Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography

Wilayat Khan[1] and Habib Ullah[2]

**[1] Department of Electrical Engineering, COMSATS Institute of IT,
Wah Cantt, 47040, Pakistan**

**[2] Department of Electrical Engineering, COMSATS Institute of IT,
Wah Cantt, 47040, Pakistan**

Abstract

With its great features like providing access to users at anytime and anywhere in the world, mobile communication has been very attractive among the users as well as operators and service providers. However, despite of several advantages, mobile communication has also been facing many security problems. In 2G and 3G technologies like GSM, GPRS and UMTS, the architectures comprise of mainly three nodes; the mobile station (MS), Visitor Location Register/Serving GPRS Support Node (VLR/SGSN), and Home Location Register /Authentication Center (HLR/AuC). These nodes are involved to encrypt/decrypt the data and authenticate the user (MS) in GSM, GPRS and UMTS. To provide security services like authentication and secure communication, the mechanism has been moved from symmetric cryptography to, despite of its complexity, asymmetric cryptography. To reduce the signaling overhead and add some other security features, we propose a new generalized approach in this paper. This is based on asymmetric cryptography for user/network authentication and communication encryption in GSM/GPRS and UMTS with reduced signaling overhead.

Keywords: *GSM, GPRS, UMTS, Authentication, Security, Asymmetric Key Cryptography.*

1. Introduction

Wireless and mobile communication systems are very famous among the customers as well the operators and service providers. Unlike wired networks, the wireless networks provide anywhere and anytime access to users. The *Global System for Mobile Communications* (GSM) occupy almost 70% of the wireless market and is used by millions of subscribers in the world [1].

In the wireless services, secure and secret communication is desirable. It is the interest of both, the customers and the service providers. These parties would never want their resources and services to be used by unauthorized users.

The services like online banking, e-payment, and e/m-commerce are already using the Internet. The financial institutions like banks and other organizations would like their customers to use online services through mobile devices keeping the wireless transaction as secure as possible from the security threats. Smart cards (e.g. SIM card) have been proposed for applications like secure access to services in GSM to authenticate users and secure payment in Visa and MasterCard [2]. Wireless transactions are facing several security challenges. Wireless data passing through air interface face almost the same security threats as the wired data. However, the limited wireless bandwidth, battery, computational power and memory of wireless devices add further limitations to the security mechanisms implementation [3].

The use of mobile communication in e/m-commerce has increased the importance of security. An efficient wireless communication infrastructure is required in every organization for secure voice/data communication and users authentication. Among the main objectives of an efficient infrastructure is to reduce the signaling overhead and reduce the number of updating *Home Location Register/Authentication Center* (HLR/AuC) while the *Mobile Station* (MS) changes its location frequently [3].

In this paper, we propose an approach based on public key cryptography which mainly focuses on user and network authentication with reduced signaling overhead and meet other security requirements like non-repudiations, safety from denial-of-service attacks and integrity of authentication signaling messages.

The rest of the paper is organized as follows. Section 2 gives a brief overview of GSM systems architecture and section 3 discusses authentication protocol used in GSM/GPRS. Section 4 describes authentication and communication encryption in UTMS. Some related work is discussed in section 5. In section 6, we propose a new approach for user and network authentication and communication encryption. Finally, after short discussion, a conclusion is drawn.

2. GSM Overview

GSM, the *Group Special Mobile*, was a group formed by *European Conference of Post and Telecommunication Administrations* (CEPT) in 1982 to develop cellular systems for the replacement of already incompatible cellular systems in Europe. Later in 1991, when the GSM started services, its meaning was changed to *Global System for Mobile Communications* (GSM) [1].

The entire architecture of the GSM is divided into three subsystems: *Mobile Station* (MS), *Base Station Subsystem* (BSS) and *Network Subsystem* (NSS) as shown in Figure 1. The MS consists of *Mobile Equipment* (ME) (e.g. mobile phone) and *Subscriber Identity Module* (SIM) which stores secret information like *International Mobile Subscriber Identity Module* (IMSI), secret key (Ki) for authentication and other user related information (e.g. *certificates*).

The BSS, the radio network, controls the radio link and provides a radio interface for the rest of the network. It consists of two types of nodes: Base Station Controller (BSC) and Base Station (BS). The BS covers a specific geographical area (hexagon) which is called a *cell*. Each cell comprises of many mobile stations. A BSC controls several base stations by managing their radio resources. The BSC is connected to Mobile services Switching Center (MSC) in the third part of the network NSS also called the Core Network (CN). In addition to MSC, the NSS consists of several other databases like Visitor Location Register (VLR), HLR and Gateway MSC (GMSC) which connects the GSM network to Public Switched Telephone Network (PSTN). The MSC, in cooperation with HLR and VLR, provides numerous functions including registration, authentication, location updating, handovers and call routing. The HLR holds administrative information of subscribers registered in the GSM network with its current location. Similarly, the VLR contains only the needed administrative information of subscribers currently located/moved to its area. The Equipment Identity Register (EIR) and AuC contains list of valid mobile equipments and subscribers' authentication information respectively [1, 5].

3. Authentication and Ciphering in GSM and GPRS

There are various security threats to networks [6]. Among these threats are *Masquerading or ID Spoofing* where the attacker presents himself as to be an authorized one, unauthorized use of resources, unauthorized disclosure and flow of information, unauthorized alteration of resources and information, repudiation of actions, and *denial-of-service*. The GSM network incorporates certain security services for operators as well as for their subscribers. It verifies subscribers' identity, keeps it secret, keeps data and signaling messages confidential and identifies the mobile equipments through their *International Mobile Equipment Identity* (IMEI). In the next subsections, we explain subscribers' authentication and data confidentiality as they are closely related to our topic [5].

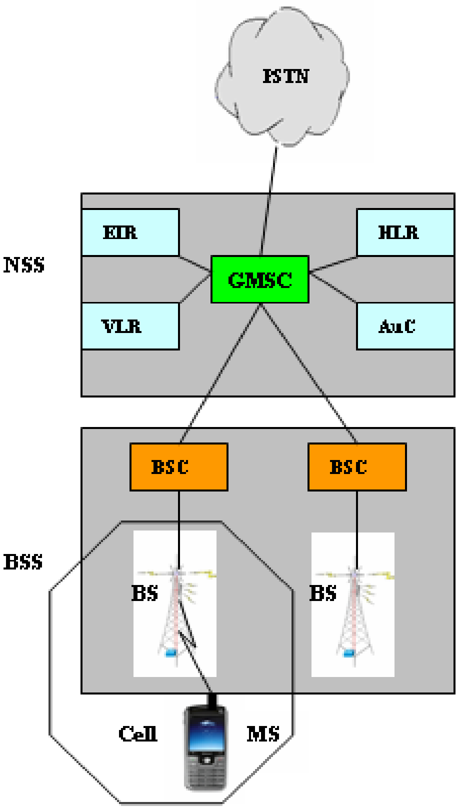

Figure 1. Components overview of GSM

3.1 Subscribers Identity Authentication

As mentioned above, the SIM card holds IMSI, phone number, authentication key Ki, subscriber-relevant data and security algorithms like authentication algorithm (A3). The HLR also stores a copy of Ki and IMSI etc.

In GSM, the users are first identified and authenticated then the services are granted. The GSM authentication protocol consists of a challenge-response mechanism. The authentication is based on a secret key Ki which is shared between HLR and MS. After a visited MS gets a free channel by requesting BS, it makes a request for its location update to MSC through BSC. The MSC, in response, asks MS for its authentication.

In the entire authentication process, the three main actors are the MS, MSC/VLR and HLR/AuC as given in Figure 2. The mobile station sends its *Temporary Mobile Subscriber Identity* (TMSI) to VLR in its request for authentication. The MS uses its real identity IMSI when it is switched on for the first time but the temporary identity TMSI is used later. The TMSI is used to provide *anonymity* to the user identity. After getting the IMSI of the mobile station from the old VLR using TMSI, the VLR sends IMSI to the corresponding HLR/AuC. The HLR/AuC uses authentication algorithm (A3) and ciphering key generation algorithm (A8) to create the encryption key (Kc) and *Signed RESult* (SRES) respectively.

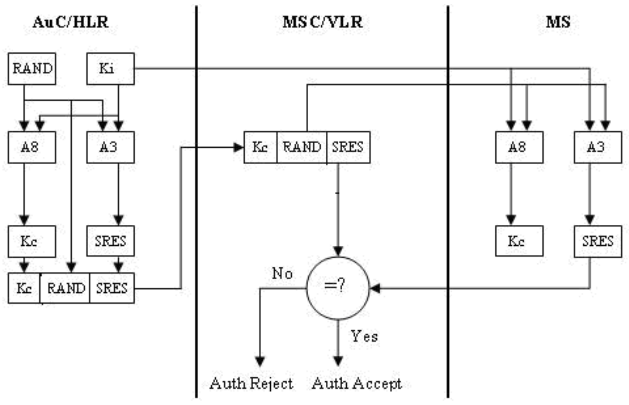

Figure 2. The GSM authentication architecture

The HLR sends the triplet including Kc, RAND and SRES to VLR. The VLR sends the RAND challenge to MS and ask to generate an SRES and send it back. The mobile station creates an encryption key Kc and SRES using algorithms A3 and A8 with the inputs secret key Ki and RAND challenge. It stores Kc to use it for encryption and sends SRES back to the VLR. The VLR compares SRES with the one sent by HLR. If they match, the authentication succeeds otherwise it fails [1, 4, 5].

3.2 User Data and Signaling Protection

The encryption key Kc is used by both of the parties (home system and mobile station) to encrypt the data and signaling information using A5 algorithm. The encryption is done by mobile equipment not the SIM because SIM does not have enough power and processing capacity [1, 4, 5].

4. Authentication and Ciphering in UMTS

The UMTS, in fact, is the result of evolution in GSM network through GPRS. The GSM networks are capable of voice communication using *Circuit Switched* (CS) technique while GPRS adds *Packet Switched* (PS) technique through the use of some extra nodes like *Serving GPRS Support Node* (SGSN) and *Gateway GPRS Support Node* (GGSN). The UMTS, incorporating GPRS nodes and *UMTS Terrestrial Radio Access Network* (UTRAN), provides both circuit switched and packet switched services with enhanced multimedia applications.

As stated in 3GPP specification [7], the circuit switched services are provided by VLR and the packet switched services are provided by SGSN. The UMTS, like GSM/GPRS, uses the concept of *Authentication Vector* (AV) but unlike GSM/GPRS, the AV comprises of five components: the random challenge (RAND), the expected response (XRES), key for encryption (CK), integrity key (IK) and the authentication token (AUTN). The VLR/SGSN requests HLR/AuC for authentication. The HLR/AuC computes the AV and is sent back as a response to VLR/SGSN without any encryption applied to it. After the authentication is completed, the cipher key CK is used to encrypt the user data and signaling information. Similarly, to preserve the integrity of the important control signals, integrity key (IK) is used.

The GSM Consortium actually provided security to GSM systems relying on s*ecurity through obscurity* where they believed that the algorithms used in GSM would be very hard to break if they were kept secret. Therefore, the GSM specifications and protocols were kept secret away from public to be studied and analyzed by scientific community.

But, eventually, the GSM algorithms were accessed by scientific community and now GSM is vulnerable to many attacks [6, 7, 10].

In GSM/GPRS and UMTS, the links between MS-VLR and VLR-HLR faces many security threats due the use of conventional symmetric key encryption and mutual trust of the parties. The VLR and HLR just rely on mutual trust they have on each other.

To implement public key cryptography, a well defined network infrastructure is needed. The *Public Land Mobile Network* (PLMN) operators are the main candidates for this to develop PKI in their systems. The 3G networks like UMTS which offers services with very high data rates is the most favorable for the operators to incorporate PKI services to their customers. To verify the authenticity of public keys, there should be a trusted third party, the *Certification Authority* (CA), to issue digital certificates to the users. These certificates are to be stored in the SIM/USIM of the mobile station. The *Mobile Execution Environment (*MExE) is an application execution environment which allows application programming and creating a *Java Virtual Machine* (JVM) in the MS. Based on the importance of secure transactions and the fact that networks operators are the big candidates for PKI implementation, it seems feasible to use public-private key pair for intra-PLMN signaling as well as for secure e/m-transaction. A new approach, with the introduction of asymmetric key cryptography, has been adopted in [8].

5. Related Work

Asymmetric key approach supported by MExE is another reason to be favorable for operators to deploy *Public Key Infrastructure* (PKI) in their systems. The asymmetric key cryptography for authentication and encryption, as mentioned in [8], is described below.

5.1 Asymmetric Cryptography in GSM/GPRS and UMTS

As in GSM/GPRS, we consider the same three nodes: MS, VLR and HLR/AuC. These nodes preserve the same roles for all the three systems: GSM, GPRS and UMTS, involved in the process of authentication and encryption.

The nodes VLR and HLR hold the same pair of public-private keys, V_H_{PrK} and V_H_{PuK}, which facilitates the key distribution process because other interconnected networks would need only one public key for corresponding VLR-HLR transactions. A second option could be to use separate public-private key pairs but it will further complicate the key distribution process. The link between VLR and HLR is secured using the VLR-HLR public key (V_H_{PuK}). The messages are encoded with this key by any of the endpoints. At the receiving end, the corresponding private key V_H_{PrK} is used for decryption.

After the channels are assigned, the users are authenticated through the exchange of messages among the nodes: MS, VLR and HLR as shown in Figure 3. The MS (SIM on mobile station) sends an *Identity Message* to VLR which includes the identity data (e.g. IMSI of the user) encrypted with MS-VLR's public key (MS_V_{PuK}). The VLR decodes it using corresponding private key (MS_V_{PrK}) and extracts the required information. The VLR encrypts it again with VLR-HLR link public key (V_H_{PuK}) and forwards it to the corresponding HLR in *Authentication Information* message. After it is decoded using VLR-HLR link private key (V_H_{PrK}), the HLR sends the user's public key (MS_{PuK}) back to the VLR in an *Authentication Acknowledgment* message. The VLR sends a random challenge *RAND* to the MS encrypted with the user's public key (MS_{PuK}) in *Authentication Request* message. The MS decodes the random number, encrypts it with its own private key and sends it back along with SK and IK to VLR in *Authentication Response* message. The VLR decrypts this message using the user's public key and checks if the random number is the same. If it is equal to the random number held by VLR, it will indicate the user authenticity as it has been signed by the user with his own private key.

Public key cryptography is computationally extensive. Therefore, it slows down the data rate. It can be better utilized when it is used for secret keys transmission. The SIM on the MS creates *secret key* (SK) and in case of

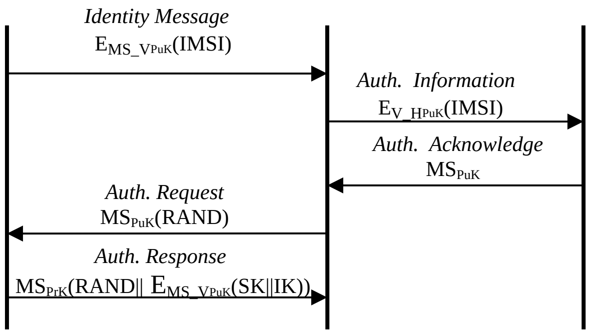

Figure 3. Authentication process using public key cryptography

UMTS an *integrity key* (IK) for the integrity of signaling messages. These two keys are concatenated, encrypted with VLR's public key (*MS_V_{PuK})* and are sent to the VLR in the *Authentication Response* message. After the authentication is successful, the data and signaling information are encrypted with the keys SK and IK to preserve the confidentiality and integrity of both the data and signals.

The public key cryptographic approach discussed in the above paragraphs is an obvious way of authentication and securing the communication especially when it is used in financial transactions like e/m-commerce. In this approach, five messages are exchanged to authenticate the user and to share the keys which brings signaling overhead. In this approach, the user (MS) is authenticated by the network before giving the service but it does not authenticate the network. One can rely only on the fact that both, the MS and the HLR, have the same secret key Ki. This can be considered a weak network authentication, but it will fail if the key Ki is stolen or accessed by a third party. The *denial-of-service* attack is possible if the attacker changes the authentication signaling (signal integrity). In the next section, we propose a general solution with reduced signaling for all the three systems GSM, GPRS and UMTS to reduce the drawbacks discussed above.

6. Authentication and Encryption in GSM, GPRS and UMTS Using Public Key Cryptography

Due to slow data rates, the public key encryption offers, it is not encouraged to be used for communication encryption. Instead, it is preferred for authentication and secret key distribution to be used in symmetric key encryption of the communication. To encrypt the data and signaling, special secret and integrity keys like SK and IK may be used respectively for communication encryption and signaling integrity.

In this section, we present a solution based on public key cryptography. This relies on the same concept of public-private keys as mentioned in the section 5. The three main entities, MS, VLR and HLR, are using four pairs of public-private keys as shown in Figure 4(a).

These three entities exchange four messages with each other as shown in Figure 4(b). The detail of the elements in each of these messages is

Identity Message = $E_{M\_V_{PuK}}$ (IK||SK||RAND) || $E_{H_{PuK}}$ (IMSI|| Ki)
Authentication Information = $E_{H_{PuK}}$(IMS||Ki)

V_H_{PrK}:	VLR-HLR link's private key
V_H_{PuK}:	VLR-HLR link's public key
M_V_{PrK}:	MS-VLR link's private key
M_V_{PuK}:	MS-VLR link's public key
H_{PrK}:	HLR private key
H_{PuK}:	HLR public key
M_{PrK}:	Mobile station's private key
M_{PuK}:	Mobile station's public key

Figure 4(a). Set of public keys used

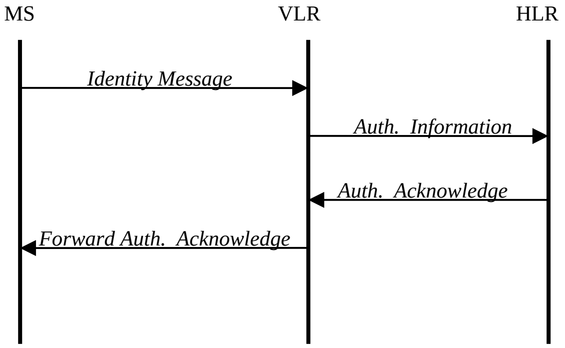

Figure 4(b). Authentication process using public key cryptography

Authentication Acknowledge = *M_{PuK}*
Forward Authentication Acknowledge = $E_{M_{PuK}}$ (RAND)

The symbol '||' represents the concatenation of two elements. The MS creates secret keys SK, IK and a random challenge RAND. It starts the authentication exchange by sending an *Identity Message* to the visited VLR. This message includes concatenation of RAND, SK and IK encrypted with public key M_V_{PuK}. The IMSI and Ki encrypted with public key *H_{PuK}* is also part of the *Identity Message* as shown in Figure 4(b). Unlike the approach in [8], the secret keys SK and IK are sent in the first message.

The VLR uses the corresponding private key M_V_{PrK} to decode the part of the message and extract the needed information RAND, SK and IK. The VLR forwards the rest of message (E_{HPuK}(IMS||Ki)) unchanged in *Authentication Information* message to the HLR. The keys

SK and IK are used later for confidentiality and integrity of both the data and signals respectively.

The HLR decodes the *Authentication Information* message with its private key H_{PrK} and gets the IMSI and Ki sent from MS. The secret key Ki is used as a random challenge for user/MS authentication. The MS and the HLR have the same secret key Ki. The HLR compares the received Ki with its own Ki. If they match, the user is authenticated. It is difficult for a third party to change this secret without being detected by HLR. The HLR can easily detect it using IMSI of the requesting user sent in the *Identity Message.*

Using the IMSI, the HLR finds the corresponding user's public key M_{PuK} and is sent to VLR in the *Authentication Acknowledge* message. This message acts as an indication to the VLR that the user has been authenticated by the HLR. The VLR uses the public key M_{PuK} to encrypt the RAND challenge received from MS in the *Identity Message*. The MS decrypts it with its own private key. The result is compared with the RAND stored at MS. If they are equal, the VLR is authenticated as it ensures the MS that the VLR is the only entity having the MS-VLR link's private key M_V_{PrK}.

This approach includes all the benefits of the previous systems. It keeps the user's identity secret, the encryption keys are distributed, users and network both are authenticated. This entire process requires four signaling messages reducing the signaling overhead.

An attack *denial-of-service* may be possible if the attacker changes the signaling contents based on which the user and network authenticates each other. For example, if the encrypted content of RAND challenge is modified or if IMSI or Ki is changed during transmission, the network and user authentication will fail even if the user and network are legitimate. To cope with this problem, *Digital Signature* [9] can be used. The end-to-end integrity of the authentication parameters should be ensured because the end entities, the VLR/HLR and the MS, make the decision of authentication. Therefore, to ensure the integrity of message contents at the ends, *hashing* (H) function combined with encryption may also be used. For example the elements IMSI and KI may be hashed using the secret key Ki and the resulted message digest is sent in the *Identity Message*. This will ensure the HLR that the parameters IMSI and Ki have not been altered during transmission.

7. Conclusions

Wireless communication, having great features, is attractive among users as well service providers. With the increase in its use, security problems of confidentiality, integrity, and authentication are also increasing. The mechanism to solve these problems has changed to public key cryptography from symmetric key cryptography. The available public key cryptographic approaches are good in security point of view but they are computationally extensive as well as have more signaling overhead. Furthermore, these approaches do not provide integrity of the initial authentication messages and authentication of the network.

In this paper, we proposed an enhanced model based on the public key cryptography. In this model, utilizing the real benefits of public key encryption, user as well as network authentication is provided. The integrity of the signaling used during the user and network authentication is ensured. The secret keys for data encryption and signaling integrity are distributed using public keys. These benefits are achieved with fewer signals reducing the signaling overhead.

As noted before, although, public key cryptography is computationally very extensive which requires large processing power, battery, and memory, but still the approach we proposed is efficient to use than the others. The rapid developments in *Integrated Circuits* (IC) and *Smart Cards* (e.g. SIM) technologies, high speed communication systems (e.g. UMTS), and significance of secure transactions (e.g. e/m-commerce) make the conditions more favorable to use public key cryptography.

References

[1] Yong Li, Yin Chen, and Tie-Jun MA, "Security in GSM", Retrieved March 18, 2008, from http://www.gsm-security.net/gsm-security-papers.shtml.

[2] N. T. Trask and M. V. Meyerstein, "Smart Cards in Electronic Commerce", A SpringerLink journal on *BT* Technology, Vol. 17, No. 3, 2004, pp. 57-66.

[3] N T Trask and S A Jaweed, "Adapting Public Key Infrastructures to the Mobile Environment", A SpringerLink journal on BT Technology, Vol. 19, No. 3, 2004, pp. 76-80.

[4] Cheng-Chi Lee, Min-Shiang Hwang, and I-En Liao, "A New Authentication Protocol Based on Pointer Forwarding for Mobile Communications", A Wiley InterScience journal on Wireless Communications and Mobile Computing, Published online, 2007.

[5] Vesna Hassler and Pedrick Moore, "Security Fundamentals for E-Commerce", Artech House London Inc., 2001, pp. 356-367.

[6] Mohammad Ghulam Rahman and Hideki Imai, "Security in Wireless Communication", A SpringerLink journal on

Wireless Personal Communications, Vol. 22, No. 2, 2004, pp. 213-228.
[7] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Mobile Execution Environment (MExE); Service Description, Stage I. Technical Specification 3G TS 22.057 version 5.2.0 (2001-10), 2001.

Wilayat Khan graduated with a B.Sc. in Computer Systems Engineering from the NWFP University of Engineering & Technology, Pakistan in 2007. He earned his MS degree from the Royal Institute of Technology (KTH) Sweden in Information and Communication Systems Security in 2009. In his MS theses, he designed a strong authentication protocol for handheld devices. In 2009, he started his carrier as a teacher at the Department of Electrical Engineering, COMSATS Institute of IT, Wah Campus, Pakistan. He has published a number of papers on wireless and mobile networks and security in international journals and conference proceedings. His research interests include wireless & mobile networks, protocol design for mobile devices, authentication, web security and smart cards security.

Habib Ullah graduated in B.Sc. Computer Systems Engineering from the NWFP University of Engineering & Technology, Pakistan in 2006 and earned M.Sc. degree in Electronics and Computer Engineering from the Hanyang University, Seoul Korea with a thesis focusing on comparative study: the evaluation of shadow detection methods. He started teaching in 2009 at the department of Electrical Engineering, COMSATS Institute of IT, Wah Campus, Pakistan. He has various publications focusing on background modeling and shadow detection. His research interests include information security, pattern recognition, behavior modeling and object segmentation etc.