Robust Delegation Signcrypted Authentication Protocol against FHLR Attack in 3GPP Wireless Communications

Esam A. A. Hagras[1], Maha Amer[2] and, Hazem H. Aly [3]

[1]Faculty of Engineering, Alexandria University, Alexandria, Egypt
[2,3] Arab Academy for Science and Technology and Maritime Transport, Cairo, Egypt.
[1]esamhagras_2006@yahoo.com, [2]maha_m.amer@hotmail.com,
[3]hazemhali@gmail.com

Abstract

In this paper, we propose a new Robust Delegation Signcrypted Authentication Protocol (RD-SAP) against the False Home Location Register Attack in 3GPP. The proposed authentication protocol is based on Public Key Signcryption technique to solve the problem of FHLR attack on Tian F Lee protocol and which provides the user identity privacy, mutual authentication, nonrepudiation. This study also presents an enhanced protocol, which is not only has the same security properties as the original protocol, but also avoids the weakness in the original protocol. Therefore this scheme enjoys both computational and communicational efficiency.

Keywords: *Robust delegation, Mobile authentication, Public key signcryption, False home location register.*

1. Introduction

Portable Communication Systems (PCSs) [4] do not require any physical circuits between subscriber and service provided. PCSs technology allows users to carry portable communication devices that are low power, low cost, and small in size with mobile networking capabilities. Radio waves being transmitted in space make it easy for anyone to eavesdrop on the contents of communication, so there are more security and privacy threats than with wire line communication system. A secure communication system should possess four major features: secrecy, authenticity, integrity, and non-repudiation [5].

With the advancement of mobile technology, wireless networks have become widely available and interconnected. For allowing people to get connected seamlessly using their mobile devices without being limited by the geographical coverage of their own home networks, roaming services have been deployed, for example, GMS [6-9], 3GPP [10], and WLANs. A typical roaming scenario involves three parties: a roaming Mobile Station (MS), a Visited Location Register (VLR) and a Home Location Register (HLR). MS, who is a subscriber of HLR, is now in a network administered by VLR. There is a direct link between MS and VLR and another between VLR and HLR. But there is no link between MS and HLR. To prevent fraudulent use of services, user authentication is a mandatory requirement. The conventional way to perform user authentication is to let VLR contact HLR who acts as a guarantor for vouching that MS is a legitimate subscriber of it.

Public key cryptosystems have been used for mobile authentication in wireless networks [1], [13], [14], [15]. He et al. [15] used blind signature to design a privacy protection scheme for mobile stations; the scheme also provides *MS* authentication and access authorization. Lee

DOI : 10.5121/ijdps.2011.2502

and Yeh [1] proposed a trust delegation based scheme, where an *MS*, that is registered to a home location register (*HLR*) or home network, proves its registration to a *VLR* (or serving network).

In this paper, we propose a new RDSA protocol against the False Home Location Register Attack in 3GPP. The proposed authentication protocol is based on Public Key Signcryption [11-12] technique to solve the problem of *FHLR* attack on Tian F. Lee protocol. Security analysis, storage capacity, computational cost and communicational overhead have been discussed for the proposed protocol.

The reminder of this paper is recognized as follows. Section 2 discusses the related work on the concept of delegation authentication protocols on 3GPP wireless communication systems. Section 3 reviews the concept of the enhanced authentication protocol of Tian-Fu Lee [12]. Section 4 describes the *FHLR* attack on the Tian-Fu Lee protocol. Section 5 presents our enhancement protocol. Section 6 proposes the security analysis. Finally Section 7 is the conclusion.

2. Related Works

Wireless communication systems [4] [16] provide mobile users with global roaming service. To support greater properties, numerous authentication approaches employ the public-key system to develop their protocols. For instance, long et al. [17] in 2004 presented a localized authentication protocol for inter-network roaming across wireless LANs. Lee et al. [18] in 2005 proposed a private authentication protocol to prevent the home location register (HLR) from eavesdropping on communication between the roaming station (MS) and the visited location register (VLR). However, due to hardware limitations, MS cannot support heavy encryption and decryption, and therefore wastes a lot of time in exponential computations.

In 2005, Lee and Yeh [1] presented the concept of delegation in wireless communication systems and proposed delegation based authentication protocol to solve the problem of data security, user privacy, computational loads and communicational efficiency in the system. Their protocol also adopted the public key cryptosystem to achieve the security requirements. To increase the communicational efficiency, and save authentication processes such that VLR does not need to contact HLR frequently, and a rapidly re-authenticate MS. Therefore, Lee protocol not only has a lower computational load for MS, but also provides greater security.

Although the protocol of Lee and Yeh exhibit non-repudiation in on line authentication process, it still has a weakness in off line authentication process. This weakness is that any legal VLR can forge authentication messages without the help of the mobile user. However, these forged messages are verified, and the mobile user cannot repudiate that he is the producer of these message. The malicious VLR can trick the HLR by these forged messages. That is, the protocol of Lee and Yeh does not have the property of non-repudiation in the off line authentication processes. Without the non repudiation property, a protocol may inspire a mobile user to deny that he has used services and refuse to pay, or inspire a services provider to overcharge a mobile user for services that he did not request [2].

In 2009, Tian F. Lee *et al*., enhanced Lee and Yeh protocol to solve the off line non-repudiation problem by using the backward hash chain to ensure that the authentication messages in off line process cannot be forged. Although the protocol of Tian *et al*. solve the off line non-repudiation problem in Lee and Yeh protocol, it still has a weakness against False Home Location Register (*FHLR*) attack. In [3], *FHLR* attack on Lee and Yeh [1] protocol has been introduced. We adapt the *FHLR* attack given in [3] to attack Tian F. Lee *et al* protocol [2] which is an enhancement Lee and Yeh protocol.

3. Review of Tian F. Lee *et al* protocol

This section briefly reviews the enhanced delegation based authentication protocol of Tian F. Lee *et al*. [2] for PCSs, some notation should be explained here: $X \to Y : Z$, denotes that the sender *X* sends a message *Z* to a receiver *Y*; $h(\cdot)$, denotes a one way hash function; $h^2(.)$, denotes that the value is hashed twice; $n_1 \| n_2$, denotes a concatenation of data n_1 and n_2; ID_V, ID_H, denotes the identity of *VLR* and *HLR*, respectively; K_{HV}, K_{VH}, denotes the secret key shared by VLR and HLR; $E_k[\bullet]$, $D_k[\bullet]$ denotes a message encryption and decryption using a secret key *k*.

3.1 Setup

HLR generates parameters *p*: a 512 bit prime; *q*: a 160 bit prime factor of (*p*-1); *g*: an element where $g = z^{(p-1)/q} \bmod p$ and $z \in [1, p-1]$; x_{HLR}: a number less than *q* as a *HLR* private key; y_{HLR}: *HLR* public key certificates by Trusted Certificate Authority (TCA) where, $y_{HLR} = g^{x_{HLR}} \bmod p$. When user MS registers in its *HLR*, *HLR* create a proxy pair keys that contains a pseudonym are used to represent the real identity of MS in the network. The relation between the pair keys and the corresponding real identity of MS are protected in a secure database located in *HLR*. No one except *HLR* can obtain any information about the real identity of MS .

When MS subscriber to his home system *HLR*, *HLR* will generate random numbers k and compute $K = g^k \bmod p$, and calculate $\sigma = x_{HLR} + kK \bmod q$, where, σ is the secret key shared by *HLR* and MS and K are the pseudonyms of MS . After that, the MS will obtain a SIM card with its own key pair (σ, K) from *HLR*. MS , generates random number "n_1", pre-computed a hash chain $h^{(1)}(n_1), h^{(2)}(n_1), \cdots, h^{(n+1)}(n_1)$ and stores them in its database, where $h^{(1)}(n_1) = h(n_1)$ and $h^{(i+1)}(n_1) = h(h^{(i)}(n_1))$ for $i = 1, 2, \ldots, n$.

3.2 On line authentication:

Step 1: $MS \to VLR : K$. MS Sends its pseudonym K to VLR

Step 2: $VLR \to MS : n_2, ID_V$

VLR Randomly generated n_2 (a number less than *q*) and sends n_1, ID_V to MS .

Step 3: $MS \to VLR :\ r, s, K, N_1, ID_H, ID_V$

MS Generates a random number t, picks $N_1 = h^{(n+1)}(n_1)$ stored in its database, signs N_1, n_2, ID_V and sends r, s, K, N_1, ID_H, ID_V to VLR, where, r, s are given by: $r = g^t \bmod p$

$$s = \sigma * h(N_1 \| n_2 \| ID_V) + t * r \bmod q .$$

Step 4: $VLR \rightarrow HLR : [N_1 \| n_2 \| K]_{K_{HV}}, ID_H, ID_V$

VLR checking if $g^s = (y_{HLR} K^K)^{h(n_1 \| n_2 \| ID_V)} r^r \bmod p$, if the verifications are not achieved, the request is rejected; otherwise, *VLR* sends $[N_1 \| n_2 \| K]_{K_{HV}}, ID_H, ID_V$ to *HLR*.

Step 5: $HLR \rightarrow VLR : [[N_1, n_3,, ID_V]_\sigma \| n_2 \| l \| C_1]_{HV}, ID_H, ID_V$

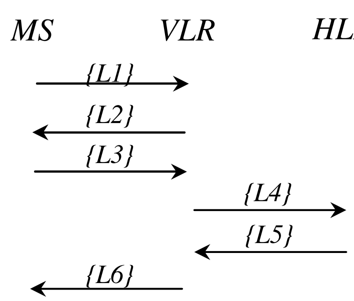
HLR decrypts the message $[N_1 \| n_2 \| K]_{K_{HV}}$ and obtains K of each MS. If he successfully searches the corresponding σ in its database according to K, then he computes $C_1 = h(N_1 \| n_2 \| n_3 \| \sigma)$, $l = N_1$ where n_3 is a random number selected by *HLR*, and sends $[[N_1, n_3, ID_V]_\sigma \| n_2 \| l \| C_1]_{K_{HV}}, ID_V, ID_H$ to *VLR*.

Step 6: $VLR \rightarrow MS : [N_1, n_3, ID_V]_\sigma, ID_V$

VLR decrypts $[[N_1, n_3, ID_V]_\sigma \| n_2 \| l \| C_1]_{K_{HV}}$ and obtains $[[N_1, n_3, ID_V]_\sigma, n_2, l$ and C_1. Then he checks n_2 and l, sets the current session key $SK = C_1$ used by *VLR* and *MS*, and forwards $[N_1, n_3, ID_V]_\sigma$ and ID_V to *MS*. Finally, *MS* decrypts $[N_1, n_3, ID_V]_\sigma$ and checks N_1 and computes the current session key $SK = C_1$.

3.3 $i-th$ Off line authentication

MS picks $h^{(n-i-1)}(n_1)$ stored in his database and sends $[h^{(n-i+1)}(n_1)]_{C_i}$ to *VLR* for $i = 1,2,\ldots,n$, where a predefined constant n is the limited times of off line authentications. On receiving the authentication message from *MS*, *VLR* checks whether $h(h^{(n-i-1)}(n_1))$ and l are equal, updates $l = h^{(n-1+1)}(n_1)$ and computes the session key $C_{i+1} = h(l, C_i)$. He also updates the count $i = i + 1$ and checks $i < n$.



$\{L1\} : K$

$\{L2\} : n_2, ID_V$

$\{L3\} : r, s, K, N_1, ID_H, ID_V$

$\{L4\} : [N_1 \| n_2 \| K]_{K_{HV}}, ID_H, ID_V$

$\{L5\} : [[N_1 \| n_3 \| ID_V]_\sigma \| n_2 \| l \| C_1]_{K_{HV}}, ID_H, ID_V$

$\{L6\} : [N_1, n_3, ID_V]_\sigma, ID_V$

Fig. 1 Mobile Authentication Scheme of Tian F. Lee protocol [2]

4. FHLR attack on Tian F. Lee *et al* protocol

In Fig. 1 an attacker can first divert the *VLR* to an *HLR* under control of the adversary, and we denote this impersonated *HLR* by *FHLR* with identification ID_F. The attacker modifies ID_H in *{L3}* to ID_F. The modified message $\{L'_3\}$ is defined in (1).

$$\{L'_3\}: r, s, K, N_1, ID_F, ID_V \tag{1}$$

After the diversion, the attacker, that acts as a *VLR*, then obtains a session key $K_{(F,H)}$ with the legitimate *HLR* of the *MS* in question, and sends $\{L'_4\}$ defined as in (2) instead of *{L4}* to the legitimate *HLR*..

$$\{L'_4\}: [N_1 \,\|\, n_2 \,\|\, K]_{K_{FH}}, ID_H, ID_F \tag{2}$$

After the attacker receives $\{L'_5\}$ (from *HLR*), which is defined as in (3), where n_3 is a random number selected by *HLR*, the attacker successfully obtains the session key C_1.

$$\{L'_5\}: [[N_1, n_3, ID_V]_\sigma \,\|\, n_2 \,\|\, l \,\|\, C_1]_{K_{HF}}, ID_H, ID_F \tag{3}$$

Let K_{VF} be the session key between *VLR* and *FHLR*, by following the protocol, after processing $\{L'_3\}$, VLR can generate $\{\overline{L_4}\}$ as defined in (4) and sends it to *FHLR* that is under control of the attacker. *FHLR* that now acts as an *HLR* to the *MS* in question can then reply to *VLR* a newly composed $\{\overline{L_5}\}$ as defined in (5). This is straightforward since *FHLR* has the encrypted $[N_1, n_3, ID_V]_\sigma$ the random number n_2 , the hashed value l and the session key C_1 between *MS* and *VLR*.

$$\{\overline{L_4}\}: [N_1 \,\|\, n_2 \,\|\, K]_{K_{VF}}, ID_V, ID_F \tag{4}$$

$$\{\overline{L_5}\}: [[N_1, n_3, ID_V]_\sigma \,\|\, n_2 \,\|\, l \,\|\, C_1]_{K_{VF}}, ID_H, ID_F \tag{5}$$

Now that *VLR* and *MS* follow the protocol and proceed to the remaining steps of the on-line and off-line authentication of Tian-Fu Lee. Figure 2 shows the messages used in this attack. This attack occurs because there is no security protection on ID_H when it is sent through communication channels to *VLR,* so in equation (5) the attacker can obtain the session key C_1 since he has K_{VF} and then the legitimate *HLR*, *VLR* and *MS* cannot know the fact that the C_1 is compromised. In our new protocol we enhance the authentication process of *Tian*-Fu Lee protocol by protecting the ID_H by using a signcryption algorithm to ensure the data security, user privacy, computational load and communicational efficiency.

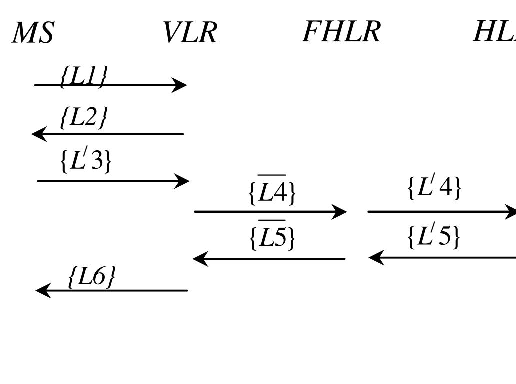
$\{L_1\}: K$

$\{L_2\}: n_2, ID_V$

$\{L'_3\}: r, s, K, N_1, ID_F, ID_V$

$\{\overline{L_4}\}: [N_1 \,\|\, n_2 \,\|\, K]_{K_{VF}}, ID_V, ID_F$

$\{\overline{L_5}\}: [[N_1, n_3, ID_V]_\sigma \,\|\, n_2 \,\|\, l \,\|\, C_1]_{K_{VF}}, ID_H, ID_F$



$\{L^{\backslash}{}_4\}:[N_1 \| n_2 \| K]_{K_{VF}}, ID_H, ID_F$

$\{L^{\backslash}{}_5\}:[[N_1, n_3, ID_V]_\sigma \| n_2 \| l \| C_1]_{K_{VF}}, ID_H, ID_F$

$\{L_6\}:[N_1, n_3, ID_V]_\sigma, ID_V$

Fig. 2, FHLR Attack on Mobile Authentication Scheme in [3]

5. Proposed RDSA Protocol

This section presents a new RDSA protocol that solves the problem of *FHLR* based on Tian-Fu Lee and signcryption algorithm and then analysis its security and performance. In our protocol we employ a signcryption algorithm [12] to provide an efficient mobile authentication scheme and to solve the problem of *FHLR* which described in the previous section. Figure 3 illustrate our protocol which works as follow.

5.1 Setup

The setup phase is similar to that of the authentication protocol of Tian-Fu Lee [2]. *HLR* and *MS* have their private/public key pairs (x_{HLR}, y_{HLR}) and (σ, K), respectively. The key pair (σ, K) is also stored in *MS*'s SIM card. Beside, *MS* generates random number n_1, pre computes a hash chain $h^{(1)}(n_1), h^{(2)}(n_1), \ldots, h^{(n-1)}(n_1)$ and stores them in its database where $h^{(1)}(n_1) = h(n_1)$ and $h^{(i+1)}(n_1) = h(h^{(i)}(n_1))$ for $i = 1, 2, \ldots, n$. Also we assume that MS has chosen a random number x_{MS} from $[1, \ldots\ldots, q-1]$, and calculates its public number $y_{MS} = g^{x_{MS}} \bmod p$, also, *VLR*'s chosen random number x_{VLR} from $[1, \ldots\ldots, q-1]$, and calculates its public number $y_{VLR} = g^{x_{VLR}} \bmod p$.

5.2 On-line authentication:

Step 1 MS→VLR: *K.*

MS sends *K to VLR*.

Step 2 VLR→MS: ID_V, y_{VLR}.

VLR sends ID_V and y_{VLR} to *MS*.

Step 3 $MS \rightarrow VLR: r, s, K, N_1, C_H, ID_H, ID_V$

MS selects a random number t from $[1, \cdots, q]$, picks $N_1 = h^{(n+1)}(n_1)$ stored in its database, sign N_1, y_{VLR}, ID_V and sends $r, s, K, N_1, EID_H, EID_V, ID_H, ID_V$ to VLR, where, r, s and EID_H, EID_V are given by:

$$(k_1, k_2) = hash(((y_{VLR})^t) \bmod p) \tag{6}$$

$$(EID_H, EID_V) = E_{k_1}[ID_H \| ID_V] \tag{7}$$

$$r = KH_{k_2}(k_1, y_{VLR}, N_1, ID_H, ID_V) \tag{8}$$

$$s = (t/(r + \sigma_{HLR-MS})) \bmod q \tag{9}$$

The output of the one-way hash is a binary number of at least 128 bits, which guarantees that, both k_1 and k_2 has at least 64 bits. The function $KH_{k2}(m)$ is a keyed hash algorithm for hashing a message *'m'* under a key k_2. *MS* sends $r, s, K, N_1, EID_H, EID_V, ID_V$ and ID_H to *VLR*.

Step 4 $VLR \rightarrow HLR : [N_1 \| y_{VLR} \| K \| ID_H \| ID_V]_{K_{HV}}, ID_H, ID_V$

1- *VLR* unsigncrypts ID_H to get (k_1, k_2) and checks the validity of its r, s.

2- *VLR* decrypts $(ID'_H, ID'_V) = D_{k_1}[EID_H \| EID_V]$

3-*VLR* computes $r' = KH_{k_2}(k_1, N_1, y_{VLR}, ID'_H)$ and checks if $r' = r$. If $r' \neq r$, reject and if $r' = r$, *VLR* sends $[N_1 \| y_{VLR} \| K \| ID'_H \| ID'_V]_{K_{HV}}, ID_H, ID_V$ to *HLR*.

Theorem 1: If the signer MS can strictly carry out above signcryption steps, the signcryption (r, s) can pass the test of validity, and the specified receiver VLR can also recover the original *HLR* identity ID_H.

Proof: $$(k_1, k_2) = hash((((y_{HLR} K^K) g^r)^{s \cdot x_{VLR}}) \bmod p) \tag{10}$$

$$= hash((((g^{x_{HLR}} (g^k)^K) \cdot g^r)^{s \cdot x_{VLR}}) \bmod p) \tag{11}$$

$$= hash(((g^{x_{HLR} + kK} g^r)^{s \cdot x_{VLR}}) \bmod p) \tag{12}$$

$$= hash(((g^{\sigma + r})^{s \cdot x_{VLR}}) \bmod p) \tag{13}$$

$$= hash(((g^{\sigma + r})^{\frac{t}{(\sigma + r)} \cdot x_{VLR}}) \bmod p) \tag{14}$$

$$= hash(((g^{x_{VLR}})^t) \bmod p) \tag{15}$$

$$= hash((y_{VLR})^t \bmod p) \tag{16}$$

Step 5 HLR→VLR: $[[N_1, n_3, ID_V]_\sigma \| y_{VLR} \| l \| C_1 \| ID_H \| ID_V]_{K_{HV}}, ID_H, ID_V$

HLR decrypts $[N_1 \| y_{VLR} \| K \| ID_H \| ID_V]_{K_{HV}}$ and obtains *K*. If he successfully searches the corresponding σ in its database according to *K*, then he computes $C_1 = h(N_1 \| y_{VLR} \| n_3 \| \sigma)$, and $l = N_1$, where n_3 a random is number, and sends: $[[N_1, n_3, ID_V]_\sigma \| y_{VLR} \| l \| C_1 \| ID_H \| ID_V]_{K_{HV}}, ID_H, ID_V$ to *VLR*.

Step 6 VLR→MS: $[N_1, n_3, ID_V]_\sigma, ID_V$

VLR decrypts $[[N_1, n_3, ID_V]_{\sigma_S} \| y_{VLR} \| l \| C_1]_{K_{HV}}$ and obtains $[N_1, n_3, ID_V]_\sigma$, y_{VLR}, l, ID_H and C_1. Then he checks ID_H, y_{VLR} and *l*, stores *l* in its database, sets the current session key *SK* = C_1 used by *VLR* and *MS*, and forwards $[N_1, n_3, ID_V]_\sigma, ID_V$

to *MS*. Finally *MS* decrypts $[N_1, n_3, ID_V]_\sigma$, checks N_1 and computes the current session key $SK = C_1$.

5.3 Off-line authentication

The Off-line authentication phase is similar to that of the authentication protocol of Tian-Fu Lee. The proposed Robust Delegation-Based Authentication protocol is shown in figure (3).

1. On-line authentication process:

MS $(\sigma, K)\,(x_{MS}, y_{MS})$ **VLR** $(K_{VH})\,(x_{VLR}, y_{VLR})$ **HLR** $((\sigma, K), K_{VH})\,(x_{HLR}, y_{HLR})$

(0) Pre-compute and store

$h^{(1)}(n_1), h^{(2)}(n_1), \ldots, h^{(n-1)}(n_1)\ (= N_1)$

(1) K →

(2) ID_V , y_{VLR} ←

(3.a) Calculate $(k_1, k_2) = hash\ (y_{VLR}^t \bmod p)$

$(EID_H, EID_V) = E_{k_1}[ID_H \| ID_V]$

$r = KH_{k_2}(k_1, y_{VLR}, N_1, EID_H, EID_V)$

$s = t/(r + \sigma) \bmod q$

(3.b) $r, s, K, N_1, EID_H, EID_V, ID_H, ID_V$ →

(4.a) Check if:

$(k_1, k_2) = hash((((y_{HLR}.K^K)g^r)^{s.x_{VLR}}) \bmod p)$

$(ID'_H, ID'_V) = D_{k_1}[EID_H \| EID_V]$

$r' = KH_{k_2}(k_1, y_{VLR}, N_1, ID_H, ID_V)$

(4.b) $[N_1 \| y_{VLR} \| K \| ID_H \| ID_V]_{K_{HV}}, ID_H, ID_V$ →

(5.a) Calculate:

$C_1 = h(N_1 \| y \| n_3 \| \sigma)$

$l = N_1$

(5.b) send:

$[[N_1, n_3, ID_V]_\sigma \| y_{VLR} \| l \| C_1 \| ID_H \| ID_V]_{K_{HV}}, ID_H, ID_V$ ←

(6.a) Check y_{VLR}, l, ID_H and Store l

(6.b) $[N_1, n_3, ID_V]_\sigma, ID_V$

(6.c) Check N_1, ID_V

(6.d) Calculate $SK : C_1 = h(N_1 \parallel y_{VLR} \parallel n_3 \parallel \sigma)$

2. i-th Off-line authentication process:

MS (C_i) ***VLR*** $(C_i, l = h^{(n-i+1)}(n_1))$

$\left[h^{(n-i)}(n_1)\right]_{C_i}$ $\longrightarrow$

Check if $h(h^{(n-i)}(n_1)) = l$

$\Rightarrow$ Updates $l = h^{(n-i+1)}(n_1)$,

$SK : C_{i+1} = h(l, C_i)$ and count $i = i + 1 < n$

Fig. 3 Proposed Robust Delegation Signcrypted Authentication Protocol

6. Security Analysis

The analysis of our protocol is similar to those of the protocol of Tian-Fu Lee *et al*, in off-line authentication processes, and therefore is not presented herein.

6.1 User Identity Privacy

In our protocol *MS* has one private/public key pair (σ, K). The real identity of *MS* is not transmitted over the entire network for authentication purposes. Because we use pseudonym *K* generated by *HLR* in the registration phase to represent the identity of *MS* in the network, no one except *HLR* can obtain any information about the identity on MS. Also for the private/public number pair (x_{MS}, y_{MS}), MS sends its public number y_{MS} to *VLR* in the registration phase and uses the generated random number *t* with the private number x_{MS} to sign N_1, y_{VLR} and ID_H, where $r = KH_{k2}(k_1, y_{VLR}, N_1, ID_H)$ and $s = t/(r+\sigma) \bmod q$. Hence our new protocol provides strong user identity privacy.

6.2 Nonrepudiation

In our protocol *MS* sends the signcrypted text *(r, s, c)* to *VLR* and then *VLR* unsigncrypt and verify this text. *VLR* accept this text if $r' = KH_{k2}$ and $(ID'_H, ID'_V) = D_{k_1}\left[EID_H \| EID_V\right]$, so, the attacker cannot forge it since k_1 and k_2 depend on *"t"* which is randomly chosen by *MS*. Therefore our protocol guarantees that *MS* generates the authentication message in online authentication processes.

6.3 Mutual Authentication

In the online authentication process, *VLR* authenticates *MS* by verifying the signcrypted text $r' = KH_{k_2}(k_1, y_{VLR}, N_1, ID_H, ID_V)$ and $(ID'_H, ID'_V) = D_{k_1}\left[EID_H \| EID_V\right]$ in step 4, and authenticate *HLR* by checking n_2 and ID_H of $\left[\left[N_1, n_3, ID_V\right]_\sigma \parallel y_{VLR} \parallel l \parallel C_1 \parallel ID_H \parallel ID_V\right]_{K_{HV}}$ in step 6, respectively. MS authenticates *VLR* and *HLR* by checking N_1 of $\left[N_1, n_3, ID_V\right]_\sigma, ID_V$ from *VLR* in step 6. *HLR* authenticates *VLR* by checking K and ID_H of $[N_1 \| y_{VLR} \| K \| ID_H \| ID_V]_{K_{HV}}$ in step 5, and authenticates *MS* through *VLR* authenticating *MS* in step 4, respectively. So, our protocol provides mutual authentication.

6.4 Computational Cost and Communicational Overhead

In this section we calculate the communicational cost and communicational overhead in each step of our scheme (in online authentication process) as seen in table I. Here we assume that n=5, so $N_1 = h^{(4)}(n_1)$ since $N_1 = h^{(n-1)}(n_1)$.

Table 1: Computational Cost and Communicational Overhead of our protocol

Message transmission	***Computational Cost***	***Communication Overhead***
(0) *MS* pre-compute and store N_1	n*HASH	0
(1) from *MS* to *VLR*	0	512*1= 64 bytes
(2) from *VLR* to *MS*	0	512+32= 68 bytes
(3) from *MS* to *VLR*	HASH=2, DIV=1, ADD=1, ENC=1, EXP=1	160*3+512+128+64 = 148 bytes
(4) from *VLR* to *HLR*	HASH=2, MUL=2, EXP=2, DEC=1, ENC=1	160+512*2+32*4= 164 bytes
(5) from *HLR* to *VLR*	HASH=5, ENC=2	160*4+32*5+512 = 164 bytes
(6) from *VLR* to *MS*	HASH=1, ENC=1	160*2+32*2= 48 bytes

EXP = modulo exponentiation, HASH = one-way or keyed hash, DIV = modulo division, MUL = modulo multiplication, ADD = modulo addition, ENC = encryption using private key, DEC = decryption using private key.

6.4 Storage Capacity

Storage capacity should be taken into account when designing security protocols for mobile network environments since the mobile equipment has limited storage capacity. Considering the example we take in figure 2, the mobile station should store the parameters p, q, $K = g^k \bmod p$, $\sigma = x + kK \bmod q$, $N_1, y_{VLR}, t, ID_H, ID_V$, $r = KH_{k_2}(k_1, y_{VLR}, N_1, ID_H, ID_V)$, $s = (t/(r + \sigma_{HLR-MS})) \bmod q$, $(EID_H, EID_V) = E_{k_1}[ID_H \| ID_V]$, x_{MS}, $(k_1, k_2) = hash(y_{VLR}^t \bmod p)$, $y_{MS} = g^{x_{MS}} \bmod p$, $y_{VLR} = g^{x_{VLR}} \bmod p$, where p is a 512 bit prime number, q is a 160 bit prime factor of $p-1$, N_1 is a hash function of 160 bit, , x_{MS}, and t are numbers less than q, r is a *Secure Hash Algorithm*-1 (*SHA*-1) of 160 bit, $C_H = (EID_H, EID_V)$ is 128 bit, the length of ID_H is 32 bit, the length of ID_V is 32 bit, and the output of the one-way hash is a 512 bit, which guarantees that both k_1 and k_2 have 256 bit where $(k_1, k_2) = hash(y_{VLR}^t \bmod p)$.

Therefore, the total length of $(q, \sigma, N_1, t, r, s, x_{MS}, K, y_{VLR}, y_{MS}, p, k_1, k_2, ID_V, ID_H, C_H)$ is given by: $160*8 + 512*5 + 32*2 + 128 = 4032$ bit = 504 bytes. The currently used SIM card consists of 16 k bytes of ROM, 256 bytes of RAM, and 8 k bytes of Electrically Erasable Programmable ROM (EEPROM) [1]. In summary, the capacity of EEPROM is large enough to accommodate the above parameters of our scheme.

7. Conclusions

This investigation addresses the weakness of the enhanced delegation-based authentication protocol raised by Tian-Fu Lee, which cannot solve the problem of *FHLR* in online authentication process. Therefore, a new Robust Delegation Signcrypted Authentication Protocol (RD-SAP) against the False Home Location Register Attack in 3GPP is presented. The proposed authentication protocol is based on Public Key Signcryption technique and which provides the user identity privacy, mutual authentication, nonrepudiation. This study also presents an enhanced protocol, which is not only has the same security properties as the original protocol, but also avoids the weakness in the original protocol. Therefore this scheme enjoys both computational and communicational efficiency.

REFERENCES:

[1] W.-B. Lee and C.-K. Yeh, “A New Delegation-based Authentication Protocol for use in Portable Communication Systems,” *IEEE Trans. Wireless Commun.,* vol. 4, NO. 1, pp. 57-64, Jan. 2005.

[2] Tian-Fu Lee, Shu-Hui Chang, Tzonelih Hwang, and Song-Kong Chong, “Enhanced Delegation-Based Authentication Protocol for PCSs”, *IEEE Trans. Wireless Commun.,* vol. 8, NO. 5, pp. 2166-2171, May 2009.

[3] Caimu Tang, Dapeng Oliver Wu, “An Efficient Mobile Authentication Scheme for Wireless Networks”, *IEEE Trans. Wireless Commun.,* vol. 7, NO. 4, pp. 1408-1416, April 2008.

[4] H.-Y. Lin, “Security and authentication in PCS," *Comput. Elect. Eng.,* vol. 25, no. 4, pp. 225-248, 1999.

[5] H.-Y. Lin and L. Harn, “Authentication protocols with non-repudiation services in personal communication systems," *IEEE Commun. Lett.*, vol. 3, no. 8, pp. 236-238, Aug. 1999.

[6] M. Rahnema, “Overview of the GSM system and protocol architecture," *IEEE Commun. Mag.,* pp. 92-100, Apr. 1993.

[7] A. Merotra and L. Golding, “Mobility and security management in the GSM system and some proposed future improvements,” *Proc. IEEE,* vol. 86, pp. 1480-1496, July 1998.

[8] T.-F. Lee, C.-C. Chang, and T. Hwang, “Private authentication techniques for the global mobility network,” *Wireless Personal Commun.*, vol. 35, no. 4, pp. 329-336, Dec. 2005.

[9] K. Al-Tawill, A. Akrami, and H. Youssef, “A new authentication protocol for GSM networks,” in *Proc. 23rd Annual IEEE Conf. Local Comput. Networks,* pp. 21-30, 1998.

[10] Nieme, Vand Nyberg K., “UMTS Security”, Nokia Research Center, Finland.

[11] Zheng, Y, “Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)”. In Advances in Cryptology - CRYPTO'97 (Berlin, New York, Tokyo, 1997) vol. 1294 of Lecture Notes in Computer Science Springer-Verlag pp. 165-179, 1997.

[12] Zheng, Y, “Signcryption and Its Applications in Efficient Public Key Solutions” Monash University, McMahons Road, Frankston, Melbourne, VIC 3199, Australia.

[13] D. Samfat, R. Molva, and N. Asokan, “Untraceability in Mobile Networks”, *in Proc. of International Conference on Mobile Computing and Networking,* 1995, P26-36.

[14] M. J. Beller, L.-F, Chang, and Y. Yacobi, "Privacy and Authentication on a Portable Communication System", *IEEE J. Select Areas Commun.,* vol. 11, NO. 6, pp. 821-829, Aug. 1993.

[15] Q. He, D. Wu, and P. Khosla, "Quest for Personal Control Over Mobile Location Privacy", *IEEE Commun. Mag.,* vol. 42, no. 5, pp. 130-136, 2004.

[16] A. Merotra and L. Golding, "Mobility and security management in the GSM system and some proposed future improvements," *Proc. IEEE,* vol. 86, pp. 1480-1496, July 1998.

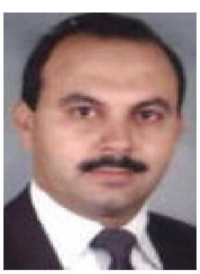
[17] M. Long, C.-H. Wu, and J. D. Irwin, "Localised authentication for internetwork roaming across wireless LANs," *IEE Proc. Commun.,* vol. 151, no. 5, pp. 496-500, Oct. 2004.

[18] T.-F. Lee, C.-C. Chang, and T. Hwang, "Private authentication techniques for the global mobility network," *Wireless Personal Commun.*, vol. 35, no. 4, pp. 329-336, Dec. 2005.

Esam A. A. HAGRAS received the B.S. degrees in Electrical Engineering from faculty of engineering, Alexandria Univ., Egypt, in 1994, M.S. degrees in Electrical Engineering from Mansoura Univ., Egypt, in 2001, respectively. During 2005-2007, he was on in Dept., of Electrical Engineering, faculty of engineering, Alexandria Univ. In Dec. 2007, he got the PhD degree in information security and communications.

His research interests in the field of information and multimedia security, chaotic cryptography, Hardware implementation of encryption algorithms on FPGA ,data compression, digital image watermarking, communication and wireless sensor network security. He has published more than twenty papers on security and communications.

Maha Amer is currently a M.S. student in Department of Communications and Electronics at Arab Academy of Science and Technology and Maritime Transport. She obtained her B.S. degree in 2006 from faculty of engineering Banha University, Egypt. Her research interests in Security, Wireless Communication Systems, Next Generation of Mobile Communication Systems, and authentication and key management's techniques in 3G and UMTS networks.



Hazem H. Ali – Professor and Chairman of Communication Department, Arab Academy of Science & Technology and Maritime Transport, Egypt. He received the B.S. degrees in Electrical Engineering from faculty of engineering, Kuwait Univ., Kuwait, in 1987; M.S. and PhD degrees in Electrical Engineering from George Washington University, USA, in 1993 VLSI Systems and circuits.

His research interests in the field of VLSI Systems, MEMs, communication and wireless sensor network security.