Signaling Traffic Analysis of GSM Authentication Protocols

by

Ali Akremi

A Thesis Presented to the

FACULTY OF THE COLLEGE OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

COMPUTER ENGINEERING

November, 1997

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

NOTE TO USERS

The original manuscript received by UMI contains broken, slanted and or light print. All efforts were made to acquire the highest quality manuscript from the author or school. Microfilmed as received.

This reproduction is the best copy available

UMI

SIGNALING TRAFFIC ANALYSIS OF GSM AUTHENTICATION PROTOCOLS

BY

ALI AKREMI

A Thesis Presented to the

FACULTY OF THE COLLEGE OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

COMPUTER ENGINEERING

November 1997

UMI Number: 1390027

UMI Microform 1390027
Copyright 1998, by UMI Company. All rights reserved.

This microform edition is protected against unauthorized
copying under Title 17, United States Code.

UMI
300 North Zeeb Road
Ann Arbor, MI 48103

Signaling Traffic Analysis of GSM Authentication Protocols

by

ALI AKREMI

A Thesis Presented to the
FACULTY OF COLLEGE OF GRADUATE STUDIES

In Partial Fulfillement of the Requirements
For the degree of

MASTER OF SCIENCE

IN

Computer Engineering

KING FAHD UNIVERSITY
OF PETROLEUM AND MINERALS
Dhahran, Saudi Arabia

November 1997

KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS

DHAHRAN, SAUDI ARABIA

COLLEGE OF GRADUATE STUDIES

This thesis, written by

ALI AKREMI

under the direction of his Thesis Advisor and approved by his Thesis Committee, has been presented to and accepted by the Dean of the College of Graduate Studies, in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN COMPUTER ENGINEERING

Thesis Committee

Dr. Khalid M. AlTawil (Chairman)

Dr. Habib Youssef (Cochairman)

Dr. Mostafa Abd – El – Barr (Member)

Department Chairman

Dean, College of Graduate Studies

14-3-98
Date

كلية الدراسات العليا
COLLEGE OF GRADUATE STUDIES

Acknowledgments

Acknowledgement is due to king Fah University of Petroleum and Minerals for support of this research.

I would like to express my deep gratitude and thanks to my advisor Dr. Khalid Al-Tawil for his invaluable guidances, useful discussion, critisism, constant encouragement and help in achieving this work. Also, I sincerely thank Dr. Habib Youssef and Professor Mostafa Abd-El-Barr for their help, patience and unlimited support.

Finally, I extend my gratitude and thanks to my wife and my children for their patience, understanding and support during the course of my MS program study.

Dedicated to

My Parents, My Wife, and my children

Contents

List of Tables

List of Figures

List of Abbreviations

BCCH:	Broadcast control Channel
BSC:	Base Station Controller
BSS:	Base Station Subsystem
BTS:	Base Transceiver Station
CBCH:	Cell Broadcast Channel
CCH:	Control Channel
FACCH:	Fast Associated Control Channel
FCCH:	Frequency Correction Channel
FDMA:	Frequency Division Multiple Access
HLR:	Home Location Register
IMSI:	International Mobile Subscriber Identity
ME:	Mobile Equipment
MS:	Mobile Station
MSC:	Mobile Switching Center

NSS:	Network and Switching Subsystem
PCH:	Paging Control
PIN:	Personal Identity Number
RACH:	Random Access Channel
SACCH:	Slow Associated Control Channel
SCH:	Synchronization Channel
SDCCH:	Standalone Dedicated Control Channel
SIM:	Subscriber Identity Module
SRES:	Signed Result
TDMA:	Time Division Multiple Access
TMSI:	Temporary Mobile Subscriber Identity
VLR:	Visitor Location Register
PUK:	Pin Unblocking Key
AMPS:	Advanced Mobile Phone System
ANSI:	American National standards Institute
BCCH:	Broadcast Control Channel
CCCH:	Common Control Channel
CCITT:	International Telegraph and Telephone Consultative Committee
CDMA:	Code Division Multiple Access
CDPD:	Cellular Digital Packet Data

DCS:	Digital Communication System
DECT:	Digital European Cordless Telephone
DQPSK:	Differential Quadrature Phase Shift Keying
ERMES:	European Radio Message System
ETSI:	European telecommunication Standard Institute
FACCH:	Fast Associated Control Channel
FCC :	Federal Communications Commission
FDD:	Frequency division duplex
GMSK:	Gaussian Minimum Shift Keying
GSM:	Global System for Mobile communication
HLR:	Home Location Register
IMSI:	International Mobile Subscriber Identity
EIA:	Electronic industry Association
EIR:	Equipment Identity Register
IS-54:	EIA Interim standard for U.S Digital Cellular (USDC)
IS-95:	EIA interim standard for U.S code Division Multiple Access
ISDN:	Integrated Services digital Network
ISUP:	ISDN User Part
JDC:	Japanese Digital Cellular
NSS:	Network Switching Subsystem

OSI:	Open System Interconnect
PACS:	Personal Access Communication System
PCH:	Paging Channel
PCN:	Personal Communication Network
PCS:	Personal Communication System
PSTN:	Public Switched Telephone Network
QPSK:	Quadrature Phase Shift Keying
SIM:	Subscriber Identity Module
SMS:	Short Messaging Service
SS7:	Signaling System No.7
TACS:	Total Access communications System
TDD:	Time Division Duplex
RAND:	Random Number
RANDM:	Random number from Mobile Station
RANDG:	Random number:Global
COUNTM:	Mobile Station event log counter
SHK:	Shared Key

THESIS ABSTRACT

Name: ALI AKREMI

Title: SIGNALING TRAFFIC ANALYSIS OF GSM AUTHENTICATION PROTOCOLS

Degree: MASTER OF SCIENCE

Major Field: COMPUTER ENGINEERING

Date of Degree: NOVEMBER 1997

Mobile communication is one of the fastest growing sectors of the telecommunication industry. Mobile users can make and receive calls while they are moving independent of time, location and network access. The new and potentially wider mobile communication market using reduced cell sizes and lower powered terminals are known as personal communication services (PCS). PCS are expected to provide an ubiquitous exchange of information (voice, data, image, video) for nomadic users. The Global System for Mobile communication (GSM) is a Pan-European digital cellular mobile system supporting widespread roaming and PCS services in a worldwide wireless communication network. Wireless systems are more vulnerable to fraudulent access and eavesdropping compared to wireline network. As a remedy for that, the Global System for Mobile communication (GSM) is giving more importance for the users's privacy and authentication process. Although the process might be giving a reasonable security level, it is overloading the network with significant signaling traffic and increasing the call set up time. The signaling load and the authentication delay are of particular importance and become the subject of widespread research interest. In this thesis, we will study and analyze the GSM privacy and authentication protocols, and propose new schemes with less signaling traffic and better call set up time.

Keywords: Global system for mobile communication, Authentication, Signaling Traffic, Roaming.

Master of Science Degree
King Fahd University of Petroleum and Minerals
Dhahran, Saudi Arabia.
November 1997

جامـــعة الملك فهد للبترول و المعادن

كليـة علـوم و هندسـة الحاسـب الآلي-قسـم هندسـة الحاسـب الآلي.

الأسم :   علـــي العكـــرمي
عنوان الرسالة: تحليل اشارات بروتوكول الهوية الأصلية فى نظام GSM
التخصص: هندسة الحاسب الآلي.
تاريخ التخرج: نوفمبر ١٩٩٧

موجز الرسالة

تعد أنظمة الاتصالات النقالة واحدة من أسرع الأنظمة في قطاع صناعة الاتصالات. لقد أصبح المشترك فى هذه الأنظمة بامكانه أن يستقبل أو يرسل مكالمة هاتفية و هو متنقلا فى أى وقت و من أى مكان. ان نظام الاتصالات النقالة الجديد ذو الانتشار الواسع و الذى يعرف باسم نظام الاتصالات الشخصي يستعمل نظام الخلية الصغيرة الحجم اضافة الى الأجهزة ذات الأحجام الصغيرة و التغذية الضعيفة. أن نظام الاتصالات الشخصي متوقع أن يقدم خدمة شاملة فى تبادل المعلومات (صوت, صورة, بيانات, و فيديو) بالنسبة للمشتركين المتجولين. يعتبر النظام الأروبي الشامل للاتصالات النقالة (GSM) من أهم الأنظمة الرقمية التى ترتكز على الخلية الجغرافية و يشمل خدمة نظام الاتصال الشخصي والتجول الواسع النطاق داخل الشبكات الأجنبية. ان النظام الشامل للاتصالات النقالة ينتمي أساسا الى نظام الاتصالات اللاسلكية حيث تعتبر الأكثر عرضة الى التصنت و اختراق الدخول على الشبكة بصفة غير مشروعة. ان نظام GSM قد عالج ظاهرة التصنت و الاختراق و ذلك باستعمال أسلوب الخصوصية و أسلوب التأكد من هوية المشترك الأصلية. على الرغم من وجود مزايا هامة من حيث ضمان السرية و سلامة التأكد من هوية المشترك للأسلوبين المذكورين, نجد فى الوقت نفسه أنهما يثقلان الشبكة بعبئ ثقيل من الاشارات و الرسائل التى تأثر سلبا على الوقت القياسي لربط المكالمة. ان حمل الاشارات و الرسائل اضافة الى التأخير الزمني فى ربط المكالمة يعتبران من أهم الأشياء التى تميز بروتكول الخصوصية و الهوية الأصلية فى نظام GSM و قد حاز على كثير من اهتمام الباحثين فى الفترة الأخيرة. فى هذه الرسالة سوف ندرس و نحلل بروتكول الخصوصية و الهوية الأصلية التابع لنظام GSM ثم نقترح بروتكولات جديدة لمعالجة مشكلة أمن الشبكة و المشتركين بأقل حمل من ناحية الاشارات و الرسائل اضافة الى زمن أقل فى ربط المكالمة الهاتفية.

درجة الماجستير فى العلوم
جامعة الملك فهد للبترول و المعادن , الظهران المملكة العربية السعودية
نوفمبر ١٩٩٧

Chapter 1

Introduction

We are all being exposed to a revolution in communications, a revolution that is taking us from a world where subscribers were constrained to communicate over fixed telephone lines, to one where a wireless and mobile communications environment has become a reality. In fact, the desire to communicate with people on the move has evolved remarquably since Guglielmo Marconi first demonstrated in 1897 radio waves's ability to provide continuous contact with ships sailing the English channel [59]. Since then, new wireless communication methods and services have been adopted by people throughout the world. Wireless communication systems, of which cordless phones, pagers, and cellular telephones are some of the most familiar examples, have experienced enormous growth over the last decade. In different countries, such systems are referred to as personal communication networks (PCN), personal communication system (PCS), Universal mobile telecommunication services (UMTS), universal personal telecommunication (UPT), and so forth [27]. Such systems and services are proposed to meet the ultimate goal of providing reliable, ubiquitous, and cost-effective communications to personal subscribers either universally or continentally. For standard development purposes, PCS is used as an umbrella term to describe services and supporting systems that provide users with the ability to communicate anytime, anywhere, and in any form. This definition encompasses the concepts of terminal mobility, personal mobility and service mobility [49]. Terminal mobility allows a terminal to be identified by a unique terminal identifier independent of the point of attachment to the network. Calls intended for that terminal can therefore be delivered regardless of its network point of attachment. Personal Mobility and service mobility are achieved primarily through the functionality of a "personal number" associated with a person and his service profile instead of a terminal. Service mobility implies that the services that a user has subscribed to, are available to him even if he moves or changes terminal equipment.

The increasing demand for mobile access to voice and non-voice telecommunication services has led to the introduction of a new generation of digital cellular telecommunication networks. The European Global system for Mobile communication (GSM) network has been the first representative which provides a unique services integrated radio interface for speech and data. The concept of cellular was proposed by Bell System in 1971 following a request from the Federal Communications Commission (FCC). The Key objectives of such a cellular system were stated as follows [27]:

- Large subscriber capacity
- Efficient use of spectrum
- Nation-wide compatibility
- Widespread availability
- Adaptability to traffic density
- Service to vehicle and portable stations
- Regular telephone service and special services
- Telephone quality of service
- Affordability.

Based on the Bell concept the effective introduction of commercial Cellular services in Europe and in the USA started in the early 1980's and already cellular systems are serving more than 30 million subscribers around the world. Today the key objectives are generally achieved by the main cellular system standards such as: Advanced mobile phone systems (AMPS) in the 800 MHz band, its 900 derivative MHz TACS (Total Access Cellular system), Nordic mobile telephone (NMT) and several other standards which can be considered as variations of the same key concepts.

1.1 The Emergence of the GSM Standard

In 1982. while the first commercial cellular services were emerging. the "Conference Europenne des Postes et Telecommunications" (CEPT) decided to set up a group called Groupe Special Mobile (the initial meaning for GSM). to work out specifications for a pan-European cellular mobile communication system in the 900 MHz band. using spectrum that had been previously reserved in 1978 by the world administrative Radio Conference (WARC). The idea behind this decision was to create. for the first time. a system that would end the traditional European fragmentation and incompatibility in the mobile field. From the beginning. the work was directed towards a second-generation cellular system. since many countries already had first-generation systems (TACS. NMT...) in use or in the implementation phase. The directives were in the beginning that the new system must take into account recent developments in the telecommunication field. such as CCITT signaling system No.7. Integrated Services Digital Network (ISDN). Open System Interconnection (OSI) and other powerful innovations [54]. Later on they agreed that the system also should be fully digital. In 1988, the European Telecommunication Standards Institute (ETSI) was created and most of the CEPT technical standardization activities were transferred to this new body, including GSM. The first GSM technical specifications were published in 1990. At that time. the United Kingdom requested a specification based on GSM but for higher user densities with low-power mobile stations. and operating at 1.8 GHz. The specification for this system. called Digital Cellular System (DCS 1800) were published in 1991.

1.2 Services Provided by GSM

The Pan-European digital network standard GSM is providing a common set of compatible services and capabilities to all mobile users. GSM services are following ISDN guidelines and are classified as tele-services or data services [54]. Tele-services include standard mobile telephony and mobile-oriented or base-originated traffic. Telephone services includes emergency calling and facsimile. Data services include computer-to-computer communication and packet-switched traffic. Data rates are varying from 300 to 9.6 kbps. Specially equipped GSM terminals can be connected to Public Switch Telephone Network (PSTN). ISDN. Public Switch Data Network (PSDN) through several possible methods. using synchronous or asynchronous transmission. A particular service unique to GSM is the Short Message Service. which allows users to send and receive point-to point alphanumeric messages up to tens of bytes. It is similar to paging services, but more comprehensive. In addition to these services, GSM is offering a number of significant advantages over the old analog systems such as:

- International and wide area roaming capability.

- Better security against fraud through terminal validation and user authentication.
- Encryption capability for information security and privacy.
- Personal and terminal mobility through the insertion of a subscriber identity module (SIM).

1.3 GSM System Architecture

The functional architecture of the GSM system consists of three main parts: the mobile station (MS), base station subsystem (BSS) and the network and switching subsystem (NSS). The mobile station is formed by two elements: the subscriber identity module (SIM) and the mobile equipment (ME). The SIM card is either a smart card (like a credit card) or a smaller size "plug-in SIM" that contains the subscriber-related information. SIM is protected by a personal identity number (PIN) code chosen by the subscriber. Base Station Subsystem: consists of the base station controller (BSC) and the transmit-receive equipment (BTS) which is deployed in the area to be covered. The network and switching subsystem (NSS) supports the switching functions and the subscriber profile/mobility management. The basic switching function in the NSS is performed by the mobile switching center (MSC) that controls several base station systems and connects all system elements through leased lines to other network elements external to GSM network [32]. In addition to the MSC, in the NSS we find the Home Location Register (HLR), the Visited Location Register (VLR), the Authentication Center (AuC) and the Equipment Identity Register (EIR). HLR contains all the administrative information of each local registered user, and where he is located. There is logically one HLR per GSM network, although it may be implemented as a distributed database. The VLR is used to retrieve information for handling calls to or from a visiting mobile user. When a mobile moves from the home system to a visited system, its location is registered at the VLR of the visited system. The Authentication center (AuC) is a protected database that stores users secret key and algorithms used for the authentication and privacy. The equipment identity register (EIR) contains a list of all valid mobile equipment on the network, where each mobile equipment is identified by its international mobile equipment identity (IMEI).

1.4 GSM Security Functions

The GSM security is addressed in two aspects: authentication and encryption. Authentication avoids fraudulent access of a cloned mobile station, whereas encryption avoids unauthorized listening. Authentication is performed by asking the terminal to give a 32 bit number called signed result (SRES). The SRES is obtained as an output result of a specific computation made on a random number (RAND) sent by the system and user private key K_i using the authentication algorithm A3 [11]. The ciphering of the radio burst of data is achieved with a second ciphering algorithm A5 applied to a key K_c chosen for each connection at each burst. K_c is computed in the same time of SRES using a special algorithm called A8. Ciphering algorithms reside in the terminals and in the Authentication center (AuC). In addition to the authentication and privacy, GSM enhances the security aspect by using a temporary substitute of the personal number of the subscriber (IMSI) called temporary mobile subscriber identity (TMSI) allocated by the network at the first time of mobile registration in a given area [68].

1.5 Objective of the Thesis

The global system for mobile communication GSM is the world's first digital cellular mobile network supporting PCS services and providing a common set of compatibilities to all users irrespective of the geographic area and the national boundaries. However, radio accessed networks are inherently less secure than fixed networks. This comes from the possibility to listen to and to emit radio waves from anywhere, without tampering with operator's equipment. In GSM, this situation is remedied by introducing several types of security functions in GSM standard in order to protect the network against fraudulent access and to ensure user privacy. These functions include:

- Authentication of the mobile users, to prevent access of unregistered users.

- Radio path ciphering, to prevent all user information from a third-party tapping;
- Subscriber identity protection, to prevent user location disclosure.

The authentication process is carried out through the challenge/response mechanism which consists of asking a question that only the right user equipment (SIM) may answer. The returned answer (SRES) computed internally in the user SIM card. will be compared in the authentication center. Users roaming between different networks have also to be authenticated by the visited networks using the same challenge/response mechanism. The visited network has to collect the visiting user authentication parameters from his home domain. The authentication process is triggered on each registration and call attempt. and it is generating an important signaling traffic due to the number of queries and updates of network databases. In addition. the process is making a delay (by increasing the call set up time) called the authentication delay. The signaling load and the authentication delay are of particular importance and become the subject of widespread research interest. In the literature, the authentication and privacy process has been studied without any analysis or attempts to reduce the invoked signaling load. This situation motivates us to analyze this problem with more emphasis on the signaling load and the authentication delay of the conventional GSM protocols. then we propose new authentication protocols used for home domain and roaming users with less signaling message load and shorter authentication delay. which improves the call set up time.

1.6 Organization of the Thesis

After introducing the GSM network in Chapter 1. wireless communications systems and their main characteristics are presented in Chapter 2. Chapter 3 is dedicated to the GSM networks outlining all important aspects of this digital cellular system. Network Security and the different security approaches are introduced in Chapter 4. The analysis of the conventional GSM authentication protocols is given in Chapter 5. Chapter 6 presents our proposed authentication protocols used for home domain users. In Chapter 7, we propose our authentication protocol used for roaming users. In Chapter 8, we summarize our work and we propose the future work for the authentication protocols that can take place in the coming GSM generations.

1.7 Summary

Mobile communications is an important paradigm that aims to provide continuous network connectivity to customers regardless of their location. In this chapter, we started first by introducing the Global system for mobile communications (GSM) as an European standard providing an ultimate solution for the personal communication services. Then, we presented the services provided, the system architecture, and the security functions introduced for the first time in a mobile communication systems. At the end of the chapter we presented the objective of the thesis and its organization.

Chapter 2

Wireless Communication Systems

In our traditional life. most people are familiar with wireless communication systems such as garage door openers, remote controllers for electronic home equipment. cordless telephones, pagers, and cellular telephones. All these systems belong to the same wireless family or mobile radio communication systems but each one is different from the other in terms of cost, complexity, performances. and type of services offered. The term mobile is commonly used to classify any radio terminal that could be moved during operation [16]. Mobile communications can include technologies ranging from paging systems. cordless telephones. to digital cellular mobile networks. In the last decade, many mobile radio standards have been developed for wireless systems throughout the world, and more standards are likely to emerge. The radio spectrum is experiencing a high demand nowadays, frequency bands are getting continuously allocated for different services. Figure 2.1 provides the names

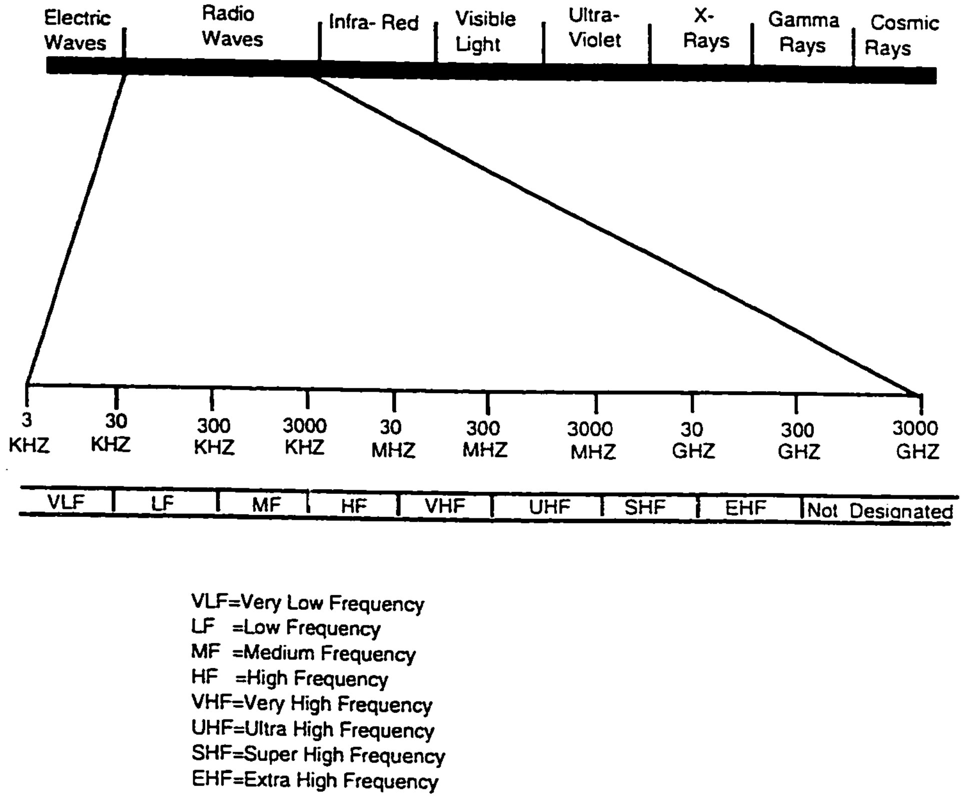


Figure 2.1: Radio Frequency Spectrum

of various frequency ranges in the radio spectrum. In this chapter, we cover the main types of wireless systems and their characteristics based on their frequency band, the modulation used, their multiple access, and the channel bandwidth used. Modulation is the process of putting information onto a high frequency carrier for transmission.

2.1 Wireless Systems

The evolution of telecommunications, from the wired phone to personal communications services (PCS), is resulting in the availability of wireless products not previously considered practical. The goal of PCS is to provide integrated communications (e.g., voice, data, and video) between mobile subscribers independent of time, locations, and mobility patterns. The common thing in all wireless personal communication activity are the desire for mobility in communication associated with the desire to be free from home or office in order to make/receive a call. Various approaches to wireless communications, taken together, are arguably the fastest growing segment of the telecommunication industry [40]. These communication approaches are distinguished mostly by their frequency band, the multiple access used, the modulation, and the duplexing techniques. Before presenting the main three types of wireless systems (paging, cordless, and cellular), we introduce two main characteristics frequently used in any wireless system: the access method and duplexing.

2.2 Access Methods in Wireless Systems

The radio channel is fundamentally a broadcast communication medium [58]. The objective of wireless communication system is to provide communication channels on demand between a portable radio station and a base station that connects the user to the fixed network infrastructure. Signals transmitted by one user can potentially be received by all other users within the range of the transmitter. Many techniques have been devised to create channels out of the communication medium. in order to use them as separate links. A given radio spectrum can be divided into a set of disjoint or non-interfering radio channels that can be used simultaneously while maintaining an accepted received radio signal. Multiple access refers to the simultaneous transmission by numerous users to or through a common receiving point [15]. In wireless radio systems, this technique is based on insulating signals used in different connections from each other to support parallel transmissions on the Uplink and Downlink, respectively [4]. Frequency multiple access (FDMA), Time division multiple access (TDMA), and Code division multiple access (CDMA) are the three major access techniques used to share the available bandwidth in a wireless communication system as shown in Figure 2.2.

- In FDMA technique, the frequency spectrum is divided into small frequency bands or channels. Channels are assigned on demand to users who request service. During the period of the call, no other user can share the same frequency band.

- The TDMA divides the radio spectrum into time slots, and in each slot only one user is allowed to either transmit or receive. In this technique each user occupies a cyclically repeating time slot, so a channel may be thought of as

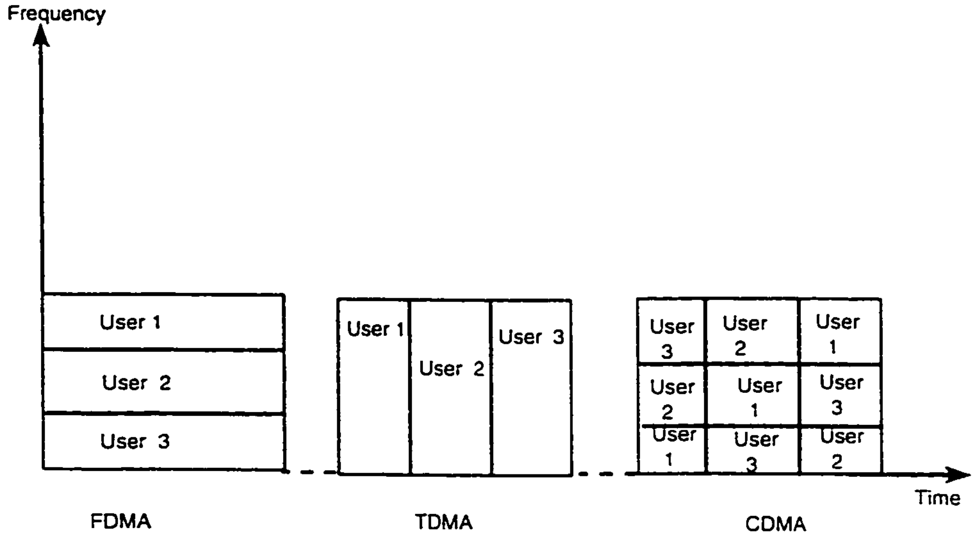


Figure 2.2: Multiple Access Methods

particular time slot that reoccurs every frame.

- In CDMA, all signals occupy the same bandwidth and are transmitted simultaneously in time. CDMA employs spread spectrum modulation, meaning that each user's digital waveform is spread over the entire frequency spectrum allocated to all users. Each signal in the set is given its own spreading sequence and it is distinguished from one another at the receiver by a specific spreading code [58]. In both FDMA and TDMA systems, channels should not be assigned to a mobile station on permanent basis. A fixed assignment strategy would either be extremely wasteful of the bandwidth or highly susceptible to co-channel interference. Instead, channels must be assigned on demand. Clearly, this implies the existence of a separate uplink channel on which mobile can notify the base station of their need for a traffic channel. This uplink channel is referred to as the random-access channel because of the type of strategy used to regulate access to it. This channel is shared by all users in the range of the base station.

The Commonly used duplexing schemes are frequency-division duplexing (FDD) and Time-division duplexing (TDD). In FDD. the base to mobile (downlink) and mobile to base (uplink) transmit simultaneously on different frequency bands. TDD systems use the same frequency band in both directions. which requires the downlink and uplink transmissions to occur in different time slots. Now we introduce some of the the most known wireless communication systems including the paging systems, cordless systems, and cellular systems.

2.3 Paging Systems

Paging systems are communication systems that send brief messages to a subscriber. Depending on the service, theses messages could be either a numeric message, alphanumeric message, or a voice message. In modern paging systems, news headlines, stock quotations, and faxes can be sent as messages. Paging and associated messaging, although not providing two-way voice, do provide a form of wireless mobile communications to many subscribers worldwide [16]. However, Radio paging systems has been available for many years and was well established before the dramatic growth of mobile telephone systems. In fact there are three types of paging services:

- *Tone only paging service* which is the most basic service that may be offered. A tone only pager, when signalled, notifies the subscriber with just a beep, light, or vibration. This tells its holder that someone is trying to contact him. The subscriber would generally have to telephone his office, home, or othe:: prearranged location, such as an answering service, to find the content of the communication intended for that subscriber. Different alert types can also be sued.

- *Numeric Paging Service* allows the calling party, either through a touch tone telephone or through an operator, to leave a numeric message such as a telephone number for the paging subscriber. The paging subscriber carries a liquid crystal display (LCD) pager capable of storing and displaying numeric digits. This paging service is widely used nowadays, since it gives the paging subscriber the most important information (the number he should call back), makes efficient use of paging air-time and uses economical paging receivers.

- *Alphanumeric Paging Service* allows the calling party, through an operator, or via personal computer (PC) and modem, to leave an alphanumeric message of any kind for the paging subscriber. The paging subscriber carries an LCD display pager capable of storing and displaying alphanumeric characters. This paging service is the most powerful, since it can give the paging subscriber a great deal of information (names, dates, telephone numbers, etc.). This paging mode allows the implementation of advanced new paging features such as customized financial information and news services. Chinese and Arabic character pagers also operate in this mode. Since alphanumeric paging conveys more information, it uses more air-time than numeric paging.

The most well known paging systems are:

- POCSAG which was developed by and named for the Post office code Standardization Advisory Group in the United Kingdom.

- Flex systems which use a high speed paging protocol developed by Motorola in conjunction with other paging industry leaders. Its speed is 1600bit/s and can be doubled to 3200bit/s and redoubled to 6400bit/s

- ERMES systems are conceived as a Pan-European project and designed by a team of international experts from paging manufacturers and European network operators, in full cooperation with the ETSI. The frequency band chosen was in the VHF band from 169.4 MHz to 169.8 MHz and is divided into sixteen 25KHz separate channels. The services that can be offered with ERMES system are tones only(at least 8 alerts), numeric (400 to 9000 characters), hence it is very useful for long messages. Also messages can be individual calls to each pager, group calls to several pagers using a common radio identity (RI) code or multiple RI codes. Messages can also be passed to all pagers enabled to receive them. This is very useful for information services (news. weather.

etc..). In addition to these features. ERMES has the international roaming service which means that a user can be paged in foreign countries if his home network and the visited network have the roaming agreement between them.

2.4 Cordless Telephone Systems

Cordless telephone systems are full duplex communication systems that use radio to connect a portable handset to a dedicated base station. The base station is connected to a dedicated telephone line from the Public switched telephone network (PSTN). Analog cordless telephones are in common use in residential application where the telephone cord is replaced by a wireless link to provide terminal mobility to the user within a limited radio coverage area. Digital cordless telecommunication systems are intended to provide low mobility. low power. two-way wireless voice communications. Terminal mobility is assured in residential. business and public access applications where the users can originate and receive calls on their portable terminals as they change locations and move at pedestrian speeds within the coverage area. As an example of cordless telephone systems, we find the Digital European Cordless Telecommunications (DECT) standard which is considered as a major development in the field of mobile communications in Europe [23]. DECT Was developed by ETSI, driven by widespread desire to serve the perceived market for local area portable personal communications. DECT can be described as a radio-access method to fixed networks which allows for mobile communications in areas with high traffic density. Generally it is understood as an equipment which consists of small. light handheld portable radio transceivers. capable of communicating with a base station over short distances.

2.4.1 DECT Systems

DECT is based on a micro-cellular radio communication system that provides low-power radio (cordless) access between portable parts and fixed parts at ranges up to a few hundred meters [16]. Its basic technical characteristics are as follows:

- Frequency band (forward and reverse): 1880-1900MHz.
- Number of carriers: 10.
- Carriers spacing: 1.728MHz.
- Peak transmit power: 250mW.
- Multiple access: TDMA ; 24 slots per frame.
- Frame length: 10ms
- Basic duplexing : TDD using 2 slots on same RF carrier.
- Channel rate 1152 Kbit/s.
- Net channel rates: 32 Kbit/s (voice) and 6.4 Kbits/s (control/signaling).

- Modulation: gaussian minimum shift keying (GMSK)

The DECT radio access allows the use of the concept of cellular radio in order to segment the geographical area [22]. The coverage area is divided into cells which can be very small. each cell is served by a base station being equipped such that it can accommodate a certain number of terminals simultaneously. In doing this. the distance to be covered by radio transmission becomes very small. hence the distance at which a certain channel can be reused is small as well. This concept provides extremely high spectrum efficiency [7].

2.4.2 Personal Access Communications System (PACS)

PACS is one of the American National Standards Institute (ANSI) air interface standards developed for the 1.9 GHz band in the United States. PACS has been optimized for both indoor wireless access and low-mobility pedestrian outdoor usage. PACS employs TDMA on the uplink and TDM on the downlink. using $\pi/4$ quadrature phase shift keying (QPSK) modulation at a symbol rate of 192 KBaud. The radio frame is 2.5 ms in duration with 8 bursts/frame. Each burst carries 120 bits of information including 80 bits of payload or user information and 40 bits or 20 symbols of overhead.

2.4.3 Personal Handyphone System (PHS)

PHS is the japanese air interface standard developed in 1993 by the research and development center for radio system. PHS is using TDD, frequency band 1895-1918 MHz, carrier spacing 300 KHz, with a total number of carriers equal to 77.

2.5 Cellular Mobile Radio System

The cellular radio concept relies on the distribution of many low powered transmitters (or base stations) each covering a limited area or cell. Each cell is allocated a set of channels. These channels can not be reused by adjacent cells otherwise radios would interfere. The frequency reuse concept is extremely carefully planned in cellular systems. The smaller cells are, the more often frequencies can be reused, and hence the greater the capacity [59]. There are a number of different analog cellular systems in many shapes and forms in use in the world such as the Advanced Mobile Phone System (AMPS), and the Nordic Mobile Telephone (NMT) [12]. The analog systems were originally targeted for a relatively selected group of users who mostly had the mobile telephones installed in their vehicles. However, with the availability of low-cost, small, lightweight, hand-held mobile terminals with longer battery life, and their increasing popularity for use every where, the demand for cellular mobile services has increased dramatically. With this huge demand, it is becoming difficult to accommodate the forecasted demand for mobile services within the existing analog cellular systems. There is a need for digital cellular systems to cope with the increased demand and provide a world wide standard giving a mass market services. In addition to that. unlike the first or early phase of second-generation cellular networks. only a limited set of functions related to telephony was required. Distinct features and enhanced grades of service are expected from the next generation of mobile cellular and wireless personal communication networks [74]. First-generation cellular systems are based on analog FM radio technology. With the objective of improving quality and increasing capacity. second generation cellular systems based on radio digital technology and advanced networking principals are expected to give good services with better quality. The coming generation will benefit from the current design flaws and can extend services in terms of quality and quantity to higher levels. Figure 2.3 shows the worldwide service evolution. In the following we present several cellular systems and outline the characteristics of each.

2.5.1 Cellular Digital Packet Data (CDPD)

Cellular Digital Packet Data (CDPD) is a data service for first and second generation cellular systems in the U.S. that uses unused bandwidth from the existing Advanced Mobile Phone System (AMPS) to provide wireless packet data connectivity. CDPD was designed to provide packet data services to the existing analog cellular telephone network. The basic structure of a CDPD network is similar to that of the cellular network with which it shares transmission channels. It CDPD does not use a mobile

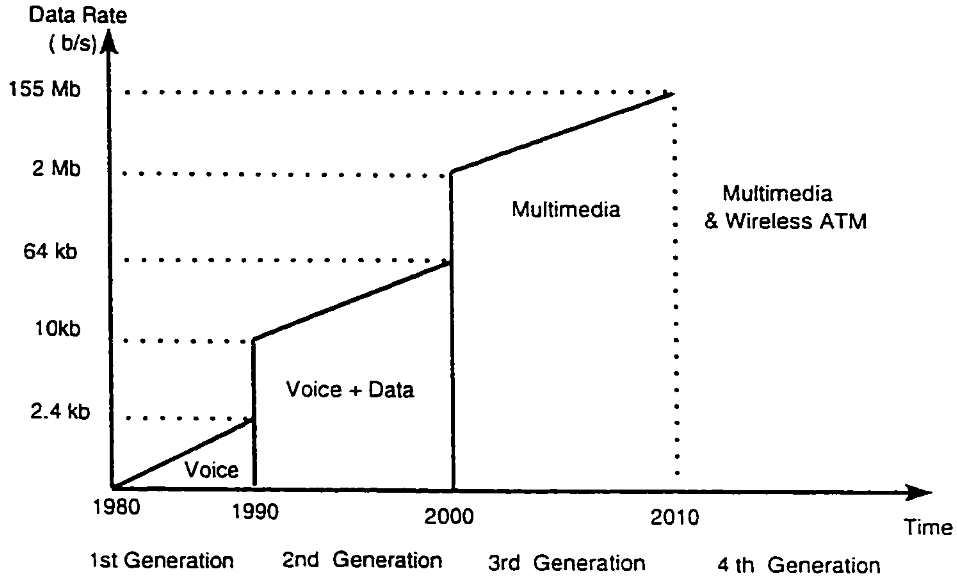


Figure 2.3: World wide service evolution

switching center (MSC), but it consists of several network entities as shown in Figure 2.4.

- Mobile End System (MES): is basically a computer with a wireless modem that communicates with a mobile database station (MDBS) through the air link

- Mobile Database Station (MDBS): is expected to be located with the cell equipment providing cellular telephone service, to facilitate the channel-sharing procedures. All the MDBSs in a service area will be linked to a mobile data intermediate system (MDIS) by microwave or wireline link.

- Mobile Data Intermediate System (MDIS): provides a function analogous to that of the Mobile Switching Center (MSC) in the GSM.

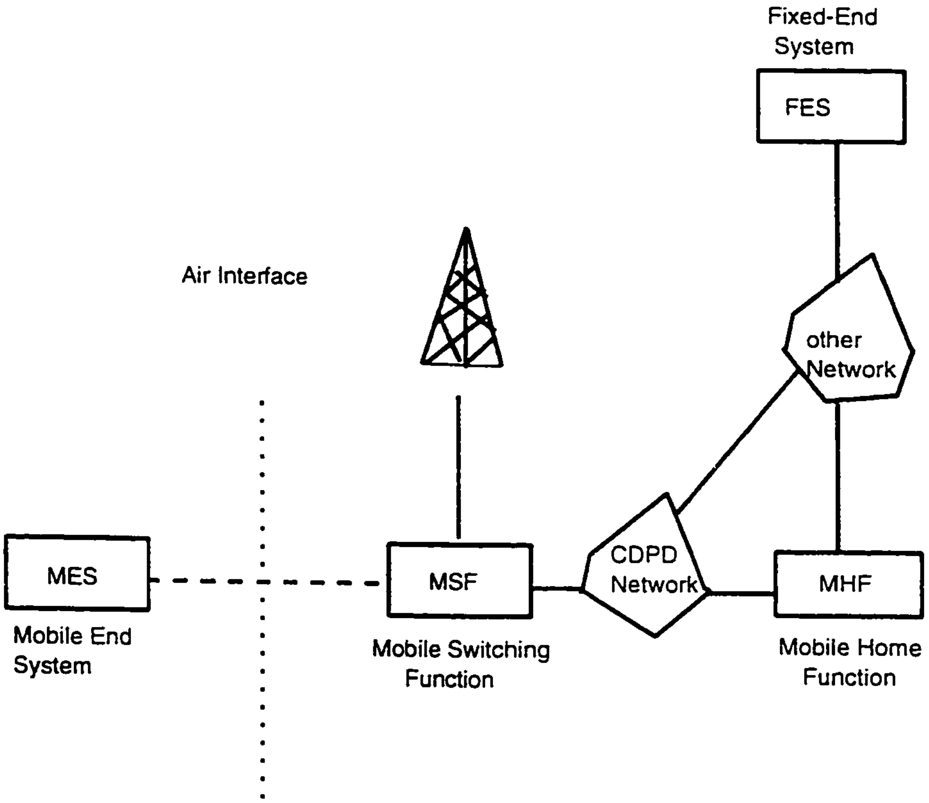


Figure 2.4: CDPD System Architecture

- Mobile home function (MHF) which provides a directory service for the users of MES by maintaining pertinent information about them.

- Mobile serving Function (MSF) which provides a registration directory to its serving area, and it transmits messages sent from the MES directly to their correct destination.

CDPD uses a multiple-access technique called digital sense multiple access (DSMA), which is closely related to carrier sense multiple access with collision detection (CSMA/CD) in local area networks. The CSMA/CD is a scheme for sharing a channel among multiple users. Each station monitors the channel before transmission and if a collision is detected the transmission is aborted and a retransmission procedure is initiated.

2.5.2 Interim Standard IS-54

The Electronic Industry Association / Telecommunications Industry Association Interim Standard (IS-54) retains the 30-KHz channel spacing of the AMPS, which uses analog frequency modulation for speech transmission and frequency shift keying for signalling [54]. IS-54 standard also supports several services, e.g., telephone service, short messages, and data services with a maximum transmission rate of 9.6 kb/s. Supplementary services include call forwarding, three party-call, and call barring. Security features include a Personal Identification Number (PIN), subscriber authentication upon connection to the system. and subscriber data encryption. Its basic technical characteristics are the following:

2.5.3 Global System for Mobile communication (GSM)

GSM is a wireless digital cellular network designed by the European standardization committees (CEPT). The system was made as a first step towards a true personal communication systems that will allow communication anywhere. anytime. and with anyone. GSM radio links use FDMA and TDMA multiple access. The frequency bands for the downlink signal and the uplink signal are 935-960Mhz and 890-915 MHz respectively and they are divided into 124 pairs of frequency duplex channels with 200 KHz carrier spacing. GSM was designed having inter-operability with ISDN in mind. Speech is the most basic teleservice provided by GSM.

2.6 Comparison

In this section we present the most known radio mobile systems in North America. Europe, and in Japan. We have chosen the most famous cellular. paging and cordless system in each area. The access method, the frequency band. the channel bandwidth, and the modulation technique are mostly the important criteria that characterize any radio mobile system. Almost all the systems presented in the following tables are using either FDMA or TDMA. However the frequency band is always different from system to another and varying from 147 MHz to 1900 MHz. using several channels with few tens of KHz. PACS. PDC. and PHS are using the DQPSK modulation. the FSK modulation in particular is used with all paging systems in the different areas. GSM standard is characterized by the use of GMSK which is considered as a strong modulation technique with several advantages over the other modulations schemes.

2.7 Summary

In this chapter, we have covered the wireless communication systems and their various characteristics. Three main categories of wireless communication systems have been presented, the paging system, the cordless systems, and the cellular systems. Systems in each category, are different from each other by their frequency band. access method used, modulation and channel bandwidth. Table 2.1. Table 2.2. and Table 2.3 outlines the most worldwide famous wireless communication systems.

Table 2.1: Major Mobile Radio Standards in North America

Standard	Type	Access Method	Frequency Band	Modulat.	Channel Bandwidth
AMPS	Cellular	FDMA	824-894 MHZ	FM	30KHz
POCSAG	Paging	Simplex	147.4-147.8 MHZ	FSK	12.5KHz
PACS	Cordless	TDMA	1.85-1.99 GHZ	DQPSK	300KHz

Table 2.2: Major Mobile Radio Standards in Europe

Standard	Type	Access Method	Frequency Band	Modulat.	Channel Bandwidth
GSM	Cellular	TDMA	890-960 MHZ	GMSK	200KHz
ERMES	Paging	FDMA	169.4-169.8 MHZ	FSK	25KHz
DECT	Cordless	TDMA	1.88-1.9 GHZ	GFSK	1.728MHz

Table 2.3: Major Mobile Radio Standards in Japan

Standard	Type	Access Method	Frequency Band	Modulat.	Channel Bandwidth
PDC	Cellular	TDMA	810-1501 MHZ	DQPSK	25KHz
NEC	Paging	FDMA	several	FSK	10KHz
PHS	Cordless	TDMA	1.895-1.907 GHZ	DQPSK	300MHz

Chapter 3

Global System for Mobile Communications (GSM)

Global System for Mobile communication (GSM) is a second generation cellular system standard that was developed to solve the fragmentation problems of the first cellular systems in Europe. With the mobile communication system, different services can be provided to customers independent of time and location [27]. Before GSM, European countries have different cellular standards where it was not possible for a customer to use mobile station throughout the continent. With the birth of GSM, mass-market mobile communications became possible. The possibility to make and receive calls through a small wireless handset, wherever you are, has more obvious appeal [27]. In fact mobile communications is not a very recent technology, but it is a rapidly evolving one, GSM is considered to be the major contribution to this evolution. Mobile services can be associated with an individual subscriber rather than a piece of equipment or a line termination. thus providing Personal Communication Services (PCS). GSM was intended to provide an integrated radio system for the mass market right across Europe and beyond ensuring international roaming. Before the GSM birth there were many European analog radio networks. their limited capacity and the lack of the compatibility with one another led to an early decision for a Pan-European system. In 1982. CEPT had alreadv formed a working committee under the name of "groupe special mobile" to develop a uniform standard for digital mobile radio in Europe. The result was a standard for narrowband (i.e.. 200 KHz bandwidth) digital voice transmission in the 900MHz frequency band [27]. A memorandum of understanding pertaining to the construction of a digital mobile radio system. was signed by the representatives of the telecommunication administrations in 14 European countries. By mid-1991. the system is ready. As in many other technological areas. communications is going through a metamorphosis, from the analog to digital. GSM is totally digital system and the benefits to the user, and the system operator are many. Through the application of digital technologies the transmission medium can be used more effectively and efficiently. Speech quality can be improved and system capacity can be increased. without, in either case, a corresponding increase in spectrum requirement. Also immunity to interference can be achieved. This means frequency bands can be reused more than often and therefore system capacity is increased [30].

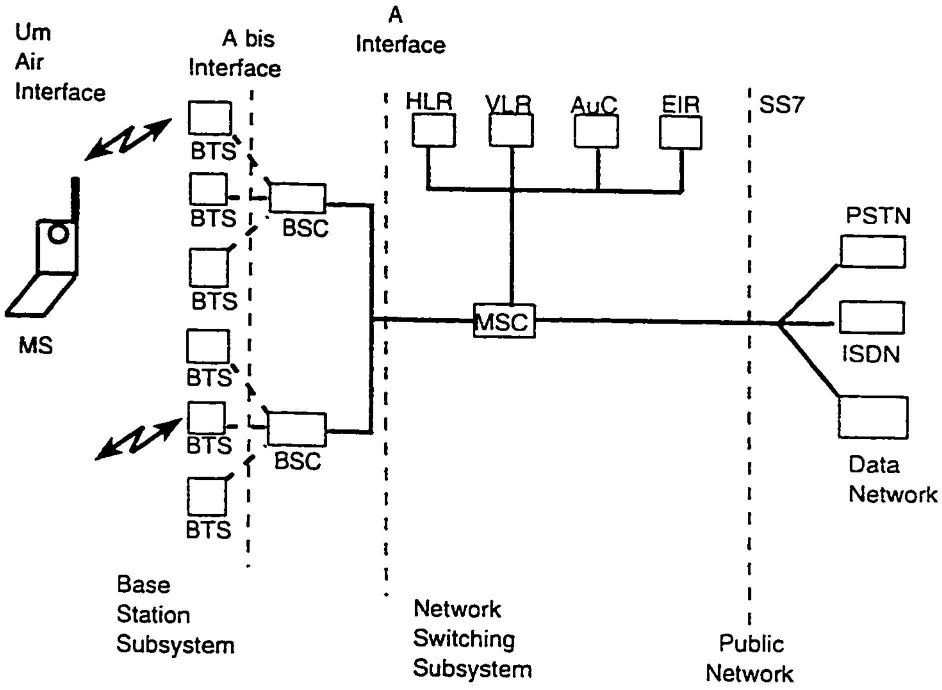


Figure 3.1: GSM System Architecture

3.1 GSM Network Architecture

GSM network can be subdivided into two major subsystems [30] as shown in Figure 3.1.

- The Base Station Subsystem (BSS).
- The Network and Switching Subsystem (NSS).

The mobile station (MS) is considered as a subsystem but is usually considered to be part of the BSS for architecture purposes.

3.1.1 Base Station Subsystem

The BSS, known as the radio network/subsystem, provides and manages radio transmission paths between the mobile stations and the Mobile Switching Center (MSC). It has all equipment needed for transmission and for controlling the connectivity of mobile subscribers. The BSS consists of many Base Station Controllers (BSC) and each one can control several Base Transceiver Stations (BTS). The BSC is connected on one side to several BTSs and on the other side to the NSS (more exactly to the MSC), and it is in charge of all the radio interface management. The Base Transceiver Station (BTS) is in contact with the mobile stations through the radio interface. BTS consists of radio transmission and reception devices including the antennas. The BSCs are physically connected via dedicated links (leased lines or microwave links) to the MSC. The interface between a BSC and MSC is called the A interface, which is standardized within the GSM. The A interface allows the service provider to use base stations and switching equipment made by different manufacturer.

- *Um air interface*: connects MSs and BTSs and it is made up of a set of physical channels that are accessible through frequency division and time division multiple access (FDMA and TDMA). Each physical channel supports a number of logical channels that are reserved for users traffic and signaling.

- *A and A bis interface*: BTSs and BSCs are interconnected through the A bis interface, whereas the BSC and the MSC are interconnected through the A interface which consists of traffic channels and signaling links used under the common Channel Signaling System No.7 (CCS7).
- *The mobile station*: consists of two parts: The subscriber Identity Module (SIM) and the Mobile Equipment (ME). The SIM is either a smart card (the same size as a credit card) or a smaller size plug-in SIM that contains the subscriber related information. The SIM is protected by a personal identity number (PIN) code chosen by the subscriber.

3.1.2 Network Switching Subsystem

The NSS manages the switching functions of the system and allow the MSCs to communicate with other networks, it also provides the external access to several customer databases. The MSC is a switching exchange forming the main core of the NSS subsystem. In addition to the MSC, there are in NSS there are four different databases:

1. Home Location Register (HLR): HLR is both a subscriber database and a set of functions needed to manage mobile user data. It contains the following type of information for each subscriber:
    - Subscription information, including identification numbers.

- Service restrictions.
- Supplementary services.
- The address of the Visitor Location Register (VLR) area for the roaming users.
- The location information for local subscribers (residing within the same area of the MSC).

2. Visitor Location Register (VLR): this database register has the IMSI (international mobile subscriber identity) which is stored temporarily, and mobile information for each roaming subscriber who is visiting the coverage area of a particular MSC. In addition to that it has the location area (LA) of a mobile user within the radio network and reachability status information. The VLR can be connected to several adjoining MSCs for a particular geographic region.

3. Authentication Center (AuC): the AuC is a strongly protected database which contains all the authentication and encryption information, needed by the HLR and VLR, for every mobile user. It protects the network against unauthorized person by denying the possibility for intruders to impersonate authorized subscribers. The AuC provides and manages the authentication keys used for authorizing subscriber access to the service provider's network.

4. The Equipment Identity Register (EIR): this database is basically to prevent the use of stolen or fraudulent MS equipment transmitting identity data not

matching with the information stored in either the HLR or the VLR. Each mobile station has its own identity information. the international mobile station equipment identity (IMEI) used to identify the equipment. The primary purpose of checking the IMEI is to guard against stolen, fraudulent. misused. or faulty mobile station equipment.

3.2 GSM Radio Interface

This interface is one of the most important interfaces for GSM. This is due to following reasons:

- The interface should be completely specified to achieve a full compatibility between mobile stations of various manufacturers and networks of different operators. This in fact is one of the main goals that should be achieved by the GSM system to give the mobility concept more freedom.
- The spectral efficiency of a cellular system which is considered as an economic factor is determined entirely by the transmission over the radio interface.

The importance of spectral efficiency is best understood when it is defined as the number of cells needed to cover a given area with a specific traffic and a given amount of radio spectrum. Spectral efficiency depends on the number of simultaneous calls which can be carried within the available spectrum. The better the efficiency, the lower the number of cells. The main concern for the design of the radio interface is to provide a high user capacity relative to the given limited radio spectrum and to transport the information efficiently.

3.2.1 GSM Radio Channels

The GSM system operates at 900 MHz and at 1800 MHz (for Digital Cellular System DCS). For the 900 MHz, there are two bands of 25 MHz which have been set a side for system use in all member countries. The 890-915 MHz band is used for MS to BTS transmission as the reverse link (uplink), and the 935-960 MHz band is used for base station to user transmission as forward link (downlink). The frequency band is divided into 124 pairs of frequency duplex channels with 200 KHz carrier spacing. The length of a GSM time frame in a frequency channel is 4.616 msec. The time frame is divided into eight time slots of length 0.577 msec. The time slots in the uplink are derived from the downlink by a delay of three time slots. This arrangement avoids transmission and receiving at the same time by mobile station. Based on the GSM concept, logical channels for users and signaling information are generated from the physical channels by means of appropriate mapping functions. A logical channel describes the function of a physical channel at a given time (frequency correction, speech transmission), whereas physical channel refers to every occurrence of a particular slot on a particular frequency, or a set of frequencies. In fact there are two basic types of GSM logical channels:

1. Traffic Channels: TCH

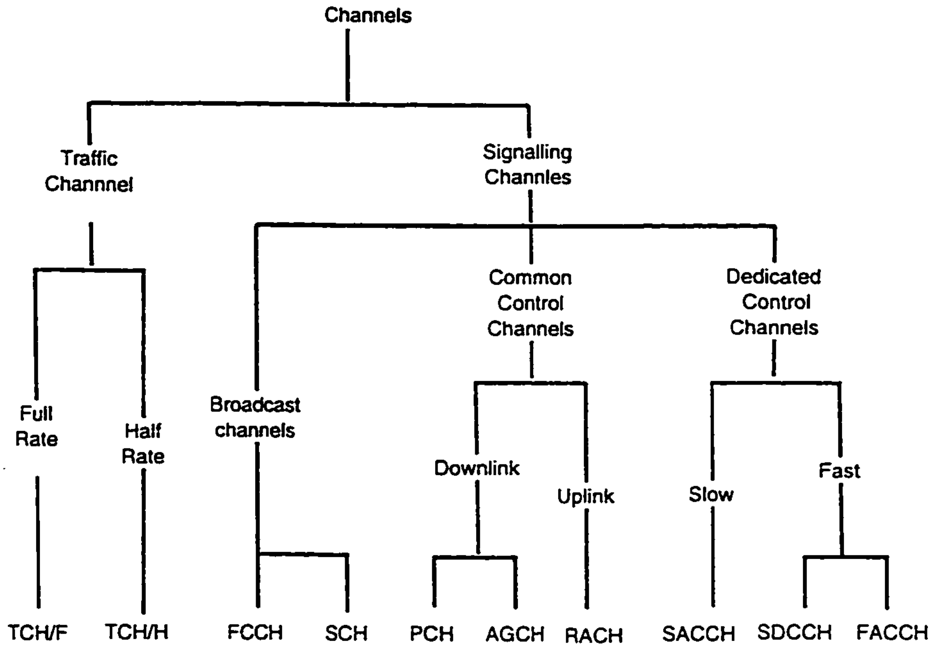


Figure 3.2: GSM Channels Structure

2. Control/signalling Channels: CCH

Traffic channels carry digitally encoded user information (voice or data) and they have identical formats and functions on both the forward and reverse links. In addition, there are logical subchannels that are used for control and supervision while the mobile is assigned a traffic channel. An example of this subchannels is the sending of a handover order to the mobile during a voice call. Control channels are typically used for call setup and they are carrying signaling and synchronizing commands between the base station and the mobile station as shown in Figure 3.2. Control channels are usually subdivided into three groups

1. Broadcast Channels (BCCH): these are used to inform the MS about system configuration parameters and are defined for the BTS to MS direction (downlink) only. BCCHs are subdivided into two subchannels:

   - The FCCH (Frequency Correction Channel) supports frequency synchronization of the MS.

   - The SCH (Synchronization channel) gives the MS information about the frame number.

2. Common Control Channels (CCCH): channels are specified as unidirectional only, either on the downlink or on the uplink. Also CCCH are subdivided into three subchannels:

   - The Paging Channel (PCH): used in downlink to page MSs.

   - The Access Grant Channel (AGCH) is used in downlink direction. to allocate a dedicated channel.

   - The Random Access Channel (RACH): it is an uplink channel that indicates an MS's request for a dedicated channel.

3. Dedicated Control Channel (DCCH): DCCH are full duplex channels, and subdivided into three subchannels:

   - Slow Associated Control Channel (SACCH) which is a duplex channel always associated with a TCH or Stand-Alone Dedicated Channel (SD-

CCH). It is also used for transmission of signalling data.

- Fast Associated Control Channel (FACCH) used to transmit signalling data when the capacity of the SACCH is not enough. The FACCH data are inserted into the associated TCH instead of traffic data.
- SDCCH which is used only for signaling in higher layers.

3.2.2 The Multiple Access Methods in GSM

A radio channel is fundamentally a broadcast communication medium. Signals transmitted by one user can potentially be received by all other users within the range of the transmitter. Many techniques have been devised to create channels out of the communication medium, in order to use them as separate links. A given radio spectrum can be divided into a set of disjoint or interfering radio channels. All the channels can be used simultaneously while maintaining an accepted received radio signal. Multiple access in wireless radio systems is based on insulating signals used in different connections from each other. The support of parallel transmissions on the uplink and downlink, respectively, is called multiple access which is used to allow many mobile users to share simultaneously a finite amount of radio spectrum. GSM system uses time division multiple access (TDMA) combined with frequency multiple access (FDMA), and a pinch of frequency hopping (FH) scheme, to provide base stations with simultaneous access to multiple users. With frequency hopping, each TDMA burst is transmitted via a different RF channel (RFCH). Thus. if the present TDMA burst happened to be in a deep fade. then the next burst most probably will not be.

- The FDMA assigns individual channels to individual users. Channels are assigned on demand to users who request service. During the period of the call. no other user can share the same frequency band.

- The TDMA divides the radio spectrum into time slots. and in each slot only one user is allowed to either transmit or receive. In this technique. each user occupies a cyclically repeating time slot. so a channel may be thought of as particular time slot that reoccurs every frame. TDMA scheme uses a gross bit rate of about 270 kb/s (with a Gaussian Minimum Shift Keying Modulation. GMSK) and requires sophisticated adaptive receiver techniques to cope with the transmission problems caused by multipath fading.

3.3 Mobility Management

Mobility management is the process of keeping track of users so that calls arriving for them can be directed to their current location [26]. The second concern in mobility management is the handoff process.

3.3.1 Location Tracking

The mobile tracking function is responsible for maintaining knowledge of the approximate location of the mobile user. Tracking procedures include registration upon power-up. power-down, and location area changed [31]. The location of the mobile station is an important issue and usually is maintained by two-level hierarchical strategy with home location register (HLR) and the visitor location register (VLR). When a mobile station is in its home location. it can be accessed directly through its HLR. When the mobile leaves its home register and moves to another location. it must register in the visitor location register (VLR) of the visited area. The home register must also be informed of this registration. To access the mobile station. the HLR is queried to find the current VLR of the mobile station [65]. The registration process is described in the following steps:

Step 1: When a mobile station moves to a new cell. it listens to the BCCH broadcast from the base station subsystem. When mobile station detects that it has entered a new location area, it sends its temporary mobile subscriber identity (TMSI) and the old location area to the new mobile switching center which forwards it to the new visitor location register (VLR).

Step 2: From the TMSI and the old location area identity, the new VLR identifies the old VLR, then sends a message to it in order to obtain the international subscriber identity (IMSI) of the mobile station. In response, the old visitor location register returns the IMSI as well as the authentication parameters to the new VLR which performs the authentication process.

Step 3: The new VLR sends an update location message to the old home location (HLR) whose address is derived from the IMSI. If the update request is accepted, the HLR provides the new visitor location register all relevant subscriber information for call handling.

Step 4: The new VLR generates a new TMSI and sends it to the the mobile station through the mobile switching center. The mobile station acknowledges the TSMI allocation.

Step 5: After step 3, the HLR sends a cancel location message to the old VLR, which acknowledges that and cancels the record for the mobile station.

3.3.2 Handover Management

When a mobile user is in conversation, a radio link connects the mobile phone to a base station. If that user moves to another base station's coverage area, the radio link to the old base station is disconnected, and a radio link in the new base station is required to continue the conversation. This process is called automatic link transfer or handoff. If there is no available channel to which the call should be switched to, the call may be dropped or terminated. The forced termination probability is an important criterion in the performance evaluation of the network. Handover may take place between physical radio channels that may belong to the

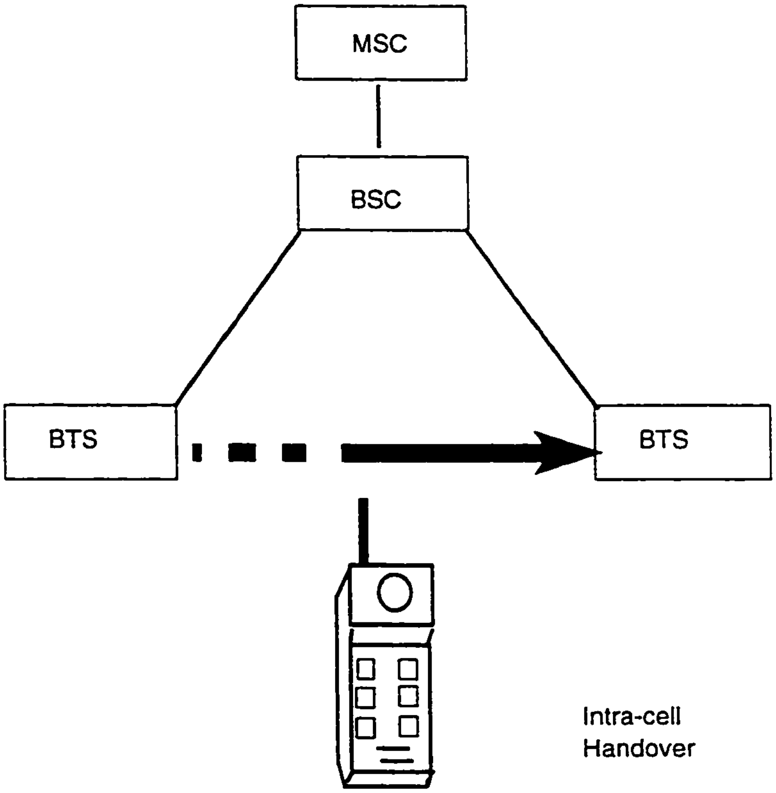


Figure 3.3: Intracell Handover

same BTS (intra-cell handover) or to different BTS (inter-cell handover). Handover controlled by the MSC is called external handover. and handover controlled by the BSS is called internal handover.

- Intra-cell handover occurs within a single BSC which controls all decisions as shown in Figure 3.3. Intra-cell handover can occur without the involvement of the MSC but the system has to inform the MSC upon completion.

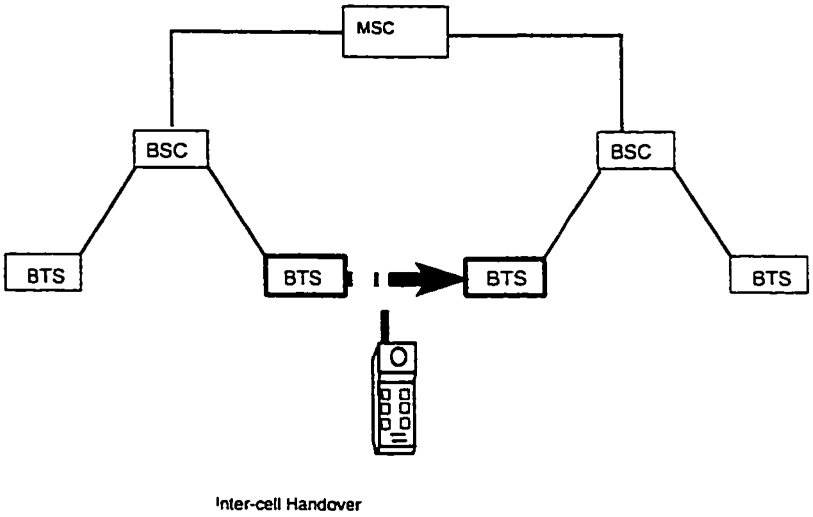


Figure 3.4: Intercell Handover

- Inter-cell handovers occurs between two different BSCs on the same MSC. Here the MSC and BSC coordinate together to perform inter-BSC handovers, but the decision is taken by the BSC as illustrated in Figure 3.4.

- Inter-MSC Handovers occurs between two BSCs on different MSCs. Here the MSC takes the decision to perform the handover as shown in Figure 3.5.

Three strategies exist to detect the need for hand-off [40]:

1. Portable-controlled handoff

2. Network-controlled handoff.

3. Portable-assisted hand-off.

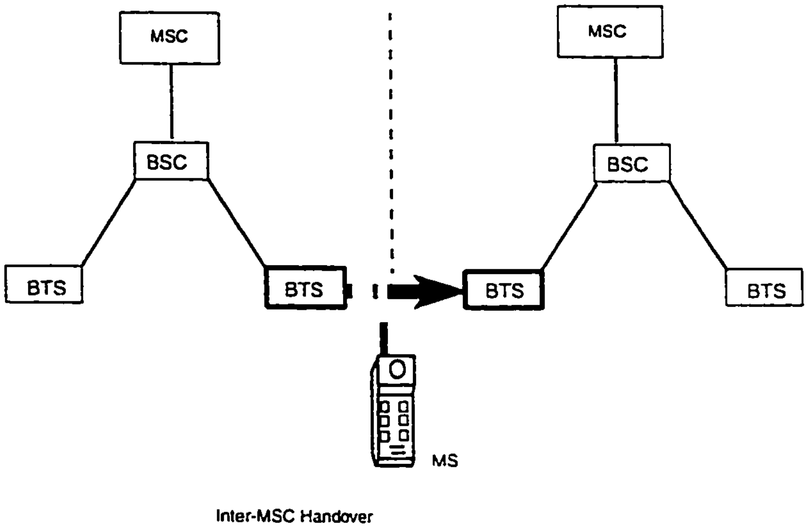


Figure 3.5: Inter-MSC Handover

The first one is the most popular technique , where the portable continuously monitors the signal strength and quality from the accessed base station and several hand-off candidate base stations. When some hand-off criteria is met. the portable checks the best candidate base station for an available traffic channel and launches a hand-off request. This technique is actually used by DECT and PACS systems. In network-controlled hand-off, the base station monitors the signal strength and quality from the portable and when these deteriorate below some threshold, the network arranges for a hand-off to another port. The network asks all the surrounding base stations to monitor the signal from the portable and report the measurement results back to the network. The network then chooses a new base station for the hand-off and informs both the portable(through the old base station) and the new base station. This kind of hand-off is mostly employed with CT2 and AMPS systems. Portable-assisted hand-off is a variant of network-controlled hand-off where the network asks the portable to measure the signals from the surrounding base stations and report those measurements back to the old base station so that the network can determine as to where a hand-off is required and to which base station. This strategy is employed by the GSM mobile standard. In current cellular mobile systems, base stations handle a hand-off call exactly the same as an originating call (that is, the hand-off call is blocked immediately if no channel is available). This is called the non-prioritized scheme. To reduce forced termination and to promote call completion, three schemes have been proposed.

- The reserved channel scheme is similar to the nonprioritized scheme, except that each base station reserves a number of channels for handoff calls.

- The queuing priority scheme exploits the characteristic overlap of adjacent coverage areas of base stations. This overlap (it is called handoff area) forms a considerable area where either base station can handle a call. If no channel is available in the new base station during handoff, the new base station buffers the hand-off request in a waiting queue. The mobile phone continues to use the channel with the old base station until either a channel in the new base station becomes available (and the handoff is connected) or the mobile phone moves out of the handoff area (and the handoff call is forced terminated).

- The subrating scheme creates a new channel for a handoff call by subrating an existing call if no channel is available in the new base station. Subrating means an occupied full-rate channel is temporarily divided into two channels at half the original rate: one to serve the existing call and the other to serve the handoff request. When the occupied channels are released, the subrate channels switch back to the full-rate channel immediately. The last two schemes have not been implemented in existing cellular communication systems. However, studies indicate that under certain conditions, these schemes can significantly improve the forced termination probability as well as the call incompletion. The selection of a particular scheme is a trade-off between the implementation cost and the performance.

3.4 Roaming

Roaming can be provided only if some administrative and technical constraints are met, like charging, and subscription agreements. There are two basic operation in roaming management: location update and terminal paging [41]. Location update is concerned with the reporting of the up-to-date cell locations by the mobile terminals. GSM networks partition their coverage areas into a number of location areas (LA). Each LA consists of a group of cells and each mobile terminal performs a location update whenever it enters an LA.

When an incoming call arrives. the network locates the mobile terminal by simultaneously paging all cells within the LA. Location updating is always initiated by the mobile station and it is carried out when the MS enters a new location area. The MS is periodically monitoring the location information broadcasted by the network on the broadcast channel. and compares it to the information previously stored in its memory. Also the MS can initiate o location update on receiving an indication from the network that it is not known in the VLR upon trying to establish a mobility management (MM) connection [25]. When an incoming call arrives. the network simply routes the call to the last reported location of that mobile user. There are four principal types of location update methods.

1. Geographic: a user updates the system when it enters a new location area.
2. Timer: the user updates the location periodically with a given average time.
3. Stimulus: the user performs a location update only when requested.
4. ON/OFF: a location update occurs only after a mobile powers on and before a mobile powers down.

The network registers the user's location in the Home Location Register HLR. Paging messages for mobile are sent to the BSS. Paging messages may include the mobile's IMSI in order to allow derivation of the paging population number. A single paging message transmitted to the BSS may contain a list of cells in which the page is to be broadcasted. The larger the paging area is defined, the lower the frequency of location updates and hence the associated traffic overhead on the network. Each paging message relates to only one mobile station, if the response message is received from the mobile, the relevant signaling connection is set up towards the MSC and the page response message is passed to the MSC.

3.5 Signaling System No.7

With the rapid growth of telecommunications, signaling methods have become more important and get a crucial role in the network architecture. Signaling constitutes the command/control infrastructure of the modern telecommunication networks, and considered as the central nervous system of a living organism. Generally, signaling is defined as the system that enables digital switching systems, network databases, and other intelligent nodes of the network to exchange messages related to call setup, supervision, teardown, information needed for distributed application processing (inter-process query/response, or user to user data), and network management information [43]. Common channel signaling (CCS) is an out-of band signaling method in which data

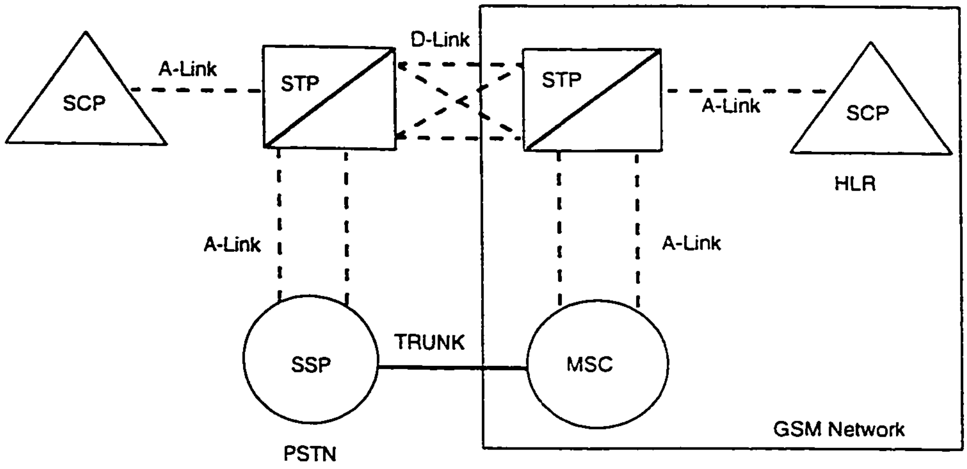


Figure 3.6: SS7 Network Architecture

channel is used to convey signaling information related to call control and network management in the telephone network. Signaling System Number 7 (SS7) issued in 1980 by the International Consultative Committee for Telephone and Telegraph (CCITT), is a CCS system with a set of protocol standards developed to satisfy the telephone operating companies' requirements for an improvement to the earlier signaling systems. The SS7 network has three distinct components as depicted in Figure 3.6:

– A service switching points (SSP) is a telephone switch interconnected by SS7 performing call processing on calls that originate, tandem (pass through) or terminates at the SSP. The MSC is an SSP with specific functions for cellular communications.

- A service control point (SCP) contains databases for providing enhanced services. An SCP accepts queries from an SSP and returns the requested information to the SSP. The 800-service database is an example of an SCP.

- A signal transfer point (STP) is a switch that relays SS7 messages between SSPs and SCPs. Based on the address fields of the SS7 messages. the STPs route the messages to the appropriate outgoing signaling links [43]. An SCP may contains an HLR or a VLR. There are six types of SS7 signaling links, the most important links are the signal link referred as the Access link (A-link). A-links are used between SSPs and STPs and can be up to 128, but generally is 16 only. A-links also connect SSPs and SCPs. Signaling links that connect STPs of different networks (GSM networks, PSTN) are called D-links. their maximum set size is 64.

3.6 The SS7 architecture

Similar to the Open System Interconnection (OSI) reference model. SS7 is based on a layered protocol architecture consisting of four functional levels as illustrated in Figure 3.7.

The lower three levels form the Message Transfer Part (MTP), which provides a simple and reliable connectionless (datagram style) service

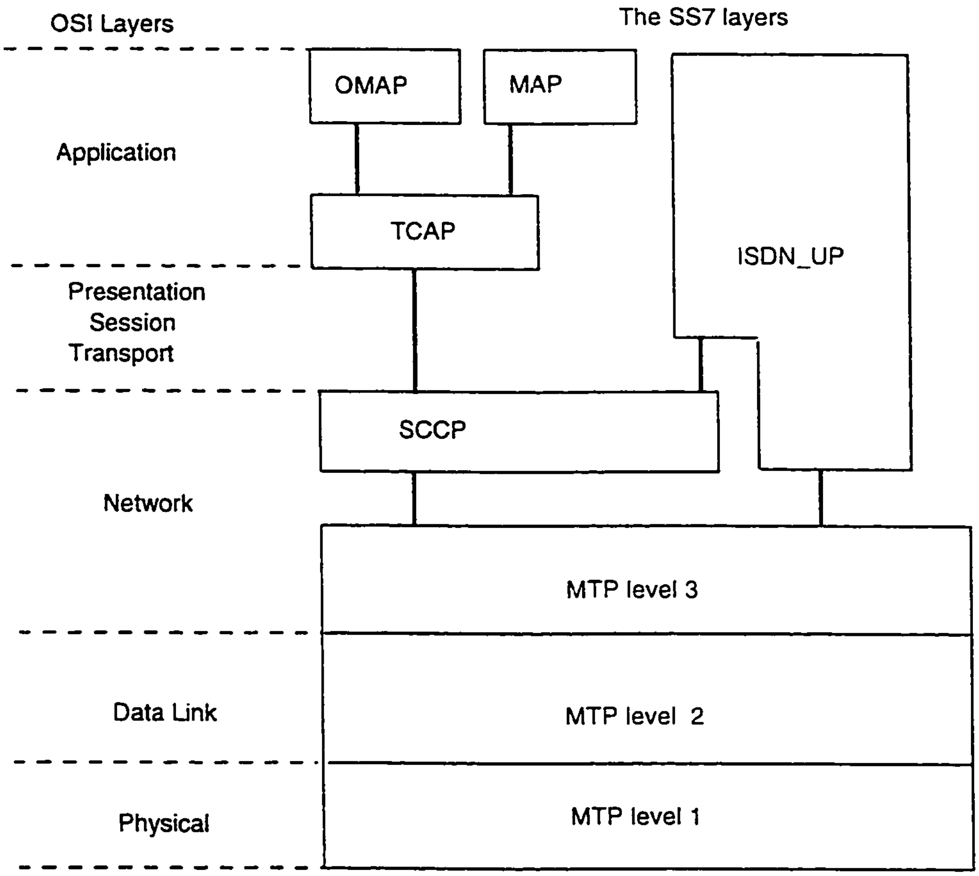


Figure 3.7: SS7 Protocol Architecture

for routing messages through the SS7 network [35]. The fourth level is known as the Signaling connection control part (SCCP). The SCCP and the MTP together form the network service part (NSP). The remaining parts deal with the actual contents of the messages. The Transaction Capabilities Application Part (TCAP) provides the ability to exchange information between applications using non-circuit related signaling. The Integrated Services User Part (ISUP) establishes circuit-switched network connections (e.g., call setup/release).

3.7 Summary

GSM, the global system for mobile communications, is a digital cellular communications standard which has rapidly gained a worldwide acceptance. In this chapter we have presented the GSM network with more emphasis on the system structure, network architecture, radio interface and mobility management. In addition to the above important parts, the signaling system No.7 (SS7) is covered since it is the official signaling protocol used in all GSM networks.

Chapter 4

Networks Security

The need for security in communications was recognized long time ago when messengers used to carry information from one place to another. Nowadays with the distributed nature of network systems, still people want to communicate privately, and the achievement of privacy and security has become increasingly important. A main characteristic of mobile communication systems is that they provide wireless access to traditional wireline networks. However, wireless transmission is vulnerable to relatively easy interception, such as fraudulent call attempts and intrusion or listening-in by third parties. This requires that special measures have to be taken to avoid any attempt of intrusion. For example, sensitive data must be protected against disclosure to an unauthorized person, fraudulent modification of messages, repeating old messages, or any kind of masquerading must be prevented [34]. All information, when transmitted over the air interface become more vulnerable to eavesdropping. For this reason, a feasible solution for implementation of secure mobile communication systems is needed. The greatest challenge in future networks will be to produce services that customers can trust. Combined with their needs for mobility, usability and global reach, this represents a difficult goal. In this chapter the security aspect in mobile communication systems will be presented.

4.1 Cryptosystem Techniques

The study of different ways to disguise messages in order to avert unauthorized interception is called cryptography [11]. Using cryptosystem in communications was mainly to prevent unauthorized persons from extracting information from the channel (eavesdropping) and also to perform the authentication process. The basic idea of cryptographic authentication consists of challenging the user or communicating party being authenticated to prove its identity by demonstrating ability to encipher or decipher some items with a secret or private key. For the privacy, the best way to protect the confidentiality of data transferred between different network resources is with encryption [5]. Encryption is a transformation of data that varies based on a secret parameter called an encryption key [13]. Data transformed (or encrypted) using an encryption key is scrambled in such a way that it can be unscrambled (or decrypted) by a similar transformation, the scrambled data is called ciphertext, and the original data is called plaintext. Most of the Encryption schemes are using two techniques:

- block encryption.
- stream encryption.

With block encryption, the plaintext is segmented into blocks of fixed size [5]; each block is encrypted independently from the others. In stream encryption, there is no fixed block size. Cryptosystem fall into two generic categories:

1. Symmetric cryptosystem, using the secret-keys.
2. Asymmetric cryptosystem, using public-key, secret key pair.

4.1.1 Secret-Key Cryptography

In a secret-key algorithm, the sender S and the receiver R share a secret key. S generates the ciphertext C=E(K,M) corresponding to the plaintext message M to be transmitted by applying an encryption transformation

E that is dependent on the key K [67].

The receiver R recovers the original plaintext M=D(K,C) from the ciphertext that it receives by applying a decrypting transformation D which is also dependent on K.

If R responds to S, it uses the same key K for encryption and S does the decryption. The data encryption standard (DES), is currently the most widely used secret-key algorithm. It encrypts 64-bit blocks of data with a 56-bit key permuting each input block passing the permuted block through 16 iterations of a function that combines substitution and transposition, performing exchange and XOR operations between the iterations and permuting again to give the resulting output block. Using symmetric cryptosystem, both the party encrypting the data, and the party decrypting it must share the same encryption key. This means that a user needs a different key for every user or service provider with which it exchanges information or messages, and each service provider would have to maintain a key for every potential customer.

4.1.2 Public-Key Cryptography

In a public key algorithm, the message is encrypted using a public key and decrypted using a private key. The public key cannot be used for decryption. To send ciphertext to R, S encrypts the plaintext data to be transmitted using R's public key K_{ru}.

When R receives the ciphertext, it decrypts it with its private key K_{rv}. Communication in the reverse direction proceeds in an analogous manner, with R encrypting plaintext using S's public key K_{su} and S decrypting it with its private key K_{sv}. Public-key suffer from the drawback of a slower cipher speed, because of the enormous amounts of processing involved [20]. There are several public-key algorithms, the Rivest-Shamir-Adelman (RSA) is one of the most widely applied algorithms. The principal advantage of asymmetric cryptography is that secrecy is not needed for the public key, meaning that only a single key pair is needed to be generated for each user or service provider, and dissemination of the keys is easier [51]. The principal disadvantage of asymmetric cryptography is its performance. As we have mentioned earlier, asymmetric cryptosystem are significantly slower than their symmetric counterparts. Because of the performance issues, asymmetric cryptography is rarely used in isolation. Instead it is used to encrypt a symmetric encryption key and checksum, which are in turn used to protect the actual data [7].

4.2 Security in Some Wireless Systems

The use of radio path allows a number of potential threats and weaknesses [18], therefore in developing any new Security system the following points have to be considered:

- The security system has to be adequate for system operator and customers.
- The radio path has to be as secure as the fixed network.
- A strong Authentication process is needed, to protect the operator against billing fraud.
- The security process must not significantly add to the delay of the initial call set up or subsequent communications;
- The bandwidth of the channel should be preserved.
- The process must not allow for increased error rates, or error propagation.
- The security system should not add excessive complexity to the rest of the system and has to be cost effective.
- Domain-specific secret or sensitive information such as the user's secret key or password should not be propagated from the home domain to a foreign domain or between foreign domains.

* Authentication in foreign domains should have minimal impact on the user interface with respect to authentication in the home domain [7].

* Messages exchanged between the home domain and the foreign domain should be kept to minimal.

4.2.1 User Authentication

Nowadays, there is an extensive use of open networks and distributed systems, that it seems to be impossible to live without these information sharing facilities. Public telecommunication networks involve the billing of their customers. With the existence of radio access, there are opportunities for fraud to be committed, such as the non billing of calls or service provided and the billing of the wrong party for these calls and services [3]. To prevent the possibility of such fraud, or the general impersonation of other subscribers, a strong authentication process to identify users has to be taken. The technique used to assure such security level is the authentication technique. The most common method of user authentication is the use of passwords. A password is a string of characters assumed to be known only to the system and the user. However in a networking environment, this method is seldom secure since the password, which is a long term secret that is changed infrequently (stored in a table), has to flow over the wire. If an eavesdropper get access to the table or picks up the password, he can masquerade as the legitimate user and gain access to all resources that the user can access for as long as his behavior is not detected and the password is not changed. This widespread but old technique has several weaknesses [8]:

- Passwords are transmitted in the clear: in most password systems, the password typed by a user is sent in cleartext over the network. This means that an intruder equipped with suitable tools can tap network lines and spy on passing traffic to collect passwords.
- Passwords are easy to guess: Since users need to memorize their passwords, they typically select passwords from within a relatively small vocabulary that they can easily remember. Thus simple attacks are also possible and passwords can be guessed by potential intruders.
- Passwords are one-way authentication: password schemes are typically used for one-way authentication only, i.e., servers ask users for their passwords, but users never question that they are communicating with the right servers, and thus never challenge a server to provide any passwords.

However, there exist many alternative techniques to password-based authentication, where users do not have to remember anything so that the risk of an intruder guessing a password is not existent. For instance, some systems base authentication on recognition of biometric information such as a voice sample, a finger-print, or a hand signature. These authentication techniques have reliability problems and require relatively expensive hardware support, so that they are found only in selected high-security environments, not in general-purpose network environment. With such techniques, users are typically provided with smart cards or chip cards equipped with a processor capable of cryptographic operations. These cards offer a way to communicate either with their owner (through a liquid-crystal display and possibly a numeric keypad) or directly with a computer/server (through an electronic interface).

4.2.2 CDPD Authentication Protocol

CDPD was developed by a consortium of several US-based leading telecommunication companies. It is intended to provide digital data transmission using existing free slots in existing cellular voice communication networks. CDPD network provides also different security services such as message confidentiality, user authentication, and key distribution. CDPD requires a logically distinct entity used as an authentication server (AS) to be present in every domain area. The AS is typically co-located with the mobile data intermediate system (MDIS) in a service provider's domain. Authentication always involves contacting the AS in the home domain. The authentication process is as follows:

Step1: before starting any type of communication, a secret key, K_r is shared between mobile unit MES and serving MDIS.

Step2: MES generates a random number and sends a triplet of network equipment Identifier (NEI), Authentication Random Number (ARN) and Authentication Sequence Number(ASN) with key K_r.

Step3: Serving MDIS decrypts the triplet and sends the plain triplet to home MDIS.

Step4: The home MDIS passes the triplet to authentication server (a logical part of home MDIS which evaluates the authenticity of the MES, then the Home MDIS sends the reply to serving MDIS.

Step5: if the home MDIS's reply is positive, then an acceptance is sent to the MES otherwise the request will be rejected.

4.2.3 Privacy and Authentication in IS-41

IS-41 is the Interim standard used in North America for locating users. The authentication process in IS-41 is as follow:

Step1: The handset determines, based on the signal transmitted by the base station, that it has entered a new Registration Area (RA) and that authentication is required to access the network. Using its secret key (shared secret data, SSD) and the Electronic serial number. the mobile identification number (MIN), and a random number obtained from the PCS service provider (PSP), the handset execute all this input data through the Cellular Authentication and Voice Encryption (CAVE) algorithm to get a registration authentication result (AUTHR).

Step2: The handset requests registration with the PSP by supplying an authentication result (AUTHR), its electronic serial number (ESN), MIN, the most significant 8 bits of RAND, and a certain COUNT where the most significant events are registered (registration, call origination, termination). This call history count is maintained by the authentication center.

Step3: The PSP system forwards the authentication request in an AUTHRQST message to the VLR serving the PSP registration area.

Step4: The VLR forwards the request to the HLR along with all the parameters it received.

Step5: In turn the HLR forwards the authentication request to the AC.

Step6: The AC retrieves from its database the SSD associated with the MIN and with the other parameters (MIN,ESN,RAND) executes the CAVE algorithm to produce the authentication result (AUTHR).

Step7: After verifying that the received result is the same as the result generated locally and the COUNT values are identical, the AC provides its response to the authentication request which eventually will be forwarded to the PSP system.

4.2.4 Security Aspect in PACS

The Personal Access Communication System (PACS) is an American National standards institute air interface standards developed for the 1.9 Ghz PCS band in the United States. The goal of the PACS security mechanism is to make it impractical for an eavesdropper to obtain sufficient information for perpetrating usage fraud. The mechanism is assured through an authentication and key agreement (AKA) protocol which in turn can support either public key AKA protocol or private key AKA protocol. The authentication consists of the verification of the user identification. Each user has a unique identifier provided by the service provider. Removing the user secret information can be done to create cloned Subscriber Unit (SU). A call counter (which indicates the call history of an SU) is used to prevent SU cloning . We notice here that PACS has a system information channel (SIC) in the System Broadcast Channel (SBC). The SIC carries a RAND and the real time used in the ciphering. As these parameters are broadcasted all the time in the SIC, the handset can perform the authentication algorithm without receiving any direct message from the network and can send the response AUTHR together with the real time parameter in the AUTH-REQ message.

4.2.5 Security in DECT System

The authentication of a portable radio termination (PT) service enables a DECT fixed radio termination(FT) to verify the identity of a PT attempting to make or receive a call through it. The service is provided using a cryptographic challenge-response (or dynamic password) mechanism. The DECT FT issues a random challenge RANDF to the PT, which responds by returning the result RES1 of this challenge transformed using a cryptographic algorithm with an authentication key K uniquely associated with it. The FT then compares RES1 with value XRES1 which it expects to receive, and the authentication is considered successful if these two values agree. DECT system uses a smart card DECT Authentication Module (DAM) which is like the SIM card in GSM. DAM as well as SIM add an extra level of mobility and allow users to move and make calls independent of the time and location.

4.3 Security in GSM Networks

The major feature of wireless communication is the usage of air radio as a conveyor of message (voice, data, and signalling information) which provides its users the ability to exchange messages or access services through a variety of communication media. However, the easy access to the radio links also makes radio transmission more prone to eavesdropping and system intruding [31]. GSM has brought significant improvements in these matters. The security-related functions of GSM are intended to achieve two goals:

1. Protecting the network against unauthorized access and is implemented by means of a strong authentication process.
2. Protecting the privacy of users.

4.3.1 Authentication Process in GSM

As a first step of security. GSM make use of the personal identity number (PIN) code in conjunction with the SIM. This code is chosen by the subscriber and is locally checked by the SIM itself. without being transmitted on the radio interface. In addition a more sophisticated method is carried out to achieve the authentication process and it utilizes a challenge/response technique [36]. This technique consists of asking a question that only the right subscriber equipment (in this case.the SIM) may answer. The crux of this method is that a huge number of such questions exist but it is very unlikely that the same question would be used twice. More precisely, the question takes the guise of a number RAND whose value is drawn randomly. The expected answer for this question is called SRES (signed result), and it is obtained as the outcome of a computation involving a secret parameter specific to the user, called K_i. The secrecy of K_i is the cornerstone on which all the security mechanisms are based. The procedure is carried out as follows:

* A challenge/response pair, called RAND/SRES, is generated if the user is being served by its home network. The 128-bit RAND is generated locally by HLR/AuC and then combined with the User's K_i through the (A3) algorithm to get the 32-bit SRES.

- * Now once SRES is ready in the home network. RAND is then sent to the MS and the computation of a local SRES is performed by combining the RAND with the K_i (stored in the SIM) through A3.
- * SRES (locally computed in SIM) is sent to the network for comparison with the SRES (computed in the network). if the two SRES are equal the MS is authenticated.

Each time a mobile station is authenticated. the network and the MS has to compute the ciphering key (K_c) which is used for ciphering and deciphering of transmitted data. The ciphering key K_c computation is basically similar to the SRES and it is carried in both the network and the MS. The algorithm used is A8. Once we have the K_c. ciphering and deciphering are performed by applying an exclusive OR operation between the radio burst and a ciphering sequence using a specific algorithm called A5 as shown in Figure 4.1.

4.3.2 Subscriber Identity Module (SIM)

GSM is the first International system employing a smart card(or SIM card) as a secure device for the authentication of the subscription and the subscriber. In fact the idea of using a microprocessor or smart card in a mobile network goes back to the early 1980s and was implemented

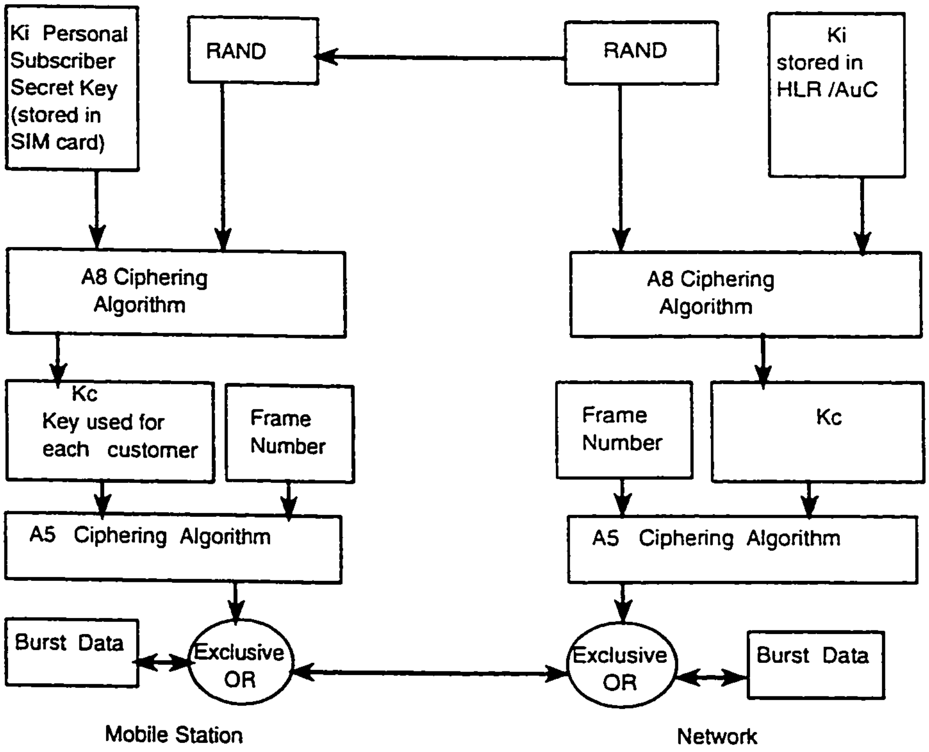


Figure 4.1: The Ciphering Process

in Germany in their analogue mobile network. The SIM gives the network operator control over all subscription and security related data. In addition to that, the concept of a removable SIM adds a new dimension of mobility to the customer. SIM and the authentication centre play the main role in the authentication process of the subscriber. Both of them contain the authentication algorithm A3 and K_i. The tasks of the SIM as a security device require the execution of complex algorithms and storage of the associated keys. The SIM itself controls user access by verifying the PIN offered by the user against a reference PIN stored in its memory. The comparison is done by the CPU of the SIM which ensures that the valid PIN does not leave the SIM. The PIN can be freely chosen and changed by the user within the range of four to eight digits. It is protected against trial and error attacks as the microcomputer records the number of consecutive false PIN entries. After three such entries, IMSI and temporary identity are not readable any longer and the ME cannot set up a connection. Access is blocked even if the SIM has been removed or a different ME is used. Another important aspect of the SIM is related to roaming. Roaming can be achieved by using the same ME to get service from two different networks with a single subscription. This flexibility allows inter-operability at a much larger scale between system based on different radio techniques. Instead of carrying the mobile station, the user would only take his SIM with him and use it with a different mobile equipment adapted to the networks to be accessed.

4.3.3 User Protection Technique in GSM

Encryption is considered as an efficient method for confidentiality, but cannot be used to protect every single exchange on the radio path. Ciphering with K_c applies only when the network knows the identity of the subscriber it is talking to. It is obvious, that ciphering cannot be applied to common channels, such as the BCCH, since it is received simultaneously by all mobile stations in any cell and its neighboring cells. For an MS moving to a dedicated channel, there is a very small period of time during which the network does not know the identity of the subscriber, and therefore cannot cipher. GSM confidentiality is of a major concern, and this problem is remedied by providing an identity alias called the temporary mobile subscriber identity (TMSI), which is used in order to avoid sending the IMSI in clear on the radio path. This alias must be agreed before between the mobile station and the network.

4.4 Contention points in the GSM Authentication Approach

The GSM authentication process rely on a major assumption that the fixed network is secure. Therefore. messages are transmitted in a clear text form between Mobile Switching Centers (MSC). However, the same assumption cannot be made for large heterogeneous network environment managed by different administrative authorities [7]. With these conditions, we have to consider a minimal assumption in a such security architecture. The second point of contention with GSM is the way of distributing user authentication information. As we have explained before the network/home domain generates a set of challenge/response pairs on the fly that the foreign domain is then supposed to use in a successive authentication flow with the end user. This solution is inefficient in terms of both bandwidth consumption and the overhead incurred in the home domain [9]. The third negative point in the GSM security system is the use of a non-published algorithm A3. A5. A8 for the authentication and privacy process. It is known that hiding algorithm has not proven to be an effective way in preventing hostile attacks. Furthermore. hidden or unknown algorithms always fail to give users a comfortable feeling of security.

4.5 Summary

In this chapter. we have covered the techniques used for network security. Most of networks are using the conventional method consisting of asking the user to provide his password. then a verification will be carried out to grant access to that user. For mobile radio networks. using password has become not efficient. several approaches are used in different wireless communication systems such as DECT. CDPD. PACS. and GSM. Since GSM is the core of this work we have extended our survey to cover the various aspects of GSM security process.

Chapter 5

GSM Authentication Protocols

Personal communication is understood as the ultimate environment allowing freedom in accessing the network with more flexibility in invoking telecommunication services. The European Global System for Mobile communication (GSM) is a digital cellular system standard providing a broad spectrum of communication capabilities and supporting personal and terminal mobility under the umbrella of Personal Communication System (PCS). Personal mobility is assured in GSM networks through the insertion of a small smart card called subscriber identity module (SIM) allowing its holder to make and receive calls independent of both network points of attachment and specific terminals. However. GSM is using the air interface as a transmission medium which is vulnerable to relatively easy interception such as fraudulent call attempts. intrusion and listening-in by third party. For this reasons. a secure mobile communication systems is adopted in GSM standard: privacy and authentication. Privacy involves ensuring that an eavesdropper cannot intercept the conversations of the parties. and authentication is used to prevent the service to be obtained fraudulently in order to avoid usage charges. Although the process of privacy and authentication is providing a good security level. it has several contention points and drawbacks such as the secrecy of the algorithm. the authentication delay. and the most important is the amount of signaling load needed to perform the privacy and authentication mechanism. The signaling load and the authentication delay are of particular importance and become the subject of widespread research interest. Estimating the performance of a signaling network protocol requires the definition of some performance measures. The number of signaling messages exchanged between network elements. and the bandwidth required for that, can be considered as a good performance criteria for evaluating GSM authentication protocol [17]. We will not be concerned with the information being exchanged. but in the signaling overhead required to carry that information. In this chapter we analyze and evaluate the GSM privacy and authentication protocol in terms of signaling messages load and authentication delay. The methodology used to obtain the analytical results is based on determining the rate at which certain procedures are invoked and the number of messages flowing between various network entities to carry out these procedures.

5.1 GSM Authentication Protocols

Authentication involves both identification and verification. Identification is the process where an entity presents its identity, while verification is the process where the identity is checked [47]. Authentication protocols are the basis of security in many distributed systems. In GSM networks, authentication is secured by checking that the subscriber identity provided by the MS corresponds to the inserted SIM. This process is carried out using a challenge/response mechanism. The mobile station is continuously listening to the location area identity (LAI) being transmitted on the broadcast channel, and is comparing the new LAI received with the last LAI (stored in the SIM) representing the last area where the mobile station was registered [27]. Whenever the received LAI is different than the old LAI stored in its SIM cards, the MS proceeds with a new registration. The registration starts first with getting access to the Stand-alone

Dedicated Control Channel (SDCCH) over which the BTS and the MS communicate to each other. then the authentication process has to be carried out as follows:

- *Step1*: the MS transmits the registration request (location update) to the base station over the SDCCH. The BTS forwards the registration request to the MSC, which informs the corresponding VLR about this request. The registration request includes the TMSI/IMSI and LAI.
- *Step2*: once the new VLR receives the IMSI, it sends a request to the HLR asking for the authentication parameters for that MS.
- *Step3*: the HLR forwards this request to the AuC.
- *Step4*: the AuC computes SRES and K_c by applying the MS's private key K_i and a RAND number to the A3 and A8 algorithms. then sends the authentication triplet (RAND, SRES, and K_c) to the VLR through the HLR.
- *Step5*: the VLR sends the RAND to the MS through the MSC, and asks the MS to compute the SRES and sends it back.
- *Step6*: the MS computes the SRES and the K_c locally using that RAND number and the K_i through the A3 and A8 algorithms, then sends SRES back to the VLR and keeps K_c for later use.

- *Step7*: the VLR once receives the SRES from the MS, compares it with the SRES provided from the AuC. If the two are equal, the MS passes the authentication process.

We can observe that some parameters are sent in the air and they are considered as public parameters and they are vulnerable to interception. The other parameters which are never sent in the air, are supposed to be private parameters either stored in the network or in the SIM card. Thus, SRES, IMSI, TMSI, and RAND are public parameters which can be intercepted by intruders. K_i, K_c are known to the network only and are never transmitted on the air.

The privacy of users is achieved by ciphering the traffic between the user's terminal and the radio base station to prevent eavesdropping and protecting the exchange of the signaling messages. The ciphering key K_c is used to cipher and decipher transmitted data, by applying an exclusive OR operation between the radio burst and a ciphering sequence using a specific ciphering algorithm A5 as shown in Figure 5.3. The secrecy of K_i is the cornerstone on which all the security mechanism is based.

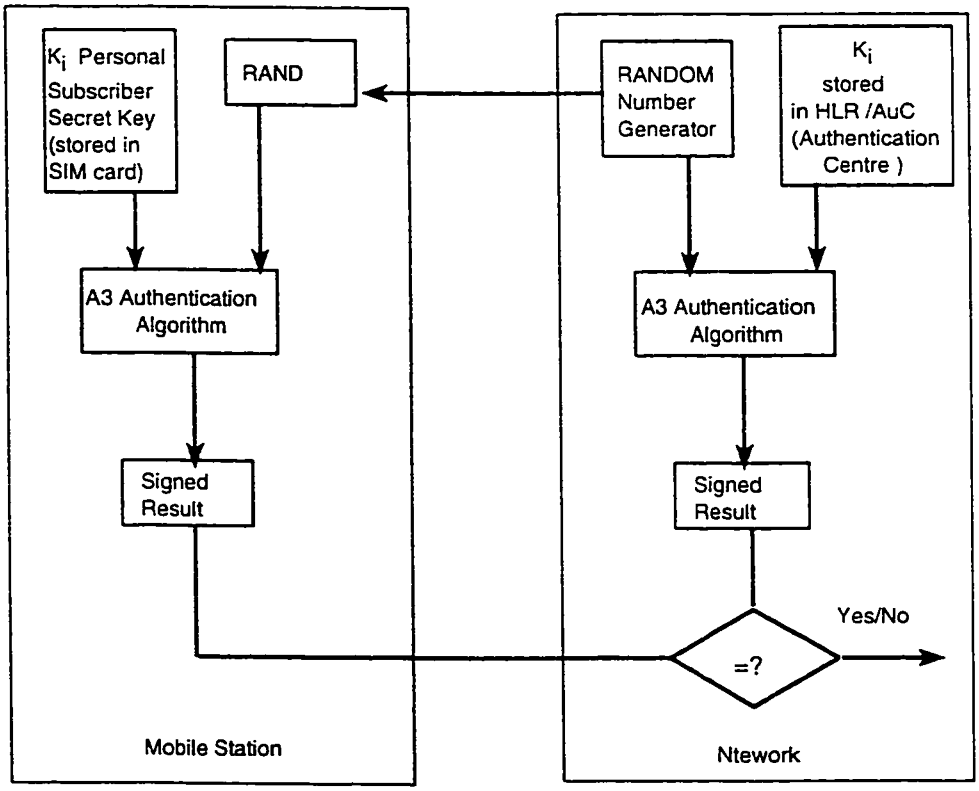

K_i Personal Subscriber Secret Key (stored in SIM card)
RAND
A3 Authentication Algorithm
Signed Result
Mobile Station
RANDOM Number Generator
K_i stored in HLR /AuC (Authentication Centre)
A3 Authentication Algorithm
Signed Result
=?
Yes/No
Ntework

Figure 5.1: GSM privacy and authentication

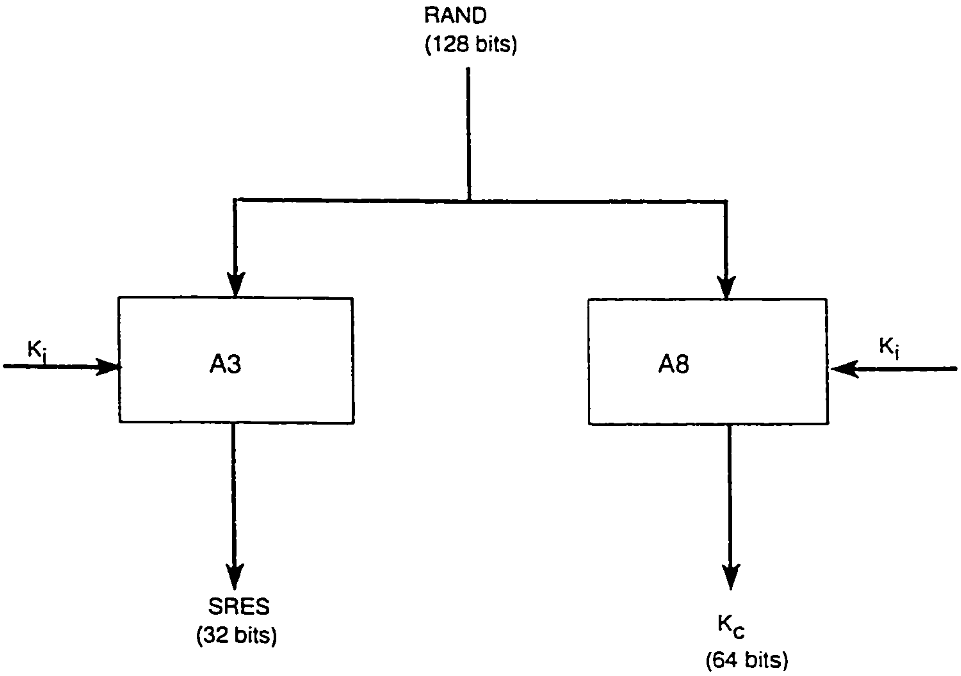


Figure 5.2: GSM privacy and authentication Results Generation

5.2 Analysis of GSM Authentication Protocols

When users move from one location area to another. the MS has to register in the new location area and implicitly deregisters from the old one. This activity is called location update or registration and used primarily to inform the network about the location of any mobile user. Depending on the implementation, registration can also be initiated by the MS on any powering up or powering down. or on a timed basis procedure [44]. The SIM detach/attach procedures mark the MS as detached/attached

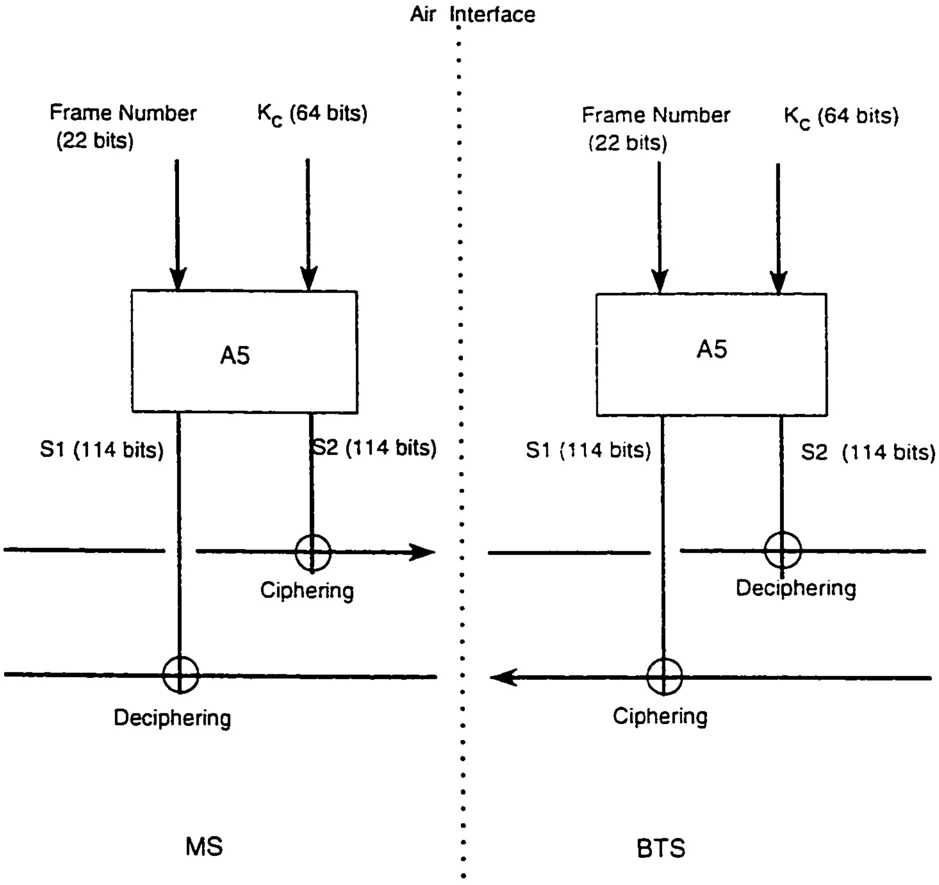


Figure 5.3: GSM ciphering and deciphering process

in the VLR (and optionally in the HLR) on MS power down or power up or subscriber information module (SIM) removed or inserted. These events produce deregistration/registration events. Privacy and authentication process is triggered on every registration. call attempts (originating or terminating) and with services change (it is a network option). The cases when authentication procedures should be used are defined in GSM recommendation 02.09. We are considering only registration/location updates, and call attempts where authentication procedures are invoked. These procedures are based on the challenge response mechanism illustrated in Figure 5.4. While this mechanism is giving a reasonable level of security, it is generating an important signaling message traffic and making the call setup more long. For the sake of the simplicity, we will use the word authentication only instead of privacy and authentication, since privacy and authentication are generally linked together because of the derivation and use of the ciphering key K_c.

In our analysis, we concentrate on the signaling load generated by these protocols and the delay that might add to the whole call setup time. A widely used terminal/user mobility model is the fluid flow mobility model described in [66]. This model assumes that mobile users carrying terminals are moving at an average velocity of v and their direction of movement is uniformly distributed over $[0, 2\pi]$, and mobile users are uni-

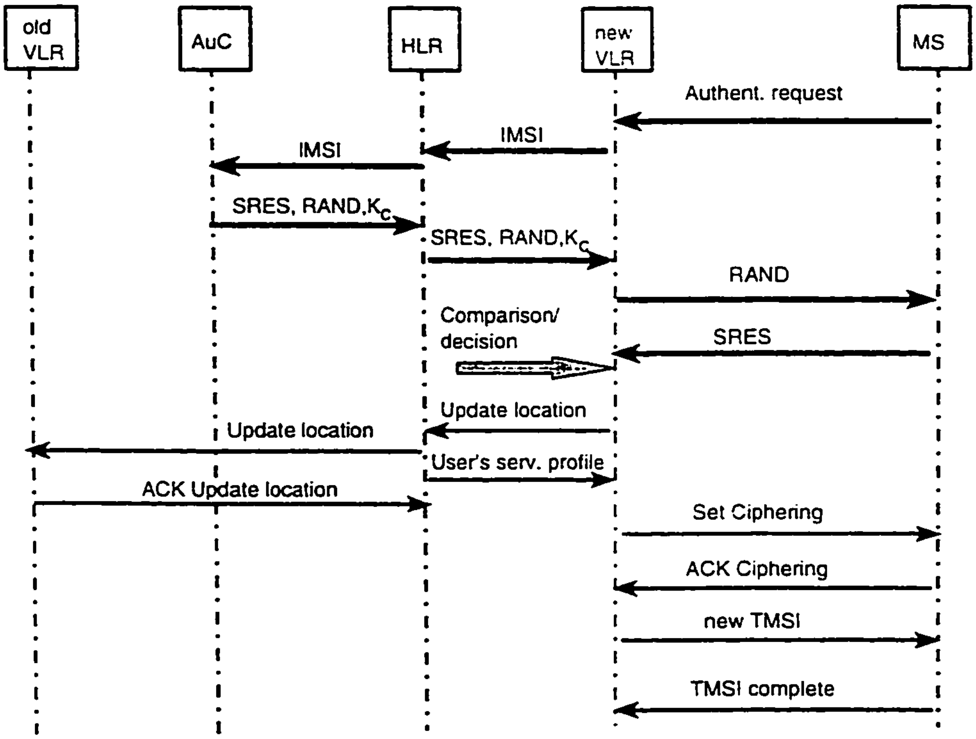


Figure 5.4: GSM challenge/response signaling flow

formly populated with the density ρ and the registration area boundary is of length L.

In [55], it has been shown that the rate of registration area crossing, R, is given by:

$$R = \frac{\rho \cdot v \cdot L}{\pi}$$

The above model is used with the following assumptions taken from a real GSM environment to analyse the traffic involved in the authentication process:

- One HLR for the whole network service area (SA), and each location area/ registration area is served with one VLR
- 64 registration areas (64 VLRs).
- Square registration area size $(8.65km)^2$ = 66.60 sq km.
- Border length L = 34.6 km.
- Mean call origination rate = Mean call termination rate = 2.6/hr/user.
- Total number of MS users =764.000.
- Mean density of MS = ρ = 267/sq km.
- Average speed of MS, v = 6.3 km/hr.

The traffic due to registration is generated by MS moving into a new registration area (RA). In the steady state, the rate at which users move into a RA is equal to the rate at which MS move out of that RA. Since every registration area is handled by one VLR. the rate of registration area crossing. R. is given by:

$$R_{Reg..RA} = \frac{267x34.6x6.3}{3600x} = 5.14/\mathrm{s}$$

and $$R_{dereg..VLR} = 5.14/\mathrm{s}.$$

This must also be equal to the number of deregistration (registration cancellation). Thus the total number of registration messages per second arriving at the HLR is equal to:

$$R_{reg..HLR} = R_{reg.VLR} \times \text{ total number of registration areas}$$

$$= 5.14 \times 64/\mathrm{s} = 329/\mathrm{s}$$

Therefore we have 5.14/s and 329/s authentication requests per each VLR and HLR respectively. Now we compute the total number of authentication requests due to call origination (CO) and call termination (CT) for the entire serving area (SA):

The total number of call originating per serving area is equal to:

$$R_{callOrig./SA} = \frac{2.6x764.000}{3600} = 551.7/\mathrm{s}.$$

and, the total number of call terminating will be equal to 551.7/s.

Thus the number of calls originating per RA is equal to:

$$R_{callOrig./RA} = \frac{551.7}{64} = 8.62/\mathrm{s}.$$

and the number of calls terminating/delivered per RA = 8.62/s.

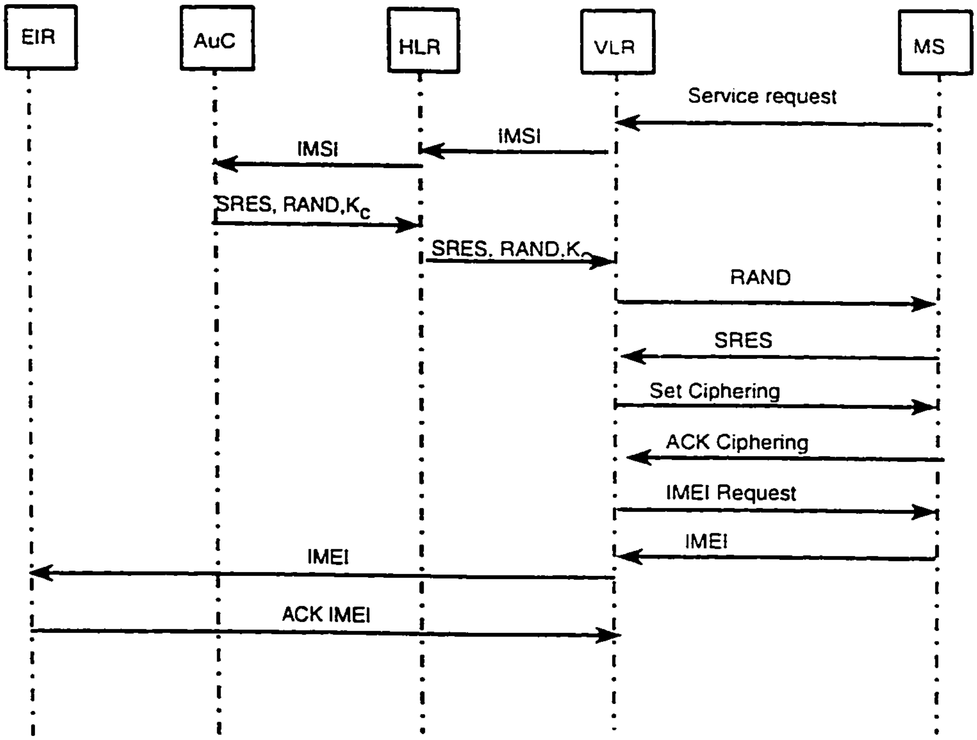


Figure 5.5: GSM call origination authentication signaling messages

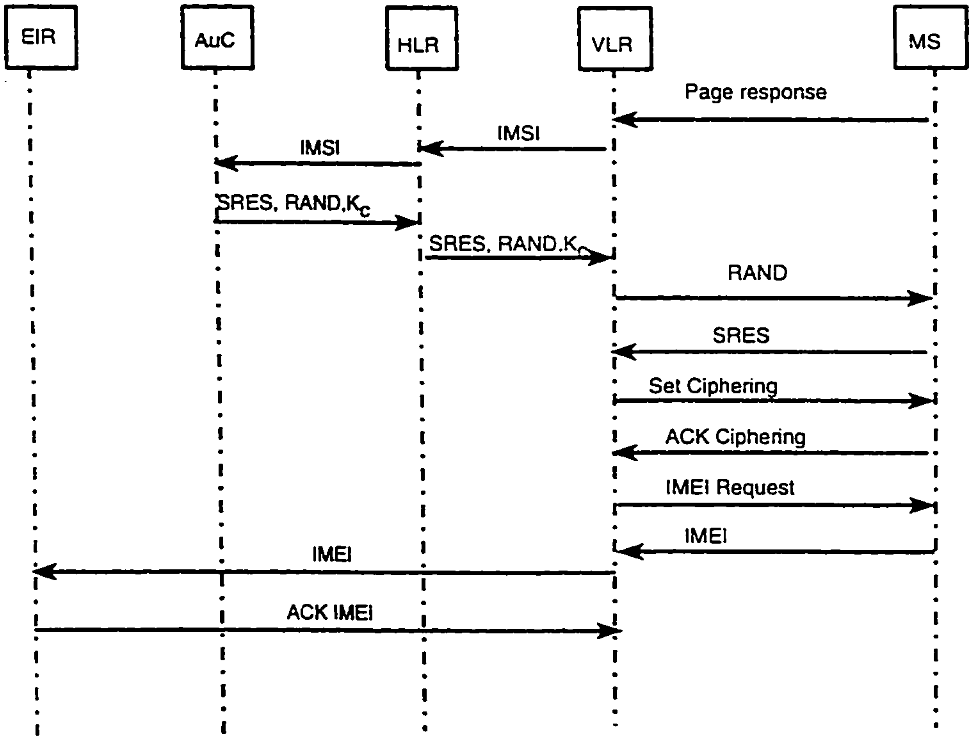


Figure 5.6: GSM call termination authentication signaling messages

Table 5.1 summarizes the total authentication request rate per VLR and HLR for each type of activity as computed above.

Table 5.1: Authentication request rate.

	VLR/sec	HLR/sec
Registration	5.14	329
Call Termination	8.62	551.7
Call Origination	8.62	551.7
Total/network	22.38	1432.4

Using the signaling messages flow between network data bases (registers) as illustrated in Figure 5.4, Figure 5.5, and Figure 5.6, we find the number of signaling messages per authentication request for the registration, call origination and call termination activities as illustrated in Table 5.2. Table 5.3 shows the total signaling messages generated here per VLR and HLR for each type of activity. For the registration, there are 5.14 authentication requests per second for the VLR and 329 for the HLR. For each authentication request, there are 5 messages processed by the VLR and 4 by the HLR as shown in Figure 5.4. The total signaling message/s for the registration activity will be for the VLR and the HLR as the following:

VLR: 5.14 X 5 = 25.7 signaling messages/s

and HLR: 329 x 4 = 1316.signaling messages/s

The above results apply for the call Termination and call Origination activities.

Table 5.2: Signaling messages per authentication request

Activity	Auc	HLR	VLR	Old VLR
Registration	2	4	5	1
Call Origination	2	4	5	0
Call Termination	2	4	5	0

Table 5.3: Total signaling messages: GSM

	VLR	HLR
Registration	25.7	1316
Call Origination	43.1	2206.8
Call Termination	43.1	2206.8
Total	111.9	5729.6

The authentication/verification delay is defined as the time interval from the instant the user starts the authentication process until the network takes the final decision (acceptance or rejection) of the user [21]. In GSM, radio interface signaling transactions and user information are transferred on dedicated channels. These channels could be used among several users employing combined random access and reservation techniques. The random access procedure is based on a slotted-ALOHA concept [15]. The stand alone dedicated control channel (SDCCH) is used for communication between the MS and the BTS. Figure 5.7 depicts the messages involved in authentication delay.

Let us assume that the time delay due to network data bases (DB) mes-

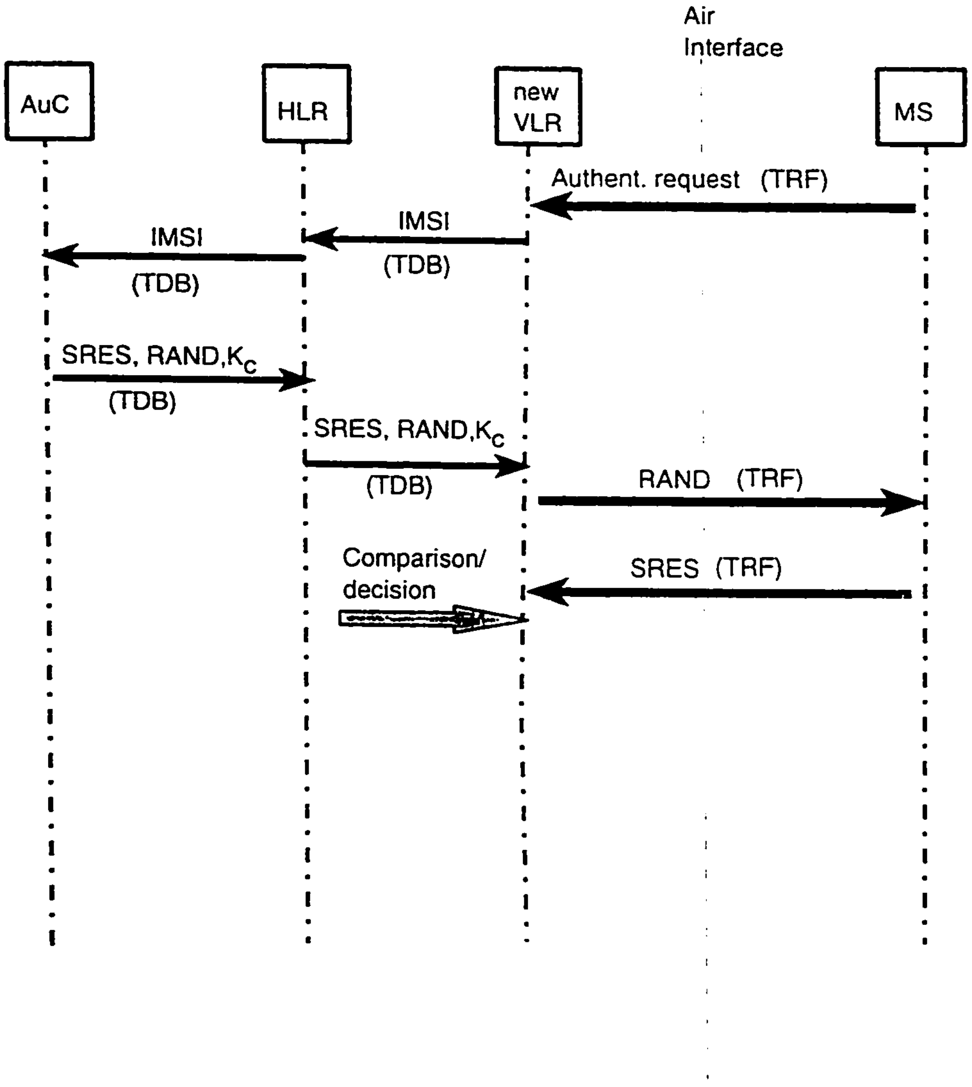


Figure 5.7: Signaling messages flow for GSM Authentication delay

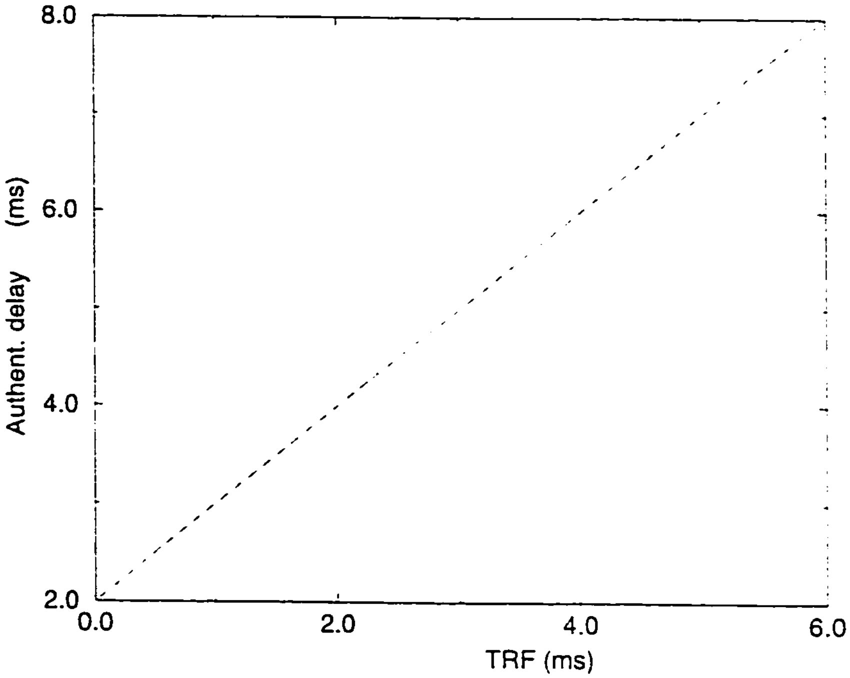


Figure 5.8: GSM Authentication delay

sage exchange. is TDB and it is the same between all of them. The time between MS and BTS is assumed to be TRF (Radio frequency). Using Figure 5.7, the authentication delay TAd for the GSM conventional protocol can be computed as:

$$\text{TAd} = 4\text{TDB} + 3\text{TRF}$$

From the equation above we can see that the authentication delay is linearly dependent on the TRF as depicted in Figure 5.8.

5.3 GSM Authentication Protocol for Roaming Users

Roaming over GSM networks in other countries is one of GSM's main attractions to subscribers. International roaming is increasingly becoming a substantial source of revenue for most of network operators over the world. The ever increasing levels of international human traffic, as a result of business or tourism, has meant that subscribers are coming to expect service from one phone no matter where they are on the planet [64]. In fact, roaming has become the main difference between the different mobile digital cellular standards. Prior to the advent of GSM, mobile networks had only national coverage, and even if two networks had adopted the same basic standards, roaming between them was sometimes impossible due to technical or political reasons. GSM brought the possibility for subscribers to use their handsets in foreign networks, without having to reach some sort of prior agreement with that foreign network. Now, roaming subscribers can receive service in all networks with which the home network has reached agreements, via one mobile number and one billing for any service, implemented on other networks, in local currency. The GSM authentication procedure for roaming users is almost the same as for local users. The idea of challenge response mechanism is still maintained. The following steps summarize the authentication protocol actually used for roaming users in GSM networks.

- *Step1*: by comparing the received LAI from the visited network and the LAI of the home network, the MS detects that it has entered a new network area, thus the MS transmits a registration request (location update) to the base station over the SDCCH. The BTS forwards the registration request to the MSC which informs the corresponding VLR about this request. The registration request includes the TMSI/IMSI and LAI.
- *Step2*: analyzing the IMSI, the VLR understands that this user is a roaming mobile station (RMS). The visited network doesn't have the capability of authenticating this RMS. Thus, the home domain has to be contacted for the authentication process. The IMSI contains information for home domain country code as shown in Figure 5.9.
- *Step3*: the VLR, through the MSC, makes a request to the home domain asking for the authentication triplet (RAND, SRES, K_c) of this RMS.
- *Step4*: the VLR in the home domain forwards the request to the AuC through the HLR.

- *Step5*: the AuC computes SRES and K_c by applying the MS's private key K_i and a RAND number to the A3 and A8 algorithms. The VLR through the MSC in the home domain, sends the authentication triplet (RAND. SRES. and K_c) to the visited network.
- *Step6*: upon receiving the triplet. the VLR in the visited network sends the RAND to the MS through the MSC and asks the MS to compute the SRES and sends it back.
- *Step7*: the MS computes the SRES and the K_c locally using that RAND number and the K_i through the A3 and A8 algorithms. then sends SRES back to the VLR and keeps K_c for later use.
- *Step8*: the VLR once receives the SRES from the MS compares it with the SRES provided from the AuC of the home domain. If the two are equal, the MS passes the authentication process.

The cornerstone in this concept is the secret key which is never transmitted in the air or given to any other network. The exchange of signaling messages between network entities is illustrated in Figure 5.10. Using the same analogy used in Section 5.2. we can derive the number of messages exchanged between network elements and in particular the crossnetwork messages (Inter MSCs). Table 5.4 summarizes all the signaling messages per authentication request for a roaming user in GSM networks.

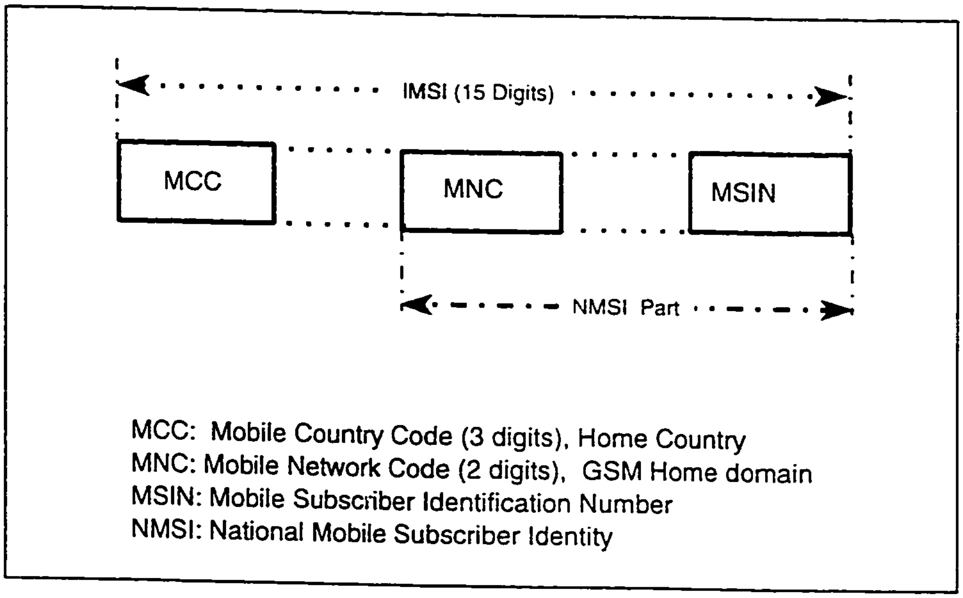

IMSI (15 Digits)
MCC
MNC
MSIN
NMSI Part
MCC: Mobile Country Code (3 digits), Home Country
MNC: Mobile Network Code (2 digits), GSM Home domain
MSIN: Mobile Subscriber Identification Number
NMSI: National Mobile Subscriber Identity

Figure 5.9: IMSI Information Codes

Table 5.4: Signaling messages per authentication request for a roaming user

	Old Network			Visited Network			InterMSC
Activity	Auc	HLR	VLR/MSC	AuC	HLR	VLR/MSC	
Regist.	2	2	4	0	4	5	2
Call Orig.	2	2	4	0	4	5	2
Call Term.	2	2	4	0	4	5	2

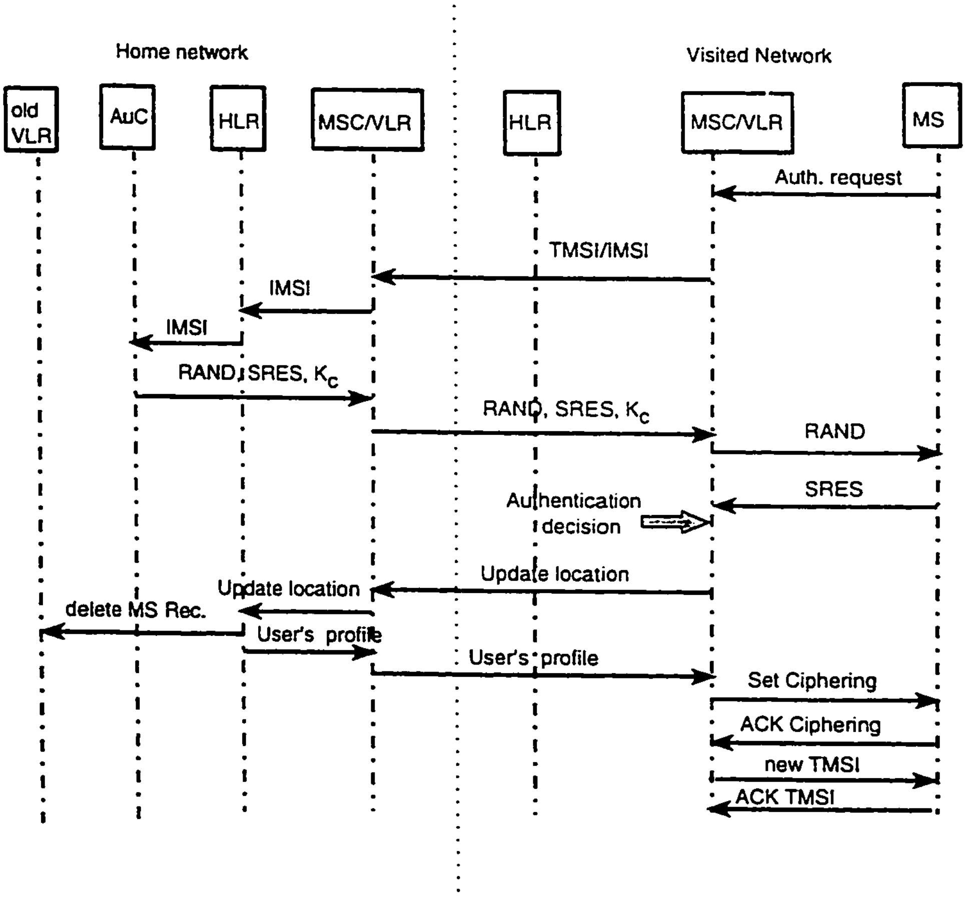


Figure 5.10: GSM authentication signaling flow for roaming users

These signaling messages add an extra overload for home domain as well as the visited network. In addition to that. roaming users will be out of service (can not make or receive calls) in case of failure of any of the home network databases or the internetwork links. In peak traffic hours. where the trunks/circuits between the home and the visited networks are completely used, roaming users can not benefit from their PCS services to which they subscribe.

5.4 Conclusion

In this chapter we have studied and analyzed the GSM authentication protocols used in authenticating local and roaming users. User's secret key is the cornerstone in the authentication process. The signaling overhead and the delay incurred in accessing the service is considered as a key traffic performance parameter for mobile communication networks. This delay is basically due to the protocol structure which is based on the challenge response mechanism. For the roaming users the delay might be more considerable, since the visited network has to contact the home domain network to authenticate the visitors.

Chapter 6

Proposed Authentication Protocol for GSM Networks

The term protocol for data communication procedure is a kind of agreement about the exchange of information in a distributed system [19]. Authentication protocols are the basis of security in many distributed systems, and in particular in wireless communication systems, GSM is one of them. In Chapter 5, we have presented the conventional GSM authentication protocol. The analysis of this protocol has shown an important signaling load generated due to the challenge response mechanism used. In addition to that, the process is giving a considerable delay, called the authentication delay, making the call setup time longer. The GSM protocol is based on the challenge response mechanism [14] which consists of sending a RAND number to the MS and challenge it for answering with the same signed result SRES already computed in the AuC using the subscriber secret key K_i. Several signaling messages have to be exchanged between different network elements. In this chapter, we propose a new efficient authentication approach, based on a basic idea, using the mobile user events counter (COUNTM) used in GSM networks for statistics. This counter is stored in the network (HLR), and it can be added to the mobile user SIM card. The counter is changing upon any activity such as registration, call terminating, call originating, SIM attach/detach. Also in our devised scheme, a random number RANDM (64 bits) is generated locally by the MS to compute a pre-authentication result AUTHR. The AUTHR is the output of A3 algorithm when RANDG and K_i are used as inputs. The counter (COUNTM) concatenated to the RANDM form the global random number called RANDG (128 bits).

6.1 Proposed Authentication Scheme

We are interested in reducing the authentication delay and the network signaling overhead by reducing the number of messages which result in a decrease of the call setup time without compromising GSM security.

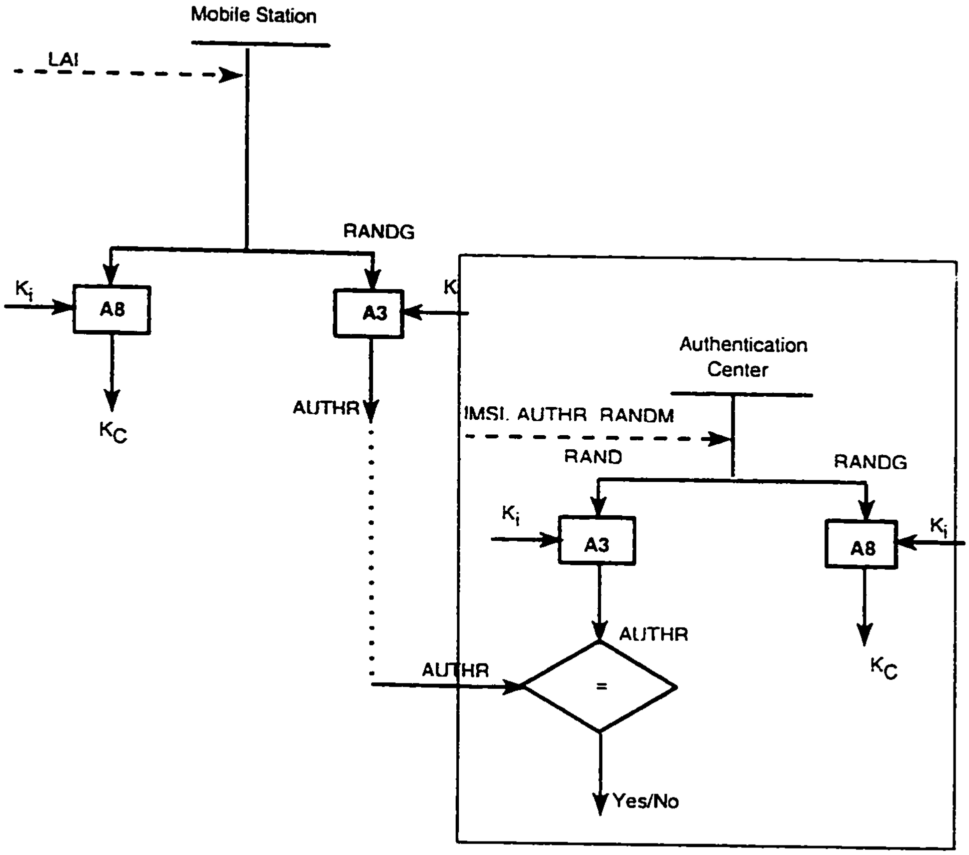
As for every network access (registration, call attempts) the MS sends a channel request over the Random Access Channel (RACH). The base station receives the request message, and allocates a Stand-alone Dedicated Control Channel (SDCCH) that will be used by the MS to communicate with the network. The proposed scheme is as follows:

* *Step1*: the MS transmits the registration request (location update) to the base station over the SDCCH. The BTS forwards the registration request to the MSC, which informs the corresponding VLR about this request. The registration request includes the TMSI/IMSI, LAI, RANDM and the AUTHR which is the output of A3 algorithm when K_i and the RANDG are applied as inputs.

* *Step2*: once the new VLR receives the IMSI, it sends a request to the HLR asking for the verification of the AUTHR of that MS.

* *Step3*: the HLR adds the MS's COUNTM to the request, then forwards it to the AuC.

* *Step4*: the AuC produces the RANDG, then computes the AUTHR and K_c by applying the MS's private K_i and the RANDG number to the A3 and A8 algorithms respectively, and finally compares the two AUTHRs. If the two are equal, the MS passes the authentication process.



K_I: Individual subscriber authentication key (128 bits).
COUNTM= MS counter (events counter) =64 bits
K_C=Cipher Key (64 bit).
RANDM=Random Number (64 bits).
RANDG=Random Numer (128 bits)=RANDM appended to COUNTM
AUTHR=Athentication result (32 bits).
A3=Authentication Algorithm.
A8=CipherKey generating Algorithm.

Figure 6.1: proposed authentication protocol

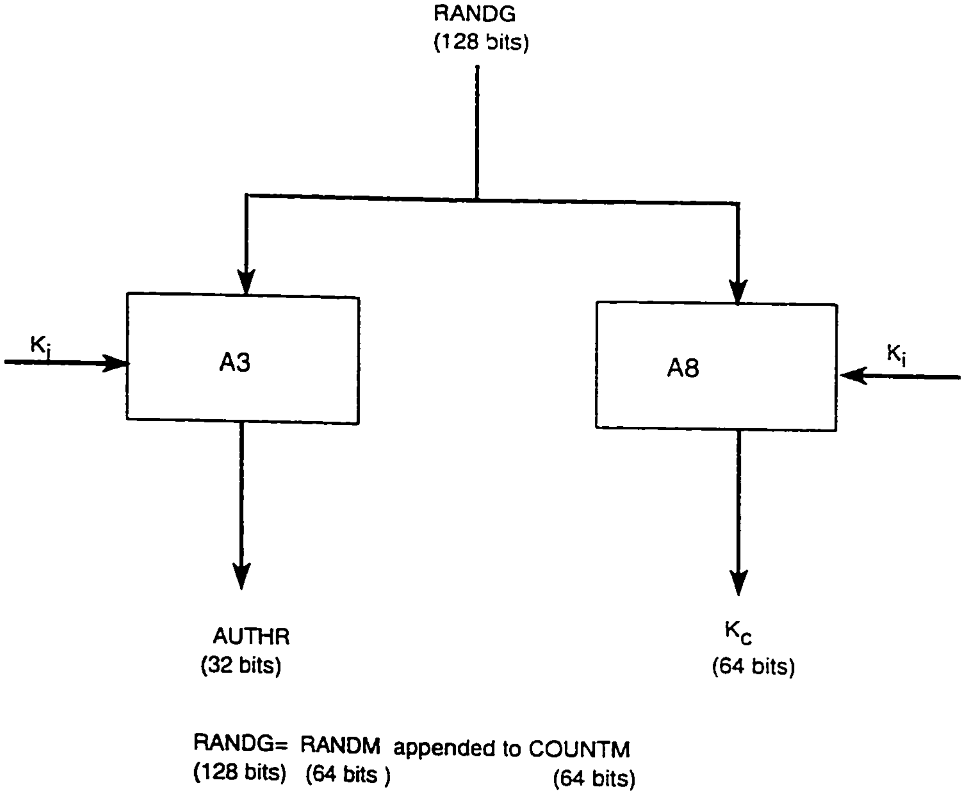

RANDG
(128 bits)
K_i
A3
A8
K_i
AUTHR
(32 bits)
K_c
(64 bits)
RANDG= RANDM appended to COUNTM
(128 bits) (64 bits) (64 bits)

Figure 6.2: AUTHR and K_c generation for the proposed scheme

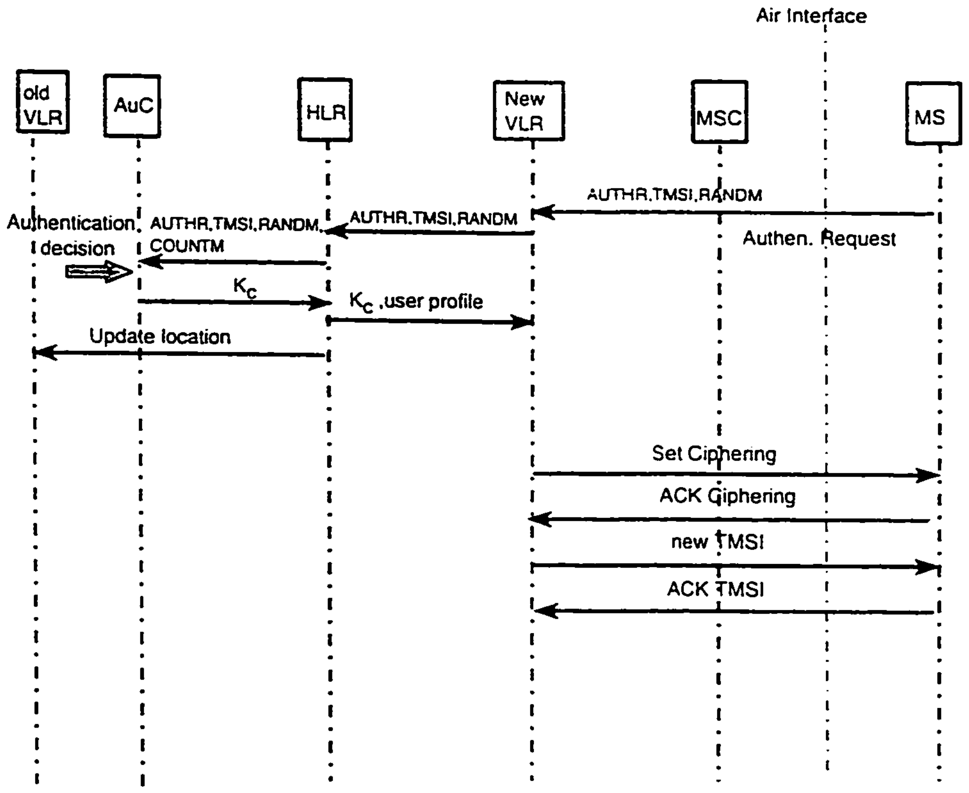


Figure 6.3: Signaling messages flow for the proposed scheme

We can observe that some parameters are sent in the air and they are considered as public parameters which are vulnerable to interception. Other parameters are never sent in the air, K_i and K_c are supposed to be private parameters stored in the network or in the SIM card. Thus, the RANDM, TMSI/IMSI, and AUTHR are public parameters. Figure 6.1 and Figure 6.2 show the proposed protocol, and Figure 6.3 depicts the corresponding signaling message flow.

6.2 Evaluation of the Proposed Authentication Scheme

In engineering a communication protocol. we are more concerned about two general requirements:

1. Correctness.
2. Efficiency.

In the context of GSM authentication protocol. correctness means that the protocol does not contain any security holes. Efficiency means that the authentication protocol does not require any excessive signaling traffic. In this section we first provide a complete specification of the proposed authentication protocol according to the recommended protocol engineering practices [19], then we address the correctness aspects of the protocol. Finally we conclude the section by providing detailed analysis of the signaling traffic and the authentication delay required by the proposed authentication protocol.

6.2.1 Protocol Specifications

Any protocol specifications should consist of the following five elements:

1. The service to be provided by the protocol

2. The assumptions about the environment in which the protocol is executed.
3. The vocabulary of message used to implement the protocol.
4. The encoding (format) of each message in the vocabulary.
5. The procedure rules guarding the consistency of message exchange.

Below we specify each of these five elements for the proposed authentication protocol:

* **Service provided**

  For the proposed scheme, the service provided is mainly to allow the GSM network to authenticate mobile users in all circumstances.

* **Protocol environment**

  The protocol is executed in wireless environment, therefore, there are possibility of intrusion, interception, masquerading and eavesdropping. The most important assumption is emphasizing the mobile user's secret key K_i which is never transmitted on the air and is stored only in two safe places, the authentication center AuC and the mobile user's SIM card.

* **Protocol vocabulary**

  The vocabulary of messages used is as follows:

  -The service request, used to make a registration or call attempt.

-Authentication request. from VLR to HLR. or HLR to AuC and used to proceed with an authentication process for that IMSI/TMSI.

-Acknowledgment. to acknowledge any received message.

* Format

Messages are encoded with the following format:

MS $\Longrightarrow$ BTS

AUTHR (32 bits). SEVREQ (8 bits). TMSI/IMSI (32/15 bits). LAI (40 bits), RANDM (64 bits).

VLR $\Longrightarrow$ HLR

AUTHR (32 bits). IMSI (15 bits). RAND (128 bits).

HLR $\Longrightarrow$ AuC

AUTHR (32 bits). IMSI (15 bits). RANDM (64 bits). COUNTM (64 bits).

* Procedure rules

The procedure rules are represented in signaling message flow shown in Figure 6.3

6.2.2 Security Correctness of the Proposed Scheme

In order to prove the correctness of our proposed scheme we use a comparison methodology between our devised approach and the traditional GSM protocol. In GSM approach. the authentication protocol consists basically of the following steps:

1. The MS sends its identity to the network with a service request.
2. The VLR/network identifies the MS and prepare the security triplet (RAND, SRES, K_c).
3. The VLR sends a RAND to MS and asks for the SRES using that RAND number.
4. The MS sends back the SRES computed in its SIM. The VLR make the comparison between SRES coming from the SIM card and the SRES computed in AuC.

For the proposed scheme, we have the following basic steps:

1. The MS prepares an AUTHR computed locally in the SIM using a RANDG, user's private key, and sends it with the service request to the network.
2. The network identifies and verifies the AUTHR coming from the MS whether is the same as the AUTHR computed locally in the AuC.

So we can see from the steps listed above that in GSM the idea of authentication is based on comparing an entity called SRES computed in two different places, the AuC and SIM. using the same input parameters RAND and K_i through A3 algorithm. In our devised scheme. the same idea is conserved. the protocol consist of computing an AUTHR in two different places. the AuC and SIM. using input parameters RANDG and K_i. then it compares them. The RANDG now consists of a COUNTM and a normal random number RANDM.

In GSM. we have SRES and RAND are used as public parameters. For our scheme. we have AUTHR. RANDM. as public parameters . K_i. K_c are still maintained as private parameters for both approaches. The RAND is used to compute SRES in the GSM approach. However for our scheme. the RANDM, is used as a part of the RANDG which is used also to compute AUTHR. The security aspect in our scheme is enhanced by using the counter COUNTM. which is not transmitted on the air. The counter is modified for every activity such as registration. successful call attempt, and SIM attach/detach. Without the counter. an intruder will not benefit from collecting the RANDM and AUTHR. In both schemes. the secrecy of K_i, which is never transmitted in the air. is still the cornerstone on which all the security mechanism is based.

6.2.3 Signaling Load of the Proposed Scheme

The term signaling refers to the set of actions required to set up a connection between hosts across network under software control [52]. Actions here are messages sent from different GSM entities. Using the same model and analysis used in Chapter 5, we find that the number of messages is clearly less than the conventional GSM protocol. In Table 6.1 we find the number of signaling message per authentication request for each database register (AuC, VLR, HLR). Using the rate of authentication request per second, given in Chapter 5 for each type of activity (registration, call termination and origination), we compute the total signaling message for the VLR and HLR as shown in Table 6.2.

Table 6.1: Signaling messages per authentication request

Activity	AuC	HLR	VLR	old VLR
Registration	1	2	2	1
Call Origination	1	2	2	0
Call Termination	1	2	2	0

Table 6.2: Total signaling messages: Proposed scheme

	VLR	HLR
Registration	10.28	658
Call Origination	17.24	1103.4
Call Termination	17.24	1103.4
Total	45.76	2866.72

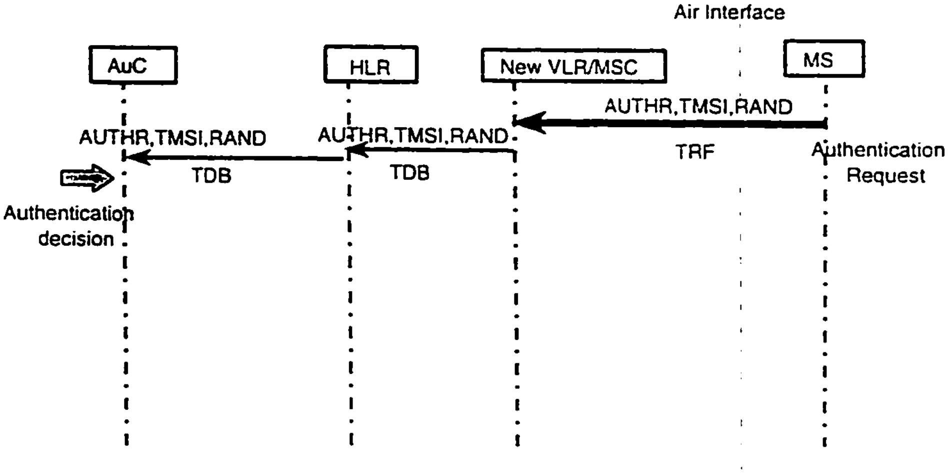


Figure 6.4: Signaling message flow for the Authentication delay: Proposed scheme

6.2.4 Authentication Delay of the Proposed Scheme

User authentication/verification delay is defined as the time interval from the instant the mobile user starts the authentication process until the network communicates its final decision (acceptance or rejection) to the user. The authentication delay will be added to the preselection or post-selection delay perceived by the user [17].

Now we compute the authentication delay provided by the proposed scheme using the same assumptions used with GSM protocol in Chapter 5. Let us assume that the network databases message exchanges, produce a delay of TDB and it is the same between all of them, and the time that

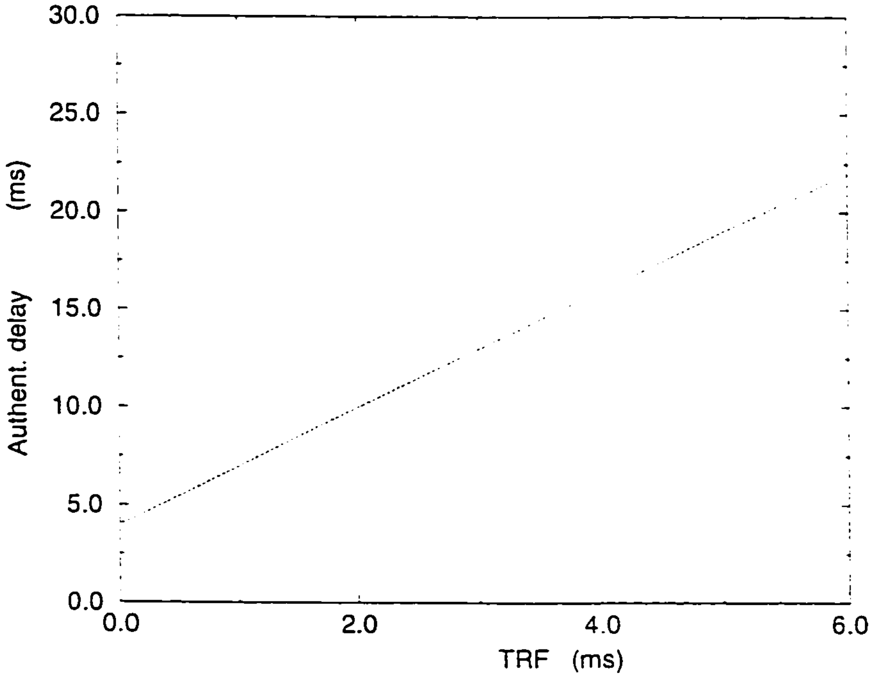


Figure 6.5: Authentication delay for Proposed scheme

the message takes from MS to BTS is denoted by TRF as shown in Figure 6.4. The authentication delay TAd can be computed as follows:

$$\text{TAd}= 1\text{TRF} + 2\text{TDB}.$$

For our proposed scheme, the authentication delay TAd is linearly proportional to TRF as shown in Figure 6.5.

6.2.5 Bandwidth Requirements

In our proposed scheme. we are using the following authentication parameters:

-The RANDM number is 64 bits.

-The size of AUTHR is 32 bits.

-LAI is 40 bits.

-Service Request (location update request/call attempt) is 8 bits.

-Temporary mobile subscriber identity TMSI is 32 bits.

The messages sent from the MS to the network (BST or VLR) for authentication will be of the following size:

RANDM + AUTHR + LAI + SEREQ. + TMSI = 64 + 32 + 40 +8 + 32 =191 bits (24 bytes). In Chapter 5. it has been shown that there is 5.14 authentication request/s. due to registration and 8.62 authentication request/s due to call attempts for each VLR. Thus for the registration activity, the bandwidth used between MS and BTS will be equal to 191x5.14=957 bits/s (119 bytes/s). and 191x 8.62 =1630 bits/s (204 bytes/s) for either call origination or call termination.

For the original GSM protocol. the following parameters are used:

-The RAND number is 64 bits.

-The size of SRES is 32 bits.

-LAI is 40 bits.

-Service Request (location update request/call attempt) is 8 bits.

-Temporary mobile subscriber identity TMSI is 32 bits.

The messages sent in the air from/to the network are the service request (8 bits), RAND (128 bits), and SRES (32 bits). Thus the maximum bandwidth will be 128 bits x 5.14=657 bits/s (83 bytes/s) for registration, and 128 bits x 8.62=1104 bits/s =138 bytes/s for call origination or termination. In both cases the bandwidth needed is still considered to be much lower than the GSM capacity.

6.3 Comparison and Discussion

GSM authentication protocols are giving a reasonable level in terms of user authentication and traffic confidentiality. However, these protocols are overloading the network databases (VLR and HLR) with a considerable amount of queries and updates, raising up two important factors in evaluating the total network performance: signaling messages load and the authentication delay. The merit of our proposed scheme can be evaluated with respect to many criteria. The first criterion is security where authentication and privacy are preserved. The MS is still authenticated using the secret key and the authentication result is computed first in the SIM card then it is send to the authentication center (AuC) for verification and validation. Also, the K_c is produced in the same time of the AUTHR and it will be used later for channel ciphering. The second criterion is the important reduction in the signaling messages between the various network elements.

Table 6.3: Total Network traffic (signaling messages/s)

	GSM	Prop. Scheme	% Improvement
VLR	111.9	45.76	50
HLR	5729.6	2864.8	50
Total	5841.5	2909.56	50

Table 6.3 outlines the difference between the GSM approach and our scheme in terms of the total number of signaling messages per second for the authentication process. The percentage of improvement is around 50 percent. Varying the MS mobility rate (the speed of movement), we can see in Table 6.4 that the proposed scheme is maintaining the same level of improvement (50 percent) in terms of total network signaling load compared to the conventional GSM approach.

The third determinant factor in our analysis is the authentication delay which is normally added to the pre-selection or post-selection delay perceived by the user. As a consequence of that, the update of the old VLR will be only after the authentication decision has been taken. If a MS

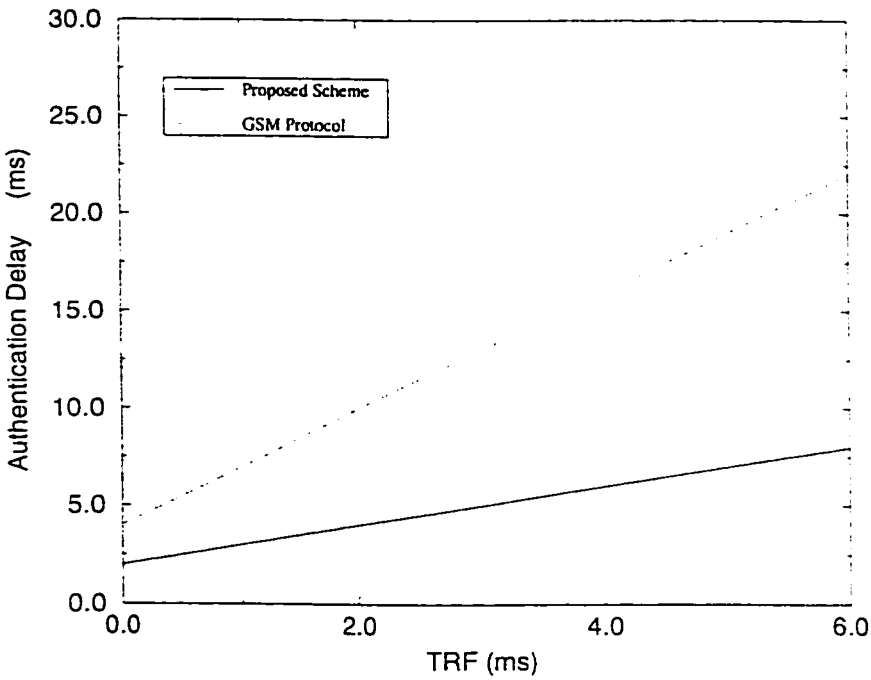


Figure 6.6: Authentication delay: comparison GSM and Proposed scheme

receives a call during that transition time. the network will page him in the area covered by the old VLR. but that MS has already moved to a new location area, therefore the paging request will be lost and the call will be aborted. The proposed scheme is clearly generating less delay than GSM protocol as shown in Figure 6.6.

The fourth advantage of the proposed scheme is the structure itself which is a very important issue in this analysis study. In the GSM challenge response mechanism, the process is based on challenging the MS after preparing the authentication triplet (SRES. RAND. K_c) in the authentication center. Then the VLR has to send the RAND number to the SIM of that MS and waits for the response (SRES). and upon comparison the authentication decision is taken. Our design concept is based on the general form of the authentication definition stated in Section 5.1. So, instead of the long process described in the GSM conventional scheme. our idea starts from preparing the authentication result in the MS. then sending it to the AuC for verification and validation in three messages only. Using a counter in the computation of the AUTHR makes the possibility of security breaches almost impossible. Another advantage of the proposed scheme is that updating (deregistration) the old VLR is faster than the GSM approach.

Table 6.4: Network Signaling Traffic with Different Mobility Rate

Mobility Rate (R)		GSM Protocol			Proposed Scheme		
Speed(V)	R	VLR	HLR	Tot.sig.	VLR	HLR	Tot. Sig.
2	1.64	94.4	4833.4	4927.8	38.08	2311.76	2349.5
4	3.28	102.6	5253.2	5335.8	41.36	2628.64	2670
6.3	5.14	111.9	5729.6	5841.5	45.76	2866.8	2912.56
10	8.2	127.2	6512.8	6640	50.88	3488.8	3539.68
15	12.3	147.7	7562.4	7710.1	59.08	3783.2	3842.28

6.3.1 RAND number generation

In GSM approach, the RAND number is generated upon user authentication request, and it is used individually only once. In the proposed scheme, a RANDM number is generated by the MS and concatenated to the mobile user's event counter (COUNTM) to form a global random number RANDG. Using the private key and RANDG, the AUTHR is computed. RANDM is the one sent to the network. Generating RANDM from MS means an extra load (hardware) is added to the mobile equipment (ME). Both the battery life and the cost will be affected accordingly by this additional function implemented in the ME. However, the extra load added due to RANDM generation will not be high compared to the load generated by the A3 and A8 algorithms.

6.4 Summary

In this chapter, we have proposed a new approach that can be used for GSM user authentication. The proposed protocol is giving the same level of security with less burdens. The user secret key K_i is still the cornerstone in the whole process. Using the same analysis used in Chapter 5, we found that our proposed scheme is outperforming the GSM authentication process in terms of signaling messages and authentication delay.

Chapter 7

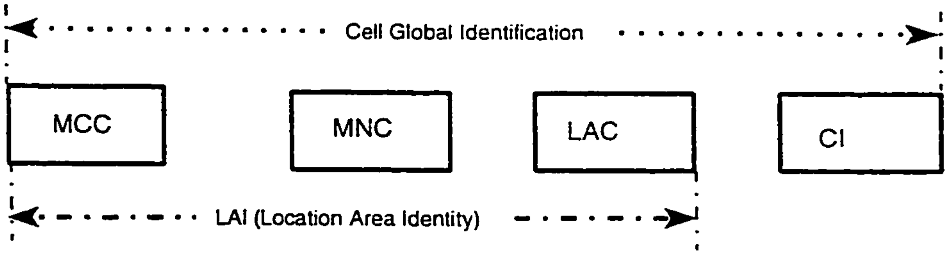
Proposed Authentication Protocol for Roaming Users

One of the main objective of the GSM standard is allowing a large scale of mobility called roaming through Europe and beyond. The authentication principles have to be maintained as if the MS is still in his home domain. The home network generates a set of challenge/response pairs on the fly that the visited network has to use them in a successive authentication flow with the end user [38, 39]. In the GSM approach, user private key K_i exists only with the home network. The visited network has to contact the home network for any attempt of user authentication resulting in a major signaling overhead. The authentication triplet (SRES, K_c, RAND) provided by the home authentication center is sent to the visited network through internetwork links. The cross network signaling messages increase the authentication delay and eventually the call setup time [31].

7.1 The Proposed Scheme

Our scheme aims to reduce the cross network signaling messages and to decrease the call setup time. The basic idea of our proposed approach consists of sharing the user's private key K_i with visited networks for users with high mobility rate and moving frequently between their home domain network and other visited networks inside the same country boundary. The visited network will authenticate these roaming users without going back to their home network to collect the authentication triplet. We assume here that the roaming mobile station (RMS) has in its SIM card all mobile network codes (MNC) sharing its private key K_i. The RMS receives LAI of the visited network upon crossing the boundary of the home network geographical area. In LAI, we find the MNC as shown in Figure 7.1.

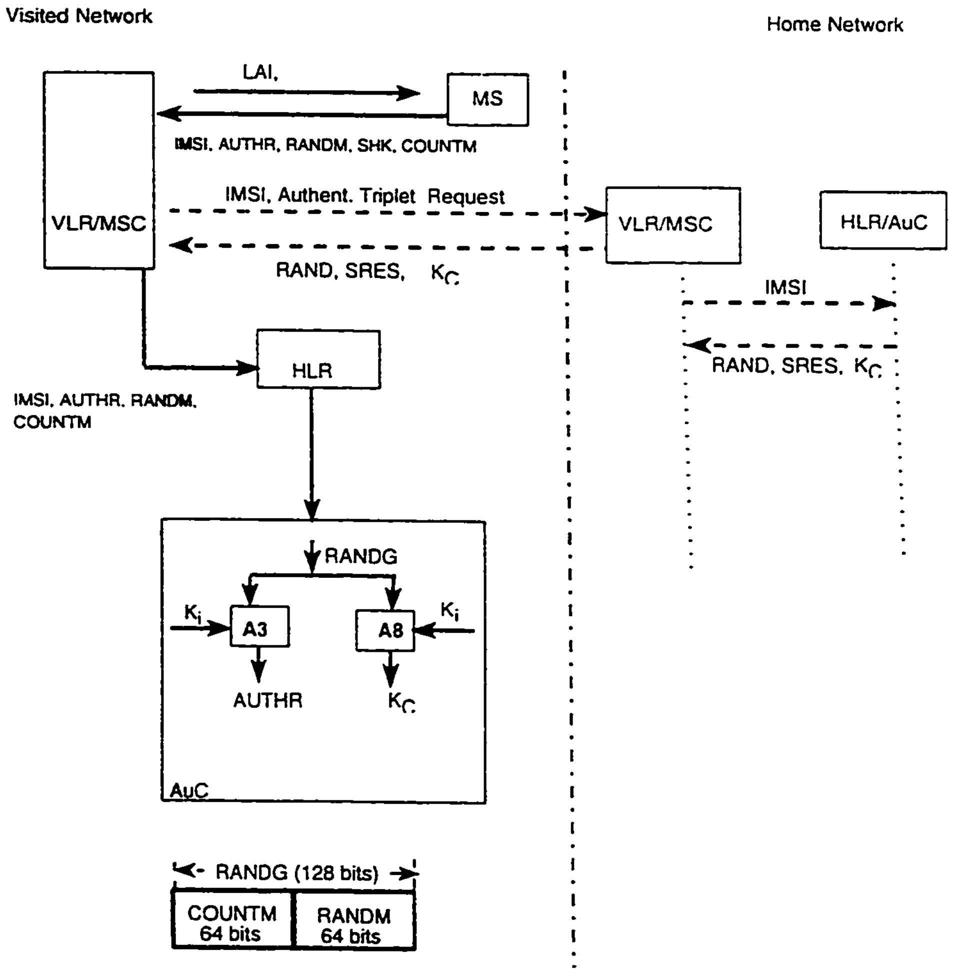
The received MNC is verified if it is stored in the SIM card or not, which means that the corresponding network is sharing the user's private key.



MCC: Mobile Country Code (3 digits), Home Country
MNC: Mobile Network Code (2 digits), GSM Home domain
LAC: Location Area Code (to identify location areas)
CI : Cell identity.

Figure 7.1: Location Area Identity information codes

The task of informing the network whether the user's key is shared or not, is carried out by a field in the service request message called sharing the key (SHK). The SHK will be set to one if the key is shared. Also to maintain the same structure of the protocol presented in Chapter 6, the mobile user counter COUNTM is assumed to be in the MS. For every activity, the COUNTM is changing and a RANDM is generated and an AUTHR is precomputed in the MS, to be used when the authentication process is needed. The COUNTM is sent to the visited network on the first registration only and it is deleted upon RMS deregistration. The AUTHR is the output of the A3 algorithm when RANDG and K_i are the inputs. RANDG is the concatenation of the a random number RANDM,



K_I: Individual subscriber authentication key (128 bits).
K_C=Cipher Key (64 bit).
RANDM=Random Number (64 bits).
RANDG=Random Number =RANDM & COUNTM (128 bits)
AUTHR=Athentication result (32 bits).
A3=Authentication Algorithm.

Figure 7.2: Proposed Authentication Scheme for Roaming users

generated by the MS. and the events log counter COUNTM as shown in Figure 7.2. The proposed scheme is as follows:

- * *Step1*: by comparing the received LAI from the visited network and the LAI of the home network. the MS detects that it has entered a new network area. thus the MS transmits a registration request (location update) to the base station over the SDCCH. The BTS forwards the registration request to the MSC which informs the corresponding VLR about this request. The registration request includes the TMSI/IMSI, LAI. the AUTHR. the RANDM. COUNTM and the SHK.

- * *Step2*: analyzing the IMSI. the VLR understands that this user is a roaming mobile station. then it checks for the SHK if it is one or not: if the SHK is one. the VLR interprets that as a registration request of a RMS whose key K_i is shared. then forwards the complete set to the HLR.

- * *Step3*: the HLR stores the COUNTM. then forwards the request message to the AuC.

- * *Step4*: the AuC produces the RANDG. then computes AUTHR and K_c by applying the MS's private key K_i and the RANDG number to the A3 and A8 algorithms respectively. Finally. the AuC compares the two AUTHRs. if the two are equal. the MS passes the authentication process.

When it is identified that the visited network is not sharing the RMS's private key. the field SHK is set to zero. The VLR will request the authentication triplet from the home network to proceed as in normal GSM authentication process.

7.2 Analysis of the Proposed Authentication Scheme

In evaluating our proposed scheme. we use the same protocol specification used in Section 6.2.1

* Service Provided.

  For the proposed scheme. the service provided is mainly to allow the GSM network to authenticate roaming mobile users having their private keys shared with the visited network.

* Protocol Environment.

  The protocol is executed in wireless environment. and between different network operators, therefore. there are possibility of intrusion. interception, masquerading and eavesdropping. The most important assumption is emphasizing on the mobile user's secret key K_i which is never transmitted on the air.

- Protocol Vocabulary.

The vocabulary of messages used is as follows:

-The service request, used to make a registration or call attempt.

-Authentication request, from VLR to HLR, or HLR to AuC and used to proceed with an authentication process for that IMSI.

-Acknowledgment, to acknowledge any received message between network elements.

- Messages Encoding. Messages are encoded with the following format:

MS ⟹ BTS

AUTHR (32 bits), SEVREQ (8 bits), IMSI (15 bits), LAI (40 bits), RANDM (64 bits), SHK (1 bit), COUNTM (64 bits).

VLR ⟹ HLR

AUTHR (32 bits), IMSI (15 bits), RANDM (64 bits), COUNTM (64 bits)

HLR ⟹ AuC

AUTHR (32 bits), IMSI (15 bits), RANDM (64 bits), COUNTM (64 bits).

- The Procedure Rules.

The procedure rules are represented in signaling message flow shown in Figure 7.3

The security requirements are still maintained since the private key is only known by the home and visited networks, and it is never transmitted on the air interface . The proposed scheme is built on the same GSM security principles. An AUTHR is computed in the MS, and in the AuC, using user's private key K_i and random number. Then, the network compares them. We also have AUTHR, RANDM, IMSI, and SHK as public information and they are sent in the air. K_i, K_c, are considered to be private keys and never sent in the air. However, in GSM approach K_c is sent with the triplet to the visited network. The proposed protocol is generating less signaling load than the GSM approach. The signaling messages flow is illustrated in Figure 7.3. Table 7.1 outlines the number of signaling messages per authentication request.

Internetwork messages are usually increasing the authentication delay, thus making the call setup time longer.

7.3 Comparison and Discussion

Gaining access to visited network while a mobile user is roaming is very important. In GSM, any failure in the home domain resources or in the internetwork signaling nodes, can prevent these roaming users from making or receiving calls. The conventional GSM authentication protocol relies

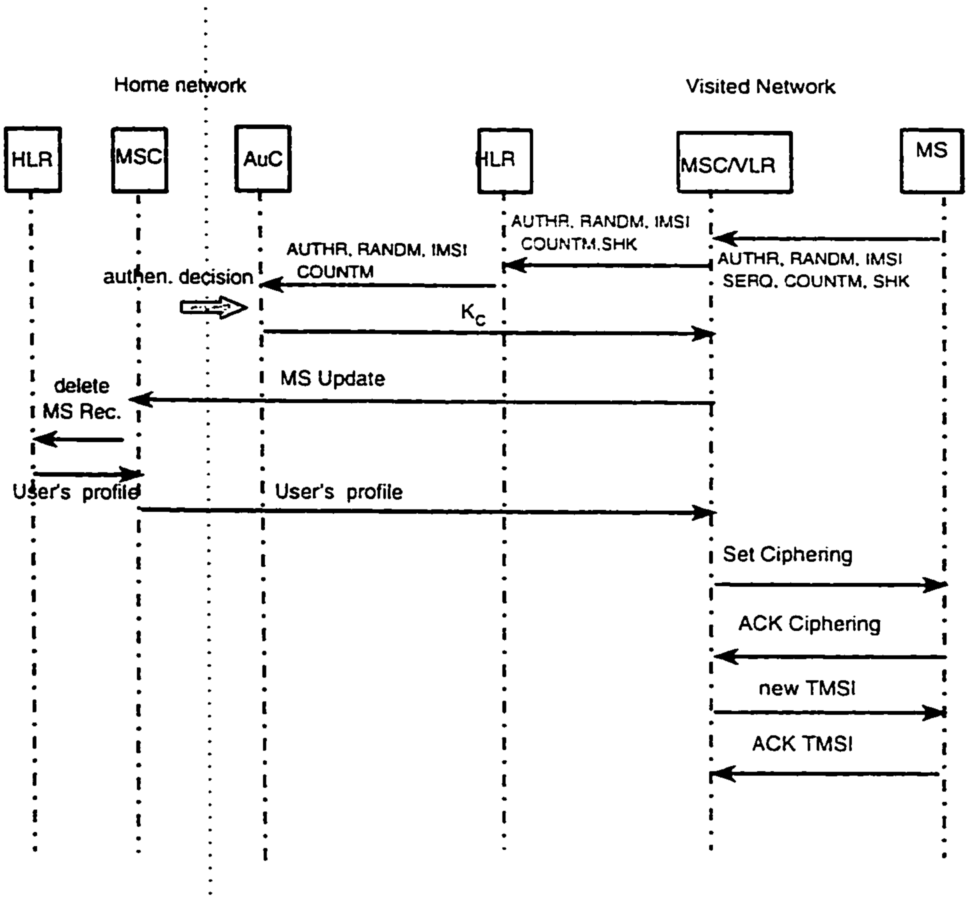


Figure 7.3: Signaling messages for the proposed authentication scheme: Roaming users

on the internetwork signaling (SS7 system) to provide visited networks with the authentication triplets. However. this concept is generating an important overhead besides the delay in the call setup time. The cost for that is important and it is a burden to both networks. The main risk here. is that the failure of the home domain equipment or a congestion in the internetwork links can lead to a complete isolation of that roaming user. The signaling messages add an extra load for home domain as well as the visited network. In addition to that. roaming users will be out of service (can not make or receive calls) in case of failure of any of the home network databases or the internetwork links. In peak traffic hours. where the trunks/circuits between the home and the visited networks are completely used, roaming users can not benefit from their PCS services to which they subscribe. Our proposed scheme is outperforming the conventional GSM scheme in terms of signaling messages and authentication delay. In Table 7.1 and Table 7.2. the difference is clear. especially in the internetwork signaling messages. The proposed scheme preserves the same GSM security, the verification and validation of authentication concept is still maintained. Our scheme can be easily applied with countries having more than mobile network system operators like the United Kingdom or the "Benelux" countries (Luxemburg, Netherlands. and Belgium). The secret key can be shared between network operators in the same country or can be exchanged between them for users with high mobility traffic. Actually mobile networks are exchanging many valuable information such as the call charges, roaming users's profile, signaling data, and charging rates. The exchange of information between network operators is assumed to be always secure and it is transparent to mobile users. Going back to the home network, the same algorithm can be used. The COUNTM is sent for the first registration to the home network to update the old record (counter value) and the process is as described in Chapter 6. The drawbacks for our scheme is that the visited network must have the same A3 and A8 algorithms stored in the SIM card of the RMS, however, most of the network operators are relying on the standard GSM A3 and A8.

Table 7.1: Authentication messages of roaming users: Proposed scheme

	Old Network			Visited Network			InterMSC
Activity	Auc	HLR	VLR/MSC	AuC	HLR	VLR/MSC	
Regist.	0	0	0	2	2	2	0
Call Orig.	0	0	0	2	2	2	0
Call Term.	0	0	0	2	2	2	0

Table 7.2: Authentication messages of roaming user: GSM protocol

	Old Network			Visited Network			InterMSC
Activity	Auc	HLR	VLR/MSC	AuC	HLR	VLR/MSC	
Regist.	2	2	4	0	4	5	2
Call Orig.	2	2	4	0	4	5	2
Call Term.	2	2	4	0	4	5	2

7.4 Summary

In this chapter we have proposed a new authentication protocol that can be used to authenticate roaming users in GSM networks. The scheme is based on sharing the RMS private key K_i between the home domain and the frequently visited networks. In analyzing the proposed scheme it has been shown that it is performing better than the conventional GSM approach in terms of signaling load and authentication delay. The delay was basically due to internetwork message exchange and the processing time needed for that.

Chapter 8

Conclusion and Future Work

8.1 Conclusion

With the extensive use of open networks and distributed systems, security aspects became more vital. Gaining access to any systems is always restricted to legal and authentic users and is always assured by using strong security control mechanisms. In the last decades, these mechanisms have experienced an important evolution which is going almost in parallel with the communication systems revolution. With the emergence of wireless systems, using radio access, there are opportunities for fraud to be committed. The conventional technique used to assure security was the use of a password. However, in a wireless networking environment, this method is seldom secure.

First generation of mobile and cordless systems have been introduced without much attention being paid to security. They were prone to a number of security breaches, including eavesdropping on the radio path using low cost scanners, and theft of terminal identities for cloning or masquerading some mobile users. The standards being developed for second generation systems such GSM and DECT, are more ambitious in their scope than those for earlier generation systems, and most of these new systems are enhancing new integrated security features using mainly cryptographic mechanisms to provide authentication, privacy of communications on the radio path and user location privacy. Authentication is the process which ensures the verification of the identity of the SIM or the subscriber. The illegitimate use of service is certainly of concern with respect to proper billing. The main players in the authentication process are the SIM card, and the authentication center (AuC) of the home network. Both contain authentication algorithm, denoted by A3, and the secret authentication key K_i which is unique to each SIM. The procedure used for the authentication process and the derivation of the ciphering key K_c is called the challenge response mechanism using non-predictable random numbers (RAND). The mechanism starts once the network has received an authentication request and established the identity of the SIM. it transmits a random number RAND as a challenge to that SIM (inside the MS). The SIM computes the response to the challenge by using the algorithm A3 with RAND and the key K_i stored in it as input data. The result or the output is called signed response SRES which is transmitted to the network to be compared with the value computed locally in the AuC. The MS is granted access to the network only if the SRES received from the MS (computed in his SIM) and the value computed by the network are equal.

In this thesis work, we have studied and analyzed the GSM authentication protocol. then we have proposed two new approaches that can be used for authentication of GSM mobile users. The first proposed scheme can be used for authenticating users in their home domain network. Its idea is basically based on preparing the authentication result AUTHR in advance then sending it to the network with the user identification. We have introduced a new idea which consists of an event log counter used in the network and in the SIM card. All events such as registration, successful call attempts, SIM attach/detach are registered in the counter. The counter (COUNTM) is concatenated to the a random number RANDM (64 bits) generated from the MS to form a global random number RANDG (128 bits). The AUTHR is the output of the A3 algorithm when RANDG and K_i are the inputs. The analysis have shown that this proposed scheme compared to the GSM approach. is achieving better security level, less signaling messages overhead and almost half of GSM authentication delay. The second proposed scheme is dedicated to GSM roaming users with high mobility rate in visiting other networks. We have assumed that, upon an agreement between the home network and the frequently visited network. the private keys of these mobile users are shared between the two networks. Our devised scheme is almost the one used in local domain network described above. but extended with some modifications and extra fields. such as the SHK field used to inform the visited network that the MS private key is shared. The analysis have shown an important internetwork signaling messages reduction resulting in a shorter authentication delay.

8.2 Future Work

We have demonstrated through our work the importance of the security aspects in mobile communication networks. We have concentrated more on the Authentication and privacy as a major factors that characterize wireless networks and in particular the GSM standards. The most critical issue in evaluating authentication protocols is the call set-up performance and the overall load. The future scope of our work involves exploring the following aspects:

* to improve the time of call setup by decreasing the number of messages exchanged between network elements. This number of messages is considerably important for the case of international roaming when users are crossing different networks. The amount of signaling traffic that crosses network boundaries is of particular importance especially if we know that the cross-network signaling links are likely to be long distance, expensive and tend to be of lower bandwidth than intra-network signaling links. Protocols similar to what we have developed for internetwork roaming users can reduce the signaling load.

* to standardize the protocols used in privacy and authentication, A3 and A8 (A5 already is common for all GSM networks), preparing for a global security protocols that might be a good platform for the universal personal communication network/system.

Bibliography

[1] Anthony Acampora, " Wireless ATM: A Perspective on Issues and Prospects," *IEEE Pesonal Communications* , pp. 8-17, Aug. 1996.

[2] Ian F. Akyildiz, Joseph S. M. Ho and Yi-Bing Lin, " Movement-Based Location Update and Selective Paging for PCS Networks," *IEEE/ACM Transactions on Networking*, vol. 4, no. 4, pp. 629-638, Aug. 1996.

[3] Ashar Aziz, "Privacy and Authentication for Wireless Local Area Networks," *IEEE Personal Communications*, pp. 25-31, First Quarter 1994.

[4] Bora A.Akyol and Donald C. Cox, "Signaling Alternatives in a Wireless ATM Networks," *IEEE Journal on Selected Areas in Communications*, vol. 15, no. 1, pp. 35-49, January 1997.

[5] Colin Boyd, "Security Architectures Using Formal Methods," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp.431-

442, June 1993.

[6] Michel J.Beller, Li-Fung Chang, Yacov Yacohi, "Security for Personal Communications Services: Public-Key vs. Private Key Approaches," *IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communications*, pp. 23-28, Oct. 1992.

[7] Michael J.Beller, Li-Fung Chang.and Yacov Yacobi, "Privacy and Authentication on a Portable Communications System," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 6, pp. 821-829, Aug. 1993.

[8] Ray Bird, I.Gopal, Amir Herzberg, Philippe A.Janson, Shay Kutten, Refik Molha, and Moti Yung, "Systematic Design of a Family of Attack-Resistant Authentication protocols," *IEEE Journal On Selected Areas in Communications*, vol. 11, no. 5, pp. 445-453, June 1993.

[9] Dan Brown, "Techniques For Privacy and Authentication in Personal Communication systems," *IEEE Personal Communications*, vol. 2, no. 4, pp. 6-10, Aug. 1995.

[10] Timothy X. Bown and Seshadri Mohan, " Mobility Management for Personal Communications Systems," *IEEE Transactions on Vehicular Technology*, vol. 46, no. 2, pp. 269-278, May 1997.

[11] J.C.Cooke and R.L.Brewster, "Cryptographic security techniques for digital Mobile Telephones," *Int. Conf. on Selected Topics in Wireless Communications*, pp. 425-428, June 1992.

[12] Luis M. Correia and Ramjee Prasad, "An Overview of Wireless Broadband Communications," *IEEE Communications Magazine*, pp. 28-33, Jan. 1997.

[13] David A. Cooper and Kenneth P. Birman, "Preserving Privacy in a Network of Mobile Computers," *Proceedings 1995 IEEE Symposium on Security and Privacy*, pp. 26-38, May 8-10 1995.

[14] Giovanna D'Aria, Flavio Muratore, and Valerio Palestini, "Simulation and Performance of the Pan-European Land Mobile Radio System," *IEEE Transaction on Vehicular Technology*, vol. 41, no. 2, pp. 177-189, May 1992.

[15] John Dunlop, James Irvine, David Roberston, and Peter Cosimini, "Performance of a Statistically Multiplxed Access Mechanism for a TDMA Radio Interface," *IEEE Personal Communications*, pp. 56-64, June. 1995.

[16] Jerry D. Gibson, "The Mobile Communications Handbook," *IEEE CRC Press*, 1996.

[17] David Grillo, "Personal Communications and Traffic Engineering in

ITU-T: The Developing E.750-Series of Recommendations," *IEEE Personal Communications*, pp. 16-28, Dec. 1996.

[18] Thomas Hardjono and Jennifer Seberry, "Security Issues in Mobile Information Networks," *IEICE Trans. Fundamentals*, vol. E79-A, no.7, pp. 1021-1026, July 1996.

[19] Gerard J. Holzman, "Design and Validation of Computer Protocols," *Prentice Hall*, 1991.

[20] Min-Shiang Hwang and Wei-Pang Yang, "Conference Key Distribution Schemes for Secure Digital Mobile Communications," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 2, pp. 416-420, Feb. 1995.

[21] Chih-Lin I, Gregory P. Pollini and Richard D. Gitlin, " PCS Mobility Management Using the Reverse Virtual Call Setup Algorithm," *IEEE/ACM Transactions on Networking*, vol.5, no.1, pp. 13-23, Feb. 1997.

[22] Jay Jayapalan and Mike Burke, "Cellular Data Services Architecture and Signaling," *IEEE Personal Communications*, Second Quarter, pp. 44-55, 1994.

[23] Bijan Jabbari, "Teletraffic Aspects of Evolving and Next-Generation Wireless Communication Network," *IEEE Personal Communica-*

tions, pp.4-8, Dec. 1996.

[24] Randy H. Katz, "Adaptation and Mobility in Wireless Information Systems," *IEEE Personal Communications*, First Quarter, pp. 6-17, 1994.

[25] Byung Chul Kim, Jin Seek Choi, and Chong Kwan Un, "A New Distributed Location Management Algorithm for Broadband Personal Communication Networks," *IEEE Transactions on Vehicular Technology*, vol.44, no.3, pp. 516-524, Aug. 1995.

[26] Timothy J. Kearns and Maureen C. Mellon, "The Role of ISDN in Global Networks," *IEEE Communication Magazine*, pp. 36-43, July 1990.

[27] Mikko Laitinen and Jari Rantala, "Integration of intelligent network services into future GSM Networks," *IEEE Communication Magazine*, pp. 76-85, June 1995.

[28] Derek Lam, Donald C.Cox and Jennifer Widom, "Teletraffic Modeling for Personal Communications Services," *IEEE Communications Magazine* , pp. 79-87, Feb. 1997

[29] Gregory S. Lauer, "IN Architectures for Implementing Universal Personal Telecommunications," *IEEE Network*, pp. 6-16, Mar./Apr. 1994.

[30] Thomas F. La Porta, Malathi Veeraraghavan, Philip A. Treventi, and Ramachandran Ramjee, "Distributed Call Processing for Personal Communications Services," *IEEE Communication Magazine*, pp. 66-75, June. 1995.

[31] Thomas F. La Porta, Malathi Veeraraghavan, and Richard W. Buskens, "Comparison of Signaling Loads for PCS Systems," *IEEE/ACM Transactions on Networking*, vol.4, no.6, pp. 840-855, Dec. 1996.

[32] Yi-Bing Lin, "No Wires attached," *IEEE Potentials*, pp. 28-33, Oct./Nov. 1995.

[33] Yi-Bing Lin, "Determining the User Locations for Personal Communications Services Networks," *IEEE Transactions on Vehicular Technology*, vol. 43, no. 3, pp. 466-472, Aug. 1994.

[34] Ping Lin and Lin Lin, "Security in Enterprise Networking: A Quick Tour," *IEEE Communications Magazine*, pp. 56-61, Jan. 1996.

[35] Yi-Bang Lin and Steven K. Devries, "PCS Network Signaling Using SS7," *IEEE Personal Communications*, pp. 44-55, June 1995.

[36] Yi-Bing Lin, "Mobility Management for Cellular Telephony Networks," IEEE Parallel and Distributed Technology, pp. 65-74, Winter 1996.

[37] Yi-Bing Lin and Anthony Noerpel. "Implicit Deregistration in a PCS Network," *IEEE Transaction on Vehicular Technology*. vol. 43. no. 4. pp. 1006-1009. Nov. 1994.

[38] Yi-Bing Lin, "Reducing Location Update in a PCS Network," *IEEE/ACM Transactions on Networking*. vol.5. no.1. pp. 25-33. Feb. 1997.

[39] Yi-Bing Lin and Shu-Yuen Hwang. "Comparing the PCS Location Tracking Strategies." *IEEE Transactions on Vehicular Technology*. vol.45. no.1, pp. 114-120, Feb. 1996.

[40] Yi-Bing Lin, Seshadri Mohan and Anthony Noerpel, "PCS Channel Assignment Strategies for Hand-off and Initial Access." *IEEE Personal Communications*. pp. 47-56. Third Quarter. 1994.

[41] Ravi Jain, Yi-Bing Lin, Charles Lo, and Seshadri Mohan. "A Caching Strategy to Reduce NEtwork Impacts of PCS," *IEEE Journal on Selected Areas in Communications*, vol. 12, no. 8, pp. 1434-1444, Oct. 1994 .

[42] Andrew D. Malyan, Leslie J. Ng, Victor C.M Leung, and Robert W. Donaldson, "Network Architecture and Signaling for Wireless Personal Communications," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 6, pp. 830-840, Aug. 1993.

[43] Abdi R. Modarressi and Ronald A. Skoog, "Signaling System No. 7: a Tutorial," *IEEE Communications Magazine*, pp. 19-34, July. 1990.

[44] Kathleen S. Meier-Hellstern, "Network Protocols for the Cellular Packet Switch," *IEEE Transaction on Communications*, vol.42, no.2/3/4, pp. 1235-1243, Feb./Mar./Apr. 1994.

[45] Seshadri Mohan, "Privacy and Authentication Protocols for PCS ," *IEEE Personal Communications*, pp. 34-38, October 1996.

[46] Seshadri Mohan, Ravi Jain, "Two User location Strategies for Personal Communications Services," *IEEE Personal Communications*, pp. 42-50, First Quarter. 1994.

[47] Refik Molva, Didier Samfat and Gene Tsudik, "An Authentication Protocol For Mobile Users," *IEE Colloquium on Security and Cryptography Applications to Radio System*, London, UK, June 1994.

[48] Refik Molva, Didier Samfat, and Gene Tsudik, "Authentication of mobile users," *IEEE Network*, pp. 26-34, March/April 1994.

[49] Refik Molva, Patricia E. Wirth, "Teletraffic Implications of Database Architectures in Mobile and Personal Communications," *Computer Networks and ISDN Systems*, vol. 28, pp. 613-618, 1996.

[50] Biswanath Mukherjee, L. Todd Heberlin, and Karl N. Levitt, "Network Intrusion Detection," *IEEE Network*, pp. 26-41, May/June.

1994.

[51] B.Clifford Neuman. "Security, Payment, and Privacy for Network Commerce," *IEEE Journal on Selected Areas in Communications*, vol.13, no.8, pp. 1523-1530, Oct. 1995.

[52] Douglas Niehaus, Abdella Battou, and Andrew McFarland, "Performance Benchmarking of Signaling in ATM Networks," *IEEE Communication Magazine*, pp. 134-143, Aug. 1997.

[53] Donal O'Mahony, "Security Considerations in a Network Management Environment," *IEEE Network*, pp. 12-17, May/June. 1994.

[54] Raj Pandya, "Emerging Mobile and Personal Communication Systems," *IEEE Communication Magazine*, pp. 44-52, June. 1995.

[55] Gregory P. Pollini, Kathleen S. Meier-hellstern, and David J. Goodman, "Signaling Traffic Volume Generated by Mobile and Personal Communications," *IEEE Communications Magazine*, pp. 60-65, June 1995.

[56] Gregory P. Pollini, and David J. Goodman, "Signaling System Performance Evaluation for Personal Communications," *IEEE Transactions on Vehicular Tecnology*, vol. 45, no. 1, pp. 131-138, Feb. 1996.

[57] Mukesh M. Prabhu, S.V.Raghavan. "Security in Computer Networks and Distributed Systems," *Computer Communications*, vol. 19, pp.

11-19, May 1996.

[58] Moe Rahnema. "Overview of the GSM system and protocol Architecture," *IEEE Communication Magazine*. pp. 92-100. April 1993.

[59] Theodore S. Rappaport. "Wireless Communications," *IEEE CRC Press*. 1996.

[60] C.Rose. "Minimizing the average cost of paging and registration: A timer-based method," *Wireless Networks*. pp. 109-116. Feb. 1996.

[61] Izhak Rubin and Cheon Won Choi. "Impact of the Location Area Structure on the Performance of Signaling Channels in Wireless Cellular Network," *IEEE Communications Magazine*. pp. 108-115. Feb. 1997.

[62] Donald L. Schilling, " Wireless Communications Going into the 21 st Century," *IEEE Transactions on Vehicular Technology*, vol. 43, no. 3, pp. 645-651, Aug. 1994.

[63] Ron Schneiderman, "Wireless Personal Communications for Future Talk," *IEEE CRC Press*, 1996.

[64] Raymond Steele, "The Evolution of Personal Communications" *IEEE Personal Communications*. Second Quarter, pp. 6-11, 1994.

[65] Sami Tabbane, "An Alternative Strategy for Location Tracking, " *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 5,

pp. 880-892. June. 1995.

[66] R.Thomas. H. Gilbert. and G. Mazziotto. "Influence of the Mobile station on the Performance of the Radio Mobile Cellular Network." *Proc. 3rd Nordic Seminar*. Paper 9.4. Copenhagen. Danmark. Sept. 1988.

[67] M.J.Toussaint. "A New Method for Analysing the Security of Cryptographic Protocols." *IEEE Journal on Selected Areas in Communications*. vol. 11. No. 5. June 1993.

[68] Mohammed Zaid . "Personal Mobility in PCS." *IEEE Personal Communications*, Fourth Quarter. pp. 12-16. 1994.

[69] Andrew J. Viterbi. "The Evolution of Digital Wireless Technology from Space Exploration to Personal Communication." *IEEE Transactions on Vehicular Technology*. vol. 43. No. 3. pp. 638-643. Aug. 1994.

[70] Bernard Walke, Dietmar Petras. and Dieter Plassmann. " Wireless ATM: Air Interface and Network Protocols of the Mobile Broadband System," *IEEE Personal Communications*. pp. 50-56. Aug. 1996.

[71] Joseph E. Wilkes. "Privacy and Authentication Needs of PCS." *IEEE Personal Communications*. vol. 2. no. 4. pp. 11-15. Aug. 1995.

[72] Gert Willmann and Paul J. Kuhn. "Performance Modeling of Sig-

naling System No. 7." *IEEE Communications Magazine*. pp. 44-55. Jul. 1990.

[73] David R. Wilson. "Signaling System No. 7. IS-41 and Cellular Telephony Networking." *Proceeding of the IEEE*. vol. 80. no. 4. pp. 644-652. Apr. 1992

[74] Patricia E. Wirth. "Teletraffic Implication of Database Architectures in Mobile and Personal Communications." *IEEE Communications Magazine* . pp. 54-59. June 1995.

[75] Tzong-Chen Wu and Hung-Sung. "Authenticating Passwords Over an Insecure Channel." *Computers and Security*. vol. 15. no. 5. 1996.

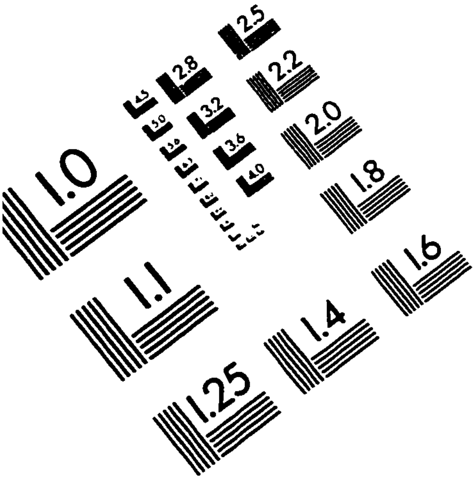
[76] Ning Zhang and jack M. Holtzman. "Analysis of Handoff Algorithms Using Both Absolute and Relative Measurements." *IEEE Transactions on Vehicular Technology*. vol. 45. no. 1. pp. 174-179. Feb. 1996.

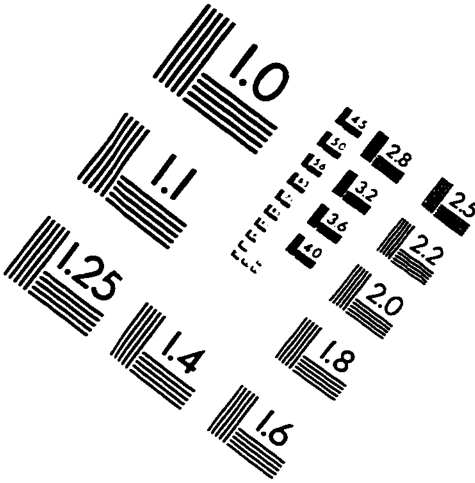
Vitae

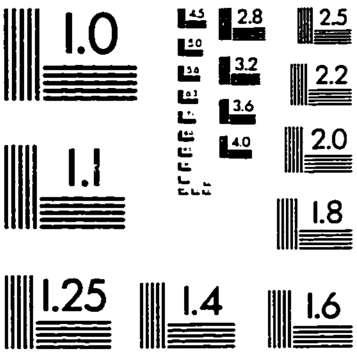
Name: ALI AKREMI

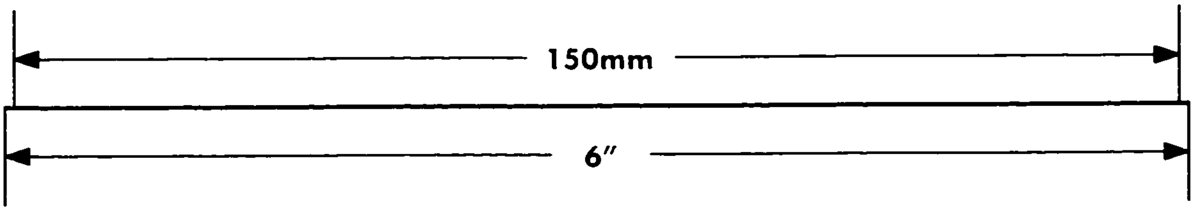
- * Received Bachelor of science in Telcommunications from "Ecole Superieure des Telecommunications, University of TUNIS, in 1985.
- * Joined the department of Computer Engineering at King Fahd University of Petroleum and Minerals in 1995.
- * Received Master of Science (M.S) degree in Computer Engineering from KFUPM in 1997.
- * Working since 1990 with Saudi Telecom as a Telecommunication Expert Engineer.

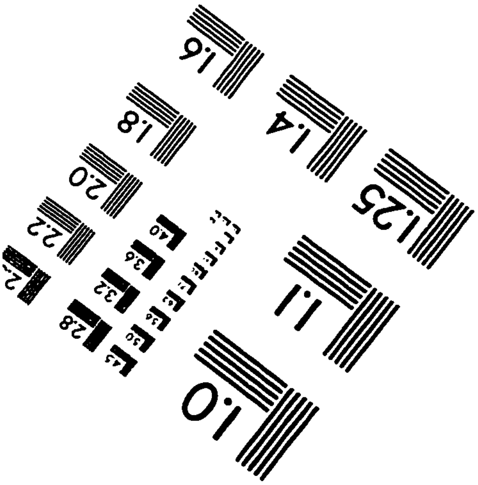
IMAGE EVALUATION
TEST TARGET (QA-3)











APPLIED IMAGE . Inc
1653 East Main Street
Rochester, NY 14609 USA
Phone: 716/482-0300
Fax: 716/288-5989

© 1993, Applied Image, Inc., All Rights Reserved