–129, 2008.

[14] K. V. M. abd Rajendra S. Katti and H. Fu, “Authentication and key agreement protocols preserving anonymity,” *International Journal of Network Security*, vol. 3, no. 3, pp. 259–270, 2006.

[15] M. Barbeau and J.-M. Robert, “Perfect identity concealment in UMTS over radio access links,” in *IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005)*, vol. 2, pp. 72–77, Aug. 2005.

[16] W.-S. Juang, C.-L. Lei, and C.-Y. Chang, “Anonymous channel and authentication in wireless communications,” *Computer Communications*, vol. 22, pp. 1502–1511, Sep. 1999.

[17] W.-D. Lin and J.-K. Jan, “A wireless-based authentication and anonymous channels for large scale area,” in *Sixth IEEE Symposium on Computers and Communications*, (Hammamet Tunisia), pp. 36–41, Jul. 2001.

[18] A. Peinado, “Privacy and authentication protocol providing anonymous channels in GSM,” *Computer Communications*, vol. 27, pp. 1709–1715, Nov. 2004.

[19] S. Wang, Z. Cao, and H. Bao, "Efficient certificateless authentication and key agreement (CL-AK) for grid computing," *International Journal of Network Security*, vol. 7, no. 3, pp. 342–347, 2008.

[20] L. Harn and W.-J. Hsin, "On the security of wireless network access with enhancements," in *Proceedings of the 2003 ACM workshop on Wireless security*, (San Diego, CA, USA), pp. 88–95, Sep. 2003.

[21] H.-Y. Lin and L. Harn, "Authentication protocols with nonrepudiation services in personal communication systems," *IEEE Communications Letters*, vol. 3, pp. 236–238, Aug. 1999.

[22] J. F. Stach, E. K. Park, and K. Makki, "Performance of an enhanced GSM protocol supporting non-repudiation of service," *Computer Communications*, vol. 22, pp. 675–680, May 1999.

[23] J. Friis, "TETRA, the industry standard from ETSI," in *2nd TETRA Middle East Conference*, (Intercontinental Hotel Dubai), May 2004.

[24] L. Buttyan, C. Gbaguidi, S. Staamann, and U. Wilhelm, "Extensions to an authentication technique proposed for the global mobility network," *IEEE Transactions on Communications*, vol. 48, pp. 373–376, March 2000.

[25] G. M. Koien, "An introduction to access security in UMTS," *IEEE Transactions on Wireless Communications*, vol. 11, pp. 8–18, Feb. 2004.

[26] 3GPP TS 33.200, "3GPP: Techinical specification group services and system aspects; 3G security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security," Tech. Rep. Release 6, 3GPP, Dec. 2004.

[27] 3GPP TS 33.200, "3GPP: Techinical specification group services and system aspects; 3G security; Network Domain Security (NDS); IP network layer security," Tech. Rep. Release 6, 3GPP, Jun. 2004.

[28] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications ACM*, vol. 21, pp. 120–126, Feb. 1978.

[29] J. B. Lacy, D. P. Mitchell, and W. M. Schell, "Cryptolib: Cryptography in software," in *Proceedings of the UNIX Security Symposium IV*, pp. 1–17, 1993.

[30] B. Kaliski, "TWIRL and RSA key size," tech. rep., RSA Laboratories, May 2003.

[31] National Institute of Satndards and Technology (NIST), "Sepecial publication 800-57: Recommendation for key management. part 1: General guideline," tech. rep., National Institute of Standards and Technology, Jan. 2003.

[32] National Institute of Satndards and Technology (NIST), "Advanced encryption standard," Tech. Rep. FIPS 197, NIST, US Department Commerce, Nov. 2001.

[33] I. T. Union, "Recommendation X.509-the directory authentication framework," tech. rep., ITU-T, Nov. 1993.

[34] 3GPP TS 29.061, "3GPP: Technical specification group core network; interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)," Tech. Rep. Release 6, 3GPP, Mar. 2005.

[35] Telecommunication Standardization Sector of ITU, "ITU-T Recommendation E.212: Identification plan for land mobile stations," tech. rep., ITU-T, 1993.

[36] K.-F. Hwang and C.-C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," *IEEE Transactions on Wireless Communications*, vol. 2, pp. 400–407, March 2003.

[37] C.-M. Huang and J.-W. Li, "Authentication and key agreement protocol for UMTS with low bandwidth consumption," *Proceedings of the 19th International Conference on Advanced Information Networking*, p. 392 V 397, 2005.

[38] F. Farhat, S. Salimi, and A. Salahi, "An extended authentication and key agreement protocol of UMTS," *Lecture Notes in Computer Science*, vol. 5451/2009, pp. 230–244, 2009.

[39] T. Matsumoto, K. Kato, and H. Imai, "Speeding up secret computations with insecure auxiliary devices," in *Advances in Cryptology-Proceeding of Crypto'88*, pp. 497–506, Springer-Verlag, 1988. Lecture Notes in Computer Science, Vol. 403.

[40] R. J. Anderson, "Attack on server assisted authentication protocols," *Electronics Letters*, vol. 28, no. 15, p. 1473, 1992.

[41] P. Beguin and J.-J. Quisquater, "Secure acceleration of DSS signatures using insecure server," in *Advances in Cryptology-Proceeding of Asiacrypt'94*, pp. 249–259, Springer-Verlag, 1994. Lecture Notes in Computer Science, Vol. 917.

[42] P. Beguin and J.-J. Quisquater, "Fast server-aided RSA signatures secure against active attacks," in *Advances in Cryptology-Proceeding of Crypto'95*, pp. 57–69, Springer-Verlag, 1995. Lecture Notes in Computer Science, Vol. 963.

[43] S.-M. Hong, J.-B. Shin, H.-L. Kwang, and H. Yoon, "A new approach to server-aided secret computation," in *Proceedings of the 1st International*

Conference on Information Security and Cryptology-ICISC'98, (Seoul, Korea), pp. 33–45, 1998.

[44] S. Kawamura and A. Shimbo, "Fast server-aided secret computation protocols for modular exponentiation," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 778–784, 1993.

[45] H. Kim, Y. Lee, S.-M. Hong, and H. Yoon, "Active trial-and-error attack on SASC protocols," *International Journal of Network Security*, vol. 2, no. 2, pp. 105–110, 2006.

[46] Z. Wang, L. Wang, Y. Yang, and Z. Hu, "Comment on Wu et al.'s server-aided verification signature schemes," *International Journal of Network Security*, vol. 10, no. 3, pp. 238–240, 2010.

[47] S.-M. Yen, "Cryptanalysis of secure addition chain for SASC applications," *IEE Electronics Letters*, vol. 31, no. 3, pp. 175–176, 1995.