NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

GSM Authentication and Security

Graduation Project
EE- 400

Student: Nashat Mansour (20011777)

Supervisor: Prof. Dr. Fakhraddin Mamedov

Nicosia - 2004

ACKNOWLEDGMENT

First of all we would thank god who gave us power and supported us with the best instructors and advisors, and thanks to the projects advisor Assoc. Prof. Dr. Fakhreddin Mamedov who has shown patience and assistance in guiding us to overcome the difficulties in this project. So thanks after all to the N.E.U. who gave all students the opportunity to be better citizens in a better future.

I would thank my family who supported me financially and mentally within the recent terrible situation down in Palestine and dedicate this happiness to them and wish that I have made them proud of me after all, as I would dedicate it to all my friends in Turkey and Cyprus who shared with me the good days and the bad days.

Abstract

Security, Authentication and Access Control are vital features that must be present in any Communications Network. The need for these features is more in the case of Wireless Mobile Communications than in Wired Communications because of the ubiquitous shared nature of the Wireless Medium. With the 3rd generation Mobile Systems about to be deployed all over the world, the issue of security in mobile Communications has gained more importance. This report attempts to summarize the general requirements for Security, Authentication and Access Control for Mobile Personal Communications and the common techniques that are used/proposed in the 2nd and 3rd generation Mobile Communication Systems for satisfying these requirements.

Table of Contents

Definitions and Abbreviations

Definitions

Confidentiality: The Property that information has not been altered in an unauthorized manner.

Data Integrity: The Property that data has not been altered in an unauthorized manner.

Entity Authentication: The provision on assurance of the claimed identity of an entity

Mobile Station (MS), User: The combination of user equipment and a user access module.

User Access Module: Either a USIM (3G) or SIM (GSM)

Abbreviations

AKA - Authentication and Key Agreement

AN - Access Network

AUTN - Authentication Token

AV - Authentication Vector

CK - Cipher Key

CKSN - Cipher Key Sequence Number

CN - Core Network

CS - Circuit Switched

HE - Home Environment

HLR – Home Location Register

IK -Integrity Key

IMSI - International Mobile Subscriber Identity

KAC - Key Administration Centre

LAI - Location Area Identifier (Identity)

MAP - Mobile Application Part

MS - Mobile Station

MSC - Mobile Services Switching Center

MT - Mobile Termination

PS - Packet Switched

RAND - Random Challenge

SQN - Sequence Number

SGSN - Serving GPRS Support Node

SIM - Subscriber Identity Module (GSM)

SN - Serving Network

TMSI - Temporary Mobile Subscriber Identity

UE - User Equipment

UEA - UMTS Encryption Algorithm

UIA - UMTS Integrity Algorithm

USIM - User Services Identity Module

VLR - Visitor Location Register

XRES - Expected Response

TE - Terminal Equipment

Introduction

The ultimate goal of Mobile Personal Communication Systems is to bring ubiquitous access to telecommunication services into widespread use. To realize this goal, the designers of these systems must overcome a lot of challenges that come across their way.

One of the most significant challenges to the system designer is the protection of network and Subscriber assets from unauthorized use. The protection of Network and Subscriber assets can be realized only through the provisioning of Security, Authentication and Access Control in the Network. The term \Security" implies the protection of Subscriber assets on the Network and the terms \Authentication and Access Control" imply the protection of Network Assets. All these form a subsystem called the Security, Authentication and Access Control Subsystem of a Communication Network.

This article discusses the Requirements for this subsystem in the realm of Mobile Personal Communications and some common Techniques or Mechanisms that are implemented in such a subsystem to satisfy those Requirements. In addition, Case Studies about these requirements and techniques are provided in the end for two Mobile Communication Systems, the 2G GSM Systems and the 3GPP Systems.

CHAPTER ONE

1. THE GSM NETWORK

1.1 Overview

During the early 1980s, analog cellular telephone systems were experiencing rapid growth in Europe, particularly in Scandinavia and the United Kingdom, but also in France and Germany. Each country developed its own system, which was incompatible with everyone else's in equipment and operation. This was an undesirable situation, because not only was the mobile equipment limited to operation within national boundaries, which in a unified Europe were increasingly unimportant, but there was also a very limited market for each type of equipment, so economies of scale and the subsequent savings could not be realized.

The Europeans realized this early on, and in 1982 the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Group Special Mobile (GSM) to study and develop a pan-European public land mobile system. The proposed system had to meet certain criteria:

1. Good subjective speech quality
2. Low terminal and service cost
3. Support for international roaming
4. Ability to support handheld terminals
5. Support for range of new services and facilities
6. Spectral efficiency
7. ISDN compatibility

In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase I of the GSM specifications were published in 1990. Commercial service was started in mid-1991, and by 1993 there were 36 GSM networks in 22 countries. Although standardized in Europe, GSM is not only a European standard. Over 200 GSM networks (including DCS1800 and PCS1900) are operational in 110 countries around the world. In the beginning of 1994, there were 1.3

million subscribers worldwide, which had grown to more than 55 million by October 1997.

With North America making a delayed entry into the GSM field with a derivative of GSM called PCS1900, GSM systems exist on every continent, and the acronym GSM now aptly stands for Global System for Mobile communications.

The developers of GSM chose an unproven (at the time) digital system, as opposed to the then-standard analog cellular systems like AMPS in the United States and TACS in the United Kingdom. They had faith that advancements in compression algorithms and digital signal processors would allow the fulfillment of the original criteria and the continual improvement of the system in terms of quality and cost. The over 8000 pages of GSM recommendations try to allow flexibility and competitive innovation among suppliers, but provide enough standardization to guarantee proper inter working between the components of the system. This is done by providing functional and interface descriptions for each of the functional entities defined in the system.

1.2. Services provided by GSM

From the beginning, the planners of GSM wanted ISDN compatibility in terms of the services offered and the control signaling used. However, radio transmission limitations, in terms of bandwidth and cost, do not allow the standard ISDN B-channel bit rate of 64 kbps to be practically achieved.

Using the ITU-T definitions, telecommunication services can be divided into bearer services, tele-services, and supplementary services. The most basic tele-service supported by GSM is telephony. As with all other communications, speech is digitally encoded and transmitted through the GSM network as a digital stream. There is also an emergency service, where the nearest emergency-service provider is notified by dialing three digits (similar to 911).

A variety of data services is offered. GSM users can send and receive data, at rates up to 9600 bps, to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks, and Circuit Switched Public Data Networks using a variety of access methods and protocols, such as X.25 or X.32. Since GSM is a digital network, a

modem is not required between the user and GSM network, although an audio modem is required inside the GSM network to inter work with POTS.

Other data services include Group 3 facsimile, as described in ITU-T recommendation T.30, which is supported by use of an appropriate fax adaptor. A unique feature of GSM, not found in older analog systems, is the Short Message Service (SMS). SMS is a bi directional service for short alphanumeric (up to 160 bytes) messages. Messages are transported in a store-and-forward fashion. For point-to-point SMS, a message can be sent to another subscriber to the service, and an acknowledgement of receipt is provided to the sender. SMS can also be used in a cell-broadcast mode, for sending messages such as traffic updates or news updates. Messages can also be stored in the SIM card for later retrieval.

Supplementary services are provided on top of tele-services or bearer services. In the current (Phase I) specifications, they include several forms of call forward (such as call forwarding when the mobile subscriber is unreachable by the network), and call barring of outgoing or incoming calls, for example when roaming in another country. Many additional supplementary services will be provided in the Phase 2 specifications, such as caller identification, call waiting, multi-party conversations.

1.3. Architecture of the GSM network

A GSM network is composed of several functional entities, whose functions and interfaces are specified. Figure 1.1 shows the layout of a generic GSM network. The GSM network can be divided into three broad parts. The Mobile Station is carried by the subscriber. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center (MSC), performs the switching of calls between the mobile users, and between mobile and fixed network users. The MSC also handles the mobility management operations. Not shown is the Operations and Maintenance Center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile services Switching Center across the A interface.

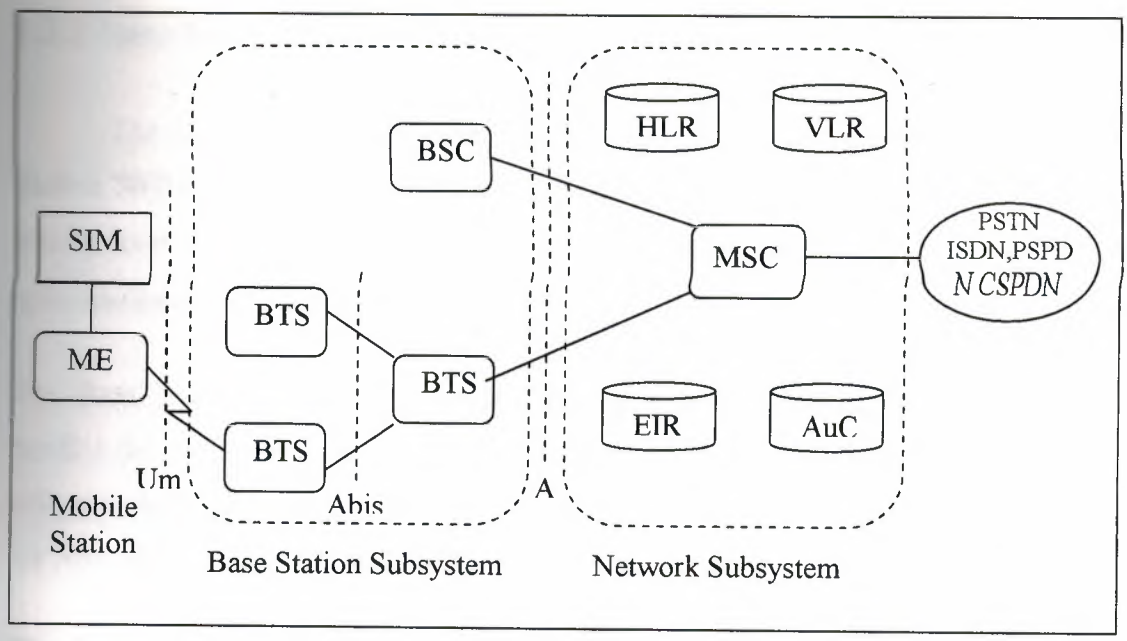

Figure 1.1 General Architecture of a GSM Network

1.3.1 Mobile Station

The mobile station (MS) consists of the mobile equipment (the terminal) and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to subscribed services irrespective of a specific terminal. By inserting the SIM card into another GSM terminal, the user is able to receive calls at that terminal, make calls from that terminal, and receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. The IMEI and the IMSI are independent, thereby allowing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

1.3.2 Base Station Subsystem

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the standardized Abis interface, allowing (as in the rest of the system) operation between components made by different suppliers.

The Base Transceiver Station houses the radio transceivers that define a cell and handles the radio-link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTSs deployed, thus the requirements for a BTS are ruggedness, reliability, portability, and minimum cost.

The Base Station Controller manages the radio resources for one or more BTSs. It handles radio-channel setup, frequency hopping, and handovers, as described below. The BSC is the connection between the mobile station and the Mobile service Switching Center (MSC).

1.3.3 Network Subsystem

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the fixed networks (such as the PSTN or ISDN). Signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7), used for trunk signaling in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call-routing and roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The location of the mobile is typically in the form of the signaling address of the VLR associated with the mobile

station. The actual routing procedure will be described later. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The Visitor Location Register (VLR) contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, all manufacturers of switching equipment to date implement the VLR together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, thus simplifying the signaling required. Note that the MSC contains no information about particular mobile stations --- this information is stored in the location registers.

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center (AuC) is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel.

1.4 Radio Link Aspects

The International Telecommunication Union (ITU), which manages the international allocation of radio spectrum (among many other functions), allocated the bands 890-915 MHz for the uplink (mobile station to base station) and 935-960 MHz for the downlink (base station to mobile station) for mobile networks in Europe. Since this range was already being used in the early 1980s by the analog systems of the day, the CEPT had the foresight to reserve the top 10 MHz of each band for the GSM network that was still being developed. Eventually, GSM will be allocated the entire 2x25 MHz bandwidth.

1.4.1 Multiple Access and Channel Structure

Since radio spectrum is a limited resource shared by all users, a method must be devised to divide up the bandwidth among as many users as possible. The method chosen by GSM is a combination of Time- and Frequency-Division Multiple Access (TDMA/FDMA). The FDMA part involves the division by frequency of the (maximum) 25 MHz bandwidth into 124 carrier frequencies spaced 200 kHz apart. One or more carrier frequencies are assigned to each base station. Each of these carrier frequencies is then divided in time, using a TDMA scheme. The fundamental unit of time in this TDMA scheme is called a *burst period* and it lasts 15/26 ms (or approx. 0.577 ms). Eight burst periods are grouped into a *TDMA frame* (120/26 ms, or approx. 4.615 ms), which forms the basic unit for the definition of logical channels. One physical channel is one burst period per TDMA frame.

Channels are defined by the number and position of their corresponding burst periods. All these definitions are cyclic, and the entire pattern repeats approximately every 3 hours. Channels can be divided into *dedicated channels*, which are allocated to a mobile station, and *common channels*, which are used by mobile stations in idle mode.

1.4.1.1 Traffic Channels

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multi-frame, or group of 26 TDMA frames. The length of a 26-frame multi-frame is 120 ms, which is how the length of a burst period is defined (120 ms divided by 26 frames divided by 8 burst periods per frame). Out of the 26 frames, 24 are used for traffic, 1 is used for the Slow Associated Control Channel (SACCH) and 1 is currently unused (see Figure 1.2). TCHs for the uplink and downlink are separated in time by 3 burst periods, so that the mobile station does not have to transmit and receive simultaneously, thus simplifying the electronics.

In addition to these *full-rate* TCHs, there are also *half-rate* TCHs defined, although they are not yet implemented. Half-rate TCHs will effectively double the capacity of a system once half-rate speech coders are specified (i.e., speech coding at around 7 kbps, instead of 13 kbps). Eighth-rate TCHs are also specified, and are used for signaling. In

the recommendations, they are called Stand-alone Dedicated Control Channels (SDCCH).

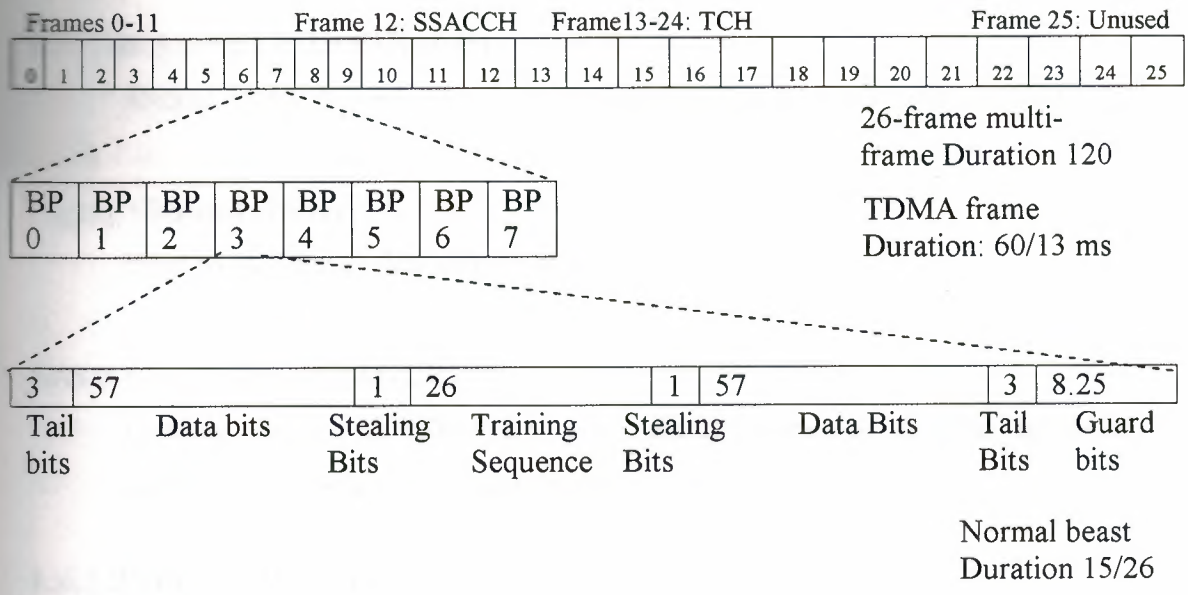

Figure 1.2. Organization of bursts, TDMA frames, and multi-frames for speech and data

1.4.1.2 Control Channels

Common channels can be accessed both by idle mode and dedicated mode mobiles. The common channels are used by idle mode mobiles to exchange the signaling information required to change to dedicated mode. Mobiles already in dedicated mode monitor the surrounding base stations for handover and other information. The common channels are defined within a 51-frame multi-frame, so that dedicated mobiles using the 26-frame multi-frame TCH structure can still monitor control channels. The common channels include:

Broadcast Control Channel (BCCH)

Continually broadcasts, on the downlink, information including base station identity, frequency allocations, and frequency-hopping sequences.

Frequency Correction Channel (FCCH) and Synchronization Channel (SCH)

Used to synchronize the mobile to the time slot structure of a cell by defining the boundaries of burst periods, and the time slot numbering. Every cell in a GSM

network broadcasts exactly one FCCH and one SCH, which are by definition on time slot number 0 (within a TDMA frame).

Random Access Channel (RACH)

Slotted Aloha channel used by the mobile to request access to the network.

Paging Channel (PCH)

Used to alert the mobile station of an incoming call.

Access Grant Channel (AGCH)

Used to allocate an SDCCH to a mobile for signaling (in order to obtain a dedicated channel), following a request on the RACH.

1.4.1.3 Burst Structure

There are four different types of bursts used for transmission in GSM. The normal burst is used to carry data and most signaling. It has a total length of 156.25 bits, made up of two 57 bit information bits, a 26 bit training sequence used for equalization, 1 stealing bit for each information block (used for FACCH), 3 tail bits at each end, and an 8.25 bit guard sequence, as shown in Figure 3.2 The 156.25 bits are transmitted in 0.577 ms, giving a gross bit rate of 270.833 kbps.

The F burst, used on the FCCH, and the S burst, used on the SCH, have the same length as a normal burst, but a different internal structure, which differentiates them from normal bursts (thus allowing synchronization). The access burst is shorter than the normal burst, and is used only on the RACH.

1.4.2 Speech Coding

GSM is a digital system, so speech which is inherently analog, has to be digitized. The method employed by ISDN, and by current telephone systems for multiplexing voice lines over high speed trunks and optical fiber lines, is Pulse Coded Modulation (PCM). The output stream from PCM is 64 kbps, too high a rate to be feasible over a radio link. The 64 kbps signal, although simple to implement, contains much redundancy. The GSM group studied several speech coding algorithms on the

basis of subjective speech quality and complexity (which is related to cost, processing delay, and power consumption once implemented) before arriving at the choice of a Regular Pulse Excited -- Linear Predictive Coder (RPE--LPC) with a Long Term Predictor loop. Basically, information from previous samples, which does not change very quickly, is used to predict the current sample. The coefficients of the linear combination of the previous samples, plus an encoded form of the residual, the difference between the predicted and actual sample, represent the signal. Speech is divided into 20 millisecond samples, each of which is encoded as 260 bits, giving a total bit rate of 13 kbps. This is the so-called Full-Rate speech coding. Recently, an Enhanced Full-Rate (EFR) speech coding algorithm has been implemented by some North American GSM1900 operators. This is said to provide improved speech quality using the existing 13 kbps bit rate.

1.4.3 Channel Coding and Modulation

Because of natural and man-made electromagnetic interference, the encoded speech or data signal transmitted over the radio interface must be protected from errors. GSM uses convolution encoding and block interleaving to achieve this protection. The exact algorithms used differ for speech and for different data rates. The method used for speech blocks will be described below.

Recall that the speech code produces a 260 bit block for every 20 ms speech sample. From subjective testing, it was found that some bits of this block were more important for perceived speech quality than others.

The bits are thus divided into three classes:

- **Class Ia** 50 bits - most sensitive to bit errors
- **Class Ib** 132 bits - moderately sensitive to bit errors
- **Class II** 78 bits - least sensitive to bit errors

Class Ia bits have a 3 bit Cyclic Redundancy Code added for error detection. If an error is detected, the frame is judged too damaged to be comprehensible and it is discarded. It is replaced by a slightly attenuated version of the previous correctly received frame. These 53 bits, together with the 132 Class Ib bits and a 4 bit tail sequence (a total of 189

bits), are input into a 1/2 rate convolution encoder of constraint length 4. Each input bit is encoded as two output bits, based on a combination of the previous 4 input bits. The convolution encoder thus outputs 378 bits, to which are added the 78 remaining Class II bits, which are unprotected. Thus every 20 ms speech sample is encoded as 456 bits, giving a bit rate of 22.8 kbps.

To further protect against the burst errors common to the radio interface, each sample is interleaved. The 456 bits output by the convolution encoder are divided into 8 blocks of 57 bits, and these blocks are transmitted in eight consecutive time-slot bursts. Since each time-slot burst can carry two 57 bit blocks, each burst carries traffic from two different speech samples.

Recall that each time-slot burst is transmitted at a gross bit rate of 270.833 kbps. This digital signal is modulated onto the analog carrier frequency using Gaussian-filtered Minimum Shift Keying (GMSK). GMSK was selected over other modulation schemes as a compromise between spectral efficiency, complexity of the transmitter, and limited spurious emissions. The complexity of the transmitter is related to power consumption, which should be minimized for the mobile station. The spurious radio emissions, outside of the allotted bandwidth, must be strictly controlled so as to limit adjacent channel interference, and allow for the co-existence of GSM and the older analog systems (at least for the time being).

1.4.4 Multipath Equalization

At the 900 MHz range, radio waves bounce off everything-buildings, hills, cars, airplanes, etc. Thus many reflected signals, each with a different phase, can reach an antenna. Equalization is used to extract the desired signal from the unwanted reflections. It works by finding out how a known transmitted signal is modified by multipath fading, and constructing an inverse filter to extract the rest of the desired signal. This known signal is the 26-bit training sequence transmitted in the middle of every time-slot burst. The actual implementation of the equalizer is not specified in the GSM specifications.

1.4.5 Frequency Hopping

The mobile station already has to be frequency agile, meaning it can move between a transmit, receive, and monitor time slot within one TDMA frame, which normally are on different frequencies. GSM makes use of this inherent frequency agility to implement slow frequency hopping, where the mobile and BTS transmit each TDMA frame on a different carrier frequency. The frequency hopping algorithm is broadcast on the Broadcast Control Channel. Since multipath fading is dependent on carrier frequency, slow frequency hopping helps alleviate the problem. In addition, co-channel interference is in effect randomized.

1.4.6 Discontinuous Transmission

Minimizing co-channel interference is a goal in any cellular system, since it allows better service for a given cell size, or the use of smaller cells, thus increasing the overall capacity of the system. Discontinuous transmission (DTX) is a method that takes advantage of the fact that a person speaks less that 40 percent of the time in normal conversation, by turning the transmitter off during silence periods. An added benefit of DTX is that power is conserved at the mobile unit.

The most important component of DTX is, of course, Voice Activity Detection. It must distinguish between voice and noise inputs, a task that is not as trivial as it appears, considering background noise. If a voice signal is misinterpreted as noise, the transmitter is turned off and a very annoying effect called clipping is heard at the receiving end. If, on the other hand, noise is misinterpreted as a voice signal too often, the efficiency of DTX is dramatically decreased. Another factor to consider is that when the transmitter is turned off, there is total silence heard at the receiving end, due to the digital nature of GSM. To assure the receiver that the connection is not dead, *comfort noise* is created at the receiving end by trying to match the characteristics of the transmitting end's background noise.

1.4.7 Discontinuous Reception

Another method used to conserve power at the mobile station is discontinuous reception. The paging channel, used by the base station to signal an incoming call, is structured into sub-channels. Each mobile station needs to listen only to its own sub-channel. In the time between successive paging sub-channels, the mobile can go into sleep mode, when almost no power is used.

1.4.8 Power Control

There are five classes of mobile stations defined, according to their peak transmitter power, rated at 20, 8, 5, 2, and 0.8 watts. To minimize co-channel interference and to conserve power, both the mobiles and the Base Transceiver Stations operate at the lowest power level that will maintain an acceptable signal quality. Power levels can be stepped up or down in steps of 2 dB from the peak power for the class down to a minimum of 13 dBm (20 milliwatts).

The mobile station measures the signal strength or signal quality (based on the Bit Error Ratio), and passes the information to the Base Station Controller, which ultimately decides if and when the power level should be changed. Power control should be handled carefully, since there is the possibility of instability.

This arises from having mobiles in co-channel cells alternating increase their power in response to increased co-channel interference caused by the other mobile increasing its power. This in unlikely to occur in practice but it is (or was as of 1991) under study.

CHAPTER TWO

2. Security, Authentication and Access Control Requirements

Specification or Design of any system begins with the requirements. To provide proper privacy, authentication and access-control for a mobile user, a cryptographic system is necessary and this section highlights the important requirements that the cryptographic system must satisfy. Some of the requirements are for the Air-Interface between the mobile user and the Network and others are for the databases that are stored in the network and information shared between network sub-systems during hand over, roaming etc,. Levels of Privacy are first defined followed by the outline of the different kinds of requirements that the Cryptographic system must satisfy.

2.1. Privacy Definitions

When privacy of users is considered, there can be four levels of privacy that could be defined [5].

2.1.1. Wired Equivalent Privacy (WEP)

his implies that the privacy provided by the wireless networks must be equivalent to their wired counterparts. The types of transactions that can be protected with this level of privacy are the routine everyday conversations of most people, especially those which are of personal nature. A Cryptographic system designed such that individual conversations might take an year or more to break would provide a secure enough system for most people.

2.1.2. Commercially Secure

This level is for conversations/transactions where proprietary information is discussed. Examples are stock transactions, mergers, acquisitions, contact negotiations, etc. This kind of security requires a Cryptographic system that takes at least 10-25 years to break.

2.1.3. Military/Government Secure

This level will be useful for the military activities of a country and the non-military government communications. The requirements for this level would be defined by the appropriate government agencies.

2.2. Requirements for End-User Privacy:

A subscriber for a Mobile System needs Privacy / Security in the following areas:

2.2.1. Security for Call-Setup information

During the Call-Setup process, the mobile terminal will communicate important call-setup information to the network. Some of the information that could be sent are: calling party number, calling card number (if any), service type requested, etc. All these information must be protected and secured from eaves-droppers.

2.2.2. Security for Speech

All Spoken communication must be properly encrypted by the cryptographic system, so that it cannot be intercepted by any eaves-dropper listening to \the radio-waves.

2.2.3. Privacy of Data

Wireless Networks have started providing high bandwidth data communication services and all these services must be encrypted properly (generally with a higher level of encryption than voice), so that they are not capable of being intercepted by someone listening the radio-waves.

2.2.4. Privacy of User-Location

Any leakage of specific signaling information on the network can lead to an eaves-dropper to approximately \locate" the position of a subscriber and thus hindering the subscribers privacy. The subscriber must be protected from such attacks on his privacy of location. Infect in the 3rd generation systems, User Positioning/Location and Location based Services are basic requirements. Thus Security of Location information becomes a still more stringent requirement in the case of the 3rd generation systems.

2.2.5. Privacy of Calling Patterns

Information related to traffic generated by a particular
user and his calling patterns should not be made available to eaves-droppers. Typical information are: caller-id, frequency of calls to some particular number, etc.

2.2.6. Privacy of User-ID

All Mobile Communication systems use some sort of a User- ID to identify its subscribers. This subscriber identification information (or the User-ID) must be protected from hackers. Transmission of this information (that too, in clear) either over the Air-Interface, or over the Network must be avoided as far as possible.

2.2.7. Privacy of Financial Transactions

All financial transactions like credit card purchases, bank-account information, etc must be given extra protection. Users may wish to speak their credit card number or punch them via the key-pad to make purchases and these information must be encrypted and protected from eaves-droppers.

2.3. Support of Roaming:

Most Mobile Communication Systems support \roaming" of users, wherein the user is provided service even if he moves into a region and led by a different service provider or a different network of the same service provider. Thus, there is requirement in the network for authenticating mobile users who roam into its area. The main problem here is that the subscriber related information that is useful for authentications present only in the Home Network of the user and is generally not accessible by the Visited (or Serving) Network. Thus, there must be a method by which subset of handset credentials are supplied to the Serving Network that is enough to authenticate the user. A complete disclosure of handset credentials may result in a security compromise.

2.4. Integrity Protection of Data

In addition to securing the data (signaling or user), there must be a provision in the network and the handset to \detect" or \verify" whether the data it receives has been altered or not. This property is called the Data Integrity. Signaling and User Data that are considered to be sensitive must be protected using this method.

2.5. Requirements for Preventing Theft of Service or Equipment:

Theft of Service and Equipment is a very serious problem in Mobile Personal Communications. The Network subsystem doesn't care whether a call has originated from a legitimate or from a stolen terminal as long as it bills the call to the correct account (the user cares though !!). There are two kinds of thefts that could be possible here, the theft of personal equipment and theft of the services offered by the service provider. The Cryptographic systems must be designed to make the reuse of stolen terminals difficult (or even impossible). Further, it should block the theft of service by techniques such as \cloning" of mobile phones, which can de done both by the hackers using stolen equipment, as well as legitimate users !!.

2.5.1. Cloning and Clone Resistant Design

Cloning" is a serious problem in contemporary mobile communication systems. Cloning refers to the ability of an imposter to determine information about a personal terminal and \clone" (or create a duplicate copy) of that personal terminal using the information collected. This kind of fraud can be easily accomplished by legitimate users of the network themselves, since they have all the information they need to clone their own personal terminal !! In this way, multiple users can use one account by cloning personal equipments. This is where equipment cloning causes a lot of problems. The Cryptographic system for the mobile network must incorporate some kind of \clone-resistant" design. The most obvious requirement for this design is the security of personal equipment information. This security must be provided for the air-interface, the network databases and the network interconnections so that personal equipment information is secure from imposters. Cloning also typically occurs in the installation and repair stages of the mobile equipment use and must be prevented.

2.5.2. User IDs and Provisioning

Since, the handset can be used by anyone, it is necessary to identify the correct person for billing purposes (i.e., the user must be identified to the Network). This may take the form a smart-card or a plug-in that plugs into a handset and is unique to a user. The process by which the network identifies the user is the Authentication process

2.5.3. Equipment Identifiers

In systems where the account information is separated (both logically and physically) from the handset (which is the case in all current mobile communication systems), stolen personal equipments and its resale could be an attractive and lucrative business. To avoid this, all personal equipment must have unique identification information that reduces the potential of stolen equipment to be re-used.

This may take the form of \tamper-resistant" identifiers permanently plugged into the and sets.

2.6. Requirements on Power / Bandwidth / Computational Usage:

Cryptographic Systems and Algorithms have varying computational complexities and some of them might produce encrypted outputs that occupy way too many bits of information more than the original. Since the Mobile Communication channels are limited by Power, Bandwidth and Battery life of handsets (which translates into the computational complexity requirement for the handset), the Cryptographic system must take into consideration the following requirements The algorithm used must be of limited computational complexity. (This applies to handsets limited by battery-power.).

_ The Encrypted outputs of the cryptographic algorithm must of limited size, so that it does not add much overhead to the system.

_ The Number of transactions between the mobile user and the network (in the case of Authentication, for example) must be as minimal as possible to conserve bandwidth and power.

2.7. Requirements on System Lifetime.

Since computing power increases by orders of magnitude every 5 years or so, a cryptographic algorithm that is difficult to break today can be a piece of cake tomorrow. This is an important fact that must be considered seriously while designing the Cryptographic system. The system must have edibility in the key lengths and the algorithm so that easy upgrade is possible from the old to the new system.

2.8. Export Control Requirements:

The U.S Federal Government considers Encryption to be a \sensitive" affair and any sale or export of technology requires export approval from the Government [2]. The basic principle is that any security technology that is exported outside the U.S must be within the \breaking" limits of the U.S Security Personnel. In case an export/import license is granted, the following is possible:

_ The Equipment (the Handset or the Network Elements) can be manufactured anywhere within the world.

_ The Equipment can be carried on trips outside the U.S.

On the other hand, if the Cryptographic system fails the security tests conducted by the Federal Government officials and an export/import license is denied, the followings laws are enforceable:

_All Personal Terminals must be made in the United States. All Personal Terminals made outside the United States will have their final assemble in the United States.

_ All Personal Terminals must be impounded (!) on leaving the United States. Since most of the companies dealing with Wireless/Mobile Communications aim to provide services to as many countries (and continents!) as possible, they better develop Cryptographic systems that pass the Export Control Tests. Again, the development of the Handsets and the Network Elements may take place at different development centers all around the world. This may require some additional export control requirements that must be taken in to consideration while making a final decision on the Cryptographic System to be developed. Further, different countries may have their own export control laws when it comes to export of Encryption Algorithms and these must be given proper consideration during the design.

2.9. Law Enforcement Requirements.

The U.S Federal Government has a requirement on Secure Communications that allows the Federal Security Personnel to monitor any conversation on the secure network for various reasons. This of course, can be done only upon court-order with a legitimate cause. All those security requirements that were discussed before this section to ensure Security and Privacy make it more difficult to support this requirement. Further, the Federal government requires that the call that must be monitored be either unencrypted or weakly encrypted or it must be able to get hold of the required keys for the monitoring process (possibly through a trusted Key-Escrow Agency).All the requirements discussed above make the design/selection of the Cryptographic system, a challenging one. The next section presents a general overview of Cryptography and commonly used Cryptographic systems.

2.10. Commonly used Security, Authentication and Access Control:

Techniques while the previous section highlighted some common cryptographic techniques, this section provides some applications of those techniques in the realm of the Wireless World, with some examples. As mentioned earlier, Authentication (or Access Control) is required to protect the Network Assets and Security (or Privacy) is required to protect the Subscriber Assets. In the wireless arena, the terms authentication and privacy are generally related to each other, since the derivation of the session key for further encryption of user data is done at the Authentication stage. From a designer's viewpoint, there are two-distinct stages in providing Privacy and Authentication and Key Agreement (AKA) - This is the process in which, the Network verifies the identity of the Mobile User and a session key is commonly derived for further encryption.

_ Encryption for Privacy - This is the process in which the session key derived in the previous stage is used to achieve encryption of user tragic for providing Privacy.From the above information, one can easily guess that the most challenging part in providing Privacy and Authentication in Mobile Networks in the AKA process. Once a session key/algorithm is securely established, developing an encrypted connection is a straight-forward issue. This section describes in detail, a general AKA model for establishing Access Control [4] and various techniques used in the 2nd generation (European (GSM) and North American (USDC)) and the 3rd generation PCS systems or Authentication and Key Agreement. Note that, the terms AKA and Access Control are used interchangeably in the following text. Encryption for Privacy is not covered in detail in this section.

Authentication and Key Agreement can be, in general, described using a a three-part security model [4].

1. The first part of the AKA process is Provisioning. It is the means by which the subscriber owning a personal handset acquires all the bondages that will enable the network to subsequently recognize him as a legitimate user.

2. The second part of the AKA process is comes into play when the subscriber has to verify his identity to a local network which, in general, may not be the home network to which he is registered (Support for Roaming).

3. The final part of the AKA model is the protocol that is executed to permit network access and establish a key for protection of user-traffic. In secret-key systems, this is

require exchange of certificates and modulo-exponentiation to complete the AKA transaction.

The discussions ensuing in this section are based on the three-part AKA model as described above (Refer fig (2.10.1)). Further, these techniques are implemented in a different fashion for Secret-Key and Public Key Systems. The first part of the discussion deals with secret-key systems like the GSM and USDC and the second part deals with certificate based AKA techniques which are proposed for the 3rd generation systems.

2.10.1. Secret Key Systems

The AKA proposals for two-secret key systems (GSM and USDC) will be explained in this section.

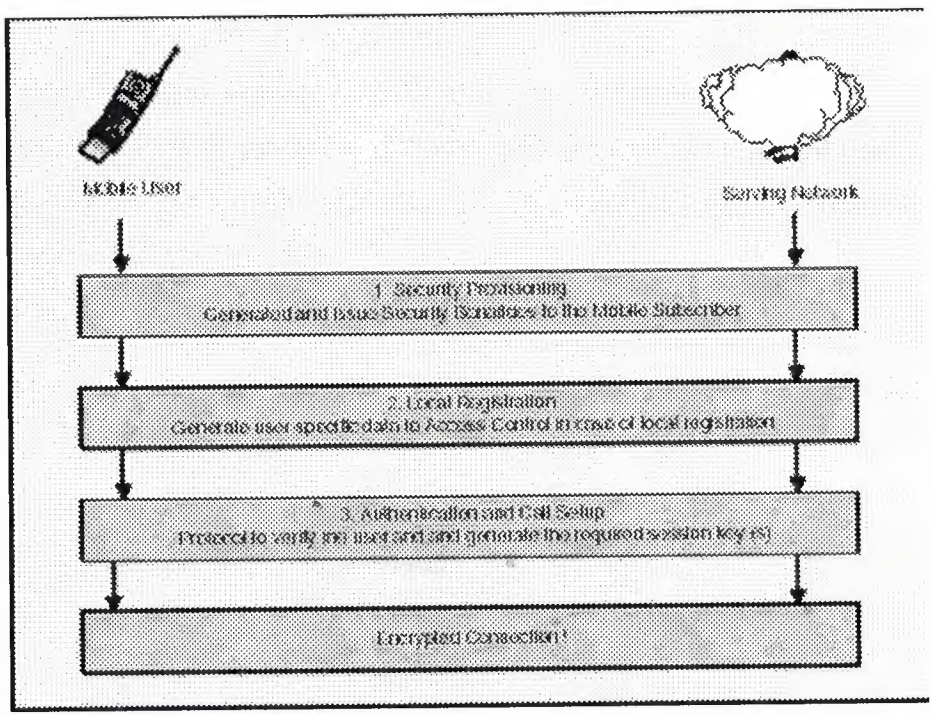

Figure 2.1 The AKA Model

2.10.1.1. Provisioning

In the 2nd generation European (GSM) systems, Provisioning is accomplished by the use of \Smart Cards" (called SIM cards). These SIM cards are issued when the user purchases the service from the service provider. This SIM often takes the form of a credit-card like device which can be inserted into the handset and contains information about his/her services that were purchased and also a 128-bit number called the \Ki" that is unique for each sim. The Ki enables the network to authenticate the user.

The Ki's never leaving the network of the home service provider. (Refer fig(2.2)). In the 2nd generation North A Mercian (USDC) Systems, Provisioning is accomplished by the use of a \A-key" that is issued to the subscriber during purchase of service. This \A-key" *is a 64-bit value that is issued to the subscriber in a confidential manner (via the U.S* Mail). The user has to enter this security parameter into his handset using the keypad.

The correct entry of the key is verified by the security software within the handset. Also, the service provider stores a copy of the \A-key" in the subscribers' home network. This direct way of informing the user about the security confides is intended to avoid the possible theft of service at the service shop or some careless miss-handling of security information in the middle. (Refer fig(2.2). A second function related to security provisioning in USDC is

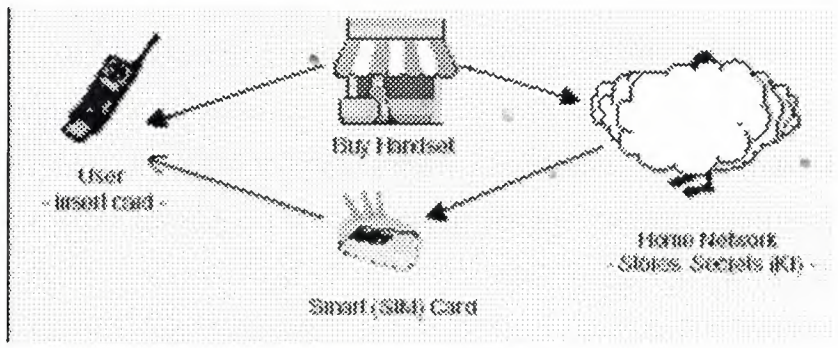

Figure 2.2 Security Provisioning in the GSM System

the derivation of a security variable called the \Shared Secret Data". This is intended tube shared between the user's home network and the visited network and is derived from the users \A-Key". This derivation process can be initiated only by the user's home network by means of an \over-the-air" protocol. The use of this data is explained in the next section.

Further, the \A-Key", like the Ki in GSM, never leaves the home network. Home Network

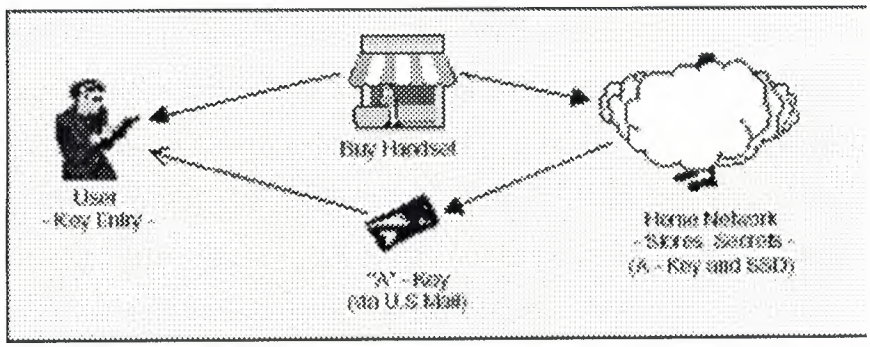

Figure 2.3 Security Provisioning in the US Digital Cellular System

2.10.1.2. Support for Roaming Access

The issue next to Provisioning of Service is the Support for Roaming Access. Mutual knowledge of secrets exchanged during provisioning allows a subscriber to be authenticated by his/her own home network. But when the subscriber moves into an area converged by another service provider, he must be still be provided service (Refer figure(2.3)). The service providers generally negotiate certain business agreements among themselves to support this \roaming facility" to the subscribers. But still an dilemma remains about the kind of authentication information that a subscriber has to provide to the \Serving Network" so that it can authorize that subscriber to receive service.

Further, all the databases corresponding to that subscriber are present in the home network to which the serving does not (infect, must not) have access. A sufficient amount of information has to be provided to the Serving Network (by the Home Network) to authenticate the user, but this information must not be adequate enough for

Network) to authenticate the user, but this information must not be adequate enough for someone in the Serving Network to impersonate the subscriber. Put simply, the Serving Network must be capable of authenticating the user, but the whole process must be controlled by the Home Network.

Both the 2nd Generation systems (USDC and GSM) have a Home Location Register (HLR) and Visitor Location Register (VLR) as integral parts of the Fixed Network. The HLR at the Switch is the Billing Database and stores all the billing information of subscribers such as Account Numbers and Secret Keys (the Kis in the case of GSM and the A-Key/SSD in the case of USDC). The VLR present in the Serving Network is the Location Database and stores information about the users who roam into the area over the Serving Network (Switch). The process of Access-Control with Roaming Support is depicted in Figure (2.10.1.3).

The user has roamed from his/her own Home Network (with the HLR) to a Serving \Network (VLR). An authentication will be performed by the VLR upon user handset registration with the VLR. The respective ow of information in the case GSM and the USDC systems will be described in the following sections

_ In the GSM System, for each subscriber the HLR stores additional information in the form of triplets that provide security information to the VLR without revealing the Ki. Each set of triples consists of a subscriber-unique random challenge RAND, an expected response SRES and a resulting cipher-key Kc. These triplets are sent to the VLR for registration. Thus, using this method, even the unauthorized interception of triplets cannot result in the permanent impersonation of the subscriber.

_ In the USDC System, the SSD is transported from the HLR to the VLR and the knowledge of the SSD enables the VLR to perform autonomous authentication of the user by deriving the challenge and the (expected) response locally. This local derivation of the challenge and the response eliminates the need for additional communication Between the HLR and the VLR for authentication. Any unauthorized interception of the SSD upon transport to the VLR could result in long-term impersonation of the subscriber. This is prevented by the use of a Call-Count for protection from this impersonation as well as handset cloning. Both the Handset and the Network maintain this Call-Count is incremented upon command from the Network. Any discrepancies in the Call-Counts maintained by the user and the network indicates theft of service and can be investigated by network personnel.

2.10.1.3. Authentication and Session Key Establishment

The final stage of the AKA process is the actual authentication protocol to be followed and the generation of the Cipher Key for further Encryption. The final goals are to assure the serving network that the handset is entitled to receive service and to develop a cipher-key for the protection of the subscriber bits over the air-interface. In both the 2nd generation systems considered, the authentication done through a challenge-response mechanism. The process is identical even if the mobile is present in the visited network, by virtue of the discussions in the previous section.

In GSM Systems, The Network begins the authentication process by either generating or selecting a random challenge/response pair, called the *RAND/SRES* respectively and sending the challenge to the mobile for authentication. A detailed description of this

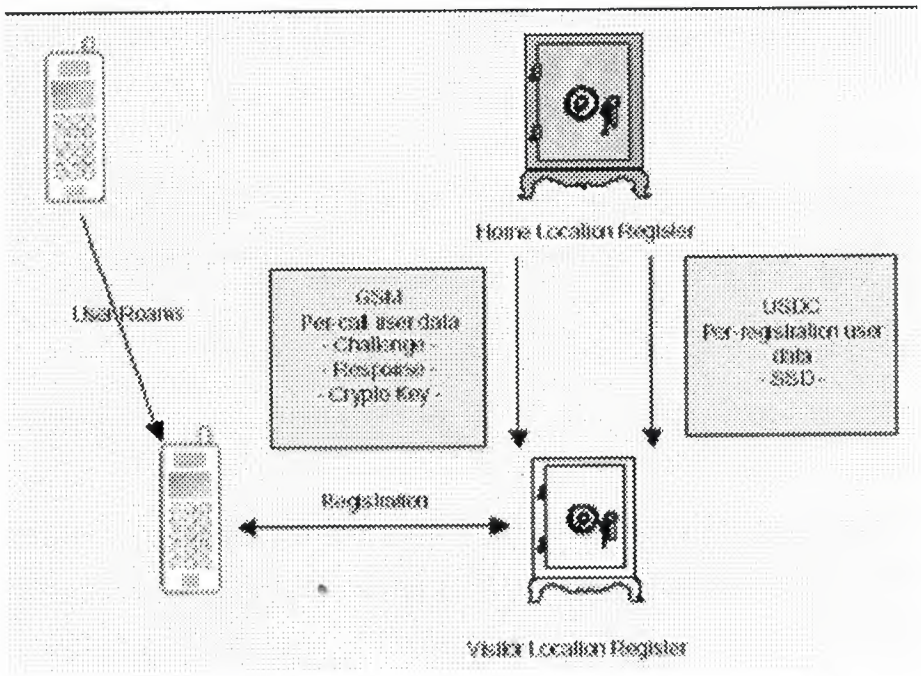

Figure 2.4 Support for Roaming Access

Challenge - response method is presented in the next section (the case-study on GSM), but Figure (2.4) provides a synopsis of the entire AKA process.

The USDC systems utilize the information in the SSD security variable to generate the challenge-response pairs. In these networks, a 32-bit global challenge is generated at frequent intervals and broadcast throughout the service area on a system information channel.

Handsets that require access to the service will compute a 18-bit authentication response *using an algorithm that uses the current global challenge and the SSD.*

This authentication response is concatenated with the registration/call-setup information and the call-count value and is sent to the home network (either from the handset or via the Serving Networks for verification. If the handset is found to be authentic and if it is currently served by a Serving Network, the SSD will be transported to the Serving Network. During a call-setup in the Serving Network, the SSD information stored locally in the Serving Network will be used to generate the challenge-response pairs and to generate the cipher keys for further encryption.

It is important to note that the authentication can do at any time at the discretion of the Home/Serving Network and that the user-identities are never transmitted in the clear-text format over the air-interface (there are exception to this, but only under some rare circumstances).

2.10.2. Public Key Systems

The Security and Authentication Protocols for the 3rd Generation PCS standards which about to emerge in the 2 GHz band are mostly some combination of the existing 2nd generation GSM/USDC standards (this is mainly done for compatibility reasons). In addition to the Secret Key mechanisms in the existing networks, few 3rd generation proposals (especially for PCS services) introduce new Public Key techniques that provide some additional benefits. Infect, these 3rd generation security proposals can be considered as some \hybrid" version of Secret-Key and Public Key Cryptosystems. In this section, we look at some possible uses of Public Key techniques in Mobile Communication Systems.

An outline of the a possible public-key mechanism proposed for the 3rd generation PCS systems is presented in Figure(2.5). For a detailed exposition, refer [7, 4].

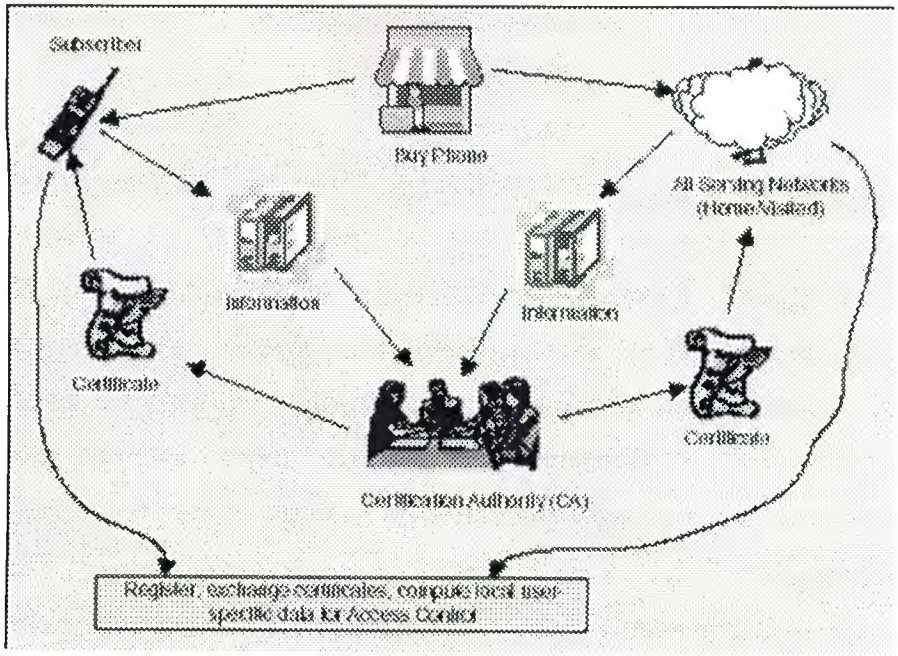

Figure 2.5 Certificate Based Public Key Systems

1. Provisioning begins when the user purchases a phone are requests for service.
2. The user then approaches a trusted \Certification Authority" (CA) with his credentials and some identification information about this handset (along with some information about the SIM module, if necessary).
3. The CA verifies the accuracy of the information and digitally \signs" a coded version of the information using its own Private Key. This signature cannot be impersonated by any other entity other than the CA. This signature forms the \certificate" for the user.
4. Any PCS Network can verify the authenticity of the certificate using the CA's public key, which can be obtained from some directories.
5. Once the certificate has bead issued to provision the particular handset, local security credentials are established with the serving network at the time of registration. This method avoids the generation of the triplets or the SSD the network transfer of this information .It is essential that the number of CAs be as minimum as possible so that they can be trusted by a large number of Service Providers. One obvious advantage of this Hybrid technique over the Secrecy Key techniques is that, the Private keys are never transmitted over the air (either in the clear-text or encrypted form) and this makes the life of the hackers all the more miserable.

CHAPTER THREE
3. Cryptography

Cryptography is traditionally defined as the art of secret writing. The basic service provided by Cryptography is the ability to send information between participants in a way that others cannot intercept or read it. Though there are many kinds of Cryptography, the ones most commonly used are those based on representing information as numbers and mathematically manipulating those numbers. This kind of cryptography provides integrity checking and authentication. This section provides a general overview of various types of cryptographic algorithms that are commonly used in practice.

Cryptographic concepts that are relevant for Wireless Communications are emphasized when necessary. Kaufman et al's book [1] provides good introduction reading material on Cryptography and Network Security Issues.

In traditional Cryptography, a message in its original form is known as plain-text or clear-text. The encrypted information is known as cipher-text and the process of producing this cipher-text is known as Encryption. The reverse process of Encryption is called as Decryption. Cryptographic Systems tend to involve an algorithm and a secret value. The secret value is known as the key. The reason for having a key in addition to an algorithms that it is difficult to keep devising new algorithms that will allow reversible scrambling of information.

There are three-types of Cryptographic functions :

_ Secret Key Cryptography.

_ Public Key Cryptography.

_ Hash Functions.

3.1. Secret Key Cryptography

Secret Key Cryptography involves the use of a single key. Given a message (or a plain-text), encryption produces the cipher-text, which is about the same length of the plain-text and decryption retrieves back the plain-text, using the same key used for Encryption. This kind of Encryption is also called as Conventional or Symmetric

Cryptography. The GSM and the U.S Digital Cellular Systems are primarily Secret Key Systems.

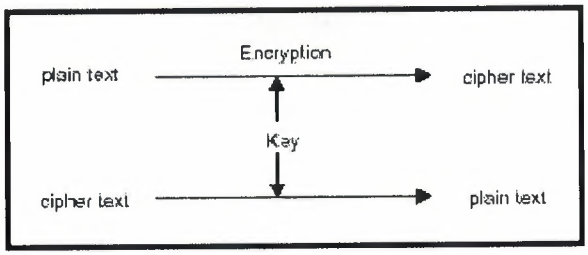

Figure 3.1 A Secret Key Cryptographic System

Secret Key Systems provide Strong Authentication functionality. This implies that someone can prove knowledge of a secret without revealing it, a functionality that is essential for Wireless Systems. Authentication is generally implemented using challenge-Response mechanism. For example, suppose A and B wish to communicate with each other and they decide upon a Key KAB to verify each other's identity. Each of them picks a random number, which is known as a Challenge and send it to each other.

The value of the random number, say x, encrypted with the Key KAB is known as the Response to the Challenge x. (This is shown in detail in Figure (3.1)). Thus, if A and B complete this exchange, they have proved to each other that they know KAB without revealing it to an imposter or an eaves-dropper. This kind of Challenge-Response mechanism is used in GSM and the USDC systems (and infect in most of the mobile communication systems) for authenticating a mobile user. One apparent aw in these kind of systems is that an eaves-dropper can form Challenge-Response pairs, since he can pose a challenge to either A or B and store the responses. To avoid this situation it is essential that the Challenges be chosen from a large enough space, say 2128 values, so that there is no significant chance of using the same challenge twice. Also, note that the Key KAB can also represent an algorithm AAB that uses the random number x and produces an encrypted value. Only A and B know the algorithm. (The GSM A3 Algorithm is one such algorithm).

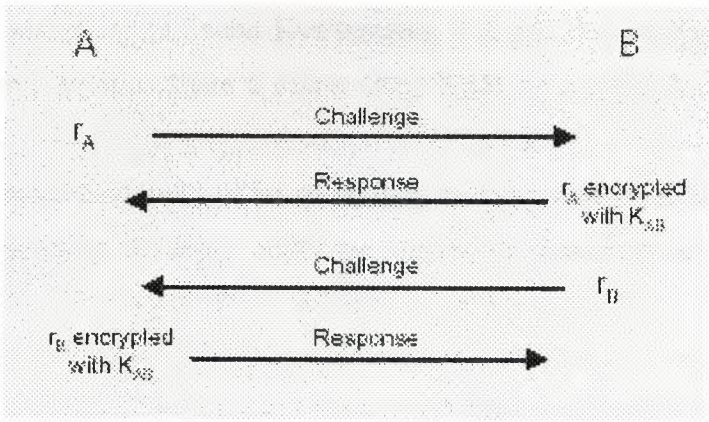

Figure 3.2 Challenge-Response Mechanism in Secret Key Systems

3.2. Public Key Cryptography

In Public key Cryptography, the keys are not shared. Instead, each individual user has two keys: a Private Key (that is not revealed to anyone) and a Public Key (that is open to the public). This kind of Cryptography is also commonly called as Asymmetric Cryptography and was invented by Define and Hellmann in 1975 [3].

In these systems, Encryption is done using the Public Key and Decryption is done using the Private Key (figure(3.1)). An Example of using Public Key Cryptography is described in the following paragraph.

Consider two people A and B wishing to communicate over an insecure channel (say, a Wireless Channel). Suppose A's <Public Key, Private Key> pair is < EA; DA > and B's pair is < EB; dB >. Assume that the public keys are known to both A and B (and the public). Figure (3,2) explains the procedure to be followed by A and B for communication.

Its clear that each person encrypts the data using the other person's Public Key which can Be decoded by the other person using his own Private Key. This kind of encryption/decryption is not much different from Secret Key Systems, but the biggest benefit of Public Key systems over Secret Key Systems comes from the Authentication mechanism.

In the case of Authentication in Secret Key systems, if A and B want to communicate with each other, they have to share a secret (Key KAB or Algorithm AAB) among themselves.

If one wants to communicate with a lot of entities he must remember a lot of secret key search corresponding to every entity he wishes to communicate. Public Key Cryptography

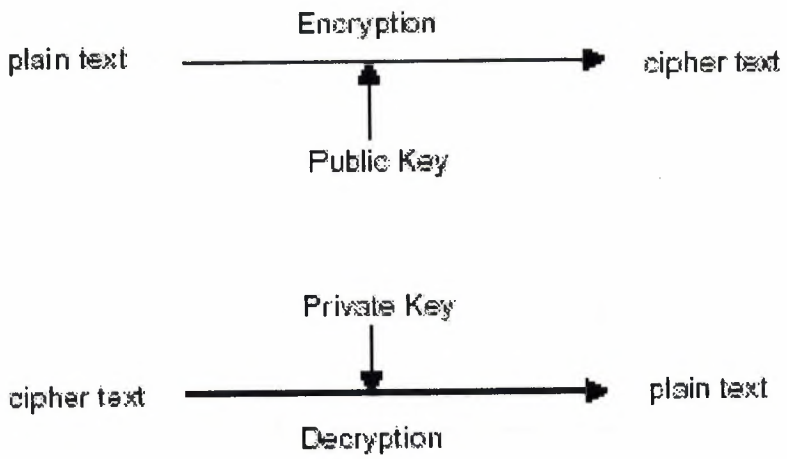

Figure 3.2.a. A Public Key Cryptographic System

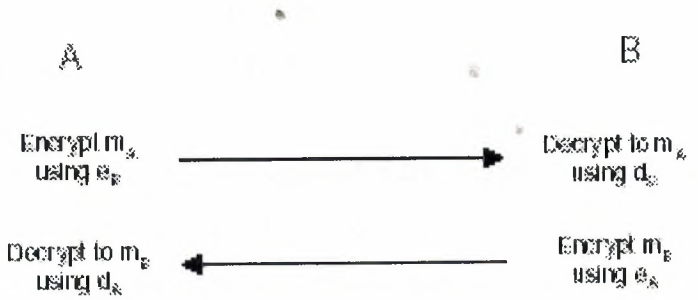

Figure 3.2.b. Information Transfer in a Public Key Cryptographic System

comes over this problem by the use of Public Keys. In this case, the entities who wish to communicate with each other have to remember only their Private Key. To communicate

with another entity, they have to \look-up" the Public Key of the other entity (from a Directory Server) and use it encrypt the messages to be communicated to that entity. For example, suppose A wants to verify (authenticate) B's identity. A chooses a random number encrypts it using B's Public Key and sends the result to B. Now, B can prove his identity by decrypting the encrypted message (the Challenge) using his Private Key and sending the decrypted random number r (the Response) back to A. shown in Figure(3.5)

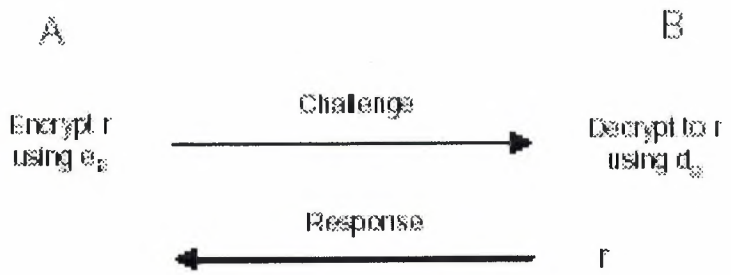

Figure 3.5. Authentication Mechanism in a Public Key System

Though Public Key systems provide a highly efficient Authentication mechanism, they are orders of magnitude slower than Secret Key systems. In case of communication networks, these public key systems require excessive computations and transfer of large-number of bits along power/bandwidth limited channels. So, these systems were not initially recommended for Wireless/Mobile Communications where Bandwidth and Power (and hence battery life of portable devices) are at a premium. This is one of the main reasons that the 2nd Generation Systems like GSM and the USDC were primarily Secret Key Systems.

But as 3rd generation systems with higher capacities are introduced, Private Key systems will begin to play an important role in providing Security, Authentication and Access Control.

Public Key Cryptography also facilitates digital signatures, whereby a person can \sign"a plain-text using his Private Key and anyone can verify the person's identity by using the Public Key of that person. Further, others cannot forge the signature of the person since it involves his private key. An illustration of Digital Signature presented in figure(3.6).

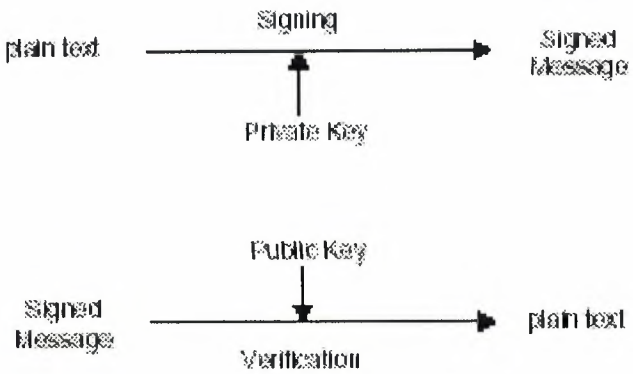

Figure 3.6 Digital Signatures in a Public Key System

3.3. Hash Algorithms

Hash Algorithms are also called as message-digests or one-way transformations. The basic idea of hashing or message-digesting is to mangle the information so badly that the process cannot be reversed. A typical example of message-digesting is password authentication in personal computer systems. For security reasons, the System does not store the actual (unencrypted) password, but a \hashed" or \digested value" of it. When a password is supplied, the system computes the \hashed" or \digested" value of the supplied password and compares it the stored hash value. If the hash values match, then the supplied password is deemed correct. Some systems, like the UNIX operating system, make the password files publicly readable (an expression of confidence in the security of the hasting algorithm). Hashing can also be used for other functions such as Message Fingerprinting, Digital Signatures, Message Integrity checking etc, the

Network Assets and Security (or Privacy) is required to protect the Subscriber Assets. In the wireless arena, the terms authentication and privacy are generally related to each other, since the derivation of the session key for further encryption of user data is done at the 4.

CHAPTER FOUR

4 .CASES STUDY OF GSM

4.1 Case Study-I: GSM Security

The GSM (Global System for Mobile Communications) is one of the most widely used 2nd Generation cellular systems in the world. GSM is a digital cellular system based on a combination of TDMA and FDMA. A part of the security in GSM comes from the fact that it is a digital system employing speech coding and channel coding algorithms, GMSK (Gaussian Minimum Shift Keying) Modulation, slow frequency hopping and a TDMA timeslot architecture. To intercept and reconstruct this signal would require more complicated and expensive equipment than a simple police scanner (as in the earlier analog systems).

An overview of the GSM Network architecture is first presented to the reader followed by a discussion of the Security, Authentication and Access Control procedures in GSM.

4.1.1 GSM Architecture

A GSM Network comprises of the Mobile Equipment (ME),the Subscriber Identity Module (SIM), the Base Station Transceiver (BTS), the Base Station Controller (BSC), the Transco ding Rate and Adaptation Unit (TRAU), the Mobile Services Switching Center (MSC), the Home Location Register, the Visitor Location Register (VLR), and the Equipment Identity Register (EIR). Together, the form a Public Land Mobile Network (PLMN) [11]. The network elements that are directly related to the security issues are covered in detail. [9] provides good introduction the GSM System. (Refer Fig(4.1)

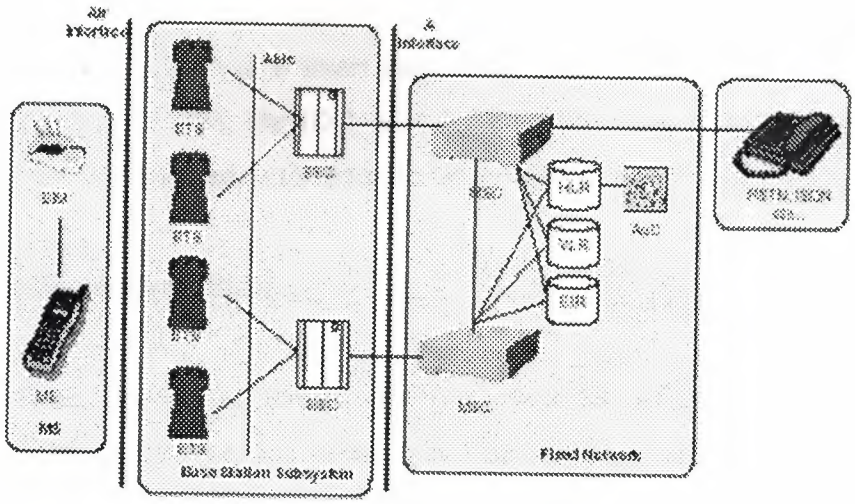

Figure4.1 GSM Architecture

4.1.1.1 Mobile Equipment

The term Mobile Equipment (ME) refers to the hand-held and portable devices supported by the GSM system.

4.1.1.2. Subscriber Identity Module

The identity of the subscriber and that of the mobile equipment are treated separately by the GSM System. The Subscriber Identity Module (SIM) determines the directory number and the calls billed to the subscriber. The SIM contains the following subscriber related information:

- The International Mobile Subscriber Identity (IMSI), which uniquely identifies a subscriber and without which the GSM service is not accessible. (Except for some specified emergency calls).
- A secret subscriber authentication key (Ki) and a cryptographic algorithm A3 which provide security functions for authenticating the SIM.
- Temporary network related data like the TMSI, LAI, Kc, forbidden PLMN's etc. (explained in later sections).
- Service related data like Language Preference and Advice of Charge.
- Card Holder Verification Information (CHV1/CHV2), the authenticates the user to the card and provides protection against the use of stolen cards.

Physically, the SIM looks like a smart card which can be inserted in the GSM ME. There are two types of SIM, the ID-1 SIM [13] and the Plug-in SIM [14]. The SIM together with the ME is called as the Mobile Station (MS).

4.1.1.3. Base Transceiver Station

The Base Transceiver Station (BTS) controls all the radio related tasks and provides connectivity between the network and the Mobile Station (MS) via the GSM Air Interface.

4.1.2.4. Base Station Controller

The Base Station Controller (BSC) takes care of all the central functions and controls a set of BTSs. The BSC and the controlled BTSs form the
Base Station Subsystem (BSS).

4.1.1.5. Mobile Switching Center

The Mobile Switching Center (MSC) controls a large number of BSCs. It is very similar to a digital telephone exchange or a switch and it handles the routing of incoming and outgoing calls and the assignment of user channels
on the A-interface.

4.1.1.6. Home Location Register

The HLR is a data repository that stores the subscriber specific parameters of a large no of subscribers. The most important parameters of a subscriber like the Ki, IMSI etc and stored in the HLR. Every PLMN requires at least one HLR and every user is assigned to one specific HLR. In most cases, the HLR contains an Authentication Center (AuC) as its integral part. The major function to the AuC is the calculation of authentication related parameters.

4.1.1.7. Visitor Location Register

The VLR network element was devised to off-load the HLR of user database related functions. The VLR, like the HLR, contains subscriber
Information, but only information for those subscribers who roam in the area for which the VLR is responsible. When a subscriber moves out of the VLR area, the HLR takes care of the relocation of this subscriber information from the old to the new VLR. A VLR may have several MSCs, but one MSC always uses one VLR.

4.1.1.8. Equipment Identity Register

Since, the subscriber identity (SIM) and the ME are treated independently by GSM, it is possible to operate any GSM ME with any valid GSM SIM. This will make cellular phone theft an attractive business and may start a possible black market for stolen GSM phones. To protect against such thefts, the Equipment Identity Register (EIR) was introduced in the GSM System. Every GSM Phone has a unique identifier, called the International Mobile Station Equipment Identity (IMEI), which cannot be altered without destroying the phone. It contains a serial number and a type identifier. On the HLR/VLR, the EIR maintains three lists:
The \White list" contains all the approved types of mobile stations.. The \Black list" contains all the mobile equipments known to be stolen or barred for various reasons. The \Grey list" allows tracing of related mobile stations.
Equipment Identification can be done by the network operator by requesting the IMEI from the ME.

4.1.2. GSM - Security/Authentication/Access Control Features

The GSM system promises to provide security over the air interface that is as good as the security offered by traditional fixed networks. The GSM standard specifies the following security features to be implemented in every PLMN.

- Subscriber identity (IMSI) confidentiality. This feature protects the Subscriber ID (IMSI) from being attacked by eaves-droppers.
- Subscriber identity (IMSI) authentication. This feature protects the Network Assets from Attacks by imposters.

- User data confidentiality on physical connections. This feature provides the protection of user speech data and other user related identification information.
- Connectionless user data confidentiality. This feature provinces protection of the message part of the connectionless user data pertaining to OSI layers 4 and above.
- Signaling information element confidentiality. This feature provinces protection to some of the network signaling information that are considered to be sensitive.

According to the standard, the implementation of these above features is mandatory over both the fixed and the access network sides. The mechanisms for implementing these features are explained in the following sections :

4.1.2.1. Subscriber Identity Confidentiality

This feature is implemented by means of Temporary Mobile Subscriber Identities (TMSIs). These TMSIs are local numbers and have significance only in a given Location Area (LA). The TMSI must be accompanied by a Location Area Identifier (LAI) to avoid ambiguities. Some of the requirements on the TMSI are:

- The new TMSI must be allocated at least in each location update procedure. This location updating whenever the mobile moves to a new Location Area (LA). Various location update scenarios involving MSCs and VLRs are illustrated in
- Whenever a new TMSI is allocated to a MS, it is transmitted to the MS in a ciphered mode. The MS should store the TMSI in a non-volatile memory together with the LAI so that these data are not lost whenever the mobile is switched off Note that, in some extreme cases (for example, when the HLR of the MS cannot be reached), the fixed network can request the MS to provide its IMSI in clear-text. These ends of situations must be avoided as far as possible.

4.1.2.2. Subscriber Identity Authentication

The GSM system is basically a Secret-Key System. The Authentication mechanism in GSM is a simple challenge-response mechanism depicted in figure (4.2). The procedure can be summarized as follows :

1. The Fixed Network transmits a non-predictable number RAND to the MS.

2. The MS computes the signature of RAND, say SRES, using an algorithm A3 and the secret key Ki and transmits the SRES back to the Fixed Network.

3. The Fixed Subsystem tests SRES for validity.

Note that, as already mentioned, the Authentication Parameters are transmitted to the VLR in the form of Authentication Vectors or Triplets that are generated by the HLR on request from the VLR. Again, various scenarios involving authentication during *location updating are presented in* .

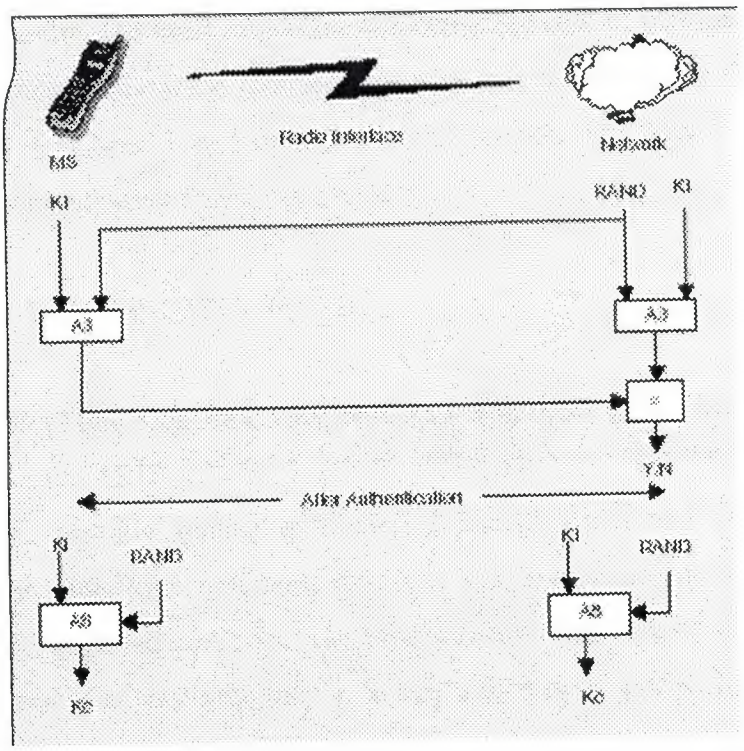

Figure4.2. Authentication And Access Control (AKA) in GSM

4.1.2.3. Confidentiality of Connectionless Data

User Information and Signaling information on Physical Connections. In GSM, the confidentiality of information (whether it is User data, Connectionless data or Signaling information) is achieved by means of a ciphering process using the Cipher Key Kc which is generated using the algorithm A8. The Ciphering Method is a stream cipher as described in .The Mutual Cipher-Keys between the MS and the Network are

set during the Authentication process(see fig(4.2)), thus constituting the AKA process for GSM.

The security mechanisms specified in the GSM standard made it one of the most secure cellular telecommunications system available during the time it was introduced. The use of authentication, encryption, and temporary identification numbers ensures the privacy and anonymity of the system's users, as well as safeguarding the system against fraudulent use.

But as time progressed, some of the security loop-holes in the GSM system started to show up very rapidly, the most important one being the lack of edibility and scalability of the entire security subsystem. The next section is a case study of the 3GPP-UMTS system which is developed based on the 2G-GSM system, but with the security-holes patched up and with additional security features.

4.2. Case Study-II 3GPP-UMTS Security

The 3GPP (Third-Generation Partnership Project) is a global-initiative involving organizations like the ARIB, CWTS, ETSI, T1, TTA and TTC. The 3GPP is involved in the production of globally applicable Technical Specifications and Technical Reports (called the 3GPP Specifications/Standards) for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support. This section provides an overview of the Security features specified by the 3G-UMTS standards. For a detailed exposition, the reader should consult the 3GPP Specifications

4.2.1. 3G Architecture

This section provides a very high level overview of the system architecture of the 3G-UMTS systems as specified by the 3GPP/ETSI .Functionally, all the network elements in the system are grouped into three entities:

- The Radio Access Network (UTRAN), that handles all radio-related functionality.
- The Core Network (CN), which is responsible for switching, routing calls and data connections to external networks.
- The User Equipment (UE), that interfaces with the User and the Radio Interface. The high-level system architecture of a 3G-UMTS based system is shown in Fig(15). The Network elements that are shown in the figure are logical network elements defined

by the 3GPP Specifications. It can be easily inferred that the 3G-UMTS system uses a similar (and well-known) architecture that has been used by all the main second generation and some first generation systems. An brief introduction to all the network elements is given below. Note that the Release-99 Specification [25] for the Universal Radio Access Network (UTRAN) by the ETSI (for UMTS) and the 3GPP are identical. Thus, the terms 3GPP Specifications and the UMTS Specifications are identical with respect to the UTRAN (Rel99). The Core Network (CN) explained in this section is based on the UMTS CN specifications

4.2.1.1. User Equipment (UE)

The UE consists of two parts:

- The Mobile Equipment (ME) is the radio terminal used for radio communication over the Uu Interface.
- The USIM (User Services Identity Module) is a smart-card (similar to the GSM SIM card) that holds the subscriber identity, authentication algorithms and stores the authentication and encryption keys and some subscriber related information.]

4.2.1.2. The Radio Access Network (UTRAN)

The UTRAN consists of two distinct logical elements:

- The Node-B is functionally similar to the Base Station (BTS) of the 2G systems. It converts the data ow between the Iu and Uu Interfaces and also takes part in some of the radio resource management.
- The Radio Network Controller (RNC) is functionally similar to the BSC (Base Station Controller) of the 2G systems. It owns and controls the radio resources in its domain (the Node-Bs connected to it).

4.2.1.3. The Core Network (CN)

The Core Network for the 3G-UMTS system is adopted from the 2G GSM CN. The main elements in the UMTS CN are:

- The Home Location Register (HLR) is a database located in the user's home network (as in the 2G Systems) that stores the master copy of the user's service profile. The

service profile consists of, for example, information on allowed services to the user, forbidden roaming areas, and supplementary service information such as status of call-forwarding and the call-forwarding number, etc. The HLR also stores the UE location on the level of the MSC/VLR and/or the Serving System.

- The Mobile Switching Center/Visitor Location Register (MSC/VLR) is the switch (MSC) and the database (VLR) that serves the UE in its current location for Circuit Switched (CS) Services. The MSC function is used to switch the CS transactions, and the VLR functionality is to hold a copy of the visiting user's service profile, as well as more precise information on the UE's location within the serving system. This part of the network that is accessed via the MSC/VLR is often referred to as the CS Domain.
- The Gateway Mobile Switching Center (GMSC) is the switch at the point where the UMTS PLMN is connected to external CS networks. All incoming and outgoing CS connections go through the GMSC.
- The Serving GPRS (General Packet Radio Service) Support Node (SGSN) functionality is similar to that of the MSC/VLR but is typically used for Packet Switched (PS) Services. The part of the network that is accessed via the MSC/VLR is often referred to as the PS Domain.
- The Gateway GPRS Support Node functionality is close to that of GMSC but is in relation to PS services.

4.2.2. 3G Security Principles

The whole 3G security architecture was designed based on three fundamental principles .

- The Security Architecture for 3G will build on the Security features of the Second-Generation systems Some of the robust features of Second generation systems will be retained.
- The 3G Security will improve on the security of the second-generation systems. Some security holes and disadvantages of 2G systems will be addressed and corrected in the 3G systems.

- 3G Security will offer new features and will secure new services offered by 3G.Before taking a look at the 3G Security Architecture, it good to take a look at the weaknesses of 2G Security, that were addressed in the 3G Security Specs.

4.2.2.1. 2G Security Weaknesses

- Active attacks using a false BTS is possible. This is because the mobile does not check the authenticity of the BTS while establishing a connection. It simply responds to the challenge posed to it.
- The cipher keys and the authentication data are transmitted in clear between and within Networks.
- Encryption, in most cases, is applied to the Air-Interface only. It does not extend far enough towards the core network resulting the clear-text transmission of signaling data across microwave and optical links. (For example, in GSM, from the BTS to the BSC).
- Data Integrity is absent in 2G Systems.
- 2G Systems were not built with a good edibility for up gradation.
- The Home Network (in 2G Systems) had no knowledge or control over how an nerving Network uses the authentication parameters supplied to it for authenticating roaming subscribers.

4.2.3. 3G Security Architecture

The 3G Specifications for Security defines 5 different Security features :

1. Network Access Security. The set of security features that provide users with secure access to 3G Services.

2. Network Domain Security. The set of security features that enable nodes in the provider domain to securely exchange signaling data, and protect against attacks on the wire line network.

3. User Domain Security. The set of Security features that secure access to mobile stations.

4. Application Domain Security. The set of Security features that enable applications in the user and in the provider domain to securely exchange messages.

5. Visibility and Configurability of Security. The set of Security features that enable the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

(Figure 4.3) provides an overview of the complete 3G Security Architecture. The mechanisms that are used to provide the above mentioned Security Features will be explored in the following sections.

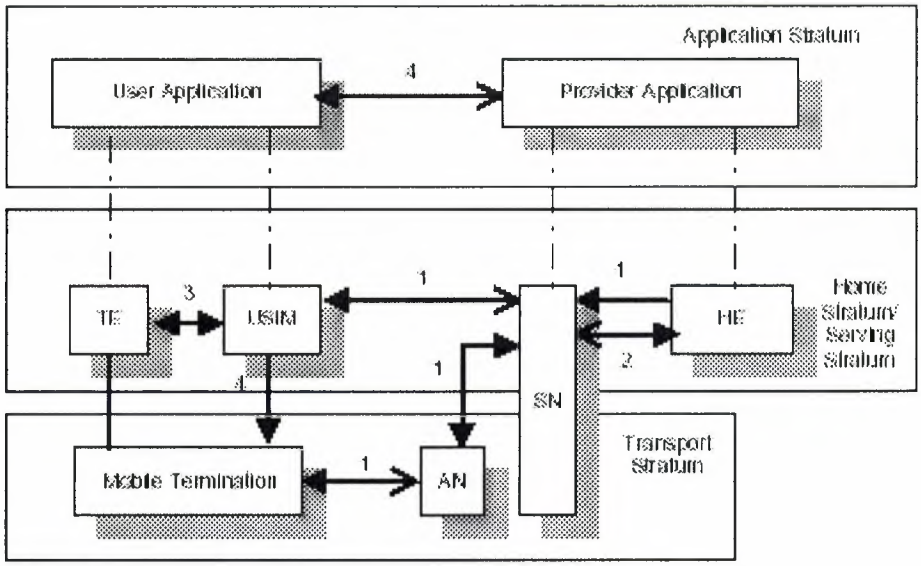

Figure 4.3. 3GPP-UMTS Security Architecture

(The numbers directly relate to the security features offered by 3G)

4.2.3.1. Network Access Security

According to its definition, this feature provides ser- Identity Confidentiality, Authentication of Users, Confidentiality of Data on the Network Access Link, Data-Integrity and Mobile Equipment Identification.

1. The User-Identity Confidentiality is achieved by the use of temporary identities (called Temporary Mobile User Identities) which have a local significance only (as in GSM).

The TMUI management and reallocation takes place during location updates just as in GSM. The transmission of the International Mobile User Identity (IMUI) over the air-interface in clear-text is avoided as far as possible. In the rare case of the mobile not being able to be identified by an SN, either the IMUI in clear-text format, or an expression which is sufficient to route the user identity request message to an

appropriate network element in HE (called the HE-id) is sent to the SN by the mobile. Authentication of Users (Authentication and Key Agreement) is achieved by means of mutual authentication between the user and the network using a secret-key K known only to the users USIM and the AuC of the users HE. In addition, the USIM and the HE keep track of counters SEQMS and SEQHE respectively to support authentication. This actual method used for authentication is through the challenge response mechanism very much similar to the GSM system (this was done to achieve maximum compatibility). A complete picture of the mechanism used in shown in Figure(4.4). An explanation of the whole process is outside the scope of this case study and a brief overview of some important points will be presented. First of all the presence of sequence numbers (denoted by `(i)' terms) strengthens the security by thwarting some security attacks that arrive out of sequence. Further the presence of

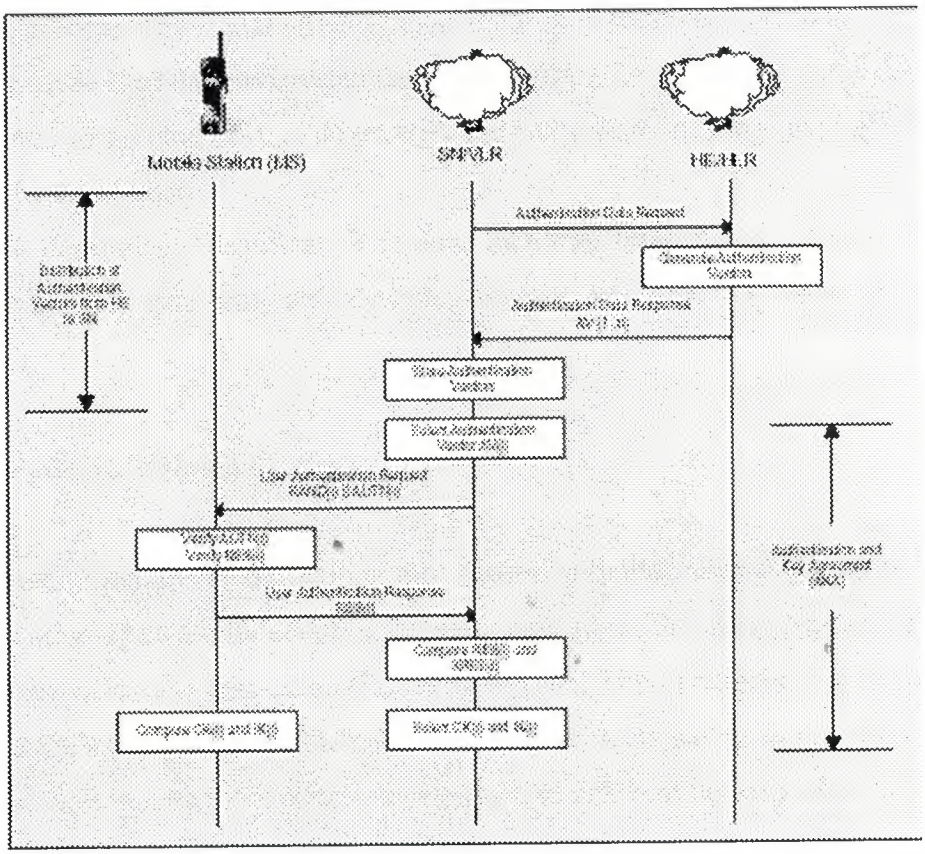

Figure 4.4. Authentication And Access Control (AKA) in UMTS

An explanation of the whole process is outside the scope of this case study and a brief overview of some important points will be presented. First of all the presence of

sequence numbers (denoted by `(i)' terms) strengthens the security by thwarting some security attacks that arrive out of sequence. Further the presence of the AUTN parameters allows the MS to verify the authenticity of the SN, a feature that is not present in the 2G systems.

2. User Data Confidentiality over the Access Network is realized by using Ciphering Algorithms between the MS and the SN. A secret Cipher Key (CK) is established as part of the Authentication and Key Agreement process. A Security Mode Negotiation between the MS and SN takes place during AKA and a Cipher Key (CK) is generated.

1. Data Integrity is the property that the data has not been altered in an unauthorized manner. This is a new security feature included in the 3G Systems. Most of the signaling information on the access link is considered to be very sensitive and must be integrity protected. The UMTS Integrity Algorithm along with a Integrity Key (IK) will be used for providing data integrity. The Integrity Key (IK) is established as a part of the AKA process. The actual integrity algorithm to be followed is realized by means of a security mode negotiation between the MS and SN.

2. Thus the MS and the SN can now verify the authenticity of the signaling information received by each other.

3. Mobile Equipment Identification is done using an International Mobile Equipment Identifier (IMEI) that uniquely identifies mobile equipment. (Similar to the GSM system).

4.2.3.2. Network Domain Security.

According to its definition, this feature provides Entity (Network Element) Authentication, Data Confidentiality (between exchanges involving Network Elements), Data Integrity, Fraud Information Gathering System. The functionality provided by this feature is highly important in the case where sensitive signaling information has to be exchanged between network elements belonging to different network elements.

This feature is implemented using a 3-layered architecture.

1. The Layer I, is a secret key transport mechanism based on an asymmetric cryptosystem and is aimed at agreeing on a symmetric session key for each direction of communication between two networks X and Y. (in the case in which the network elements involved belong to the same network operator, the layer-1 is not required).

The actual key exchanges take place between certain elements called the Key Administration Centers (KACs) of the network operators X and Y. During this stage, the Cipher and Integrity Keys (CK and IK) for protecting the signaling data are also established.

2. In Layer II, the agreed symmetric keys for sending and receiving data are distributed by the KACs in each network to the relevant network elements. This takes place within the network of a single operator. It is clear that the distribution of the symmetric keys to the network elements must be carried out in a secure way, as not to compromise the whole system. Special Key Distribution mechanisms are in place to support this feature.

3. Layer III, uses the distributed symmetric keys for securely exchanging sensitive data between the network elements of one operator (internal use) or different operators (external use) by means of a symmetric encryption algorithm. The encrypted (authenticity/integrity protected) messages will be transported via the MAP protocol

These three layers provide the Entity Authentication, Data Confidentiality and Integrity features. The Fraud Information Gathering System Specifications are yet to be released

4.2.3.3. User Domain Security.

According to its definition this feature provides User to USIM Authentication and USIM to Terminal Authentication.

1. The User to USIM authentication is accomplished by the means of a secret (a PIN) that is stored securely in the USIM. The user can have access to the USIM only if he/she proves knowledge of the secret. More information about this feature can be found in

2. The User To Terminal Authentication is accomplished by using a secret that is stored securely in the USIM and the Terminal. To gain access to the Terminal, the USIM has to prove knowledge of the secret. More information about this feature can be found in

4.2.3.4Application Security

3G Systems will provide the capability for operators or third party providers to create applications which are resident on the USIM (similar to SIM Application Toolkit in GSM). Thus, there exists a need to secure messages which are transferred over the 3G network to applications on the USIM, with the level of security chosen by the network operator or the application provider. The features provided to ensure security of messages are:

- Entity Authentication of Applications.
- Data Origin Authentication of Application Data.
- Data integrity of Application Data.
- Replay Detection of Application Data.
- Sequence Integrity of Application Data.
- Proof of Receipt.

Complete implementation specifications for these features are not yet specified completely.

But these features are most likely to be implemented based on the GSM SIM Application Toolkit Security features. Enhancements on the GSM security features will be required in the areas of Key Management Support, Enhancement of Security Mechanisms / features, increased edibility in algorithm choice and security parameter size. Further issues such as IP security and Access to User Profile Data are not completely addressed.

4.2.3.5. Security Visibility and Configurability.

- Ideally, all the security features must be transparent to the user. But in some cases and in accordance with the user's concern, the user must be provided greater visibility into the operation of the security features. Few example features that are possible are the indication of the access network encryption, indication of the network-wide encryption and the indication of the level of security.
- In 3G Mobile Systems, the user and the user's HE can configure whether the use or the provision of a service should depend on whether a security feature is in operation. This feature is called Configurability. Some of the features suggested by the 3GPP standards are
- Enabling/Disabling User-USIM Authentication.
- Accepting/Rejecting Incoming non-ciphered Calls.
- Setting up or Not Setting Up non-ciphered Calls.
- Accepting/Rejecting the use of certain ciphering algorithms.

Conclusion

The issue of Security in Mobile Communications has been addressed in the early days of its development. This has a lot of advantages in terms of edibility and scalability of the security subsystem in a Mobile Communication Network. In the case of traditional public wired networks, security was just a patchwork effort that resulted in order to block holes after they were uncovered. This leads to the conclusion that in the near future, Wireless Networks will be more secure than existing Wired Networks. This has obvious advantages in users trusting their Wireless Service provider for more number of Applications, including financial transactions, which really translates into a increase in the market for Wireless Services.

REFERENCES

[1] Charlie Kaufman, Radii Perelman, Mike Spicier, \Network Security - PRIVATE Communication in a PUBLIC World", Prentice Hall Series in Computer Networking and distributed Systems, Upper Saddle River, NJ.

[2] US Federal Law on Administration of Export Controls on Encryption Products, http://www.pub.
whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1996/11/15/4.text.1

[3] W Define, M E Hellmann, \New Directions in Cryptography", IEEE Transactions on Information Theory,
v 22, n 6, 1976, pp 644-654.

[4] Dan Brown, \Techniques for Privacy and Authentication in Personal Communication Systems ", IEEE
Personal Communications, August 1995, pp 6-10.

[5] Joseph E Wilkes, \Privacy and Authentication Needs of PCS", IEEE Personal Communications , August1995, pp 11-15.

[6] David R Smith, Susan D Simon, Lawrence E Canutillo, \Trials of Wireless, Secure Electronic Mail", IEEE Personal Communications, August 95, pp 28-33.

[7] Chang-Seop Park, \On Certificate Based Security Protocols for Wireless Mobile Communication Systems", IEEE Network, September/October 1997, pp 50-55.[8] Yair Frankel, Amir Herzberg, Paul A Karger, Hugo Krawczyk, Charles A Kunzinger, Moti Yung,
\Security Issues in a CDPD Wireless Network", IEEE Personal Communications, August 1995, pp16-27.

[9] Gunnar Heine, \GSM Networks: Protocols, Terminology and Implementation",Artech House Publishers,1999.

[10] ETSI Website: http://www.etsi.org

[11] GSM 01.02:\Digital Cellular Telecommunications System (Phase 2+); General Description of a Public Land Mobile Network (PLMN)".

[12] GSM 02.17:\Digital Cellular Telecommunications System (Phase 2+); SubscriberIdentity Modules; Functional Characteristics".

[13] GSM 02.07:\Digital Cellular Telecommunications System (Phase 2+); Mobile Station (MS) features".

[14] GSM 11.11: \Digital Cellular Telecommunications System (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface".

[15] GSM 02.16:\Digital Cellular Telecommunications System (Phase 2+); International Mobile Station Equipment Identities (IMEI)".

[16] GSM 02.09:\Digital Cellular Telecommunications System (Phase 2+); Security Aspects".

[17] GSM 03.20:\Digital Cellular Telecommunications System (Phase 2+); Security Related Network Functions".

[18] ETSI Website: http://www.etsi.org/dvbandca/ALGO/listtest.htm (Contains information about Export Control Licenses and Prices of some security algorithms developed by the ETSI).

[19] GSM Phone Secrets - http://www.cellular.co.za/gsm-phonesecrets.htm.[20] CERTICOM, www.certicom.com, A company focusing on elliptic-curve cryptographic techniques for wireless communications.

[21] GSM Inside (Hacker) Website - http://www.gsminside.com/.[22] The Smart Card Developer Association - http://www.scard.org/.

[23] The RSA Security Inc - http://www.rsasecurity.com/.[24] 3GPP Website: http://www.3gpp.org/

[25] 3GPP Release 99 Specifications Website: http://www.3gpp.org/ftp/Specs/December_99/

[26] UMTS 23.01, \UMTS Network Architecture".

[27] Harri Holma and Antti Toskala, \WCDMA for UMTS: Radio Access For Third Generation Mobile Communications", John Wiley and Sons.

[28] 3G TS 21.133, \ 3rd Generation Partnership Project; Technical Specification Group(TSG); 3G Security; Security Threats and Requirements".

[29] 3G TS 33.102 Release 99, \ 3rd Generation Partnership Project; Technical Specification Group (TSG);3G Security; Security Architecture".

[30] 3G TS 33.120 Release 99, \ 3rd Generation Partnership Project; Technical Specification Group (TSG); 3G Security; Security Principles and Objectives".

[31] 3G TS 33.900, \ 3rd Generation Partnership Project; Technical Specification Group (TSG); A Guide to 3rd Generation Security".

[32] GSM 02.22, \ Personalization of GSM Mobile Equipment (ME); Mobile Functionality Specification".

[33] GSM 09.02, \Mobile Application Part (MAP) Specification".