# An Improvement on An Efficient Mobile Authentication Scheme for Wireless Networks

**Jian-Zhu Lu[*], Xiuwei Fan, Jipeng Zhou, Hao Yang**
Department of Computer Science, Jinan University
No.601 Huangpu Road West, Guangzhou, 510632, China. Ph./Fax: +86-020-85220227
*Corresponding author, e-mail: tljz@jnu.edu.cn, fanxw@yahoo.com.cn, tzhoujp@jnu.edu.cn,
yanghao@tom.com

***Abstract***

*Mobile communication network has brought us great convenience. However, network security issues are outstanding increasingly. Authentication is the most essential procedure for preventing illegitimate, unauthorized or insecure devices from making access to the network. Tang and Wu proposed an efficient mobile authentication scheme for wireless networks, and claimed the scheme can effectively defend all known attacks to mobile networks including the denial-of-service attack. This paper strengthens the security of the scheme by authenticating the identity of visited location register such that any adversary cannot obtain the communication key between a mobile user and a service provider, or prevent them from establishing this key. An improvement is proposed to remedy these flaws. Our design is a less strong requirement for a mobile user MS in the communication cost than that of Tang and Wu's.*

***Keywords****: elliptic-curve cryptography, mutual authentication, mobile communication, security*

## 1. Introduction

Wireless networks permit a mobile user to access the services provided by service providers. As the characteristics of openness and terminal mobility, the data being transferred can be intercepted by the attackers. Mobile network security is somewhat more concentrated and complex than that of wired network. Protocols for authentication of two parties are fundamental for achieving secure communication over public, insecure networks. For secure communications in the roaming environment, it is important to provide a way for authentication between a mobile user and a service provider.

In mobile networks, there are three entities: a mobile station (MS), a home location register (HLR), and a visited location register (VLR). A typical approach to securing roaming service for a MS between his HLR and a VLR being visited is to employ strong authentication measures. When a MS roams to a foreign network managed by a VLR, it performs authentication with the VLR, under the assistance of his HLR. A successful run of the authentication and key agreement protocol ends up with the MS and the VLR sharing an authenticated symmetric key, which can be used to encrypt further communications between the MS and the VLR.

Several authentication protocols for global roaming service have been developed for mobile networks [1-10]. Particularly, in 2006, Jiang et al. proposed a mutual authentication and key exchange protocols using secret splitting principle in [6]. Lee and Yeh in [7] presented a delegation-based authentication protocol for use in portable communication system. In 2008, Tang and Wu in [8] produced a possible attack to Lee-Yeh's scheme, and proposed an efficient mobile authentication scheme called EMAS to overcome this flaw. Subsequently, they also propose a scheme on EMAS for protecting mobile privacy in wireless networks in [9].

Because an unauthorized service provider can't join the service networks without a valid credential, we focus only on authorized but dishonest insiders. In this article, we show that the scheme in [8] suffers from one of the following weaknesses: (1) the communication key between a mobile user and a legal service provider will be exposed to a dishonest service provider; or (2) under control of an adversary, a dishonest service provider can prevent a roaming user from establishing a communication key with a legal service provider. In the former case, there would be a serious accounting problem with their scheme. In the latter case, a mobile user can't obtain

*Received May 27, 2013; Revised July 17, 2013; Accepted July 26, 2013*

the desired services from legal providers. A preliminary version of this article published in [10] focuses on the study about the leakage of a communication key by a dishonest VLR, but does not study a DOS attack for an initiator by the First-Come-First-Served (FCFS) policy.

The remainder of this paper is organized as follows. Section 2 reviews Tang-Wu's scheme. We analyze its secure weaknesses in Section 3. Section 4 describes our improvement, and Section 5 presents its security and performance analysis. Finally, we make some conclusions in Section 6.

## 2. Review of Tang-Wu's Scheme

Tang-Wu's scheme mainly consists of two phases, namely, trust delegation initialization (TDI), and efficient mobile authentication (EMA). We assume that $T$ is a generator of an additive group $G$ on an elliptic curve and $p$ is the largest prime factor of the order of $T$. Let $h: Z_p^* \mapsto Z_p^*$ be a collision resistant one-way hash function and $\Pi: G \mapsto Z_p^*$ be a point representation function. The symbol $\hat{+}$ denotes a point addition operator in $G$, and $[X]_K$ denotes a message $X$ encrypted with a key $K$ using a symmetric encryption algorithm. The scheme works as follows:

1) TDI

Let $Y = xT$ be the public key of HLR whose private key is $x$. First, a new MS sends his/her real identity IDM to a HLR or home network for registration. Then HLR sets key usage restrictions on IDM in $m_w$, and generates MS's verification /delegation key pair $(\Gamma, \sigma)$ by calculating

$$\Gamma = (h(\mathrm{IDM} \mid m_w)T) \hat{+} (\kappa T)$$

$$\sigma = -xh(\Pi(\Gamma)) - \kappa \text{ (in } Z_p^*\text{)}$$

where $\kappa$ is a random number. Finally, HLR publishes $(\mathrm{IDM}, m_w, \Gamma)$ and delivers $(\sigma, m_w)$ to the MS through a secure channel. HLR always keeps the mapping relationship of IDM and $\sigma$.

MS accepts the delegation key $\sigma$ if $h(\mathrm{IDM} \mid m_w)T = (\sigma T) \hat{+} (h(\Pi(\Gamma))Y) \hat{+} \Gamma$.

2) EMA

Suppose there is a secure channel to protect the traffic between a VLR and the HLR. Let the statement $\{A \to B : M\}$ denote that $B$ receives a message $M$ from $A$.The mutual authentication between a MS and a VLR is illustrated in Figure 1. The details of EMA are as follows:

**Step 1**. $\mathrm{MS} \to \mathrm{VLR}$ : $S_1 = \{R, s, \mathrm{IDH}, m_w, C, N\}$

MS generates a ciphertext $C = [ck, ts, T_{\exp}, N]_\sigma$ and a digital signature $(R, s)$ as follows:

$$R = kT$$

$$s = \sigma - kh(\Pi(R) \mid N) \bmod p$$

where $ck$ is the communication key between the MS and the VLR, $T_{\exp}$ is the expiration time of communication key, and $k$ and $N$ are two random numbers. IDH is the HLR's identity of. A timestamp $ts$ is also selected by MS to counter replay attacks.

**Step 2**. $\mathrm{VLR} \to \mathrm{HLR}$ : $S_2 = \{\mathrm{IDM}, C\}$

On receipt of message from MS, the VLR checks the warrant $m_w$ for restrictions, and authenticates MS by using the attached digital signature $(R, s)$.

$$(sT) \hat{+} \Gamma \hat{+} (h(\Pi(\Gamma))Y) \hat{+} (h(\Pi(R) \mid N)R) = h(\mathrm{IDM} | \mathrm{m}_w)T$$

If yes, the VLR passes the information from MS with the identity IDM in $m_w$ and ciphertext $C$ to the HLR.

**Step 3**. $\mathrm{HLR} \to \mathrm{VLR}$ : $S_3 = \{C_{V,H}, [T_{V,M}]_\sigma\}$

Let $K_{V,H}$ be the session key between the VLR and the HLR, and IDV is the VLR's identity. The HLR obtains the delegation key $\sigma$ from its database, and then decrypts $C$ to obtain IDM, $T_{\exp}$, $ts$, $ck$, and $N$. Afterwards, HLR can compute $C_{V,H} = [\mathrm{IDM}, T_{\exp}, ts, ck, N]_{K_{V,H}}$ and $[T_{V,M}]_\sigma$, where $T_{V,M} = \{\mathrm{IDV}, N\}$.

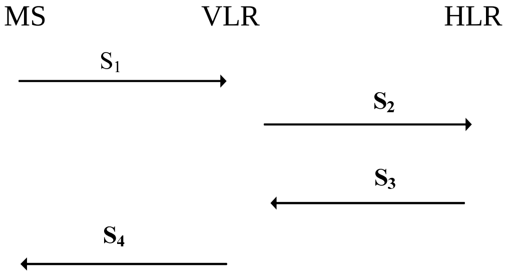

Figure 1. EMA protocol in Tang-Wu's scheme

**Step 4**. $\text{VLR} \rightarrow \text{MS}: \ S_4 = \{\text{IDH},[\text{IDV}, N,[T_{V,M}]_\sigma]_{ck}\}$

With the response from the HLR, the VLR can decrypt $C_{V,H}$ with the session key $K_{V,H}$ to obtain IDM, $T_{\exp}$, $ts$, $ck$ and $N$. After checking the validity of expiration timestamp $T_{\exp}$ and consistence of $N$, the VLR sends $[\text{IDV}, N, \ [T_{V,M}]_\sigma]_{ck}$ to the MS for authentication.

The MS decrypts the received message and $[T_{V,M}]_\sigma$ using $ck$ and $\sigma$, respectively. By the consistence of IDV and $N$, the MS can authenticate the VLR.

## 3. Toward Dishonest VLR of EMA

Let us assume that a HLR adopts the traditional FCFS policy, which has been shown to optimize the maximum response time metric in Bender et al. [11], for authenticating the received requests. The general framework for achieving mobile authentication in wireless networks proposed in [8] is interesting, but suffers from a attack launched by dishonest VLRs. An adversary can either get the communication key $ck$, or prevent an initiator MS from establishing this key with a VLR. The reasons are as follows. First, the HLR forwards $ck$ to a VLR who can't be demonstrated as a candidate of MS's access. Second, the HLR's response $[T_{V,M}]_\sigma$ utilized to disclose the VLR's identity may be dropped by a dishonest VLR.

Based on the idea of keeping a forged request at the front of the corresponding legal request in HLR's authentication process, the adversary now launches a attack to the VLR and the HLR. Figure 2 provides a high-level description of the attack. As shown in the figure, the attack consists of three stages, namely delaying the processing of $\text{S}_1$, sending a forged request to the HLR before $\text{S}_2$, and processing the HLR's response.

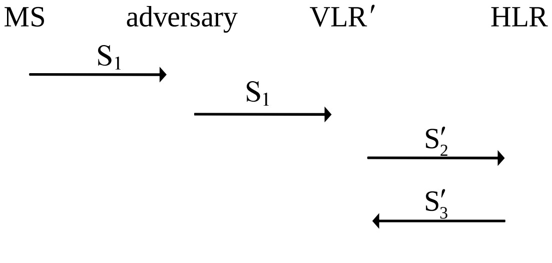

Figure 2. The attack for EMA in Tang-Wu's scheme

The first stage starts when a MS transmits a message $\text{S}_1$ to the VLR. At this time, the VLR will receive a large number of forge requests with digital signatures. This effectively means that the VLR delays the processing of the latter received message $\text{S}_1$. In this scenario, benign VLRs may certainly decide not to forward a message $\text{S}_2$ to the HLR before MS's signature in $\text{S}_1$ is verified. This, however, would also allow malicious users to waste the time of a VLR. A single malicious user may simply send a large number of false requests with digital signatures to the VLR, entangle it in processing false requests and verifying digital signatures, and eventually cause MS's signature verification delay. An adversary may generate much higher impact by deploying multiple malicious users in the VLR's local region.

In the second stage, a dishonest insider generates a request $\mathrm{S}_2'$ using the MS's message $\mathrm{S}_1$, and sends it to the HLR before the VLR does. We denote the dishonest insider by $\mathrm{VLR'}$ with identification $\mathrm{IDV'}$. A session key $K_{V',H}$ is established in advance between $\mathrm{VLR'}$ and the HLR before the authentication process. The adversary with a compatible radio receiver/ transmitter can easily eavesdrop ongoing radio communication link from the MS to the VLR to gain the MS's request $\mathrm{S}_1$. Then, the adversary sends $\mathrm{S}_1$ to $\mathrm{VLR'}$ who generates a request $\mathrm{S}_2'$ using IDM in $\mathrm{m}_w$ and $C$ in $\mathrm{S}_1$. That is,

**Step 2'**. $\mathrm{VLR'} \rightarrow \mathrm{HLR}$ : $S_2' = \{\mathrm{IDM}, C\}$.

In the last stage, when message-dropping attacks may exist in the HLR's response relay, $\mathrm{VLR'}$ drops the HLR's response (entirely or selectively), while participating in the authentication process. As a result, $[T_{V',M}]_\sigma$ (= $[\mathrm{IDV}', N]_\sigma$) authenticating the identity $\mathrm{IDV'}$ and their interrelation will be entirely lost, and the MS knows nothing about the authentication process between the HLR and $\mathrm{VLR'}$.

Because the content of $C$ in $\mathrm{S}_2$ actually says nothing about the need for the MS associated with the VLR, a message $[T_{V,M}]_\sigma$ from the HLR exchanged with the VLR will prove the VLR's identity. $\mathrm{S}_2$ is composed of the MS's identity IDM and the appropriate authentication data, $C$, which includes the key $ck$, an expiration date $(ts, T_{\exp})$ and a nonce $N$. Of course, to authenticate the request, the HLR needs that $C$ is encrypted with $\sigma$ and $N$ is a nonce. In particular, the HLR is aware of the VLR's identity and session key $K_{V,H}$ but do not know whether the VLR is the need for the MS, and sends $ck$ and $[T_{V,M}]_\sigma$ to it even if it is dishonest.

The response message $[T_{V,M}]_\sigma$ may be drop by a dishonest VLR. We note that this form of the authentication process has two disadvantages. First, It forces the HLR to verify the freshness of $N$ in $C$; if both the cipher text $C$ and IDM are same in two requests from different VLRs, the key $ck$ may be leaked. Second, the initiator MS may be vulnerable to a denial-of-service (DoS) attack when the HLR verifies the freshness of $N$ in $C$ with FCFS policy.

**Case 1**: A leakage of communication key.

We first assume that HLR does not verify the freshness of nonce $N$ when all of MS's ciphertexts $C$ s can be correctly decrypted. We discuss different VLRs' requests that can be generated using the same message $\mathrm{S}_1$ and are all valid in the HLR authentication process.

Because there is no evidence of the need for the initiator MS to access the related VLR and $\mathrm{VLR'}$, the HLR generates the messages $[T_{V',M}]_\sigma$ and $[T_{V,M}]_\sigma$ to MS. Remember that $\mathrm{S}_2'$ is a ``good'' structure request: $S_2' = \{\mathrm{IDM}, C\}$. It follows that $C$ can be decrypted to build the following tuple $M_C$ = $\{ck, ts, T_{\exp}, N\}$ with IDM's delegation key $\sigma$ by the HLR, who can also authenticate MS. We note that $M_C$ is then appended $(\mathrm{IDM}, [T_{V',M}]_\sigma)$ and given to $\mathrm{VLR'}$. That is,

**Step 3**. $\mathrm{HLR} \rightarrow \mathrm{VLR}$ : $S_3' = \{C_{V',H}, [T_{V',M}]_\sigma\}$ (*)

where $C_{V',H} = [\mathrm{IDM}, T_{\exp}, ts, ck, N]_{K_{V',H}}$ and $T_{V',M}$ = $\{\mathrm{IDV}', N\}$. $\mathrm{VLR'}$ passes the authentication of the initiator MS if and only if $T_{V',M}$ matches the nonce and its identity. Similarly, $\mathrm{S}_2$ can be utilized to return the answer by transmitting, the retrieved tuple $M_C$ and $(\mathrm{IDM}, [T_{V,M}]_\sigma)$ with the session key $K_{V,H}$ for the VLR.

A dishonest $\mathrm{VLR'}$ forwards the request $\mathrm{S}_2'$ to the HLR, but drops the reply $[T_{V',M}]_\sigma$, thus preventing its dishonest operations from being detected by the initiator MS while at the same time getting the communication key $ck$. As the HLR discloses $M_C$ to $\mathrm{VLR'}$, it must also disclose its associated communication key $ck$ to $\mathrm{VLR'}$. After $\mathrm{VLR'}$ receives $\mathrm{S}_3'$ from the HLR, which is defined as in ($*$), it successfully obtains the communication key $ck$ by decrypting $C_{V',H}$ with the session key $K_{V',H}$. Subsequently, the adversary can get the services from the VLR by impersonating the MS. It is straightforward to see that the VLR, MS and HLR cannot know the fact that the communication key $ck$ is leaked. Note that an attacker may directly launch this attack from the second stage without relying on the first stage conditions for delaying the processing of $\mathrm{S}_1$.

**Case 2**: A DOS attack to an initiator.

Now, assume that the HLR checks the freshness of nonce $N$ with FCFS policy when all of MS's ciphertexts $C$ s can be correctly decrypted. Here, we address a specific DoS attack for the initiator MS. A dishonest insider $\mathrm{VLR'}$ drops entirely HLR's response to prevent the MS from establishing the communication key with the VLR; and multiple compromised VLRs, controlled by the same adversary, may collaborate in launching this attack.

The HLR using the freshness of nonce $N$ can't identify a forged request. That is, if a request has a previously seen nonce $N$, the receiver may simply consider it as a forged one and drop it. Note that the freshness of nonce $N$ is relative to a request instance $\mathrm{S}_1$, not to the initiator MS. The forged message $\mathrm{S'}_2$ arrives first, and assures that the nonce of $C$ in $\mathrm{S}_2'$ is fresh. Due to the freshness of nonce $N$, HLR transmits a response to $\mathrm{VLR'}$.

The MS can't establish a communication key with the VLR since the legal request $\mathrm{S}_2$ is rejected by the HLR. The legal request, $\mathrm{S}_2$, with the same nonce $N$ may then arrive. When the freshness of the nonce is used as above discussion, the legal request will be discarded incorrectly by the HLR. $\mathrm{VLR'}$ in these cases is not able to access the services of the VLR, since the MS doesn't create a communication key with the VLR and, therefore, it drops entirely the response from the HLR.

## 4. Improvement

(1) Basic idea

Let VLR be a service provider to be accessed by a MS, and IDV be the VLR's identity. Two techniques can be used to construct a secure and efficient mobile authentication scheme. First, in order to authenticate the VLR's identity in the run of EMA, IDV is added to the ciphertext $C$ as soon as the MS generates a request to be sent to the HLR via the VLR. Second, A timestamp in the request can be treated as a nonce generated by the MS. Using the fact that the timestamp is monotone increasing for each request of the MS, the HLR can easily check its freshness.

(2) Description of improved scheme

Like Tang-Wu scheme [3], our improvement also consists of TDI and EMA two protocols. Since the setup procedure is the same as TDI proposed in [5], we only describe EMA procedure as shown in Figure 1.

**Step 1.** $\mathrm{MS} \to \mathrm{VLR}:\ S_1 = \{R, s^*, \mathrm{IDH}, m_w, C^*, ts\}$.

A MS picks a random number $k \in Z_p^*$ , and chooses a communication key $ck$, then generates a ciphertext $C^*$ and a digital signa-ture $(R, s^*)$ as follows:

$$C^* = [\mathrm{IDV}, ck, ts, T_{\exp}]_\sigma$$

$$R = kT$$

$$s^* = \sigma - kh(\Pi(R) \mid N^*) \bmod p\ ,$$

where $ts$ is the current timestamp made by MS, and $N^* = \mathrm{IDH|m}_w \mid C^* \mid ts$. The ciphertext $C^*$ provides effective means to validate both the initiator MS and its need to access a VLR with identification IDV. Here, $ts$ is treated as a nonce generated by MS, and $T_{\exp}$ is the time limit on key $ck$.

**Step 2.** $\mathrm{VLR} \to \mathrm{HLR}:\ S_2 = \{\mathrm{IDM}, C^*\}$.

On receipt of message $S_1$ from the MS, the VLR checks the warrant $m_w$ for restrictions, and authenticates the MS by using the attached digital signature $(R, s^*)$.

$$(s^*T) \overset{\frown}{+} \Gamma \overset{\frown}{+} (h(\Pi(\Gamma))Y) \overset{\frown}{+} (h(\Pi(R) \mid N^*)R) = h(\mathrm{IDM|m}_w)T$$

If yes, the VLR passes the ciphertext $C^*$ and the identity IDM in $m_w$ to HLR.

**Step 3.** $\mathrm{HLR} \rightarrow \mathrm{VLR}$ : $S_3 = \{C^*_{V,H}, [T^*_{V,M}]_\sigma\}$ .

The HLR first searches the delegation record $(\mathrm{IDM}, m_w, \sigma)$ from its database, and then decrypts $C^*$ to obtain IDV, $ck$ , $T_{\exp}$ , and $ts$ . Furthermore, the HLR checks the validity of expiration timestamp $T_{\exp}$ and the consistency of the VLR's identity with IDV in $C^*$ . If both are true, the HLR replaces the delegation record $(\mathrm{IDM}, m_w, \sigma)$ with $(\mathrm{IDM}, m_w, \sigma, ts)$ in the database. When receiving MS's next cipheretxt $C'^* = [\mathrm{IDV}', ck', ts', T'_{\exp}]_\sigma$ , the HLR compares $ts'$ in $C'^*$ with the stored $ts$ . if $ts' \le ts$ , the HLR rejects this request since it is a replay request. If $C'^*$ is valid, the HLR replaces $(\mathrm{IDM}, m_w, \sigma, ts)$ with $(\mathrm{IDM}, m_w, \sigma, ts')$ .This mechanism can resist replay attacks.

To generate the response of the request, the HLR computes $C^*_{V,H} = [\mathrm{IDM}, T_{\exp}, ts, ck]_{K_{V,H}}$ and $[T^*_{V,M}]_\sigma$ , where $T^*_{V,M} = \{\mathrm{IDV}, ts\}$ .

**Step 4.** $\mathrm{VLR} \rightarrow \mathrm{MS}$ : $S_4 = \{\mathrm{IDH},\ [\mathrm{IDV}, ts, [T^*_{V,M}]_\sigma]_{ck}\}$ .

With the response from the HLR, the VLR checks the validity of expiration timestamp $T_{\exp}$ and consistence of $ts$ after decrypting $C^*_{V,H}$ with the session key $K_{V,H}$ . Then, for MS's authentication, the VLR proceeds to generate a ciphertext $[\mathrm{IDV}, ts, [T^*_{V,M}]_\sigma]_{ck}$ .

The MS decrypts the received $[\mathrm{IDV}, ts, [T^*_{V,M}]_\sigma]_{ck}$ and $[T^*_{V,M}]_\sigma$ using $ck$ and $\sigma$ , respectively. By the consistence of IDV and $ts$ , the MS can authenticate the VLR.

## 5. Security Discussion and Performance Analysis

(1) Security discussion

We analyze the security provided by the improvement. As the basic requirements ($C_1$) to ($C_4$) on mobile authentication in [8] are entirely preserved, the associated security properties hold true here as well and we will not repeat them. EMA in the improvment does not suffer from the trouble to check the freshness of a nonce in traditional nonce-based authentication protocols. Attacks such as DOS attack to a MS or the impersonation attack of VLRs described in Section 3 are avoided. In the following, we only discuss the improved security features of EMA in Section 4:

**Impersonation Attacks** : The impersonating attacks can be efficiently prevented in the improvement by providing secure mutual authentication mechanisms between a roaming MS and VLR, MS and HLR, or VLR and HLR. Consider the following impersonation attack scenarios in the EMA.

An attacker hasn't the power to impersonate a legitimate VLR to cheat a MS, since he does not possess the correct values $ts$ and $[T^*_{V,M}]_\sigma$ . An outside attacker, by intercepting the exchanging messages in Steps 1 and 2, first obtains $C^* = [\mathrm{IDV}, ck, ts, T_{\exp}]_\sigma$ and $\{C^*_{V,H}, [T^*_{V,M}]_\sigma\}$ . Then, she/he replays previously reply messages (e.g., $[T'^*_{V,M}]_\sigma$ ) to cheat the MS. However, her/his identity and the nonce $ts$ are different from those within $C^*$ in the replayed messages and, therefore, the attack would be discovered by MS. At the same time, a MS can't be cheated by an inside attacker impersonating the visited VLR. Since the inside attacker doesn't know the delegation key $\sigma$ , it is impossible for her/him to generate $[T^*_{V,M}]_\sigma$ .

It is impossible for an attacker to impersonate a HLR while communicating with a VLR and to impersonate a VLR while communicating with a HLR, since neither the long-term secret key $K_{V,H}$ nor a valid IDV in $C^*$ is possessed. Hence, while communicating with the HLR in Step 2, she/he can't generate the valid messages to guarantee that the matching of IDV is done in a consistent way. In addition, the lack of key $K_{V,H}$ implies that it can not decrypt the response

$C^*_{V,H}$. Likewise, she/he generate the responding confirmation $C^*_{V,H}$ while communicating with the VLR in Step 3.

A MS and its HLR can authenticate their messages so that an attacker cannot impersonate them any more. Without the delegation key $\sigma$, the attacker can't generate a valid ciphertext $C^*$ in Step 1. Similarly, it is impossible for an attacker to generate the responding confirmation $[T^*_{V,M}]_\sigma$ in Step 3.

**Replay attacks and DoS attacks:** In DoS attacks to a HLR, an attacker aims to consume the HLR's critical resources. In the improvement, for every access request $S_1$ from all users that have registered in a HLR, a VLR can check the validity of the login message in time, and the HLR only needs to perform the symmetric encryption/decryption operations. At the same time, it is dificult for an attacker to lauch the DoS attack to a MS, since the HLR can use the consistency of the VLR's identity with IDV in $C^*$ to check if the VLR is the need of initiator MS. Furthermore, we make use of the timestamp $ts$ as a nonce to prevent replay attacks. Thus, our solution does not suffer from this attacks.

**The man-in-the-middle attacks:** In the man-in-the- middle attacks, an attacker can impersonate a VLR and fool the previous requester MS to connect to the attacker, instead of to the VLR. The attacker can then capture the MS's session key. In the improvement, the identity of each party in the scheme is authenticated, the scheme is secure against man-in-the-middle attacks. The authenticity of a request from MS is confirmed in time. VLR verifies the attached digital signature $(R, s^*)$ to guarantees the authenticity for the request received from MS. By verifying the consistency of identity of VLR with IDV in $C^*$, HLR can know if VLR is going to be accessed by MS. If the check of VLR's identity fails, then an attacker could redirect that message $S_1$ at Step 1, say to $\mathrm{VLR}'$, before the VLR receives it, with the subsequent result that MS would unknowingly communicate with $\mathrm{VLR}'$ instead of VLR.

Following decryption at Step 4, MS verifies that the message really is a reply by HLR to the current session key $ck$, by checking the consistency of IDV and $ts$ with them in $[T^*_{V,M}]_\sigma$. If the check of VLR's identity fails, the message at Step 4 are redirected to another VLR, say to $\mathrm{VLR}''$, after the VLR sends it. As a result, MS communicates with $\mathrm{VLR}''$, rather than the intended VLR.

(2) Performance analysis

The storage and the computation in the improvement are about the same costs as those in the scheme [10]. Let $|x|$ be the length of binary string $x$. No computation cost needs to be added by MS, except the additional storage space $|ts|$ in HLR for each MS.

Table 1. Communication costs comparison in the EMA protocol

| | $S_1$ (bits) | $S_2$(bits) | $S_3$(bits) | $S_4$ (bits) |
|---|---|---|---|---|
| Ref.[10] | 1320+$\|m_w\|$ | 584 | 968 | 896 |
| Our | 996+$\|m_w\|$ | 456 | 516 | 504 |

We adopt SHA-256, which has a 256-bit output, to implement the one-way hash function. We also implement the random-number generator by SHA-256 in the improvement. In general, the length of the identity of each user is usually less than 128 bits. Thus, we let the length of the user's identity be 128 bits. Besides, the length of every random number produced by the random-number generator is 256 bits and the length of every timestamp is about 60 bits. It is recommended that the security strength of $q$ based on ECDLP isn't less than 160 bits in [12] [Page 27]. The communication key of block cipher can be set as short as $|ck|$= 80 bits [8] while the improvement still enjoys strong security. Our EMA protocol uses overall structure similar to that of the scheme in [8], but our design is more efficient than theirs. Table 1 shows the communication costs of two protocols, where Ref.[10] denotes the protocol in [10]. Our design is a less strong requirement for MS in the communication cost than that of Ref.[10].

## 6. Conclusion

In this paper, we show that Tan-Wu scheme suffers from a dishonest VLR's attacks in roaming services. We also propose an improvement. Compared to Tang-Wu's scheme [8], our design is more secure and efficient than theirs.

## Acknowledgements

We thank the professor Kefei Chen at Shanghai Jiaotong university for his suggestions on improving an earlier version of this article. We also thank the anonymous reviewers for their helpful comments. This work was supported in part by the National Natural Science Foundation of China under Grants 61070164 and 61272415, by the Provincial Natural Science Foundation of Guangdong under Grants 2009B010800023, 2010B090400164 and S2011010002708, and by the Projects in the Scientific Innovation of Jinan University under Grants 11611510.

## References

[1] Deng S, Hu Z, Niu X, Yang Y. A Wireless Mutual Authentication and Key Agreement Protocol. *ACTA Electronica Sinica*. 2003; 31(1):135-138.

[2] Hwang R, Su F. A New Efficient Authentication Protocol for Mobile Networks. *Computer Standards and Interfaces*. 2005; 28(2):241-252.

[3] Ngo HH, Wu X, Le PD, Srinivasan B. An individual and group authentication model for wireless network services. *Journal of Convergence Information Technology*. 2010; 5(1): 82-94.

[4] Wang L, Zhang R. An Improved Authentication Approach for Mobile DRM Systems. *Advances in information Sciences and Service Sciences*. 2012; 4(23):198-206.

[5] Zhang D, Ma Z, Mo J, Yang Y. A Delegation-Based Protocol for Anonymous Roaming Authentication in Mobile Network. *International Journal of Digital Content Technology and its Applications*. 2013; 7(3): 623-630.

[6] Jiang Y, Lin C, Shen X, Shi M. Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks. *IEEE Transactions on Wireless Communications*. 2006; 5(9): 2569-2577.

[7] Lee W, Yeh C. A New Delegation-based Authentication Protocol for Use in Portable Communication Systems. *IEEE Transactions on Wireless Communications*. 2005; 4(1): 57-64.

[8] Tang C, Wu DO. An Efficient Mobile Authentication for Wireless Networks. *IEEE Transactions on Wireless Communications*. 2008; 7(4):1408-1416.

[9] Tang C, Wu DO. Mobile Privacy in Wireless Networks Revisited. *IEEE Transactions on Wireless Communications*. 2008; 7(3): 1035-1042.

[10] Lu J-Z, Zhou J. *The security of an efficient mobile authentication scheme for wreless networks*. In Proceedings of the 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM) Topic: Communication, Networking & Broadcasting. Chengdu, China. 2010: 1-3.

[11] Bender MA, Chakrabarti S, Muthukrishnan S. *Flow and stretch metrics for scheduling continuous job streams*. Proceedings of the 9th ACM-SIAM Symposium on Discrete Algorithms (SODA). Philadelphia, PA, USA. 1998: 270-279.

[12] NIST FIPS PUB 186-3 Digital Signature Standard (DSS). U.S. Department of Commerce. June 2009.