Volume 5, Issue 6, June 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Conferral Supervision in GSM Cellular Scheme

V. Renuka
M.Sc Information Technology
Sri Krishna Arts and Science College,
Coimbatore, Tamil Nadu, India

S. Gomathi
Asst. Prof., Dept. of Information Technology
Sri Krishna Arts and Science College,
Coimbatore, Tamil Nadu, India

Abstract— Nowadays all peoples are demanding the wireless cellular access. Global System for Mobile Communication (GSM) is the standard of wireless technology which is used in world wide. It provides us to make a call, send SMS and Internet facility. In this paper, we concentrate on architecture, security protocol. Architecture elaborates the components that are used in GSM. It explains the three subsystem of the GSM architecture. They are Radio subsystem (RSS), Network and switching subsystem (NSS) and Operation subsystem (OSS). Security mechanisms are achieved through the A3, A5 and A8 algorithms. GSM provides the two types call flow and also provides the SMS flow. GSM protocol uses these algorithms for its strength. GSM is also implemented in SMS alert security in Mobile Banking.

Keywords— GSM, BSC, MSC, VLR, HLR

I. INTRODUCTION

European Telecommunications Standards Institute (ETSI) developed the standard GSM (Global System for Mobile communication). GSM is a digital cellular networks that are used by mobile phones. GSM standard employing Time-Division Multiple-Access (TDMA) spectrum-sharing. The GSM architecture explains the three subsystems are Radio subsystem (RSS), Network and switching subsystem (NSS) and Operation subsystem (OSS). Radio subsystem controls the base station and controllers. It performs necessary functions like encoding/decoding of voice, rate adaption to maintain radio connections with an MS. The Base Station Controller (BSC) controls several base stations by managing their radio resources. Many BSCs are connected to Mobile Services Switching Center (MSC) in NSS. Network and switching subsystem is the part of the network most similar to a fixed network, sometimes just called the "core network". Core Network (CN) consists of several databases like Visitor Location Register (VLR) and Home Location Register (HLR). Gateway MSC (GMSC) which connects the GSM Network to PSTN and ISDN. MSC provides several functions like registration, authentication, location updating, handovers and call routing using HLR and VLR. HLR is the major database and stores all user-specific information elements.VLR is a dynamic database, responsible for copies of all relevant information for the user from HLR. It also stores the dynamic information about subscriber location. Operation subsystem maintains the network. The Equipment Identity Register (EIR) and Authentication Center (AuC) in the third subsystem, OSS contains device information and algorithms for authentication, encryption/decryption and generation of session keys respectively.

The security mechanism offers confidentiality and authentication. GSM uses some security protocols for authentication between the base station and the mobile station. It was the first one which introduces encryption and cryptographic mechanisms for confidentiality and authentication of telephone system. But GSM also suffers from some security problems similar to weak encryption and authentication algorithms, along with short length of secret key and no authentication process for the network. The algorithm that are used in GSM are A3, A5 and A8. GSM uses General Packet Radio Service (GPRS) for data transmissions like browsing the web [1]. The Global System for Mobile Communications (GSM) occupies almost 70% of the wireless market and is used by millions of subscribers in the world [2]. Phones on this type of GSM network actually use a Subscriber Identity Module (SIM) card. One of the main objectives of the GSM network is to facilitate effortless access to cellular and satellite systems across international lines.

II. LITERATURE REVIEW

A. Review 1

The authors Atishay Bansal, Dinesh Sharma, Gajendra Singh and Tumpa Roy published a paper on the title "New Approach for Wireless Communication Security Protocol by using Mutual Authentication" in An International Journal (ACIJ), Vol.3, No.3, May 2012. In this paper they elaborate GSM architecture, working and drawbacks of existing protocol. The GSM architecture contains the three subsystem are Mobile subsystem, Base station subsystem and home subsystem. It also explains the working and drawbacks of existing protocol. The drawbacks of existing authentication protocol are: a) MS and VLR does not support bilateral authentication, b) VLR and HLR consumes huge bandwidth, c) VLR needs high storage space, d) overloaded in HLR with authentication of mobile stations. The proposed authentication protocol is to improve the drawbacks of the existing authentication protocol. The proposed authentication protocol security is based on the A3, A5 and A8 algorithm.

B. Review 2

The author Karun Madan published a paper on the title "An Investigation of GSM Architecture and Overlaying with Efficient Security Protocol" in the International Journal of Computing and Business Research (IJCBR) Volume 3 Issued in Jan 2012. In this paper the author explains the SMS alert security for the M-banking. This system gives alert SMS to the user during payment transfer, withdrawal and transactions. It uses security protocols to provide security for the data. It uses one time password. This system provides the secure banking. It is user friendly.

C. Review 3

The author Ankita Jain,Arjun Rajput published a paper on the title "GSM Architecture and Call Flow" in the International Journal of Engineering Technology Science and Research IJETSR Volume 2 Issue 4 April 2015. In this the author explains the GSM Architecture, call flow and SMS flow. GSM architecture is the telecommunication system which depend on this architecture. This architecture is the not only the infrastructure but also the software, encryption and secure the data. It also explains the three subsystem of the architecture. They are Base Station subsystem, Network and Switching Subsystem and Operational Support System. They also elaborate the components involved in the architecture are MS, BSC, MSC, BTS, HLR, VLR, AuC and EIR. This paper explains the call flow and SMS flow. It handles the handover during traffic in ongoing calls.

III. GSM ARCHITECTURE

GSM architecture is shown in the figure 1. There are three subsystems. They are Mobile Station Subsystem, Base Station Subsystem and Home Station Subsystem. Mobile Station (MS) consist of Mobile Equipment (ME) and smart called Subscriber Identity Module (SIM). ME is identified by International Mobile Subscriber Identity (IMSI). IMSI is used for subscriber authentication. Authentication uses the subscriber secret key.

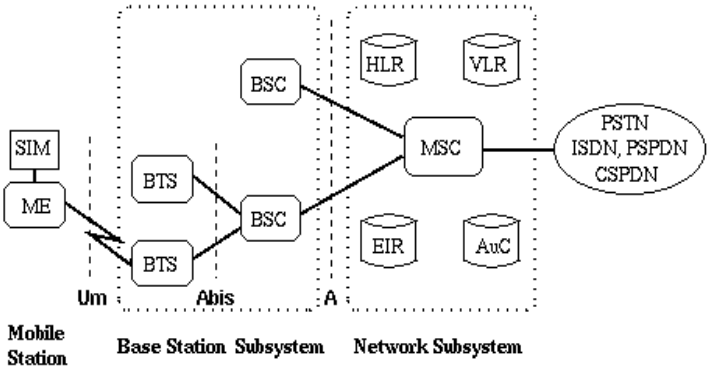

Fig. 1 GSM Architecture

The Base Station Subsystem consists of Base Transceiver Station (BTS) and Base Station Controller (BSC). Through Base Station Subsystem Mobile Switching Center are connected with Mobile Station. The Home Station Subsystem has five parts. They are Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Authentication Center (AuC) and Equipment Identity Register (EIR). HLR contains whole details of the customer such as SIM card details with IMSI. IMSI is a primary key. Call diverting and call forward also the work of HLR. VLR stores the current information of the user. It stores the roaming details. VLR is a temporary database that stores the roamed area by the subscribers. Only one VLR serves each base station [3]. The EIR is a database that contains a list of all valid mobile equipment which is identified by its international mobile equipment identity (IMEI). It helps to provide security and prevents uses of network by mobile station that have been approved. The AuC contains the authentication and encryptions keys that are stored in each user SIM card for authentication and encryption over radio channel [4]. The Um is the interface between the ME and BSS. A is the interface between the BSS and MSC.

IV. WORKING OF EXISTING PROTOCOL

Figure 2 shows the working of existing protocol.

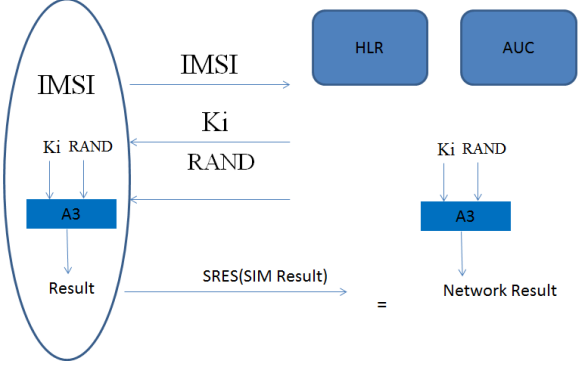

Fig. 2 Working of existing protocol

A. The working of the existing GSM Protocols are explained below

- The user sends the authentication request to VLR when they enter the new MS. The request contains the Temporary Mobile Subscriber Identity (TMSI) and Location Area Identity (LAI).
- The new VLR can use the TMSI to get the IMSI from the old VLR, after receiving the TMSI. Then the new VLR sends the IMSI to HLR.
- The HLR/AuC then generates *n* copies of the triplet authentication parameters {*RAND*, *SRES*, *Kc*} and then the HLR sends them to the VLR through a secure channel.
- After receiving these authentication parameters, the VLR stores the parameters in its database and then he/she authenticates the mobile station for each call by selecting a triplet {*RAND*, *SRES*, *Kc*}. RAND is forwarded to MS by VLR.
- He/she can compute *SRES* and *Kc*, when RAND is received by MS and send the computed *SRES* back to the VLR. *Kc* is stored in MS for secret communication.
- *SRES* received by VLR 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.

V. DRAWBACKS OF EXISTING PROTOCOL

There are some drawbacks in GSM existing protocol. The drawbacks of the existing protocol are:

- MS and VLR does not support bilateral authentication: MS can be authenticate by VLR but VLR cannot authenticate by MS.
- VLR and HLR consume huge bandwidth: MS wants to establish session key each time. VLR sends request to HLR, which consumes huge bandwidth.
- VLR needs high storage space: HLR sends n copies of RAND number each time. So VLR needs large database to store n copies of RAND number.
- Overloaded in HLR with authentication of mobile stations: VLR request HLR each time to authenticate MS. It makes the HLR overload.

VI. WORKING OF PROPOSED AUTHENTICATION PROTOCOL

It provides three phases. They are distribution of ID's of VLR from HLR, registration phase and mutual authentication phase [5].

A. Distribution of IDv to each VLR

Unique identification value is distributed by the HLR to each VLR which comes under its region. The MS authenticate VLR with the help of IDv, when the certificate is generated with the help of security algorithms Ki and A3.

B. Initial Registration Phase

HLR stores the IMSI number. MS send its IMSI number to the local HLR. HLR gets the secret key (Ki) corresponding to the IMSI number of the MS. Using the IMSI number HLR generates the session key (Kc). HLR send this session key to the MS.

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

C. Mutual Authentication Phase

In this phase protocol provides authentication between the MS and VLR. The steps are as follows:

- MS will send TMSI number and signature (SIG) to the corresponding VLR. So VLR stores the SIG of the MS for the future use.

$$SIG=A3\ (Ki,IMSI)$$

- HLR authenticate VLR by the details send by the VLR are IMSI number, SIG and the IDv.
- HLR send CERT_VLR certificate to the VLR which is generated by HLR.

$$CERT\_VLR = A3\ (Ki, IDv)$$

- VLR send its certificate in the encrypted form to the MS, MS authenticate VLR with the reference of IDv and decypt the certificate.
- During authentication each other MS will send its SIG and Kc to the VLR. VLR will send its CERT_VLR will send to MS by VLR. Then VLR verifies the SIG and MS verifies the CERT_VLR, So that the connection can be established with the authorized party.

These proposed protocols can fix the drawbacks of existing protocol and work efficiently.

VII. SMS SOLUTION FOR SECURE BANKING

The secure banking through mobiles are done by protocol sequence. It gives the security alert message to the user.

A. Protocol Sequences

Secure SMS protocol is classified into two parts[6]. They are message generation and message security checks. The mobile generates the message and send the message to the server of the bank. Then the server checksthe messages through security checks and decode the message.

B. Generating and Sending protecteted SMS Messages

User keeps all the security information in the mobile device. These details are used to send secure message to the server. The mobile device has a preset version of pattern bytes [7] which are inserted while creating the message. Hash value can ensure the message integrity for the receiver side [8]. Message integrity is needed to encrypt the messages which are used for computing the message digest. The key used in this algorithm construct one-time password for encryption of the user [9].

C. Receiving and Decoding protected SMS Message

After receiving the message, server breaks the message and first checks the pattern of the version bytes. By doing this server come to know that message is fit for the secure SMS protocol [10]. Next, the server checks if the account identifier is exist in the server database as well. Now the server recovers the sequence number and checks if the sequence number recovered from the message matches with the sequence number from the server's database. Now server gets the one-time password from the database. This password is indexed by sequence number and the account identifier. So the server uses this password as the decryption key to decipher the encrypted contents. After successful decryption, one-time password is discarded [11]. After all this, the server uses the secure contents required for the computing message digest. The algorithm used by the mobile device computes the message digest. Now server compares the two digests for checking the message integrity [12]. After this, server takes the PIN from the message and then compares it with the account holder's PIN from the server's database. The server performs the requested transaction after all the above mentioned security checks.

VIII. TYPE OF CALLS

There are two different calls. They are

- Onnet: Where the calling party and the called party are of the same operator
- Offnet: Where the calling party and the called party are of different operator whether it is international or local call.

A .CASE I – Onnet

When the call is onnet the operator use its own network to originate and end the call. So in onnet, the operator sends the call from MSC to the other MSC which then forwards the call to the nearest BSC. The BSC then transfers the signal to the closest BTS letting the call terminate at the MS of the called number.

B. CASE II – Offnet

When the call is offnet, the MSC transfers the call to the GMSC (Gateway MSC) which then sends the call to the MSC of the called party or transfers the call to the Carrier (international call). The MSC of the Bnumber receives the call from the carrier which like previous case, takes the call to the BSC. BSC then takes the call to BTS which then finally transfers it to the MS of the called party (Bnumber). In an offnet(local) call the call terminating operator is paid by call originating operator. Whereas, in the offnet(international) call the call originator pays the carrier, who then pays to call terminating operator. As we are here to generate revenue and increase the income, the rates for international calls are much higher than the local calls. The payment is done on the predefined currency. Every operator and carrier has a contract which defines the rate at which they will pay to each other. Normally, the payment is done in relation to the duration of the calls travelled from the operator to the carrier and vice versa. Once the call is complete (Onnet or Offnet)MSC and OCS generate a ticket called CDR – Call Detail Record or Call Data Record. The CDR contains:

- Anumber- Calling Party
- Bnumber- Called Party
- Timestamp – At what time did the call originate
- Duration – How long did the call last for

IX. SMS FLOW

Short Message Service (SMS) - It is a service provided by the operator to send text messages. SMSC (Short Message Service Center) provides the SMS service. SMSC acts like a "store and forward" element. When the mobile phone is switched off the message is stored in SMSC, once if it is on the message will be sent. Once the subscriber (Anumber) sends a message to Bnumber, The message travels through the MSC and lands in the SMSC from where the SMS is further routed to Bnumber. The SMSC now forwards the message to the MSC of the receiving subscriber (Bnumber), which in turn finally sends the message to the receiving subscriber.

X. CONCLUSIONS

GSM is the base standard of telecommunication system. From 2G to upcoming 4G and 5G using the basic standard and they embedded other protocols to reach high data speed.GSM is the most popular standard. GSM is most popular and used worldwide. It uses many authentication protocols for their security. It secures the data efficiently. The drawbacks of the protocols are overcome in the new authentication protocol. SMS alert system of M-banking provides security through the GSM. They use the protocols and one time password for encryption and decryption. So the data are secured by these functions. GSM provides the two types of call flow and also provide SMS flow. GSM also used in other elements which are used in real-time.

REFERENCES

[1] http://en.wikipedia.org/wiki/GSM
[2] Friedhelm hillenbrand (editor): GSM and UMTS, the creation of Global Mobile Communication, Wiley 2001
[3] Scourias, J. (1997) Overview of Global System for Mobile Communications. [Internet]. Available from: <http://www.shoshin.uwaterloo.ca/~jscouria/GSM/gsmreport.html> [Accessed 26 Sep 2006].
[4] Kriegl, J. (2000) *Location in Cellular Networks*. DiplomaThesis, University of Technology Graz, Australia
[5] 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).
[6] SMSSpoofing: Everything you ever wanted to know about SMS spoofing. http://www.smsspoofing.com , 2008.
[7] Burak Bayoglu: Performance evaluation of WTLS handshake protocol using RAS and elliptic curve cryptosystems, 2004
[8] Wagner, D. *GSM Cloning.* Smartcard Developer Association and ISAAC security research group. Available from: http://www.isaac.cs.berkeley.edu/isaac/gsm.html (1998); accessed 28 October 2006
[9] R. Chaudhri, G. Borriello, and W. Thies. FoneAstra: Making mobile phones smarter. In ACM Workshop on Networked Systems for Developing Regions. ACM, Oct. 2009
WAP Forum, Wireless Application Protocol Architecture Specification, Version 12-Jul-2001, from http://www.wapforum.org, 2001.
[10] Kelvin Chikomo, Ming Ki Chong, Alapan Arnab, Andrew Hutchison. Security of Mobile Banking
[11] A. Chaia, A. Dalal, T. Goland, M. J. Gonzalez, J. Morduch, and R. Schiff. Half the world is unbanked. Financial Access Initiative Framing Note, Oct. 2009.

