

NEW APPROCH FOR WIRELESS COMMUNICATION SECURITY PROTOCOL BY USING MUTUAL AUTHENTICATION

¹Atishay Bansal, ²Dinesh Sharma, ³Gajendra Singh, ⁴Tumpa Roy

¹atishaybansal@gmail.com, ²kumardinesh3381@yahoo.com,
³gajendrasingh0836513024@gmail.com

⁴tumpa.nit@gmail.com

Department of Computer Science and Information Technology GLNAIT, Mathura, U.P

ABSTRACT

In this paper, a new Global System of Mobile Communication (GSM) authentication protocol is proposed to improve some drawbacks of the existing GSM authentication architecture including: (a) not supporting bilateral authentication between MS and VLR; (b) huge bandwidth consumption between VLR and HLR; (c) storage space overhead in VLR; (d) overloaded in HLR with authentication of mobile stations, The main emphasis of this paper to improve some of these drawbacks of the existing GSM architecture. In addition, this new proposed authentication protocol does not change the existing GSM architecture and the robustness of the proposed protocol is the same as that of the original GSM protocol, which is based on the security algorithms A3, A5, A8.

KEYWORDS

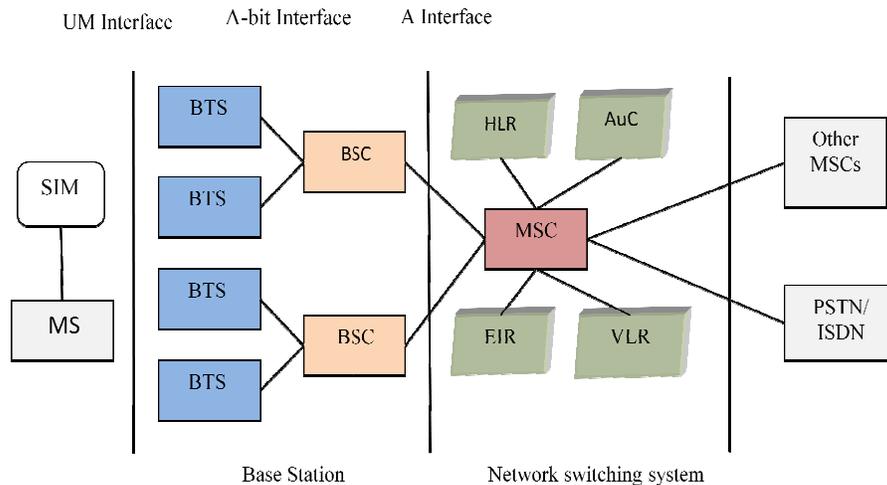
Network Protocols, Wireless Network, Mobile Network, SIM, IMSI, Auchentication centre , man in middle attack.

1. INTRODUCTION

Since the early 1980s, the Global System for Mobile Communication has been the most popular standard for mobile phones in the world. It has become the worldwide wireless standard and is used by the peoples in more than 200 countries. However, security is the major issue as far as the wireless communication is concerned. Two security problems, confidentiality and subscriber identity authentication are main security issues in mobile communication. Maintaining confidentiality means protection of message from improper kind of access. On the other hand, a good identity authentication system means that no unauthorized user gets the required services from the home system. In the original design, mobile users are authenticated by using a shared-secret cryptographic system. To equip the GSM system with better power of security, in this paper, we shall focus on developing the solutions to possible user authentication problems.

2. GSM NETWORK

In the GSM Network, three subsystems involved are the mobile station (MS) subsystem, the base station subsystem, the home subsystem. The MS subsystem consists of the mobile equipment (ME) and the smart card called the subscriber identity module (SIM). The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. The base station subsystem consists of the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These are the connections between the mobile stations and the Mobile Switching Center (MSC). The home subsystem is composed of five parts, the Mobile Switching Center (MSC), the Home Location Register (HLR), the Visitor Location Register (VLR), the Authentication Center (AuC), and the Equipment Identity Register (EIR). We explain the difference between HLR and VLR as follows. The HLR is a database that contains complete information of the local customer. It is the main database. The VLR contains the roamer information. The VLR make sure that you are a valid subscriber and then retrieves just the enough information from the distant HLR to manage your call.

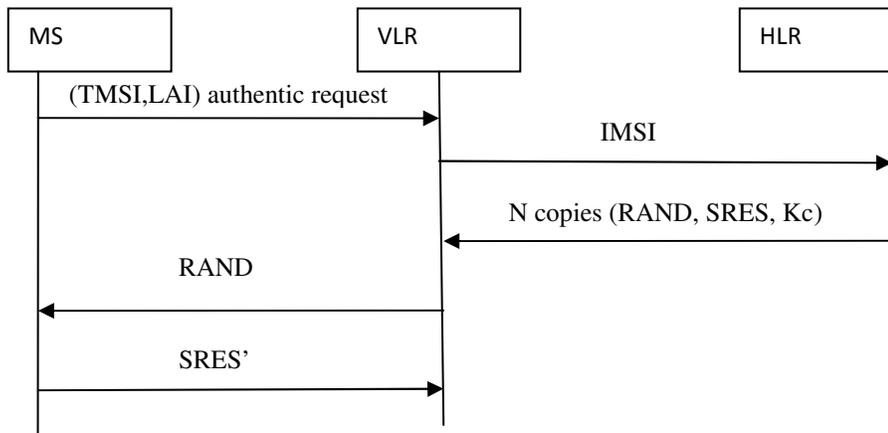


3. GSM SECURITY NETWORK

3.1 A review of GSM authentication protocol for the roaming users

In this section, we shall briefly review the current GSM authentication protocol for roaming users. The notations to be used throughout this paper will be shown below:

HLR	The Home Location registers
VLR	The Visitor Location Register
AuC	Authentication Center
MS	Mobile Station
TMSI	Temporary Mobile Subscriber Identity
IMSI	International Mobile Subscriber Identity
LAI	Location Area Identity
IDv	Identification of VLR
Ki	Secret Key between MS and HLR
RAND	Random number generated by HLR
A3, A5, A8	Three algorithms on which security of GSM is based
SIG	Signature
Kc	Session Key between MS and VLR
CERT_VLR	Certificate of visited VLR



4. Analysis of current GSM Authentication protocol

4.1 Working of Protocol

Let's first see the working of the existing GSM authentication protocol as shown in the above figure. The details are described as follows :

- (1) When MS enters a new visiting area and requires new communication services, he/she sends an authentication request to the visited VLR. The request contains the TMSI and the LAI.

(2) After receiving the TMSI, the new VLR can use the TMSI to get the IMSI from the old VLR. Then the new VLR sends the IMSI to HLR.

(3) The HLR/AuC then generates n copies of the triplet authentication parameters $\{RAND, SRES, Kc\}$ at a time for the mobile station to use later for each call, and then the HLR sends them to the VLR through a secure channel.

(4) After receiving these authentication parameters, the VLR keeps them in its own database and then he/she selects a triplet $\{RAND, SRES, Kc\}$ to authenticate the mobile station for each call. Then the VLR forwards the selected $RAND$ to the MS.

(5) When the MS receives $RAND$, he/she can compute $SRES$ and Kc and send the computed $SRES'$ back to the VLR. Then the MS keeps Kc for secret communication.

(6) Once the VLR receives $SRES'$ from the MS, it compares it with the selected $SRES$. If they are the same, the MS is authenticated; otherwise, the MS is not a legal user.

4.2 DRAWBACKS OF EXISTING PROTOCOL:-

(a) Not supporting Bilateral Authentication: This is the major setback of the existing protocol, in which the MS can be authenticated by the VLR but VLR cannot be authenticated by the MS thus supporting unilateral authentication.

(b) Huge Bandwidth consumption between VLR and HLR: As per the existing protocol each time when MS wants to establish a session, VLR has to request for the authenticity of that MS from the HLR thus consuming huge bandwidth.

(c) Storage space overhead in VLR: Since each time HLR sends the n copies of $RAND$ number to the VLR, thus VLR have to save all these n copies in its database thus making the database of VLR overloaded.

(d) Overload in HLR with authentication of MS: Since every time VLR request to the HLR for the authenticity of MS thus making the database of the HLR overloaded.

(e) Man- In- Middle attack: Since in the existing protocol there is unilateral authentication, so any unauthorized user can be able to know the contents of the session that is going on between MS and VLR because VLR is not authenticated by the MS.

(f) Impersonating attacks: Any attacker can impersonate himself as VLR and try to get the required data for him because this existing protocol supports unilateral authentication and MS can easily be fooled by the attacker.

5. Review work

To fix the above drawbacks, some revised GSM authentication protocols have been proposed [6-8] but those protocol change the basic security architecture of the GSM. Some of this protocol are not suitable for the ramming users and none of the protocols can fix all of the above drawbacks at a time. Furthermore, some protocols require that some additional hardware

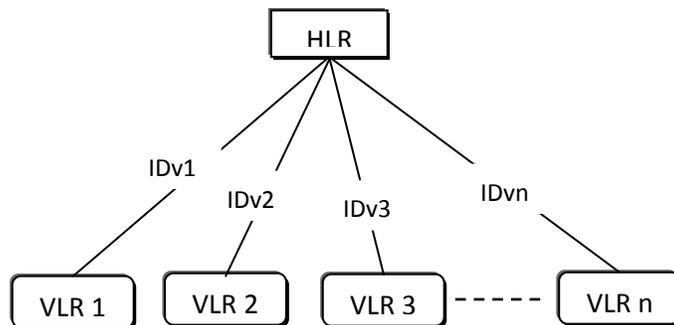
be added to the system, and others are changed to public-key cryptography, which means more computational costs. In 2004, Hwang et al. proposed an anonymous channel protocol where the mobile station could request services privately under the visit network [5]. The protocol uses tickets, secret key cryptosystem, and public key cryptosystem techniques. The architecture of the protocol is different from the GSM. Since the protocol uses a public key cryptosystem, the computational cost is very high. However, they cannot properly address the roaming users, furthermore their protocols are not suitable for roaming users. To a mobile user frequently roaming to another VLR, communication overheads occur. In 2004, Hahn et al. proposed an improved GSM authentication protocol for roaming users [9] they improved the GSM authentication protocol to reduce the signaling load for a roaming user. The protocol exploits the enhanced user profile containing a few VLR IDs a mobile user is most likely to visit. However, the protocol cannot solve all of the above problems and is not flexible. In 2006, Kumar et al. proposed an efficient identity based mutual authentication scheme for GSM [10]. It support the mutual authentication and reduce the storage overhead of VLR. But it changes the basic security architecture of the GSM and is not suitable for the roaming users. In 2006, Ammayappan et al. proposed an improvement to the GSM authentication protocol, based on Elliptic Curve Cryptography (ECC)[11] change the architecture and the computational cost is high for public key cryptography.

6. The Proposed GSM Authentication Protocol for the users

It has three phases which provides distribution of ID's of VLR from HLR, registration phase and the last one is mutual authentication phase.

6.1 Distribution of IDv to each VLR

In this phase HLR will distribute a unique identification value to each VLR which comes under its region. This IDv help the VLR to be authenticated by the mobile station when the certificate is generated with the help of Ki and A3 security algorithm.

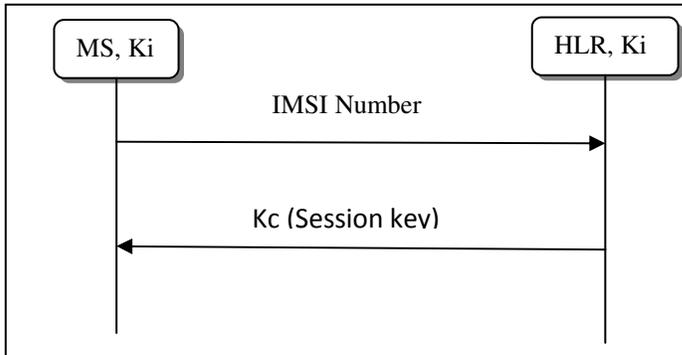


6.2 Initial Registration Phase

It is the registration phase, in which the mobile station (MS) sends its IMSI number to the local HLR which having a large database store the IMSI number. And according to the IMSI number HLR will get the secret key (Ki) of that particular MS. Now HLR will generate the session key (Kc) related to that IMSI number and send this session key to the MS.

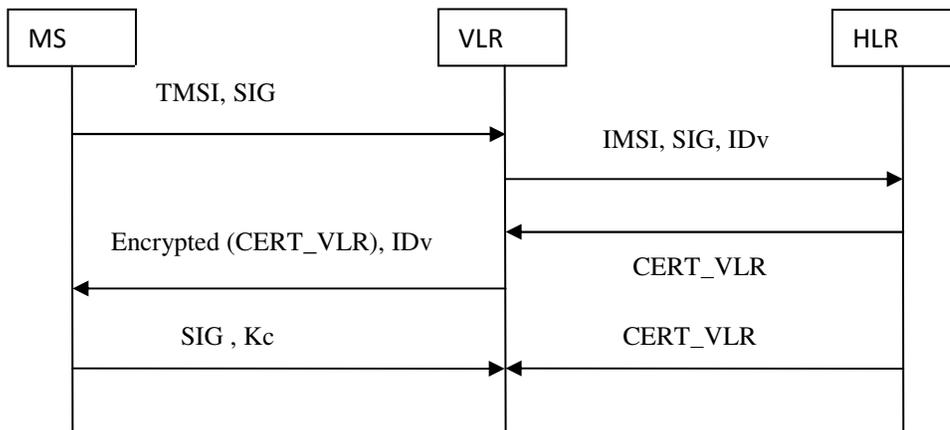
$$Kc = A8 (Ki , IMSI)$$

And after the generation of session key that particular mobile station will get registered with the HLR, and HLR will save IMSI number in its database.



6.3 Mutual Authentication Phase

This is the last phase of our proposed protocol, in this phase mobile station and the VLR will be authenticated by each other during the calls made and attended by the mobile station with the help of HLR. So this proposed protocol will provide the mutual authentication between MS and VLR.



The Steps are given below

(a) In the first step MS will send the temporary mobile subscriber identity (TMSI) number and the signature (SIG) to the corresponding VLR. So VLR will store the SIG of that MS in its database for the future use.

$$\text{SIG} = A3 (\text{Ki}, \text{IMSI})$$

(b) In the second step VLR will send the IMSI number, SIG and the IDv of itself to the HLR so that VLR can be authenticated by the HLR and there is no problem for HLR to give access rights to that VLR.

(c) In the third step HLR will generate CERT_VLR for that particular VLR and send back to that VLR, so the VLR will store its certificate into its database for the future reference.

$$\text{CERT_VLR} = A3(\text{Ki}, \text{IDv})$$

(d) In the fourth step VLR will now send its certificate in the encrypted form to the MS so that at the time of authentication of VLR MS can use this as a reference and also its IDv value so that MS can decrypt the certificate.

(e) In the fifth step at the time of authenticating each other (MS and VLR) MS will send its SIG and Kc to the VLR and VLR will send its CERT_VLR to MS so that SIG can be verified by VLR and CERT_VLR can be verified by MS, So that the connection can be established with the authorized party.

6. GOAL ANALYSIS

Our goal to propose the new authentication protocol is to improve the drawbacks of the existing protocol. We have achieved these goals with this proposed protocol in the following way:-

(1) *Not supporting bilateral authentication*; this is the main drawback of existing protocol and we have suggested a way to provide bilateral authentication between MS and VLR as shown in the last step of our proposed protocol in which both MS and VLR are having authentication proofs of each other.

(2) *Huge bandwidth consumption between VLR and HLR*; as per the existing protocol every time when MS wants to create a session VLR have to request the authenticity of that MS, so that's why there is huge bandwidth consumption between VLR and HLR. But in our protocol VLR have to request for the

authenticity of MS only one time when VLR gets the SIG of that particular MS as shown in first step.

(3) *Storage space overhead in VLR*; since HLR sends the n copies of RAND number to VLR for every request of the authenticity of MS and VLR have to save all the copies, this creates its database overloaded. But in our proposed protocol VLR have to save only the SIG of that particular MS and the certificate send by the HLR so there will be less storage in the database of VLR.

(4) *Overload in HLR with authentication of MS*; since every time VLR request HLR for the authenticity of MS when MS wants to establish a session this creates overload in the database of HLR. But in our proposed protocol VLR will request only single time when the first call is made

by the MS; the HLR will issue VLR with the certificate and HLR would not have to calculate n copies of RAND number each time, so there will be less overload in HLR as compared to existing authentication protocol.

(5) *Man- In- Middle attack*; to resist this type of attack a solution to establish mutual authentication is proposed in our protocol. In our protocol, MS can verify the VLR by the received CERT_VLR. It cannot be created unless the adversary knows Ki and IDv. On the other hand, VLR can verify the MS by the received SIG. This also cannot be created unless the adversary knows the Ki.

(6) *Impersonating attacks*; an unauthorized user may try to impersonate one party to communicate with another party. If the attacker tries to impersonate MS, he/she cannot generate the correct SIG and cannot be able to continue the protocol. If he/she tries to impersonate VLR, he/she cannot generate the correct CERT_VLR. So our proposed protocol also successful in keeping the impersonation attacker away.

7. CONCLUSION

Nowadays, 3G mobile systems are becoming more and more popular in the market. However, the cost for base station construction is still very high. Many telecommunication companies still use the old standard of GSM or integrate the GSM system with their 3G systems. Therefore, the GSM system is still popular and widespread because of its simplicity and efficiency. Many authentication protocols have been developed to improve the original authentication protocol of GSM, but mostly cannot solve the problems without modifying the architecture of GSM. In this paper, we have pointed out the drawbacks of the GSM authentication protocol and presented a new authentication protocol that can fix all the drawbacks. Also, the concept of this protocol can also be applied to 3G mobile systems.

REFERENCES

- [1] B. Mallinder, "An overview of the GSM system," *Proc.Nordic Seminar on Digital Band Mobile Radio Commun*., pp.12-15, Sept. 1988.
- [2] Cheng-Chi Lee · I-En Liao · Min-Shiang Hwang,"*An effiecient Authentication protocol for mobile communication*" Springer Science+Business Media,LLC2010.
- [3] Refik Molva, Didier Samfat and Gene Tsudik,"*An Authentication protocol for mobile users*","IEEE Colloquium on security and cryptography applications to radio system,London ,UK, ",June 1994.
- [4] Moe Rahnema,"*Overview of GSM system and protocol architecture*",*"IEEE communication magazine"*,pp.92-100,April 1993.
- [5]]Gregory P.Pollini, David J.Goodman,"*Signalling system performance evaluation for personal communication*",*"IEEE Transactions on vehicular Technology"*,Vol.45, no.1, pp.131-138 ,Feb 1996
- [6] Yi Bing Lin,"*No wires attached*",*"IEEE potentials"*,pp.28-33,Oct/Nov 1995.
- [7] Jay Jayapalan and Mike Burke,"*Cellular Data sevices architecture and signalling*",*"IEEE personal communication,second quarter,"*,pp.44-55, 1994.

- [8] Kavitha Ammayappan, Ashutosh Saxena and Atul Negi, "Mutual Authentication and Key Agreement based on Elliptic Curve Cryptography for GSM". In International conference on advanced computing and communications, 2006(pp.183-186), Dec.
- [9] Chin-Chen Chang*, Jung-San Lee, Ya-Fen Chang(2005). "Efficient authentication protocols for GSM". Computer Communications, 28, 921-928.
- [10] Khalid Al-Tawil, Ali Akrami, Habib Youssef. "A New Authentication Protocol for GSM Networks". In IEEE 23rd Annual Conference on Local Computer Networks(LCN'98)(pp.21-30).
- [11] Kalaichelvi, V., and Chandrasekaran, R.M. (2008). "Secure Authentication Protocol for Mobile". In International conference on Computing, Communication and Networking(pp.124), Dec, 2008.
- [12] Kumar, K.P., Shailaja, G., Kavitha, A., and Saxena, A. (2006). "Mutual Authentication and key agreement for GSM". In International Conference on Mobile Business(pp.25-28), June, 2006
- [13] Hwang, M.-S., Lee, C.-C., & Lee, J.-Z. (2004). "A new anonymous channel protocol in wireless communications." International Journal on Electronics and Communications, 58(3), pp. 218-222.
- [14] Peinado A. (2004) "Privacy and authentication protocol providing anonymous channels in GSM", Computer Commun., vol. 27, pp. 1709-1715, 2004.
- [15] Y. Boichut, P.-C. Héam, O. Kouchnarenko, and F. Oehl (2004). "Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols." In Proceedings of Automated Verification of Infinite States Systems (AVIS'04), ENTCS, 2004.
- [16] Chang, C. C., Lee, J. S., & Chang, Y. F. (2005). "Efficient authentication protocols of GSM." Computer Communications, 28, 921-928.
- [17] Ozer Aydemir and Ali Aydin Selcuk, (2005) "A Strong User Authentication Protocol for GSM", 14th IEEE International Workshop on Enabling Technologies Infrastructure for Collaborative Enterprise (WETICE'05), Linkopings University, Sweden
- [18] Toorani, M.; Beheshti Shirazi, A.A. (2008) "Solutions to the GSM Security Weaknesses", Next Generation Mobile Applications, Services and Technologies, 2008. Page(s): 576 - 581
- [19] Fanian, A., Berenjkoub, M., & Gulliver, T. A. (2009). "A new mutual authentication protocol for GSM networks." In Canadian conference on electrical and computer engineering, pp. 798-803.

Authors

Atishay Bansal

Mr, Atishya Bansal is a B.tech student of GLNA institute of technology '12 batch with the specialization of Information & technology. His areas of interest are Data mining and network security. He is also interested in artificial robotic programming.



Dinesh Sharma

Mr, Dinesh Sharma is a B.tech student of GLNA institute of technology '12 batch with the specialization of Information & technology. His areas of interest are Data mining and network security. He is also interested in ethical hacking.



Gajendra Singh

Mr, Gajendra Singh is a B.tech student of GLNA institute of technology '12 batch with the specialization of Information & technology. His areas of interest are peer to peer network and network security.



Tumpa Roy

Ms. Tumpa Roy obtained her B.tach from WBUT during 2009. She has completed her M.tech in Computer Science in 2011. She is working as a Asst. Professor in Computer Science, GLA group of institution since july 2011. Her research areas include Network Security, mobile communication, ECC.

