Design and Analysis of Improved GSM Authentication Protocol for Roaming Users

GeneBeck Hahn[1], Taekyoung Kwon[2], Sinkyu Kim[3], and JooSeok Song[1]

[1] Department of Computer Science, Yonsei University, Seoul, Korea
{gbhahn, jssong}@emerald.yonsei.ac.kr
[2] School of Computer Engineering, Sejong University, Seoul, Korea
{tkwon}@sejong.ac.kr
[3] National Security Research Institute, Daejeon, Korea
{skkim}@etri.re.kr

Abstract. In this paper, we improve the GSM (Global System for Mobile Communications) authentication protocol to reduce the signaling loads on the network. The proposed protocol introduces a notion of the enhanced user profile containing a few of VLR IDs for the location areas where a mobile user is most likely to visit. We decrease the authentication costs for roaming users by exploiting the enhanced user profile. Our protocol is analyzed with regard to efficiency and is compared with the original protocol.

1 Introduction

GSM, an european standard for the second generation mobile networks, intrinsically provides three security functions[1][2].

- Authentication for subscriber's identity
- Anonymity for subscriber's identity
- Confidentiality for data on the radio path

While providing the security functions listed above, the GSM networks suffers from excessive signaling loads for the transmission of authentication parameters. This indicates that the GSM authentication protocol requires significantly high costs while a number of communicating mobile users frequently move through the location areas. Considering the tremendously growing mobile users, this problem must become critical[2]. In this paper, we improve the GSM authentication protocol to reduce the costs of roaming user authentication. The basic concept of our protocol is to utilize the enhanced user profile containing a group of VLR (Visitor Location Register) IDs. Among the VLRs, the master VLR is defined as a VLR to which a mobile user performs location registration, while the slave VLR is a VLR to which a mobile user performs location update. It means that a mobile user moves from the location area covered by master VLR to the other areas covered by slave VLRs. In our protocol, the master VLR manages several slave VLRs to reduce the signaling traffics for authenticating roaming users. This paper is organized as follows. Section 2 summarizes the operations of GSM authentication protocol and describes its drawbacks. Section 3 proposes an improved GSM authentication protocol without modifying the fundamentals of GSM systems. In Section 4, we show that our protocol improves the original protocol with regard to efficiency. Finally, Section 5 concludes this paper.

2 GSM Authentication Protocol

GSM authentication protocol utilizes the challenge-response mechanism with secret key protocol which is used for either the mobile user authentication or the session key generation. In GSM systems, the communicating users store the session key in the SIM (Subscriber Identity Module) card and the network stores the key in the secure database called AuC (Authentication Center)[4]. SIM is unique to each mobile user and can be inserted to the mobile terminal. Also, SIM contains the service related information for each mobile user and a unique 128 bit key Ki that is used to identify and authenticate itself to the network[5].

2.1 Original Protocol

The detailed operations of original protocol are summarized as follows[7][8].

1. While entering a new location area, a mobile user sends an authentication request which involves the TMSI (Temporary Mobile Subscriber Identity) and LAI (Location Area Identity) to the VLR.
2. The VLR checks the TMSI and derives an IMSI (International Mobile Subscriber Identity) from the TMSI. Then, the VLR forwards it to the HLR.
3. The HLR/AuC generates a 128 bit RAND corresponding to the received IMSI. Then, the HLR derives a 32 bit SRES (Signed RESult), 64 bit Kc through A3, A8 algorithm. This is done by using the RAND and the private key of the mobile user, results of which are returned to the VLR with RAND.
4. The VLR chooses a RAND from one of the triplet and forwards it to the mobile terminal.
5. The mobile terminal generates SRES, Kc through A3, A8 algorithm. This is also done by using the RAND and Ki stored in the SIM. The session key Kc is kept for the secure communication and the SRES is sent to the VLR.
6. Finally, the VLR compares it with the SRES sent from the HLR. If the two are equal, the mobile user is regarded as legal and the user authentication is completed.

2.2 Drawbacks of the GSM Authentication Protocol

In order to perform the user authentication, the VLR must contact to the HLR since the private key of a mobile user is stored in the HLR. The problem is that the triplets provided by the HLR are sent to the VLR via various intermediate links and this incurs dramatic signaling traffics to GSM networks. Besides, the excessive stream of signaling traffics may increase the authentication delay. As we will see, large portions of the GSM network traffics are generated from the consistent signaling between mobile users and network[5][9]. Fig. 1 depicts the flow of signaling messages generated while a mobile user performs either the location registration or update.

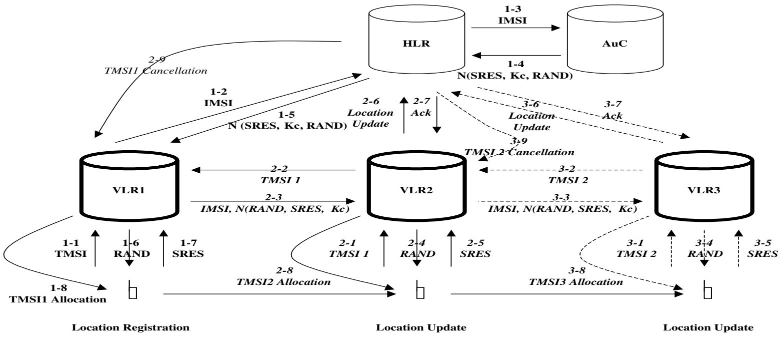

Fig. 1. GSM authentication protocol for roaming users

Since we explained the authentication procedure during location registration in Section 2.1, we skip this in this section. Instead, we illustrate the authentication procedure during location update. A mobile user first performs location registration to VLR1. As a result of successful authentication, VLR1 allocates a TMSI1 to the mobile user. In this point, we assume that the mobile user subsequently moves to the area covered by VLR2. Then, following steps of user authentication are performed.

2-1 The mobile user sends a TMSI1 to VLR2.
2-2 VLR2 forwards the TMSI1 to the location area managed by VLR1.
2-3 VLR2 receives an IMSI, together with a few of authentication triplets from VLR1.
2-4 VLR2 chooses a RAND from one of the authentication triplets and sends it to the mobile terminal.
2-5 The mobile terminal calculates a SRES and send it back to VLR2. VLR2 then performs the user authentication.
2-6 After the user authentication is completed successfully, VLR2 sends a location update message to HLR and updates the location of the mobile user.
2-7 HLR returns an acknowledgement for the user's location update to VLR2.
2-8 VLR2 assigns a TMSI2 to the mobile terminal.
2-9 HLR finally transmits a TMSI1 cancellation message to VLR1.

In case that the mobile user moves to the location area managed by VLR3, the similar steps of authentication procedure are performed.

3 Proposed Protocol for GSM Roaming Users

3.1 Basic Idea

In order to reduce the signaling traffics for roaming user authentication, our protocol exploits the enhanced user profile. The enhanced user profile is maintained in the HLR and the mobile terminal. The location areas corresponding to the VLR IDs in the enhanced user profile can be selectively chosen by mobile users at the enrollment to the service provider. Also, the areas can be adaptively modified by mobile users' preference. In our protocol, the HLR in advance knows of the location ares where each mobile user is most likely to visit. Besides, the master VLR manages a group of slave VLRs. In detail, the master VLR transmits authentication triplets to the slave VLRs and maintains the state of mobile users' movement within the areas specified in the enhanced user profile. Thus, our protocol does not require a location update to the HLR as long as a mobile user roams within a group of areas indicated by the enhanced user profile. Instead, the location update of mobile user is sent from the slave VLRs to the master VLR. For doing this, the TMSIs assigned from the areas in the enhanced user profile must contain the ID of master VLR. As a result, the slave VLRs can identify the master VLR and notify the master VLR of the mobile user's location change.

Our protocol must be installed on the HLR and VLR. As a result, the HLR knows of the master VLR by checking the VLR ID in the enhanced user profile when a mobile user performs location registration. The HLR regard the other VLRs in the enhanced user profile as slave VLRs and delegate its role to the master VLR. In addition to the fields for the VLR IDs in the enhanced user profile, we consider another field for the case where a mobile user moves to the area that is not indicated by the enhanced user profile. In this case, the VLR ID for the corresponding area is inserted into this field and the original protocol is performed. Specifically, the current VLR receives the authentication triplets from the master VLR and performs the authentication procedure. When the user authentication is completed successfully, the VLR transmits a location update directly to the HLR for the consistency between itself and HLR.

3.2 Protocol Description

Fig. 2 illustrates the functional steps of our protocol and describes the flow of signaling messages while a mobile user crosses several areas specified in the enhanced user profile. The main steps that must be focused on are the authentication procedure during location update. As presented in Fig. 2, our protocol utilizes the enhanced user profile containing three VLR IDs, i.e., VLR1, VLR2 and VLR3. The noticeable difference between the original protocol and our protocol is that the VLR1 acts as master VLR and VLR2/VLR3 act as slave VLRs. In case that a mobile user performs location registration to VLR1, the original protocol is performed and this is depicted in the step 1-1 through 1-8. If the mobile user moves to the area covered by VLR2, following steps of authentication procedure are performed.

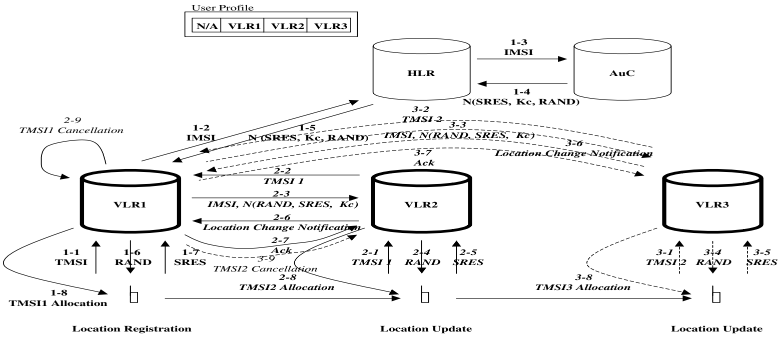

Fig. 2. Proposed GSM authentication protocol for roaming users

2-1 The mobile user sends a TMSI1 to VLR2.
2-2 VLR2 forwards the TMSI1 to the area where a mobile user performs location registration, i.e., the area managed by VLR1.
2-3 VLR2 receives an IMSI along with the authentication triplets from VLR1.
2-4 VLR2 chooses a RAND from one of the triplets and sends it to the mobile terminal.
2-5 The mobile terminal calculates a SRES and returns it to VLR2. The SRES is used to check the validity of the mobile user.
2-6 After the user authentication is completed successfully, VLR2 sends a location change notification to VLR1.
2-7 VLR1 forwards an Ack to VLR2.
2-8 VLR2 allocates a new TMSI, i.e., TMSI2 to the mobile terminal.
2-9 VLR1 sends a TMSI1 cancellation message to itself, i.e., the area that previously allocated a TMSI to the mobile terminal.

When the mobile user moves to the area managed by VLR3, similar steps of authentication procedure are performed and this is presented in the step 3-1 through 3-9. In summary, the proposed protocol can trace the location areas where a mobile user is most likely to visit. Basically, our protocol exploits the concept of mobile users' local movement, i.e., the local mobility. Specifically, large number of mobile users can be regarded as commuters roaming within a few of limited areas including home, office, school, etc. This stems from the fact that the mobility pattern of most roaming users could be quite routine and their roaming coverage might be confined to a few areas. By using the localized feature of user roaming, our protocol does not entirely rely on the HLR for whole steps of user authentication. Thus, the proposed protocol can perform an efficient roaming user authentication.

4 Performance Analysis

We regard the signaling loads as the most essential criterion to evaluate the performance of authentication protocol. While focusing on the criterion, we perform a few of simulations and compare the performance of our protocol with that of original protocol. For doing this, we use the Fluid flow mobility model[2].

4.1 Fluid Flow Mobility Model

The Fluid Flow mobility model basically assumes the following parameters. By using these parameters, we can obtain the numerical results for the signaling traffics during the roaming user authentication[2][11].

- Average speed of mobile users : $\upsilon = 6.3km/hr$
- Average density of mobile users : $\rho = 267/km^2$
- Moving direction of mobile users : [0, 2π]
- Border length of a location area : l = 8.65km
- Total border length of a location area : L = 34.6km
- One HLR for 64 location areas, each controlled by one VLR

At first, we can compute the number of location registrations to VLR.

$$R_{Reg,VLR} = \rho * \upsilon * L = \frac{267 * 6.3 * 34.6}{3600\pi} = 5.14/s \qquad (1)$$

We can also derive the number of location registrations generated at HLR.

$$R_{Reg,HLR} = R_{Reg,VLR} * NumberofAreas = 5.14/s * 64 = 328.96/s \qquad (2)$$

4.2 Numerical Results for the Authentication Signaling Loads

We define the parameters to calculate the costs of roaming user authentication:

- TC_{HV} : Transmission Cost between HLR and VLR
- TC_{VV} : Transmission Cost between VLR and VLR
- TC_{HM} : Transmission Cost between HLR and Master VLR
- TC_{MS} : Transmission Cost between Master VLR and Slave VLR
- TC_{VM} : Transmission Cost between VLR and Mobile Terminal
- PC_H, PC_V : Processing Cost at HLR, VLR
- PC_M, PC_S : Processing Cost at Master VLR, Slave VLR

According to the signaling flows described in Fig. 1 and 2, the authentication costs for the original protocol and our protocol can be derived as:

$$AC_{original\_reg} = 4TC_{VM} + 2TC_{HV} + 3PC_V + 2PC_H \qquad (3)$$

$$AC_{proposed\_reg} = 4TC_{VM} + 2TC_{HM} + 3PC_V + 2PC_H \qquad (4)$$

$$AC_{original\_up} = 4TC_{VM} + 3TC_{HV} + 2TC_{VV} + 6PC_V + PC_H \qquad (5)$$

$$AC_{proposed\_up} = 4TC_{VM} + 4TC_{MS} + TC_{VV} + 4PC_S + 2PC_M \tag{6}$$

We assume that the transmission cost is proportional to the distance between the network entities. We also assume that the transmission cost through wireless link is much higher than the transmission cost through wired link. Additional parameters are depicted as follows.

- p : Residential probability to the areas indicated by the enhanced user profile
- r : Registration ratio to the location areas

By using the aforementioned parameters, we present a few of simulation results. Fig. 3 shows the authentication signaling loads with the varying residential probabilities. We obtain the simulation results for the time interval 100(sec). As presented in Fig. 3, our protocol ensures better performance than the original protocol as p increases. When p is 0, the performance of both protocol is equal since in this case, the mobile users move through the areas that are not specified in the enhanced user profile. The gap of performance between the two protocol gets into maximum when p is 1. This stems from the fact the the mobile users roam only within the areas indicated by the enhanced user profile.

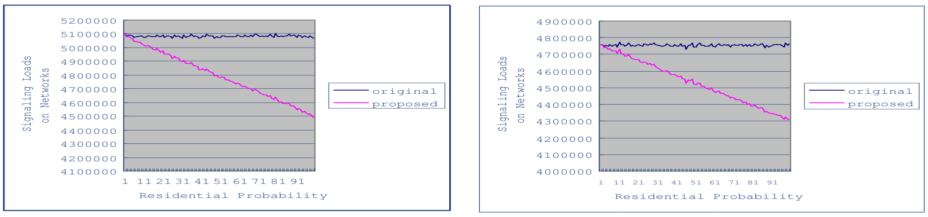

Fig. 3. Results with varying p where Registration Ratio = 10%, 30%

Fig. 4 shows the results with the varying registration ratio. Similarly, our protocol ensures better performance than the original protocol as r decreases. As r decreases, the authentication cost during the location update is incrementally added to the total signaling loads. By examining all the simulation results, we can conclude that our protocol generates less signaling traffics than the original protocol while authenticating the roaming users.

5 Conclusion and future work

In this paper, we design and analyze the improved authentication protocol for GSM roaming users. Our protocol aims at reducing the excessive signaling traffics for roaming user authentication. For doing this, we exploit the enhanced user profile and utilize the localized features of users' mobility. As a result of performance evaluations, we present that our protocol avoids the inefficiency of original

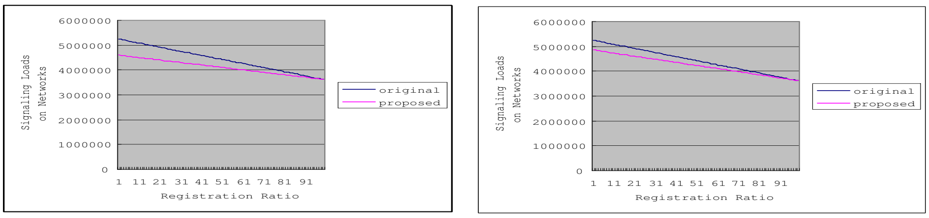

Fig. 4. Results with varying Registration Ratio where p = 100%, 60%

protocol where whole steps of roaming user authentication procedure must rely on the HLR. Our protocol does not make much modifications to the fundamentals of GSM systems. Thus, our protocol can satisfy the security requirements of GSM authentication protocol. Specifically, our protocol can maintain the similar level of security implications as original protocol.

References

1. Sanjoy Paul, "Privacy and Authentication Needs of PCS", *IEEE Personal Communications* , pp. 11-15, Aug. 1995.
2. Cjii Hwa Lee, Min Shiang Hwang, Wei Pang Yang, "Enhanced Privacy and Authentication for the global system for Mobile Communications ,", *Wireless Networks* , Vol. 5, pp. 231-243, 1999.
3. Chi-Chun Lo, Yu-Jen Chen, "A Secure Communication Architecture for GSM Networks ,", *IEEE Pacific Rim Conference on Communications , Computers and Signal Processing* , pp. 221-224, 1999.
4. Khalid Al-Twail, Ali Akrami, Habib Youssef, "A New Authentication Protocol for GSM Networks ,", *Proceedings of IEEE Annual Conference on Local Computer Networks* , pp. 21-30, 1998.
5. Dan Brown, "Techniques for Privacy and Authentication in Personal Communication System ,", *IEEE Personal Communications* , pp. 6-10, August, 1995.
6. Samarakoon, M.I., Honary, B, "Novel authentication and key agreement protocol for low processing power and systems resource requirements in portable communications systems ,", *Novel DSP Algorithms and Architectures for Radio Systems (1999/184), IEE Colloquium on* , pp. 9/1 -9/5, 1999.
7. Khalid Al-Tawil, Ali Akrami, "A New Authentication Protocol for Roaming Users in GSM Networks ,", *Proceedings. IEEE Int'l Symposium on Computer and Communications* , pp. 93-99, 1999.
8. Sesharri Mohan, "Privacy and Authentication Protocols for PCS ,", *IEEE Personal Communications* , pp. 34-38, 1996.
9. 3GPP TS 03.20 V8.1.0(2000-10) 3rd Generation Partnership Project; Digital Cellular Telecommunications System (Phase 2+); Security related Network Functions(Release 1999)
10. ETSI TS 100 614 V8.0.0(2000-04) Digital Cellular Telecommunications System (Phase 2+); Security Management (GSM 12.03 Version 8.0.0 Release 1999)
11. S.Mohan, R.Jain, "Two User Location Strategies for Personal Communications Service ,", *IEEE Personal Communications* , First Quarter, pp. 42-50, 1994.
12. L.Kleinrock, Queueing Systems, Vol.1, Wiley-Interscience, 1975