Extension of Authentication Protocol for GSM*

Cheng-Chi Lee† Min-Shiang Hwang‡ Wei-Pang Yang†

Department of Computer and Information Science†
National Chiao Tung University
1001 Ta Hsueh Road,
Hsinchu 300, Taiwan, R.O.C.
Email: {cclee, wpyang}@cis.nctu.edu.tw

Department of Information Management‡
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@cyut.edu.tw
Fax: 886-4-23742337

July 4, 2002

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-005.

‡Corresponding author: Prof. Min-Shiang Hwang

Extension of Authentication Protocol for GSM

Abstract

In this paper, an extension of the authentication protocol for GSM is proposed to improve some drawbacks of the current GSM authentication protocol including: (1) not supporting bilateral authentication; (2) huge bandwidth consumption between VLR and HLR; (3) stored space overhead in VLR; (4) overloaded HLR with authentication of mobile stations. As a result, our new extension of the authentication protocol does not only improve these drawbacks but also achieve our five requirements: mutual authentication, reduction of bandwidth consumption, less storage of VLR database, security, and efficiency. The merit of the proposed protocol is that it does not make a fuss and alter the existing architecture of GSM at all. The robustness of our new protocol is also based on security algorithms $A3$, $A5$, and $A8$.

Keywords: Authentication, GSM, Mobile Communications, Security.

1 Introduction

Nowadays, the Global System of Mobile communications (GSM) has been wide spread in the world. It has always been the standard of the Pan-European digital cellular system [5] and has also become the worldwide wireless communication standard [18, 20]. GSM brings so much convenience for people's life that anyone can use it to communicate with anyone else in almost any place at any time. However, people are most worried about two major security issues, which are privacy and authentication [2, 3, 9]. Privacy refers to the guarantee that the communication messages do not intercepted by an eavesdropper [7]. On the other hand, authentication is done to ensure that any unauthorized user cannot fraudulently obtain his/her required services from the home domains [12, 15].

In the GSM architecture [18, 20], the Mobile Stations (MS) communicates through radio links with the Base Stations (BS), which is in turn connected to the Mobile Switching Centers (MSC). The MSC is responsible for transiting signals between radio links and wirelined networks. The Home Location Register (HLR) and the Visitor Location Register (VLR) are two databases in GSM. HLR is responsible for storing subscribers' information and locations; on the other hand, VLR is responsible for storing the information of visiting subscribers. The Authentication Center (AuC) stores the subscribers' secret keys and generates authentication parameters for the authentication protocol on the request of HLRs. The authentication protocol is defined in GSM recommendation 02.09 [4]. In the GSM authentication protocol, several drawbacks can be found as follows: (1) it lacks the capability of authenticating base stations (VLR); (2) it increases bandwidth consumption between VLR and HLR; (3) the space overhead in VLR occurs; and (4) the authentication of the mobile stations overloads HLR.

Recently, many authentication protocols for GSM have been proposed. Among them, Harn and Lin's protocol [6] (proposed in 1995) can solve Drawback (2). They use two more one-way functions. In addition, they can provide non-repudiation services. However, the overhead occurs in the computations of one-way functions by each subscriber in each session. In 1998, Al-Tawil et al. [1] proposed a new authentication protocol with less signaling traffic and better call set up time. Their protocol cannot solve the above drawbacks but adds a "mobile user events counter" ($COUNTM$) into HLR and MS's SIM card. In 1999, Lo and Chen [16, 17] proposed a secure communication for GSM. Their protocol is more secure than the existing GSM. However, its architecture is changed to public-key cryptography, and they cannot solve the above drawbacks either. Stach et al.'s protocol [22] employs an additional one-way function to establish trust between an MS and VLR for the purpose of non-repudiation of service. Its architecture is also changed, but they still have not had the above drawbacks improved. Later, Lee et al. [14] proposed an enhanced privacy and authentication for GSM. They can solve Drawbacks (2)-(4). The merit of their protocol is maintaining the existing architecture of GSM.

In this paper, an extension of the authentication protocol for GSM is proposed which improves above drawbacks of the existing GSM authentication protocol. The goals of this paper are as follows:

- To achieve mutual authentication between MS and VLR
- To reduce bandwidth consumption between VLR and HLR
- To reduce the stored space in VLR
- The authentication of an MS is done by VLR without the assistance of the MS's HLR
- The existing architecture of the GSM authentication protocol is not changed

The rest of this paper is organized as follows. In the next section, the existing GSM authentication protocol will be reviewed. Then, our new extension of the GSM authentication protocol will be discussed in Section 3. Section 4 will analyze the security of our proposed protocol. In Section 5, there will be further discussions about our proposed protocol, and finally Section 6 will conclude this paper.

2 Overview of Authentication Protocol for GSM

In a GSM network, authentication is an important process that consists of identification and verification [3, 19] to ensure that the network services will not to obtain fraudulently.

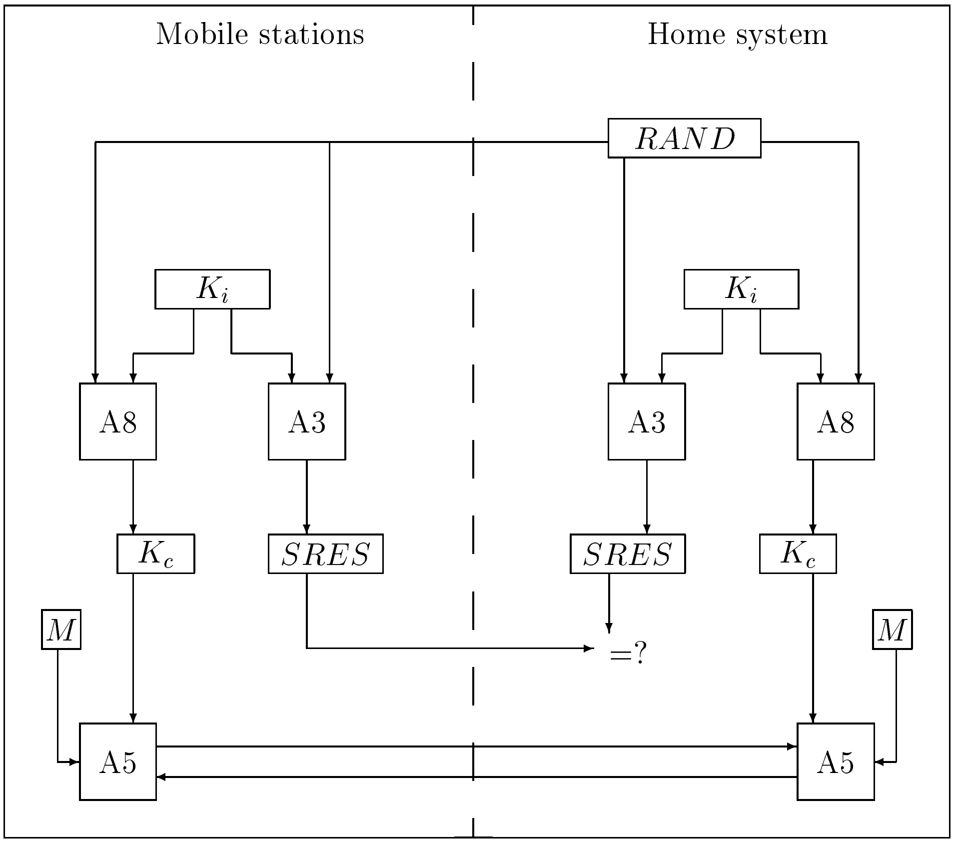

Figure 1: Architecture of GSM

The security of GSM is based on algorithms $A3$, $A5$, and $A8$. The architecture of GSM is shown in Figure 1 [11]. The outputs of $SRES$ and K_c are computed, respectively, using K_i and $RAND$ through algorithm $A3$ and $A8$ as inputs, where K_i is the mobile station's secret key shared between the mobile station and the home system (HLR) and saved in the subscriber identity module (SIM) card, and $RAND$ is generated by HLR. $SRES$ is a certificate to authenticate mobile stations, and K_c is the session key between mobile stations and base stations (VLR). To transmit message confidentially, algorithm $A5$ is used to encrypt/decrypt the transmitted messages.

To authenticate mobile stations in GSM, a challenge/response mechanism through message exchanges between the mobile station and base station is carried out. This can oftentimes lead to overload signaling [1]. In the following, we shall review the existing GSM authentication protocol [18, 20] as shown in Figure 2.

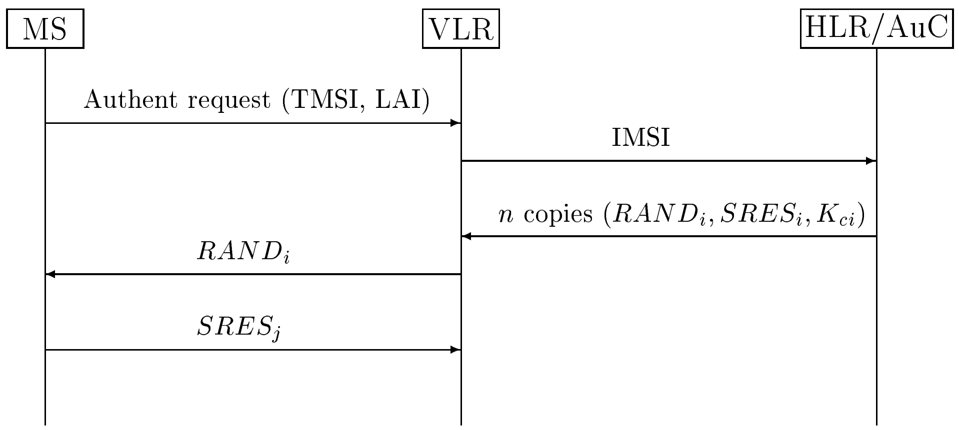

Figure 2: The authentication protocol for GSM

(1) When an MS enters a new visiting domain to require new services, he/she sends an authentication request to VLR. The request contains the Temporary Mobile Subscriber Identity (TMSI) and the Location Area Identity (LAI) [1].

(2) Through the received TMSI, the new VLR obtains the International Mobile Subscriber Identity (IMSI) from the old VLR. Then the new VLR sends the IMSI to HLR.

(3) The HLR then generates n copies of the triplet authentication parameters $\{RAND_i, SRES_i, K_{c_i}\}$ at a time for the mobile station to use later for each call, and then the HLR sends them to the VLR.

(4) The VLR receives the authentication parameters and stores them in his/her database, and then he/she selects a triplet $\{RAND_i, SRES_i, K_{c_i}\}$ to authenticate the mobile station. Then the VLR forwards the selected $RAND_i$ to the MS.

(5) When the MS receives $RAND_i$, he/she can compute $SRES_j$ and K_{c_j} and send $SRES_j$ back to the VLR. Then the MS keeps K_{c_j} for secret communication.

(6) Once the VLR receives $SRES_j$ from the MS, it compares this $SRES_j$ with the selected $SRES_i$. If they are the same, the MS is authenticated.

Note that as long as an MS stays in the coverage area of this VLR, the VLR has the ability to authenticate the MS when requiring no other n copies of the triplet authentication parameters from HLR. When the VLR uses up the set of parameters, she/he can just make a request for another set of authentication parameters from HLR to authenticate the MS.

3 Extension of the Authentication Protocol for GSM

3.1 Drawbacks of the Authentication Protocol for GSM

It is found that the authentication protocol for GSM have four drawbacks as follows:

- It is not a mutual authentication mechanism between mobile stations and base stations (VLR). GSM only provides unilateral authentication for the mobile stations. Using the challenge/response mechanism, the identity of a mobile station is verified. However, the identity of VLR cannot be authenticated. It is therefore possible for an intruder to pretend to be a legal network entity and thus to get the mobile stations' credentials [13].

- The VLR must turn back to the HLR to make a request for another set of authentication parameters when the MS stays in the VLR for a long time and exhausts her/his set of authentication parameters for authentication. There is a bandwidth-consumption between VLR and HLR [21].

- Every mobile station in the particular VLR has n copies authentication parameters himself/herself. The parameters are stored in the particular VLR's database, and then space overhead occurs.

- The authentication of an MS is done in VLR and must be helped by the HLR of the MS for each communication.

3.2 The Requirements of Our Authentication Protocol for GSM

In this subsection, we set up five requirements that our new extension of the GSM authentication protocol should satisfy. In the following, the five requirements are listed and illustrated.

- Mutual authentication:

  The proposed authentication protocol should be able to achieve bilateral authentication between MS and VLR. Using the challenge/response mechanism, the identity of MS and VLR can be verified. In the HLR-authenticating-VLR process, MS can make sure that he/she is communicating with a legitimate network entity.

- Reduction of bandwidth consumption:

  In GSM, authentication parameters are distributed by the HLR to the VLR in the form of n copies of triplet authentication parameters. Each of these parameters is used only once by the VLR during authentication. Hence, the parameters are consumed quickly. Then the VLR must go back to the HLR frequently to require another set of authentication parameters. This increases bandwidth consumption. The proposed protocol is supposed to reduce the bandwidth consumption.

- Reduction of the storage of VLR database:
  In GSM, because the particular VLR stores n copies of the triplet authentication parameters of each MS, the database space is easily used up. The proposed protocol is supposed to cut down the space consumption in VLR. Hopefully, in our new protocol, VLR should only store a copy of the authentication parameters instead of n copies in her/his database.

- Authentication of MS is to be done by VLR instead of HLR, even if VLR does not know MS's secret key K_i and algorithm $A3$ [14].

- The proposed protocol must keep the security and efficiency of the existing GSM authentication protocol. It should not add any extra computations, and neither should it change the architecture of the existing GSM system.

3.3 Our Authentication Protocol for GSM

To overcome the above four drawbacks and meet all the above five requirements, an extension of the authentication protocol for GSM is proposed in this paper.

The key concept of our new protocol is that the HLR of the MS gives the visiting VLR of the MS authorization (Temporary secret Key, TK_i) to authenticate the MS without knowing the secret key K_i of the MS. If the MS stays in the coverage of his/her visiting VLR for a long time, the VLR does not go back to HLR to require another set of authentication parameters to identify the MS. The VLR only uses the TK_i of HLR given with her/his generated $RAND_j$ for each call to compute $SRES$ and then identifies the MS, where $RAND_j$ is a random number generated by the visiting VLR in the subsequent calls. Only one $RAND_j$ is generated by the visiting VLR for each

jth call no matter how long the MS stays in the coverage of the visiting VLR. Therefore, the visiting VLR only saves a copy of the authentication parameters ($RAND$, TK_i) of the MS to identify the MS instead of n copies needed in the existing GSM authentication. In addition, since the visiting VLR does not go back to HLR to require another set of authentication parameters, the signaling load is reduced between the VLR and HLR.

In addition, our proposed authentication protocol does not only identify the MS but also verify the legality of the visiting VLR. This is called mutual authentication. No fraudulent VLR or anyone at all can pretend to be the legal VLR to fool the MS because only real VLR has her/his certificate $Auth\_VLR$ that is authenticated by the HLR of the MS.

The authentication process is described as follows and depicted in Figure 3.

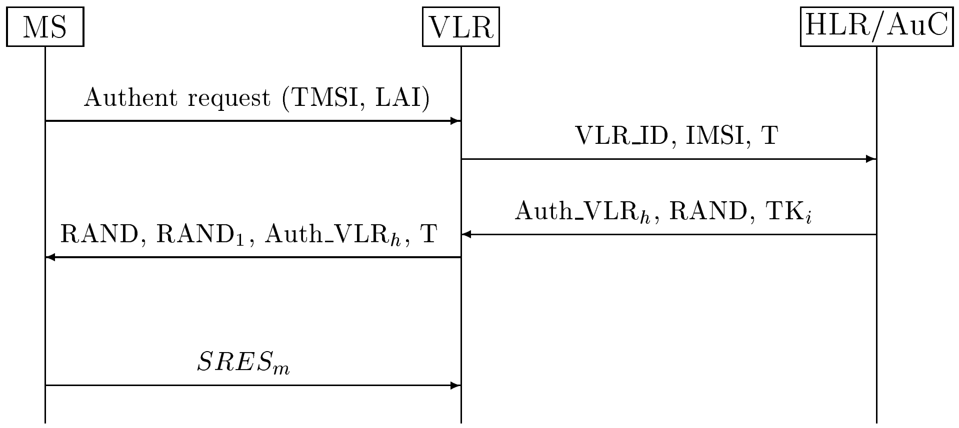

Figure 3: Our authentication protocol for GSM

(1) This process is similar to process (1) of the existing authentication for GSM in Section 2. The authentication request adds a time-stamp T to authenticate the VLR and prevents from the replay attack [8, 10].

(2) The same way as the existing authentication process for GSM, the VLR obtains the IMSI of the MS. Then she/he sends the IMSI along with

her/his identification VLR_ID and time-stamp T to the HLR of the MS through a secure channel.

(3) Once the HLR of the MS receives these messages, she/he checks if the identity VLR_ID of the visiting VLR of the MS is a legal VLR and if T is not obsolete. Then the HLR computes the certificate of the visiting VLR, $Auth\_VLR_h$, and the temporary secret key of the MS, TK_i, through algorithm $A3$, using (K_i, T) and (K_i, $RAND$) as inputs, respectively. The K_i is a secret key between MS and his/her HLR, and $RAND$ is generated by the HLR. Over a secure channel, the HLR of the MS sends $Auth\_VLR_h$, $RAND$, and TK_i to the visiting VLR of the MS.

(4) When the VLR receives these messages, she/he computes the $SRES$ through algorithm $A5$ using $RAND_1$ and TK_i as inputs, where $RAND_1$ is the random number generated by the VLR for this call. In the next call, the VLR should generate another random number $RAND_j$. That is to say, as long as the MS stays in the coverage of the visiting VLR, the VLR does not need to go back to HLR to require another set of authentication parameters. The VLR only generates a different $RAND_j$ for each jth call. Then, the VLR forwards $Auth\_VLR_h$ and $RAND$ along with the generated random number $RAND_1$ and T to MS.

(5) Upon receiving these messages from the visiting VLR, the MS first checks if the VLR's certificate $Auth\_VLR_h$ is valid by verifying if T is in use as $Auth\_VLR_m$ is and if T is the same as it was when last sent, where $Auth\_VLR_m$ is computed through algorithm $A3$ using (K_i, T) as inputs. Then, $Auth\_VLR_m$ is compared with the received $Auth\_VLR_h$. If they are the same, the identity of the VLR is authenticated. Then the MS uses algorithm $A3$ to generate TK_i with his/her secret key K_i and $RAND$ as inputs, and then he/she continue using TK_i and $RAND_1$ through

algorithm $A5$ as inputs to generate $SRES_m$ which is then sent back to the VLR.

(6) Once the VLR receives $SRES_m$ from the MS, it compares $SRES_m$ with $SRES$. If they are the same, the MS is authenticated.

The security of our new authentication protocol for GSM is also based on algorithms $A3$ and $A5$. In addition, we do not change the architecture of the existing GSM.

4 Cryptanalysis

Due to the fact that we adopt the architecture of the existing authentication protocol for GSM as it is, the security of our new protocol, which is the same as that of the existing authentication protocol for GSM, is based on algorithms $A3$, $A5$, and $A8$. In addition, to authenticate the legality of the visiting VLR, we add a time-stamp T to the authentication protocol for GSM. Relying on the HLR of the MS to generate a certificate $Auth\_VLR$ using T and the MS's secret key K_i as inputs for the visiting VLR of the MS, the VLR can be authenticated by the $Authe\_VLR$.

The time-stamp is generated by the MS, which enhances the security of our proposed protocol against the replay attack. Although an attacker can intercept T and $Auth\_VLR$ and then forge the VLR the replay still cannot succeed because T is incorrect. The MS can also check if the T is the same as it was when sent the last time even if the fake VLR replays T and $Auth\_VLR$.

Since the secret key K_i is only known to MS and HLR, and nobody can forge them to fool others. Without the knowledge of K_i, $Auth\_VLR$ and $SRES$ cannot be computed by anyone. Therefore, the security of our proposed protocol is based on K_i. For authenticating the MS, the visiting VLR only generates a different $RAND_j$ to compute $SRES$ for every jth call. The security here is based on HLR giving VLR authorization to authenticate the MS.

In addition, It is assumed that a secure channel between VLR and HLR is setup before mobile communications. It is feasible to use some cryptographic techniques such as symmetric cryptosystems or asymmetric cryptosystems [23].

5 Discussions

In the previous sections, we have reviewed the existing authentication protocol for GSM and shown their drawbacks. We have also described our new extension of the authentication protocol for GSM. In the following, we shall demonstrate that our proposed protocol can achieve our requirements.

- Mutual authentication:

  In fact, it is assumed that the HLR is a trusted authority with the capability to identify the VLR. For example, the HLR can use cryptographic techniques such as *digital signatures* [23], to identify the VLR. Once the VLR is identified, the HLR can distribute her/his certificate $Auth\_VLR$ to the VLR. By authenticating the $Auth\_VLR$, MS can ensure that he/she is communicating with a legitimate VLR. Therefore, the proposed protocol can achieve bilateral authentication between MS and VLR.

- Reduction of bandwidth consumption:

  In the proposed protocol, the HLR gives the VLR TK_i to authenticate MS. As long as the MS stays in the coverage area of the visiting VLR, the VLR can use the TK_i to authenticate MS for each call. Since the visiting VLR does not go back to HLR to require another set of authentication parameters, the signaling load is reduced between the VLR and HLR. Therefore, the proposed protocol can reduce bandwidth consumption.

- Reduction of the storage of VLR database:

  In the proposed protocol, it is seen that the VLR only stores a copy of authentication parameters ($RAND, TK_i$) instead of n copies ($RAND_i$, $SRES_i$, K_{c_i}). Therefore, the proposed protocol can save VLR database space.

- In the existing authentication protocol for GSM, authentication of MS is to be done by VLR with the assistance of HLR when the authentication parameters are used up. In the proposed protocol, authentication of MS is to be done by VLR alone without the presence of HLR. The key point here is that the HLR gives the visiting VLR of the MS authorization TK_i to authenticate the MS without knowing K_i.

- Due to its simplicity and efficiency, the GSM system is widespread in the world. In order not to lose these advantages, the proposed protocol does not add any computations to it, nor is there any change in the architecture of the existing GSM system. The security of our new protocol is still based on algorithms $A3$, $A5$, and $A8$.

Although the proposed protocol can achieve our requirements, the existing GSM system and the proposed protocol as well are still not supported with security functions as follows.

- Data integrity:

  Data integrity is not available in the GSM system. The system cannot ensure that the transmitted messages between MS and VLR do not modified by an intruder.

- Non-repudiation:

  The system does not provide the non-repudiation of origin or delivery.

- End-to-end confidentiality:

  GSM only ensures the confidentiality of data between MS and VLR over wireless networks. It does not provide end-to-end confidentiality. Generally, it is assumed that a secure channel between VLR and HLR over a fixed network is already setup.

- Traffic confidentiality:

  The GSM system also lacks traffic confidentiality. Traffic flow analysis may reveal some information [23].

To equip the system with the above security functions, a symmetric cryptosystem or an asymmetric cryptosystem can be employed. However, in view of mobile phone's power and computational ability, the GSM system is still popular and widespread in the world because of its simplicity and efficiency.

In Section 1, we have mentioned that many authentication protocols cannot achieve our requirements as shown in Table 1. Theses protocols do not only not meet our all requirements, but also change the architecture of the GSM authentication protocol. The original GSM uses the simple and efficient algorithms A3, A5, and A8 due to the small battery consumption of mobile station. In our protocol, it keeps the advantage that did not change the architecture of the GSM system. In other words, it can meet our all requirements. In 1999, Lee et al. [14] proposed a protocol that does not change its architecture. However, it cannot achieve mutual authentication between MS and VLR.

Next, we show that our protocol is superior to the original GSM and Lee et al.'s protocols. The original GSM and Lee et al.'s protocols do not support mutual authentication between MS and VLR. In original GSM and Lee et al.'s protocols, VLR sends random number to MS for generating signal result (SRES). MS only generates and returns SRES to VLR, but not authenticate the VLR. Therefore, both of original GSM and Lee et al.'s protocols cannot achieve mutual authentication between MS and VLR. Since VLR does not ask HLR for another set of authentication parameters in Lee et al.'s and our protocols, the bandwidth consumption is less than that of the original GSM protocol. In addition, VLR requires storing n copies of the authentication parameters in the original GSM protocol. In Lee et al.'s and our protocols, VLR only requires storing a copy of the authentication parameters instead of n copies of that in its database.

Table 1: Comparisons among the GSM authentication protocols

	Original	Ours	[14]	[6]	[1]	[17]	[22]
MA	No	Yes	No	No	No	Yes	Yes
RBC	No	Yes	Yes	Yes	Yes	No	No
RSV	No	Yes	Yes	No	No	No	No
AMVH	No	Yes	Yes	No	No	No	No
CAG	-	No	No	Yes	Yes	Yes	Yes

*MA: Mutual Authentication, RBC: Reduction of Bandwidth Consumption, RSV: Reduction of the Storage of VLR database, AMVH: Authentication of MS by VLR instead of HLR, CAG: Change Architecture of GSM.

6 Conclusions

In this paper, we have pointed out that the existing authentication protocol for GSM has some drawbacks as Subsection 3.1 shows. To overcome these disadvantages, we have proposed a new extension from the protocol that can satisfy our requirements and achieve goals as Subsection 3.2 and Section 1 show.

Acknowledgements

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC90-2213-E-324-005.

References

[1] Al-tawil, K., Akrami, A., and Youssef, H.: 'A new authentication protocol for GSM networks,' *IEEE 23rd Annual Conference on Local Computer Networks (LCN'98)*, 1998, pp. 21-30

[2] Aziz, A., and Diffie, W.: 'Privacy and authentication for wireless local area networks,' *IEEE Personal Communications*, 1994, 1, (1), pp. 24-31

[3] Beller, M.J., Chang, L.F., and Yacobi, Y.: 'Privacy and authentication on a portable communications system,' *IEEE Journal on Selected Areas in Communications*, 1993, 11, pp. 821-829

[4] ETSI. 'Recommendation gsm 02.09: Security related network functions,'. tech. rep., European Telecommunications Standards Institute, ETSI, June 1993

[5] ETSI. 'Recommendation gsm 03.20: Security related network functions,'. tech. rep., European Telecommunications Standards Institute, ETSI, June 1993

[6] Harn, L. and Lin, H.Y.: 'Modification to enhance the security of the GSM protocol,' *Proceedings of the 5th National Conference on Information Security*, May 1995, Taipei, Taiwan, pp. 416-420

[7] Hwang, M.S.: 'Dynamic participation in a secure conference scheme for mobile communications,' *IEEE Transactions on Vehicular Technology*, 1999, 48, (5), pp. 1469-1474

[8] Hwang, M.S.: 'A remote password authentication scheme based on the digital signature method,' *International Journal of Computer Mathematics*, 1999, 70, pp. 657-666

[9] Hwang, M.S. and Lee, C.H.: 'Authenticated key-exchange in mobile radio network,' *European Transactions on Telecommunications*, 1997, 8, (3), pp. 265-269

[10] Hwang, M.S., Lee, C.C., and Tang, Y.L.: 'An improvement of SPLICE/AS in WIDE against guessing attack,' *International Journal of Informatica*, 2001, 12, (2), pp. 297-302

[11] Hwang, M.S., Tang, Y.L., and Lee, C.C.: 'An efficient authentication protocol for GSM networks,' *AFCEA/IEEE EuroComm'2000*, May 2000, Munich, Germany, pp. 326-330

[12] Hwang, M.S. and Yang, W.P.: 'Conference key distribution protocols for digital mobile communication systems,' *IEEE Journal on Selected Areas in Communications*, 1995, 13, pp. 416-420

[13] Karger, Paual, A., Frankel, Y., and Herzberg, A.: 'Security issues in a CDPD wireless network,' *IEEE Personal Communications*, 1995, 2, pp. 16-27

[14] Lee, C.H., Hwang, M.S., and Yang, W.P.: 'Enhanced privacy and authentication for the global system for mobile communications,' *Wireless Networks*, 1999, 5, pp. 231-243

[15] Lin, H.Y. and Harn, L.: 'Authentication protocols with nonrepudiation services in personal communication systems,' *IEEE Communications Letters*, 1999, 3, pp. 236-238

[16] Lo, C.C. and Chen, Y.J.: 'A secure communication architecture for GSM networks,' *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, 1999, pp. 221-224

[17] Lo, C.C. and Chen, Y.J.: 'Secure communication mechanisms for GSM networks,' *IEEE Transactions on Consumer Electronics*, 1999, 45, (4), pp. 1074-1080

[18] Mallinder, B.: 'An overview of the GSM system,' *Proc. Third Nordic Seminar on Digital Land Mobile Radio Commun.*, Setp. 1988, Copenhagen, Denmark, pp. 12-15

[19] Molva, R., Samfat, D., and Tsudik, G.: 'Authentication of mobile users,' *IEEE Network*, 1994, 8, pp. 26-34

[20] Rahnema, M.: 'Overview of the GSM system and protocol architecture,' *IEEE Communication Magazine*, April 1993, pp. 92-100

[21] Samfat, D., Molva, R., and Tsudik, G.: 'Authentication of mobile users,' *IEEE Network*, 1994, 8, pp. 26-34

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

[23] Stallings, W.: '*Cryptography and Network Security: Principles and Practice*,' Prentice Hall, 1999, second edition