# An Enhancement of Authentication Protocol and Key Agreement (AKA) For 3G Mobile Networks

**Mustafa AL-Fayoumi** *fayoumi6@yahoo.com*
*Faculty of Engineering and Sciences*
*Al-Kharj University*
*Riyadh, 11942, Saudi Arabia*

**Ja'afer AL-Saraireh** *sarjaafer@yahoo.com*
*Information System*
*Applied Science University*
*Amman, 11931, Jordan*

**Abstract**

This paper proposes a secure authentication mechanism by integrating the public key with the hash-chaining technique. The propose protocol satisfies the security requirements of third generation (3G) mobile networks. Also provide the protection of the international mobile subscriber identity (IMSI) to ensure subscriber un-traceability, key refreshment periodically, strong key management and a new non-repudiation service in a simple and elegant way. The proposed protocol is more secure protocol than the other available authentication protocols. To avoid the complicated synchronization as in universal mobile telecommunications system (UMTS) the proposed protocol does not use sequence number (SEQ), the management of a hash chain is simple and elegant compared to that of SEQ. This proposed protocol is secure against network attacks, such as replay attacks, guessing attacks, and other attacks.

**Keywords:** Mobile Security, 3G, AKA, public-key, cryptography.

## 1. INTRODUCTION

In order to provide security services in wireless networks, authentication is used as an initial process to authorize a mobile terminal for communication through secret credentials [1] [2]. In authentication process, a mobile terminal is required to submit secret materials such as certificate or "challenge and response" values for verification. Without strong authentication, mobile networks access is unprotected through the release of message contents, modification of message or denial of service can be accomplished easily by an intruder.

There are three entities participating in the UMTS security architecture, home environment (HE), serving network (SN) and mobile station (MS). Figure 1 illustrates the UMTS architecture. The HE contains the home location register (HLR) and authentication centre (AuC). The SN consists of the visited location register (VLR) and the Serving GPRS Support Node (SGSN). The VLR handles circuit switched traffic, but the SGSN handles the packet switched traffic [3].

Authentication procedure is executed when the MS moves from one registration area (RA) to another one (location update) during the process of calls origination and call termination. The MS is continuously listening to the broadcast message from VLR/SGSN to identify the location area by using location area identity (LAI) and the MS compares the LAI which is received with the LAI that stored in the universal subscriber identity module (USIM). When the LAI is different than the MS executes authentication procedure [2].

An authentication mechanism is a process designed to allow all participants show their legality and verify the other participant's identities that involved in the networks. This mechanism using secret key K, and cryptographic algorithms - include three message authentication codes f1,

f1*and f2 and four key generation functions f3, f4, f5 and f5*- [3] [4] [5] that are shared between MS and the HLR/AuC. This is known as authentication and key agreement protocol (AKA). The AuC maintains a counter called sequence number (SQNHLR), where user MS maintains a counter (SQNMS), whose initial value for these counters are set to zeros [4] [5].

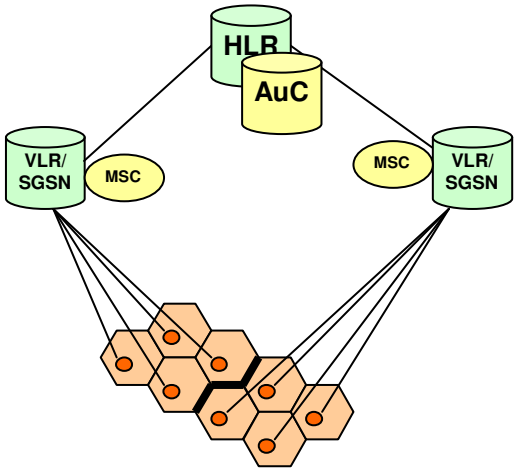


**FIGURE 1:** UMTS Architecture

There are three goals for the UMTS AKA [4]: a mutual authentication between the user and the network; an establishment of a cipher key and an integrity key upon successful authentication; and a freshness assurance to the user of the established cipher and integrity keys.

There are two phases in AKA protocol [4] [3]

i. *MS* registers with its *HLR/AuC* and then generates and distributes authentication vectors from the *HLR/AuC* to the *VLR/SGSN*.
ii. The authentication and key agreement procedure between the *MS* and the *VLR*.

Figure 2 describes authentication mechanism as follow:

1. When the MS moves to new *VLR/SGSN* area then MS sends *(IMSI)* authentication request to *VLR/SGSN*.
2. *VLR* passes this authentication request to *HLR*.
3. *HLR* generates authentication vectors *AV(1..n)* and sends authentication data response *AV(1..n)* to *VLR/SGSN*, where each authentication vector is called a quintet This *AV* consists of five components: random number (*RAND*), expected response (*XRES*), cipher key (*CK*), integrity key (*IK*) and authentication token (*AUTN*). The authentication vectors are ordered by the sequence number $SQN_{HLR}$. The authentication vector is generated according to the following sequence:
   i. *HLR/AuC* generates $SQN_{HLR}$ and *RAND*.
   ii. *HLR/AuC* computes $XRES = f_2(K,RAND)$, $CK = f_3(K,RAND)$, $IK = f_4(K,RAND)$, Anonymity Key $AK = f_5(K,RAND)$, Message Authentication Code $MAC = f_1(K,SQN||RAND||MAF)$, where *MAF* is Message Authentication Field and $AUTN = (SQN \oplus AK||AMF||MAC)$ where $\oplus$ is exclusive OR operation.
   iii. *HLR/AuC* $SQN_{HLR}$ is increased by 1.
4. *VLR* stores authentication vectors. In the $i^{th}$ authentication and key agreement procedure, *VLR/SGSN* selects the $i^{th}$ authentication vector *AV(i)*, and sends (*RAND (i), AUTN(i)*) to *MS*. In the *VLR* one authentication vector is needed for each authentication instance. This means that the signalling between *VLR* and *HLR/AuC* is not needed for every authentication events.
5. *MS* computes and retrieves the following:

i. Anonymity key *AK = F5 (Rand, K)*, *SQN =( (SQN* $\oplus$ *AK)* $\oplus$ *AK)*, computes expected message authentication code $XMAC = f_1 (SQN, RAND, AMF)$ and then,
ii. Compares *XMAC* with *MAC* which is included in *AUTN*. If *XMAC* is not equal to *MAC* then *MS* sends failure message to the *VLR/SGSN*, else if *XMAC* is equal *MAC* then *MS* checks that the received *SQN* is in the correct range i.e. $SQN > SQN_{MS}$. If *SQN* is not in the correct range then *MS* sends failure message to the *VLR/SGSN*, else if it is in the correct range, then *MS* computes the Response $RES = f_2 (K, RAND)$, and $CK = f_3 (K, Rand)$,
iii. After that, it sends *RES* to *VLR/SGSN.*

6. *VLR* compares the received *RES* with *XRES*. If they match, then authentication is successfully completed.
7.

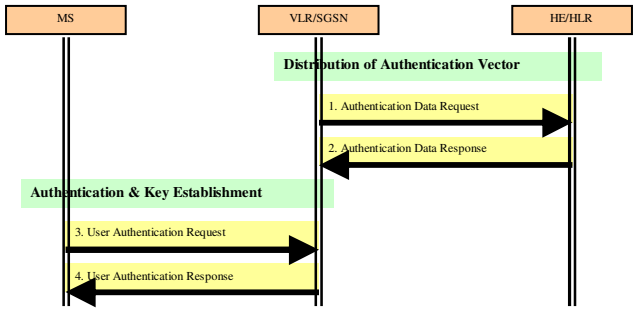


**FIGURE 2:** Authentications and Key Agreement Protocol

This paper is organized as follows. Section 2, the literature review and related works is presented. In Section 3, the framework for the proposed protocol is described. The operation modes for the proposed protocol are described in Section 4. The description of initial and subsequent authentication for the proposed protocol is presented in Section 5. The security analysis for the proposed protocol is presented in Section 6. In Section 7, a comparison with UMTS AKA protocol and related works is carried out. The paper is concluded in Section 8.

## 2. RELATED WORKS

Several authentication schemes have been proposed for mobile networks to enhance the security of mobile communication systems. However, these schemes cannot fulfill the security requirements of 3G mobile systems [6]. Specifically, the schemes proposed by [7] [8] [9] [10] [11] [12] [13] [14] and [15] were not designed based on 3G mobile systems and incur much computational overheads. The authentication techniques for 3G mobile networks are presented by [8] [16] [17]; but these techniques did not address other security issues, such as end to end security, anonymity and confidentiality issues.

The International Telecommunication Union (ITU) proposed three authentication techniques for International Mobile Telecommunications-2000 (IMT-2000), which is the global standard for 3G. These techniques only provide some security features and have some weaknesses. The first technique is based on the use of symmetric key cryptosystems and a challenge-response exchange. This technique requires too many authentication messages and does not ensure end to end security. Also, assuming the connection between the network operator and service provider is secure; the messages that are transmitted through the connection are vulnerable. The second authentication technique is based on the unilateral use of a digital signature scheme and a challenge-response exchange. This technique did not provide mutual authentication or end to end security and created high computation costs. The third technique is also based on the use of a digital signature scheme. The public key certificates and timestamps are combined to provide user identity confidentiality and unilateral entity authentication in a single mechanism. The third technique is the same as the second technique; but did not provide mutual authentication, end to end security and created high computation costs. In all of these techniques the authentication

technique is fixed, such as that the network operators of visited domains must be involved in the authentication procedure between roaming users and home service providers. This represented a common weakness in the three techniques.

An end to end authenticated session key exchange protocol based on the certificate over several distinct networks is presented by [18]. This protocol is not built upon a certain public key system, but the protocol can be built upon Modular Square Root (MSR) or RSA. The proposed protocol has some disadvantages, such as the public key systems (MSR and RSA) require large storage and bandwidth requirement during the execution, and the user identifications are stored in certificates and these certificates are exchanged between the users and the network in the plain text, and thus user identity confidentiality is not provided.

Asymmetric cryptography in UMTS networks is proposed by [19]. This method consists of the introduction of public-private key pairs for the transactions between the *VLR* and *HLR*, as well as the *MS* and *VLR*. The information exchanged between the *VLR* and the HLR is based on the good trust link between these nodes. However, according to specifications that define GSM, GPRS and UMTS, there is no mutual authentication between the *VLR* and *HLR*, and no data encryption takes place when these two nodes communicate. The *HLR* consider that the *VLR* is a trusted partner, and based on this consideration it delivers information to the *VLR*, and the *VLR* delivers information to the *HLR*. The link between the *VLR* and *HLR* is exposed to any kind of attack (e.g. masquerading, data distortion, etc.).

Using public keys in the authentication process in mobile networks was abandoned because of backwards compatibility with GSM and for the performance consideration [20] [21] [22].

UMTS AKA has some problems, including bandwidth consumption between a serving network and a user's home network, space overhead of the serving network. Huang and Li propose an extension of UMTS AKA protocol, called UMTS X-AKA, to overcome the above mentioned problems of UMTS AKA [23].

Zhang and Fang, Zhang and Fujise , and Zhang showed that the 3GPP AKA protocol is vulnerable to a variant of the false base station attack [4] [24] [25] [26]. The vulnerability allows an adversary to redirect user traffic from one network to another. It also allows an adversary to use authentication vectors corrupted from one network to impersonate all other networks. Zhang and Fang presented a new authentication and key agreement protocol, which overcomes redirection attack and drastically lowers the impact of network corruption. The protocol, called adaptive protocol AKA (AP-AKA), also eliminates the need of synchronization between a mobile station and its home network [4].

A new technique for public key image authentication using fussy computations for El-Gamal authentication technique is proposed by [27]. A mutual authentication key and key exchange protocol suitable for application is proposed by [28]. This protocol named F-MAKEP. The F-MAKEP scheme integrated into Wireless Transport Layer Security (WTSL) framework; the security was enhanced while more computation overhead was incurred.

The UMTS AKA protocol has the problem of the bandwidth consumption between *SN* and *HN*. It is attractive to choose a suitable length (*L*) value for *AV* in the third generation mobile networks. So, many techniques are developed to minimize the authentication signalling cost and network bandwidth with consumption by selecting the dynamic length (*L*) for an authentication vector. Yet with this improvement, Lin and Chen (and AL-Saraireh and Yousef, are still there are bandwidth consumption [3][29].

The technique of Lin and Chen [29] basically estimates the number of authentication requests in current visited network based on the number in the previous visited network. Whereas the method of AL-Saraireh and Yousef [3], estimates the number of authentication requests in current visited network based on the history of mobile movements and the arrival rate for events.

## 3. FRAMEWORK FOR PROPOSED PROTOCOL

In third generation mobile systems, many emerging services, such as the World Wide Web, stock quotes, e-mail account and multimedia, can be accessed through a wireless link. When a mobile user roams far from his home domain and wants to access these services, the user may intend to use the servers in a visited domain instead of the ones in his home domain. To meet today's needs for wireless communication the protocols need to be highly secure, and require low computational overhead and thus low power.

To acquire mobile services in visited domains, mobile users must be authenticated. Normally, the VLR/SGSN in a visited domain is unable to solely perform the authentication procedure without any prior knowledge of the roaming user; hence, the visited domain requires the participation of the home domain to authenticate the user.

In fact, the VLR/SGSN in the visited domain may simply forward the authentication request to the home domain and check the reply to see if the user has been successfully authenticated. In this way, the role that the VLR/SGSN in the visited domain plays is more like that of an authentication proxy. This paper presents a secure and efficient authentication framework for mobile systems, where VLR/SGSN have the capability to authenticate the user or roaming user without intervention of HLR in the home network during origination and termination of the call. Basically, the proposed authentication framework consists of the same parts as in the UMTS systems, three nodes are involved in the authentication protocol; namely, the Mobile Station (MS), the Visitors Location Register (VLR), and the Home Location Register (HLR).

To enhance the 3G AKA protocol, the proposed authentication protocol has adopted three major techniques: digital signature, Message Authentication Code (MAC) and hash chaining. Public key cryptography has not previously been used in mobile communication environments due to performance constraints. It was not consider suitable for second generation systems because of the resulting length of messages and the necessary computational loads. New protocols for authentication between user and network have been developed to overcome these problems. The proposed protocol is based on a digital signature cryptography scheme. A true non-repudiation service among HLR, VLR and MS can only be achieved via a public-key system using digital signatures [30]. A digital signature can be used in a public-key system to replace HMAC.

One-way function is a variation of the message authentication code as with the message authentication code, a hash function accepts a variable size message *M* as input and produces a fixed size output, referred to as a hash code *H (M)*. The hash code is a function of all the bits of the message and provides an error detection capability. When it changes any bits in the message result in a change to the hash code, a hash function *H* has some properties [31].

The proposed protocol uses a one-time password/hash-chaining technique which was proposed by Lamport [32]. It used a hash function with one-way property to construct a sequence of hashing value. They designed it in a remotely accessed computer system. One of the aims of the one-way hash function is to prevent eavesdroppers discovering the password and to reduce the computing time, which this technique has used in many applications [33].
In this method, let the user (claimant) and the server (verifier) deal with the secret *(M)* as a seed of hash value and *f(M)* be a one-way function, when a user (i.e., the one wishes to be authenticated) wants to register or log in the system, then the user should construct $f^n(M)=f(f(\ldots(f(M)\ldots)))$, where $n$ represents the maximum number of services that the user can request after the registration phase ( i.e., the composition of $nfs$ ), and sends $f^n(M)$ to the server (i.e., the one decides whether the user is who it is). Then the server uses it to compute a sequence of passwords $f^{n-1}(M), f^{n-2}(M), \ldots, f(f(f(M))), f(f(M)), f(M)$ and the server stores those. The user holds $f^n(M), \ldots, f(f(f(M))), f(f(M))$.

After the registration is completed, each hash chain can be used by the claimant to prove itself to the server $N$ times. In the $j^{th}$ session, the user provides $f^{n-1}(M)$ to ask for a connection to prove itself. The server can verify the correctness of $f^{n-1}(M)$ by means of the one way function by computing $f(f^{n-1}(M))$ and the server needs to store $f^{n-1}(M)$ as the last value of user to authenticate the next visit. So, the user reveals $f^{n-1}(M)$, $f^{n-2}(M),\ldots,f(M)$, and $M=f^{0}(M)$ in sequence to prove itself $n$ times. In this way $f^{n-j}(M)$ can be used as a proof of the $j^{th}$ connection.

In the proposed protocol the dynamic concept achieved through management the dynamic keys between the MS ⇔ HLR/AuC and MS ⇔ SGSN/VLR. In other words the dynamic mechanism works at two levels by the keys refreshment are used whether at MS/HLR and MS/VLR for each Initial and subsequent authentication session respectively. Moreover, this property provides service providers with the ability to develop proprietary authentication mechanisms and adjust the keys in run time.

Where in the dynamic key agreement the HLR/AuC is determine number of subsequent authentication procedure that will be executed for each time the initial authentication procedure starts which will discusses in the following section.

When MS makes a service contract with his/her home network HLR generates the public and private keys and subscribes public key to MS and keeps it in its database and save KHU, IMSI and $Cert_M$ in the SIM/USIM of MS. In the initial authentication procedure the MS encrypt an Authentication Request Message between MS to HLR ($AUTHM_H$ ) by HLR's public key that has been saved in the SIM. HLR decrypt it by its private key, and then refresh the new public key and send back to MS within Authentication Data Response Message between HLR to MS ($RAUTHM_H$) to use it in the second time. Consequently, Dynamic key management is achieved at the level of MS and HLR/AuC.

Meanwhile, the MS generates a session key $K_{VM}$ = f ($K_{VM}$, IK ⊕ CK) as a shared key between MS and SGSN/VLR, where IK and CK are a nonce numbers and $f^{n}$(M) where $f^{n}$(M) is a one-way hash chaining function and n represents the maximum number of services that the MS can request after initial authentication, then send it within $AUTHM_H$ to SGSN/VLR through HLR. The VLR save $K_{VM}$, CK and f n(M) under the ID of that user and sends Authentication Data Response Message between VLR to MS ($RAUTHM_V$ ) encrypted by the session key KVM of its response message.

In the subsequent authentication procedure the MS generates a new session key $K_{VM}$' = $f$ ($K_{VM}$, IK ⊕ CK), where IK is a new generated nonce and $K_{VM}$ is the shared key. CK is in the messages sent by the MS to the VLR in the initial authentication procedure. Meanwhile, the MS produces $f^{n-i}$(M), where ( i) is the number of services that have been requested, and M is the secret key generated in the initial authentication. VLR generates a new session key $K_{VM}$' using the same function used by the MS and then encrypts $RSAUTH_{UV}$ = (IK+1 ⊕ TMSI) with $K_{VM}$', and then sent is sent back to the MS. After that upon receipt of the response message, the MS decrypts the $RSAUTH_{UV}$ using $K_{VM}$'.

The subsequent authentication procedure only contains two message exchanges. The nonce number IK transmitted between the MS and VLR is used to refresh the session key. In this way, the encryption key used for every session is different. Except for the first session key, key generation is performed by both the MS and VLR. The first session key is generated by the MS and sent to the VLR. After that, the VLR can generate the following session key by itself. By using $K_{VM}$ and IK ⊕ CK as two inputs, the MS and VLR can generate the same new session key if the inputs are identical. Consequently, Dynamic key management is achieved at the level of MS and SGSN/VLR.

Therefore, using the refreshment keys concept in both MS, SGSN/VLR and HLR/AuC according to the n and t value which has determined by MS and HLR/AuC respectively, the subscribed

service period (t) is used to determine whether the service request is out-of-date or not, and (*n*) is used to determine the number of times and the ith session to perform the subsequent authentication procedure dynamically, without transfer any clear parameters. In the i-th session, the user provides $f^{n-i}$ (M) to ask for a connection to proof of the i-th connection. Consequently, Dynamic key management is achieved at the level of MS and SGSN/VLR.

## 4. OPERATION MODES

In this proposed protocol, VLR/SGSN in SN maintains the profiles and privileges of the registered MS. Thus, only the MS's home network (HLR) can initially authenticate the MS. Another entity, the VLR/SGSN in SN, is responsible for forwarding the MS's authentication request to the HLR in HN. In the proposed protocol, after initial authentication has been performed, the VLR/SGSN in SN is then capable of authenticating the MS when it is required. The proposed authentication protocol contains two operation modes for initial and subsequent authentication.

i. **Registration and Distribution of Authentication Information (Initial Authentication):** This procedure is used when a mobile user (MS) leaves his home domain and roams to a visited domain. The user may request services from the network operator of the visited domain. In this case, the initial authentication shown in Figure 3 is performed between the three parties. First, the request message is generated by the MS and sent to the authentication VLR/SN in the visited domain. Since the VLR/SN is unable to authenticate the MS by itself, it forwards it to the HLR in MS's home domain. The verification procedure is performed by the HLR. A response message is generated corresponding to the authentication result as authentication vector (AV). The VLR/SN forwards the response message to the MS and decides whether or not to provide the service to the MS according to the authentication result. Here, the VLR/SN caches some authentication information, which can be used in subsequent authentication. The response message lets the MS know whether the authentication was successful or not. After the initial authentication, both the VLR/SN and MS obtain the authentication result from the HLR/HN and share some secret information without intervention of HLR/HN.

ii. **Authentication and Key Agreement (Subsequent Authentication):** After initial authentication, the VLR/SGSN has the ability to authenticate the MS in subsequent communication. If the MS remains in the same visited domain and requests services, then the user should ask for subsequent authentication. MS similarly generates an authentication request message, which should contain the information shared between the MS and VLR/SN; the VLR/SN then uses this information to authenticate the MS. As mentioned above, the VLR/SN has cached information needed to authenticate MS. After authenticating the MS, the VLR/SSN sends a response message containing the authentication result to the MS. The MS receives the response message and learns whether the authentication was successful or not.

## 5. DESCRIPTION OF THE PROPOSED PROTOCOL

In this section, the proposed protocol shows how the proposed framework can be applied to improve the performance of authentication in call setup services. The proposed protocol satisfies the security requirements of third generation mobile systems and has the advantages of a dynamic framework.

The proposed scheme involves the use of a public key of HLR and VLR, which is used for a legitimate MS to encrypt an authentication key that generated by the MS himself/herself and passes it to VLR. Moreover, we simply employ a challenge response to resist the replay attacks.

The proposed authentication protocol is divided into two procedures; the first one is called the initial authentication procedure, which flow from MS⇔VLR⇔HLR. The second one is limited between MS⇔VLR and is called the subsequent authentication procedure.

### 5.1 Initial Authentication Procedure

To mitigate the computation burden of mobile equipment, the encryption is clone in MS side since the public key operation takes O (K2) complexity but private key operation takes O (K3) complexity with the typical modular exponentiation algorithms used to implement the RSA algorithm, where K is the number of bits in the modulus. Table 1 gives the software speeds of RSA [34]. RSA goes much faster if we choose a value of e carefully. Therefore, we suggest the exponent value e should be smaller. In order to make use of public key cryptography on the low-computation mobile equipment, the related research can be found in [35].

| **RSA Speeds for Different Modulus Lengths with an 8-bits 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* |

**TABLE 1:** Software speeds of RSA

In 2003, RSA Laboratories recommends the minimum key length for general data is 1024 bits without any specifying lifetime [36]. NIST recently recommends 1024 bits for RSA, which is taking into account the lifetime of the data. For security concerns and the execution speeds of the public key encryption, we suggest the value of public key length is optimally 1024 bits.

Before we describe the common registration phase of the proposed mechanism, we assume the following operations are performed when MS makes a service contract with his/her home network HLR:

- HLR generates the Public and Private Keys.
- HLR subscribes (Public Keys) to MS.
- HLR produces a certificate $Cert_M$ to (Public Keys) and keeps it in its database. HLR writes $K_{HU}$, IMSI and $Cert_M$ in the SIM/USIM of MS.
-

At first, the scheme consists of four messages exchanged between the MS, VLR and HLR. The message flows are indicated in Figure 3. The notations are defined as follows:

NOMENCLATURE

| | |
|---|---|
| *IMSI* | *International* Mobile Subscriber Identity |
| *TMSI* | Temporary Mobile Subscriber Identity generated by HLR/AuC |
| $K_{HU}$, $K_{HP}$ | Public/private key pair of HLR |
| $K_{VU}$, $K_{VP}$ | Public/private key pair of SGSN/VLR |
| $K_{HU}'$ | The new HLR's public key |
| $K_{VM}$, | Session key shared by the MS and SGSN/VLR |
| $K_{VM}$ | $f$(IK, CK): session key between the MS and VLR, the function $f$ may be a simple function. e.g. the XOR of IK and CK. $h$ ($K_{VM}$, $IK \oplus CK$) |
| *IK, CK* | Nonce numbers |
| *T* | Subscribed Service Period |
| $f$ ( ) | A one way Hash function; |
| $AUTH_{MH}$ | Authentication Request Message between MS to HLR<br>$ID_M$, $ID_H$, $E_{KHU}$ ( IMSI‖ IK ‖CK‖ $K_{VM}$‖ $f^n$ (M)‖ $n$‖$ID_V$) |
| $AUTH_{VH}$ | Authentication Request Message between VLR to HLR<br>$ID_V$, $E_{KVP}$ ($ID_V$, $R_V$) |
| $RAUTH_{MH}$ | Authentication Data Response Message between HLR to MS<br>$E_{KHP}$ ($ID_H$ ‖ IK+1$\oplus$ TMSI ‖T‖ $K_{HU}'$ ‖ $K_{VU}$ ) |
| $RAUTH_{MV}$ | Authentication Data Response Message between VLR to MS<br>$E_{KVP}$ ($E_{KVM}$ (IK+1), TMSI )) |

$RAUTH_{HV}$ Authentication Data Response Message between HLR to VLR
$E_{KVU}$ ($R_V$ ‖ IK ‖CK‖ $K_{VM}$‖ $f^n$ (M)‖$n$ ‖ T ‖ TMSI)
$ID_M$ The identity of the MS
$ID_V$ Identity of VLR
$ID_H$ Identity of HLR
$\oplus$ Logical computation, bit-wise exclusive or operation

To exercise the proposed protocol, this section describes how that can be applied to enhance the authentication procedure. It is known that the authentication process is achieved by all the authentication entities of 3G mobile network. The proposed authentication protocol is divided into two procedures; the first one is named Initial authentication procedure, which flow from MS⇔VLR⇔HLR. The second one is limited between MS⇔VLR is the Subsequent authentication procedure.

In the proposed authentication protocol, we assume that MS⇔HLR/AuC and SGSN/VLR⇔HLR/AuC have the public/private key pair and use Public-Key cryptosystems. In addition, there is public key infrastructure so that public keys can be correctly and efficiently distributed. This enables all entities of network (3G) to mutually authenticate each other easily. MS can obtain the public key of the VLR to be sent by the HLR. At first, the MS sends secret message to challenge the VLR and HLR, and the VLR also sends secret message to challenge the HLR. However these secret messages are encrypted with its public and private key respectively. After that the VLR and HLR send a message to response the MS that decrypt by it's private key. The HLR also decrypts the secret messages to response the VLR based on VLR's public key. If the processes are finished, they can achieve mutual authentication between all participants, and refresh the HLR's public key.

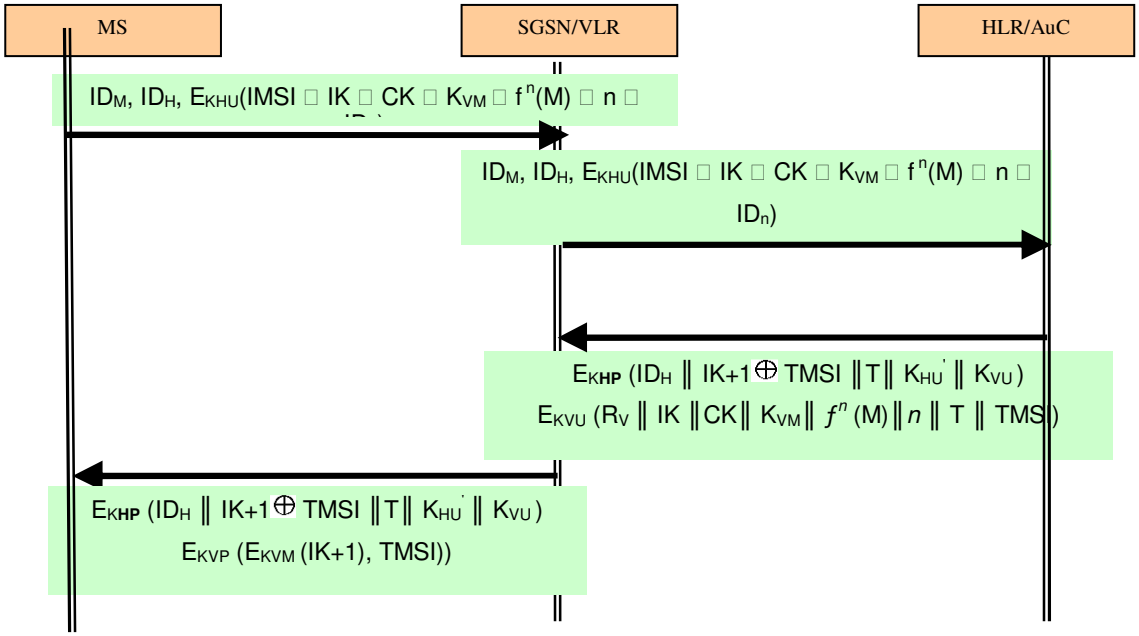


**FIGURE 1:** Proposed Initial authentication procedure

**Step 1:** M1 Authentication Request Message
When an MS needs to authenticate itself to all entities of network to access or utilize of network services, The MS invokes the distribution of authentication procedure by sending the Authentication Request messages to the HLR/AuC (***AUTH***$_{MH}$) through VLR. Authentication

between the MS and his HLR/AuC relies on the use of its public key KHU. This process is achieved as follows:
The MS generates the following:

1. The Nonce Numbers IK, CK
2. The Session Key $K_{VM}$
3. M is secret information
4. $f^n(M)$ where $f^n(M)$ is a one-way hash function and n represents the maximum number of services that the MS can request after initial authentication. Here $f^n( ) = f(f^{n-1}( ))$, $f^1( ) = f( )$.

The MS sends ***$AUTH_{HM}$*** to VLR:
$AUTH_{MH}= ID_M, ID_H, E_{KHU}(IMSI \square IK \square CK \square K_{VM} \square f^n(M) \square n \square ID_n)$, where $ID_M$ is the identification of the MS that HLR can verify his signature.

**Step 2:** M2 Authentication Request Message
When the VLR receives the message from the MS, it passes the message to the HLR, and sends the $AUTH_{VH}$ of its challenge message to the HLR. However, the $(ID_V \| R_V)$ $K_{VP}$ is encrypted by its private key. After receiving these messages, the HLR decrypts by their corresponding private and public key them access the database to obtain the CertM and $Cert_V$, respectively.

$$ID_V, E_{KVP} (ID_V, R_V)$$

**Step 3:** M3 Authentication data Response Message
The HLR sends $RAUTH_{HM}$ encrypted by HLR's private key and $RAUTH_{HV}$ encrypted by VLR's public key of its response messages to the VLR, respectively. After receiving these messages, the VLR decrypts $RAUTH_{HV}$ by his secret key to get $R_V$, TMSI, IK, CK, $K_{VM}$, $f^n$ (M), n and T. Then, the VLR saves $f^n(M)$, n, and CK for subsequent authentication and session key generation.

$$RAUTH_{HM} = E_{KHP} (ID_H \| IK+1 \oplus TMSI \| T \| K_{HU}' \| K_{VU})$$

**Step 4:** M4 Authentication Response Message
The SGSN/VLR sends $RAUTH_{HM}$ encrypted by HLR's private key and $RAUTH_{VM}$ encrypted by VLR's private key of its response to the MS. After receiving these messages, the MS decrypt $RAUTH_{HM}$ by HLR's public key to get $K_{VU}$, $K_{HU}$', IK+1, TMSI and $ID_H$. After getting $K_{HU}$', it knows that key refreshment is successfully. Filially, it gets KVU that has sent from HLR to decrypt $RAUTH_{VM}$ to obtain $E_{KVM}$ (IK+1), TMSI and then encrypt $E_{KVM}$ (IK+1) to get IK, then MS verifies the value of (IK + 1) if it is correct, then the authentication is successful, and the MS gets new temporary identities, TMSI'. Also, $K_{VM}$ becomes the shared key used by the MS and SGSN/VLR, the authentication process is finished.
$RAUTH_{HM} = E_{KHP} (ID_H \| IK+1 \oplus TMSI \| T \| K_{HU}' \| K_{VU})$
$RAUTH_{VM} = E_{KVP} (E_{KVM} (IK+1), TMSI ))$

### 5.2 Subsequent Authentication Procedure

After the initial authentication, SGSN/VLR gets a secret key KVM that it shares with the MS and subsequently can accomplish the authentication by itself. That is, subsequent authentication only happens between the MS and SGSN/VLR using two message exchanges. Figure 3.2 exhibits the subsequent authentication procedure, and the authentication steps are described as follows.

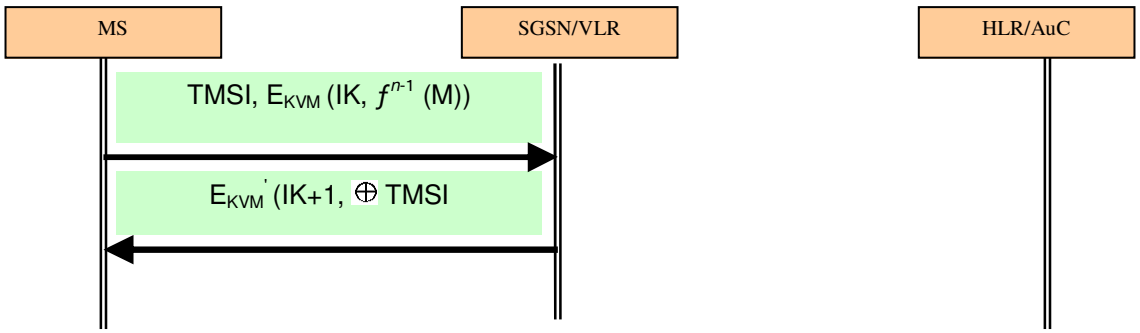


**FIGURE 4:** Subsequent authentication procedure

The notations in Figure 2 are defined as follows:

- $SAUTH_{MV}$: TMSI, $E_{KVM}$ (IK, $f^{n-1}$ (M))
- $SRAUTH_{VM}$: $E_{KVM}'$ (IK+1, ⊕ TMSI)

**Step 1:** The MS generates a new session key $K_{VM}' = h\ (K_{VM}, IK \oplus CK)$, where *IK* is a new generated nonce and $K_{VM}$ is the shared key. *CK* is in the messages sent by the MS to the VLR in the initial authentication procedure. Meanwhile, the MS produces $f^{n-j}(M)$, where *i* is the number of services that have been requested, and *M* is the secret key generated in the initial authentication. The MS sends $SAUTH_{MV}$ that encrypted the session key $K_{VM}$ to the VLR, which contain *IK*, $f^{n-j}(M)$.

$SAUTH_{UV}$: TMSI, $E_{KVM}$ (IK, $f^{n-1}$ (M))

**Step 2:** SGSN/VLR first checks the subscribed service period of the mobile user for the requested service. If the service request is not made within the valid subscribed service period, the service request is rejected. The procedure then restarts from step 1.1. Else SGSN/VLR decrypt $SAUTH_{MV}$ by the shared session key $K_{VM}$ and compares the result with *IK*. Moreover, SGSN/VLR computes $f(f^{n-j}(M))$ to verify whether it is the same as the number, $f^{n-i+1}(M)$, which SGSN/VLR saved in the last authentication. If they are identical, the MS has been authenticated successfully. SGSN/VLR send $RSAUTH_{MV} = (IK+1 \oplus TMSI)$ encrypted by the new session key $K_{VM}'$, which was generated using the same function that used by the MS. Upon the MS receipt of the response message, the MS decrypts the authenticator using $K_{VM}'$.

$SRAUTH_{UV}$: $E_{KVM}'$ (IK+1, ⊕ TMSI)

## 6. SECURITY ANALYSIS

In accordance with the proposed scheme, it is assumed that a VLR has powerful computation ability and has no worry about power supply, which means it can handle more complex calculations. Since we consider the low computation ability and low power of mobile equipments, we make the RSA encryption be clone in MS side. Table 3.1 indicates that the RSA encryption provides far superior performance than decryption.

Furthermore, the session key $K_{VM}$ is generated by MS. The VLR will use the key to verify the MS again when he/she requires a service, e.g. making a call etc. We assume that the authentication key is generated through a secure random number generator and kept securely for each related parties. Based on the recommendation of RSA Laboratories and NIST, 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, which means it can hardly be broken using today's computer 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.

Furthermore, the KHP is supposed to be kept secretly by HLR. Base on these hypothesis, we make the following security analysis to prove that our modification is robust and against to replaying, guessing and substitution attacks. Note that the analysis is based on the UMTS.

In this section, we will discuss the security of the proposed protocol. In order to ensure that the proposed protocol is secure, we will analyze and discuss the attack methods. The security requirements of third generation mobile systems are mutual authentication, MS anonymity, end-to-end security, non-repudiation, and data integrity and data confidentiality. The proposed scheme can fulfill all of these requirements.

First, consider the authentication requirement. It is clear that the proposed authentication protocol can authenticate MS, HLR/AuC and SGSN/VLR. Because the message sent to the HLR/AuC is encrypted using its public key $K_{HU}$, there is no one except for the home HLR/AuC can decrypt the message. Therefore, authentication between the MS and the HLR/AuC can be achieved using $K_{HU}$. Consequently, mutual authentication is achieved.

Next, consider MS anonymity. To provide MS anonymity, the permanent identity IMSI of MS is never exposed in the plain-text mode. A cracker cannot get the real identity of MS by eavesdropping on the authentication messages on both wireless and wired networks.

Consider the requirement of non-repudiation; our protocol can also satisfy this requirement. By using the one-way function, we can achieve non-repudiation. In the $i^{th}$ session, the user provides $f^{n-i}$ (M) to ask for a connection. The SGSN/VLR can verify the correctness of $f^{n-i}$ (M) by means of the one way function, but it cannot derive $f^{n-i}$ (M) from $f^{n-i+1}$(M). In this way, $f^{n-i}$ (M) can be used as a proof of the $i^{th}$ connection. Whenever a random challenge occurs, the SGSN/VLR can be required to show $f^{n-i}$ (M).

The requirement of end-to-end security is also addressed in the proposed protocol. When a MS makes a call, the caller and callee negotiate a common encryption key to encrypt the data flowing over the channel. Since the full communication path is protected, data confidentiality and integrity are both achieved. The communication between the two parties in both wired and wireless paths is protected with the encryption key $K_e$. Therefore, end-to-end security is achieved in this way.
The proposed authentication protocol achieves all the requirements shown above. The proposed scheme is superior to other published schemes. The proposed protocol can prevent common attacks as follows:

**i. Replay Attacks**

It can repulse replay attack, a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. Hackers capture old messages and replay them at later times. By replying to the message it appears to be legal. Suppose *MS* wants to prove its identity to the *HLR*. The *HLR* requests its *IMSI* as proof of identity, which *MS* dutifully provides (possibly after some transformation like a hash function). Meanwhile, the hacker is eavesdropping on the conversation and keeps the *IMSI*. After the interchange is over, the hacker connects to the *HLR* posing as the first *MS*. When asked for proof of identity, the hacker sends the first MS's *IMSI* read from the last session, which the HLR must accept.

The proposed authentication protocol can prevent the replay attack by the freshness properties. The MS refreshes the session key by using the nonce to ensure the freshness of authentication sessions. Since the MS and SGSN/VLR must input IK to generate a new session key; the session key can be refreshed for each authentication process. If an attacker replaces the TMSI of an intercepted authentication message and replays the authentication request, the attack will not succeed because the $AUTHM_H$ is encrypted using $K_{HM}$, so the replay attack is infeasible.

**ii. Guessing Attacks**

Password authentication is widely used by many security systems. However a password is vulnerable under dictionary attack in which an attacker can guess the password successfully. In the proposed scheme, the key refreshment method prevents the guessing attack. In each authentication process, the subscriber uses different keys to request registration and authentication. Public key cryptosystems provide a means for preventing the guessing attack. Since the public key digital signature is used to sign the message, the guessing attacks fail. It has been shown that the signatures are distributed so that the attacker is unable to guess a signature value which is shared by different messages.

**iii. Substitution Attacks**

If an attacker replaces some fields of the authentication request, then the authentication will fail. For example, if an attacker replaces any parameter in the initial authentication, the SGSN/VLR will find the nonce *IK'* is different from the nonce *IK* encrypted along with the authentication status sent by the HLR/AuC. Because the nonce used by the SGSN/VLR is the same as the one used by the HLR/AuC, SGSN/VLR can compare them to verify the MS. Therefore, our protocol can resist the substitution attack. Moreover, even if an attacker gets the session key, he will not have the ability to generate new session keys. This is because session key generation involves *CK*, and because only the MS and SGSN/VLR know the *CK*. The above analysis shows that our protocol can successfully prevent this kind of substitution attack.

From the above security analysis, we can find that our scheme is secure and fully satisfies the security requirements. Furthermore, the authentication key $K_{VM}$ is only aware by MS and VLR. It can assure that in the later services request phase, only the legitimate MS will be allowed to use the service provided by VLR. Since MS has no reason to compromise the $K_{VM}$ to a third party, therefore, our scheme ensures that except the related participants, no one can harm the rights and interests of MS

## 7. SIMULATION RESULTS AND A COMPARISON WITH RELATED WORK

The Comparisons of the proposed Protocol with current UMTS protocol are listed in table 1. The authentication vector is used by UMTS and AP-AKA protocol to reduce the number of access to HLR/AuC. While using of authentication vector causes the bandwidth consumption and storage overhead. In UMTS AKA, the HLR/AuC cannot authenticate MS. While the proposed protocol, allows HLR/AuC to authenticate the MS. There is protocol proposed by Harn and Hsin AKA and X-AKA protocol that used hash chain. The bandwidth consumption and overhead is occurred by using of several hash chain.

An analytic model is proposed to investigate the impact of the size of the authentication vector array in order to minimize the cost [3] [29]. A dynamic length of authentication vector array based on prediction of the mobile user's residence time in the VLR/SGSN is proposed by [3]. Consequently, it is able to reduce the network traffic and to avoid the bottleneck at HLR/AuC. There are differences between these works and the proposed E-AKA, because these works do not change the original UMTS AKA protocol and tries to find a suitable size for the authentication vector.

| Comparison with Items | UMTS | Proposed Protocol |
|---|---|---|
| Symmetric or Asymmetric | Sym | Sym+Asym |
| Mutual authentication between MS and HN | ≠ | = |
| Mutual authentication between MS and SN | ≠ | = |
| Confidentiality of user identity during roaming | ≠ | = |
| User Traffic Confidentiality | = | = |
| True non-repudiation of service | ≠ | = |
| Signaling data integrity | = | = |
| Reduction of bandwidth consumption between SN and HN | ≠ | = |
| Reduction of storage space overhead for SN's database | ≠ | = |
| Element synchronization between MS and HN | = | ≠ |

(=: is achieved by the protocol; ≠: is not achieved by the protocol)

**TABLE 1:** A Comparison of the Proposed Protocol with UMTS Protocol

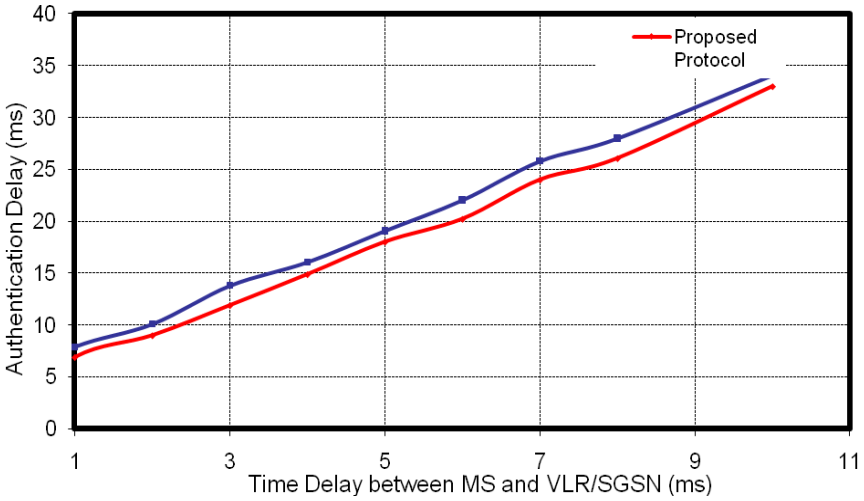


**FIGURE 6:** Authentication delay for current and proposed protocol

The simulation in this thesis was executed 20 times. The results of the 20 simulations were then averaged to obtain accurate results. The length of the communication system simulation was run for several hundreds of seconds (400 seconds) in order to obtain accurate and consistency results and reaches a steady state not influenced by short time differences. Simulations were performed on an Intel P4 1.67 GHz machine with 512MB of RAM.

The results show that the authentication delay is minimized when compared with the current protocol, as illustrated in figure 6. Therefore, the performance and the authentication delay time have been improved significantly.

## 8. CONCLUSION

A novel mutual authentication scheme based on integrating the public key with the hash-chaining technique has been proposed. This scheme provides secure authentication mechanisms for mobile systems where the concepts of TMSI and key refreshment are adopted. Using TMSI can protect the subscriber's true identity, and key refreshment can make authentication process more secure. In addition, the bi-unilateral and mutual authentication among UE, VLR and HLR have been adopted that resulted in a more secure protocol than the other available authentication protocols. This proposed protocol fulfills the security requirements of the third generation mobile systems. 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.

The proposed protocol achieved the following goals:

1. Provides mutual authentication between the user MS and the HN.
2. Provides mutual authentication between the user MS and the SN.
3. The establishment of a cipher key and an integrity key upon successful authentication.
4. Reduces the signaling traffic between serving network and home network and reduces the size of authentication information to be stored in the serving network.
5. Element synchronization between MS and HN.
6. HN allows SN to authenticate MS, then VLR/SN authenticates MS without any intervention from the subscriber's HN

## 9. REFERENCES

[1] Al-Saraireh J., and Yousef S., "A New Authentication Protocol for UMTS Mobile Networks", EURASIP Journal on wireless communications and networking, vol. 2006, pp. 1-10, Article ID 98107, 2006.

[2] Salgarelli L., Buddhikot M., Garay J., Patel S., and Miller S.. "The Evaluation of wireless LANs and PANs – Efficient Authentication and Key Distribution in Wireless IP Networks". IEEE Personal Communication on Wireless Communication, vol. 10, no. 6, pp. 52-61, 2003.

[3] Al-Saraireh J., and Yousef S., "Analytical Model: Authentication Transmission Overhead Between Entities in Mobile Networks", Elsevier, Computer Communications Journal, vol. 30, no. 9, pp. 1713-1720, 2007.

[4] Zhang M., and Fang Y., "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol", IEEE Transactions on wireless communications, vol. 4, no. 2, pp. 734 – 742, 2005.

[5] 3GPP, "3G Security, Specification of the MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions f1, f1*, f2, f3, f4, f5 and f5*, document 1: General", 3rd Generation Partnership Projec, 2001.

[6] Cheng S., Shieh S., Yang W., Lee F., and Luo J., "Designing Authentication Protocols for Third Generation Mobile Communication Systems", Journal of Information Science and Engineering, vol. 21, pp. 361-378, 2005.

[7] Brutch T., and Brutch P., "Mutual authentication, confidentiality, and key Management (MACKMAN) system for mobile computing and wireless communication", Proceedings of the 14th Annual Computer Security Applications Conference, pp. 308-317, 1998.

[8] Dell'Uommo S., and Scarrone E., "The mobility management and authentication authorization mechanisms in mobile networks beyond 3G", Proceedings of the 12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 44-49, 2001,

[9] Horn G., Martin K., and Mitchell C., "Authentication Protocols for Mobile Network Environment Value-Added Services", IEEE Transactions on Vehicular Technology, vol. 51, no. 2, pp. 383-392, 2002.

[10] Lee C., Hwang M., and Yang W., "Enhanced Privacy and Authentication for the Global System for Mobile Communications", Wireless network Journal, Kluwer Academic Publishers, vol. 5, no. 3, pp. 231-234, 1999.

[11] Lee C., Hwang M., and Yang W., "Extension of Authentication Protocol for GSM", IEE Proceeding Communication, vol. 150, no. 2, pp. 91-95, 2003.

[12] Lee C., Li L., and Hwang M., "A remote User Authentication Scheme Using Hash Function", ACM Operating Systems Review, vol. 36 no. 4, pp. 23-29, 2002.

[13] Lin C., and Shieh S., "Chain authentication in mobile communication systems", Journal of Telecommunication Systems, vol. 13, pp. 213-240, 2000.

[14] Looi M.,"Enhanced authentication services for internet systems using mobile networks", IEEE Global Telecommunications Conference, vol. 6, pp. 3468-3472, 2001.

[15] Molva R., Samfat D., and Tsudik G., "Authentication of Mobile Users", IEEE Network, vol. 8, no. 2, pp. 26-34, 1994.

[16] Putz S., and Schmitz R. (2000), "Secure Interoperation between 2G and 3G Mobile Radio Networks", 3G Mobile Communication Technologies, 2000, First International Conference on (IEE Conference Publication No. 471), London, UK, Pp. 28-32.

[17] Putz S., Schmitz R., Tonsing F., "Authentication Schemes for Third Generation. Mobile Radio Systems", Personal, Indoor and Mobile Radio Communication., The 9th IEEE International Symposium on Personal, vol. 1, pp. 126-130, 1998.

[18] Park C., "On Certificate-Based Security Protocols for Wireless Mobile Communication Systems", IEEE Network, vol. 11, no. 5, pp. 50-55, 1997.

[19] Grecas C., Maniatis S., and Venieris I., "Towards the introduction of the asymmetric cryptography in GSM,GPRS, and UMTS networks", Sixth IEEE Symposium on Computers and Communications, Proceedings, pp. 15-21, 2001.

[20] Argyroudis G., Verma R., Tewari H., and Mahony D., "Performance Analysis of Cryptographic Protocols on Handheld Devices", 3rd IEEE International Symposium on Network Computing and Applications (NCA 2004) Proceeding, pp. 169 – 174, 2004.

[21] Kambourakis G., Rouskas A., and Gritzalis S., "Using SSL/TLS in Authentication and Key Agreement Procedures of Future Mobile Networks", IEEE 4th International Workshop on Mobile and Wireless Communications Network, vol. 2002 , pp. 152 – 156, 2002.

[22] Kambourakis G., Rouskas A., and Gritzalis S., "Advanced SSL/TLS-Based Authentication for Secure WLAN-3G Interworking", IEE Communications, vol. 151, no. 5, pp. 501-506, 2004.

[23] Huang C., and Li J., "Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption", AINA2005, 19th International Conference on Advanced Information Networking and Applications (AINA'05), vol. 1, pp. 392-397, 2005.

[24] Zhang M., "Provably-Secure Enhancement on 3GPP Authentication and Key Agreement Protocol", Cryptology ePrint Archive, Report 2003/092, 2003. [online]. Last accessed on 10 April 2006 as Available at http://eprint.iacr.org, 2003

[25] Zhang Y., and Fujise M., "An Improvement for Authentication Protocol in Third-Generation Wireless Networks", IEEE Transaction on Wireless Communications, vol. 5, no. 9, pp. 2348-2352, 2006.

[26] Zhang Y., and Fujise M., "Security Management in the Next Generation Wireless Networks", International Journal of Network Security, vol.3, no.1, pp. 1-7, 2006.

[27] Adi W., Dawood A., Mabrouk A., and Musa S. , "Low complexity image authentication for mobile applications", IEEE South East Conference, Richmond, USA, pp. 20-20, 2007.

[28] Yijun H., Nan X., and Jie L., "A Secure Key Exchange and Mutual Authentication Protocol for Wireless Mobile Communication", IEEE International Conference on Availability, Reliability and Security, ARES'07, Vienna, Austria, pp. 558 – 563, 2007.

[29] Lin Y, and Chen Y., "Reducing Authentication Signaling Traffic in Third-Generation Mobile Network", IEEE Transactions on Wireless Communications, vol. 2, no. 3, pp. 493-501, 2003.

[30] Harn L., and Hsin W., "On the Security of Wireless Network Access with Enhancements", Proceedings of the 2003 ACM workshop on Wireless Security, San Diego, USA, pp. 88-95, 2003.

[31] Burnett S. and Pause S, "RSA Security's Official Guide to CRYPTOGRAPHY", McGrawn, Hill, 2002.

[32] Lamport L., "Password authentication with insecure communication", Communication of ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[33] Al-Fayoumi M., Nashwan S., Yousef S. and Alzoubaidi A., "A New Hybrid Approach of Symmetric/Asymmetric Authentication Protocol for Future Mobile Networks", Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob, pp. 29-38, 2007

[34] Lacy, J., Mitchell, D. and Schell, W., "CryptoLib: Cryptography in Software." Proc. Fourth USENIX Security Workshop, October 1993.

[35] M.J. Belier, L. Chang, and Y. Yacobi, "Privacy and Authentication on a Portable Communications System", Global Telecommunications Conference, pp 1922- 1927, Dec. 2-5, 1991.

[36] M. Hwang, S. Chong and H. Ou, "On the security of an enhanced UMTS authentication and key agreement protocol", European Transactions on Telecommunications, Vol. 22, Issue 3, pp. 99–112, April 2011