NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

THE GSM SYSTEM

BLACK

Graduation Project
EE – 400

Student: Moeen Wazir Abbasi (970827)

Supervisor: Prof. Dr. Fakreddin Memadov

Lefkosa – 2001

ACKNOWLEDGMENTS

First I want to thank Prof. Dr. Fakreddin Memadov to be my supervisor. Under his guidance, I successfully overcome many difficulties and learn a lot about GSM. In each discussion, he explained my questions patiently, and I felt my quick progress from his advises. He always helps me a lot either in my study or my life. I asked him many questions in Data Communication and Communication Architecture and he always answered my questions quickly and in detail.

Thanks to Faculty of Engineering for having such a good computational environment.

I also want to thank my friends in 'NEU': M. Haroon Khan, Muhammad Atif Malik and my housemates. Being with them made my 4 years in 'NEU' full of fun.

Finally, I want to thank my family, especially my parents. Without their endless support and love for me. I would never have achieved my current position.

CONTENTS

ABSTRACT

GSM (Global System of Mobile Communication) has been well known as the world's most popular standard for new cellular radio and personal communication equipment throughout the world. From this point of view, we would like to introduce to the readers some basic understandings about GSM architecture, services, and location management methods.

In the first topics, we introduce GSM architecture that consists of three main sub-systems. The first sub-system named Base Station Sub-system (BSS). The BSS provides and manages radio transmission path between the mobile station and the mobile switching centers. The second sub-system of GSM architecture is Network and Switching Sub-system (NSS). This sub-system manages the switching functions of the system and allows the mobile switching centers to communicate with other networks. The last sub-system is known as Operation Support Sub-system (OSS). This sub-system's major functionality consists of supporting the operation and maintenance of GSM. It allows the system engineers to monitor, diagnose, and troubleshoot all aspects of the GSM system. The above three basic sub-systems built the GSM architecture. They function and interact to each other to enable successful communication with the best performance. In the NSS there are different databases called Home Location Register (HLR), Visitor Location Register (VLR), and the Authentication Center (AuC). These three databases have been again functionally investigated in more details in the third part of this research about location management.

The next major part of this research introduces GSM services. GSM services can be classified as either Tele services or Data services. Tele services include standard mobile telephony and mobile-originated traffic. Data services include computer-to-computer communication and packet switched service. In general, GSM services consist of telephone service, facsimile, Videotex, Teletex, data transfer, alphanumeric page, cells broadcast, ...etc. Several new data services within the Phase 2+ are being added. They are High Speed Circuit Switched Data (HSCSD), General Packet Radio Service (GPRS).

The last part of this research introduces quite carefully about the most concerned topic of GSM: location management methods. The location management methods based on users' mobility (known as location) and coming call rate (known as paging) characteristics. There is trade-off between these two procedures. If the location cost is high (the user location knowledge is accurate), the paging cost will be low (paging messages will be only transmitted over a small area), and vice versa. We first introduce all the present location methods ranging from no location management (Level 0), to manual registration (Level 1), to automatic management (Level 2). Level 0 means no location management where users were able to generate a call through any base stations and paging messages addressed to the called mobiles were transmitted through all BSs. This level 0 method is therefore as simple as it could be: no location management is realized; the system does not track the mobiles. This method is usually referred to a flooding algorithm. Level 1 of location management method is relatively simple. It just requires the management of an indicator, which stores the current location of the user. The mobile is just limited to scanning the channels to detect paging messages. Level 2 makes use of location area (LAs). Location areas allow the system to track to mobiles during their roaming in the network. The paging procedure therefore only occurs in the current user's LA. This method requires the uses of databases. These databases HLR, VLR have been mentioned earlier in the GSM architecture. Databases will contain the current LA identity of the mobiles when they are moving from one LA to another. Furthermore, we present the limits of these present location management methods in order to introduce the location management methods for third generation system. The location management methods for third generation are classified into two major groups: memory-less methods, and memory-based methods. These location methods have been investigated, and introduced by Sami Tabbane who presently teaches and performs research at ESPTT.

I hope that this brief research about GSM: architecture, services, and location management methods will contribute the readers a basic understanding about the world's most popular standard for cellular radio and personal communication - The Global System of Mobile Communication .

INTRODUCTION

Global System for Mobile (GSM) is a second generation cellular system standard that was developed to solve the fragmentation problems of the first cellular systems in Europe. GSM is the world's first cellular system to specify digital modulation and network level architectures and services. Before GSM, European countries used different cellular standards throughout the continent, and it was not possible for a customer to use a single subscriber unit throughout Europe. GSM was originally developed to serve as the pan-European cellular service and promised a wide range of network services through the use of ISDN. GSM's success has exceeded the expectations of virtually everyone, and it is now the world's most popular standard for new cellular radio and personal communications equipment throughout the world. It is predicted that by the year 2000, there will be between 20 to 50 million GSM subscribers worldwide.

GSM was first introduced into the European market in 1991. By the end of 1993, several non European countries in South America, Asia, and Australia had adopted GSM and the technically equivalent offshots, DCS 1800, which supports Personal Communication Services (PCS) in the 1.8 GHz to 2.0 GHz radio bands recently created by the governments throughout the world.

Since GSM's technical fields are too broad, in this research, we just can introduce briefly some basic architectures, services that GSM provides to help the readers have an outline about GSM. Next, we will concentrate upon one of the most concerned topics : Location management Methods for GSM. This topic investigates the need for mobility in the access links within the network, the solution between two basic procedures : location and paging. The strong antagonism is the lower cost for location management, the higher cost for paging cost, and vice versa.

CHAPTER ONE

1. INTRODUCTION OF GSM

1.1 Definition

A cellular mobile communications system uses a large number of low-power wireless transmitters to create cells—the basic geographic service area of a wireless communications system. Variable power levels allow cells to be sized according to the subscriber density and demand within a particular region. As mobile users travel from cell to cell, their conversations are handed off between cells to maintain seamless service. Channels (frequencies) used in one cell can be reused in another cell some distance away. Cells can be added to accommodate growth, creating new cells in unserved areas or overlaying cells in existing areas.

1.2 History

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 Groupe Spécial Mobile (GSM) to study and develop a pan-European public land mobile system. The proposed system had to meet certain criteria. Good subjective speech quality.

- Low terminal and service cost
- Support for international roaming
- Ability to support handheld terminals
- Support for range of new services and facilities
- Spectral efficiency

- 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 network s 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 conti nent, 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 a nd 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 amon g suppliers, but provide enough standardization to guarantee proper interworking 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.

1.3 Mobile Communications Principles

Each mobile uses a separate, temporary radio channel to talk to the cell site. The cell site talks to many mobiles at once, using one channel per mobile. Channels use a pair of frequencies for communication—one frequency (the forward link) for transmitting from the cell site and one frequency (the reverse link) for the cell site to receive calls from the users. Radio energy dissipates over distance, so mobiles must stay near the base station to maintain communications. The basic structure of mobile networks includes telephone systems and radio services. Where mobile radio service

operates in a closed network and has no access to the telephone system, mobile telephone service allows interconnection to the telephone network (see *Figure 1.2*).

1.4 Early Mobile Telephone System Architecture

Traditional mobile service was structured in a fashion similar to television broadcasting: One very powerful transmitter located at the highest spot in an area would broadcast in a radius of up to 50 kilometers. The cellular concept structured the mobile telephone network in a different way. Instead of using one powerful transmitter, many low-power transmitters were placed throughout a coverage area. For example, by dividing a metropolitan region into one hundred different areas (cells) with low-power transmitters using 12 conversations (channels) each, the system capacity theoretically could be increased from 12 conversations—or voice channels using one powerful transmitter—to 1,200 conversations (channels) using one hundred low-power transmitters. Figure 1.1 shows a metropolitan area configured as a traditional mobile telephone network with one high-power transmitter.

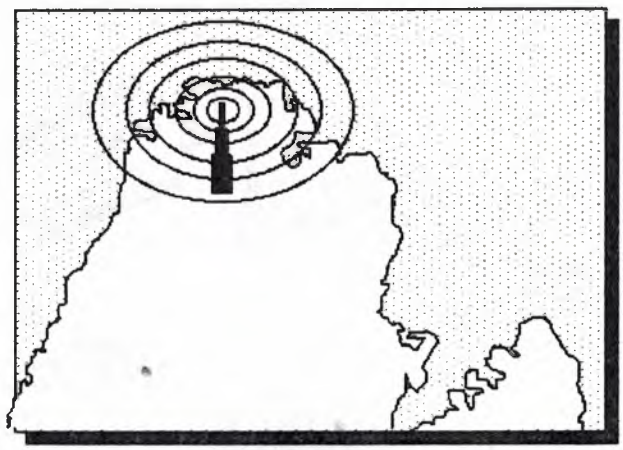

Figure 1.1 Early Mobile Telephone System Architecture

1.5 Services Provided by GSM

From the beginning, the planners of GSM wanted ISDN compatibility in terms of the services offered and the control signalling 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, teleservices, and supplementary services. The most basic teleservice 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 interwork with POTS.

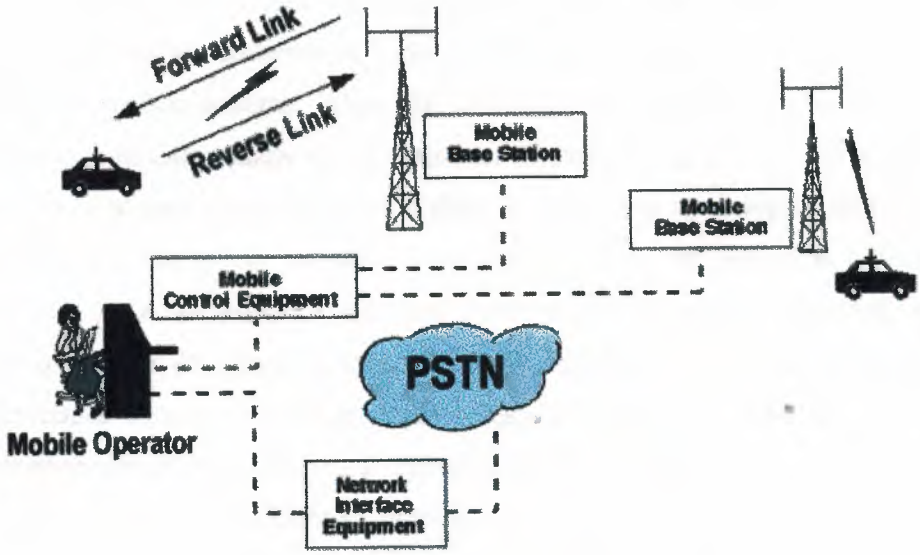

Figure 1.2 Basic Mobile Telephone Service Network

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 bidirectional 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 teleservices 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.

1.6 Digital Systems

As demand for mobile telephone service has increased, service providers found that basic engineering assumptions borrowed from wire line (landline) networks did not hold true in mobile systems. While the average landline phone call lasts at least 10 minutes, mobile calls usually run 90 seconds. Engineers who expected to assign 50 or more mobile phones to the same radio channel found that by doing so they increased the probability that a user would not get dial tone—this is known as call-blocking probability. As a consequence, the early systems quickly became saturated, and the quality of service decreased rapidly. The critical problem was capacity. The general characteristics of time division multiple access (TDMA), Global System for Mobile Communications (GSM), personal communications service (PCS) 1900, and code division multiple access (CDMA) promise to significantly increase the efficiency of cellular telephone systems to allow a greater number of simultaneous conversations. Figure 1.3 shows the components of a typical digital cellular system.

The advantages of digital cellular technologies over analog cellular networks include increased capacity and security. Technology options such as TDMA and CDMA offer more channels in the same analog cellular bandwidth and encrypted voice and data.

Because of the enormous amount of money that service providers have invested in AMPS hardware and software, providers look for a migration from AMPS to digital analog mobile phone service (DAMPS) by overlaying their existing networks with TDMA architectures.

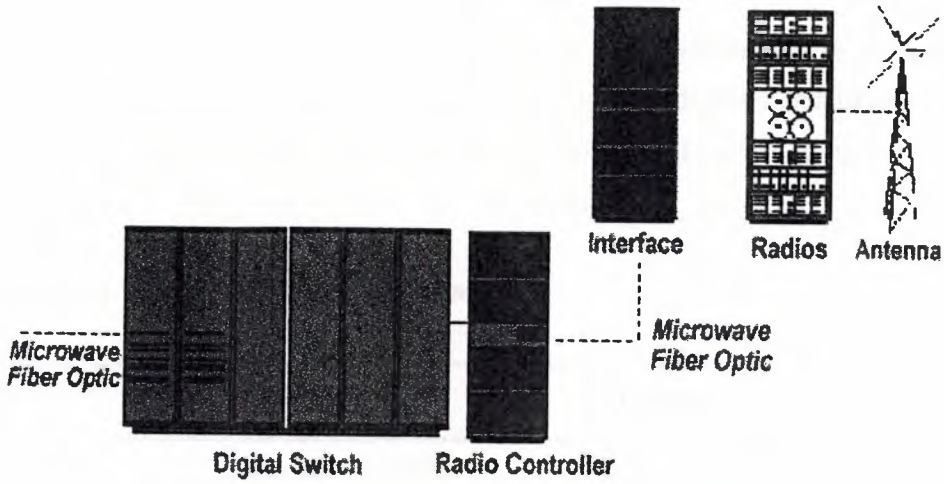

Figure 1.3 Digital Cellular System

1.7 Time Division Multiple Access (TDMA)

North American digital cellular (NADC) is called DAMPS and TDMA. Because AMPS preceded digital cellular systems, DAMPS uses the same setup protocols as analog AMPS. TDMA has the following characteristics:

1. IS–54 standard specifies traffic on digital voice channels
2. initial implementation triples the calling capacity of AMPS systems
3. capacity improvements of 6 to 15 times that of AMPS are possible
4. many blocks of spectrum in 800 MHz and 1900 MHz are used

5. all transmissions are digital
6. TDMA/FDMA application 7. 3 callers per radio carrier (6 callers on half rate later), providing 3 times the AMPS capacity

TDMA is one of several technologies used in wireless communications. TDMA provides each call with time slots so that several calls can occupy one bandwidth. Each caller is assigned a specific time slot. In some cellular systems, digital packets of information are sent during each time slot and reassembled by the receiving equipment into the original voice components. TDMA uses the same frequency band and channel allocations as AMPS. Like NAMPS, TDMA provides three to six time channels in the same bandwidth as a single AMPS channel. Unlike NAMPS, digital systems have the means to compress the spectrum used to transmit voice information by compressing idle time and redundancy of normal speech. TDMA is the digital standard and has 30-kHz bandwidth. Using digital voice encoders, TDMA is able to use up to six channels in the same bandwidth where AMPS uses one channel.

Table 1.1 AMPS/DAMPS Comparison

	Analog	**Digital**
standard	EIA–553 (AMPS)	IS–54 (TDMA + AMPS)
spectrum	824 MHz to 891 MHz	824 MHz to 891 MHz
Channel bandwidth	30 kHz	30 kHz
channels	21 CC/395 VC	21 CC / 395 VC
conversations per channel	1	3 or 6
subscriber capacity	40 to 50 conversations per cell	125 to 300 conversations per cell
TX/RCV type	continuous	time shared bursts

carrier type	constant phase variable frequency	constant frequency variable phase
mobile/base relationship	mobile slaved to base	authority shared cooperatively
Privacy	poor	better—easily scrambled
noise immunity	poor	high
fraud detection	ESN plus optional password (PIN)	ESN plus optional password (PIN)

1.8 Extended Time Division Multiple Access (E–TDMA)

The E–TDMA standard claims a capacity of fifteen times that of analog cellular systems. This capacity is achieved by compressing quiet time during conversations. E–TDMA divides the finite number of cellular frequencies into more time slots than TDMA. This allows the system to support more simultaneous cellular calls

1.9 Fixed Wireless Access (FWA)

FWA is a radio-based local exchange service in which telephone service is provided by common carriers (see *Figure 1.4*). It is primarily a rural application—that is, it reduces the cost of conventional wireline. FWA extends telephone service to rural areas by replacing a wireline local loop with radio communications. Other labels for wireless access include fixed loop, fixed radio access, wireless telephony, radio loop, fixed wireless, radio access, and Ionica. FWA systems employ TDMA or CDMA access technologies.

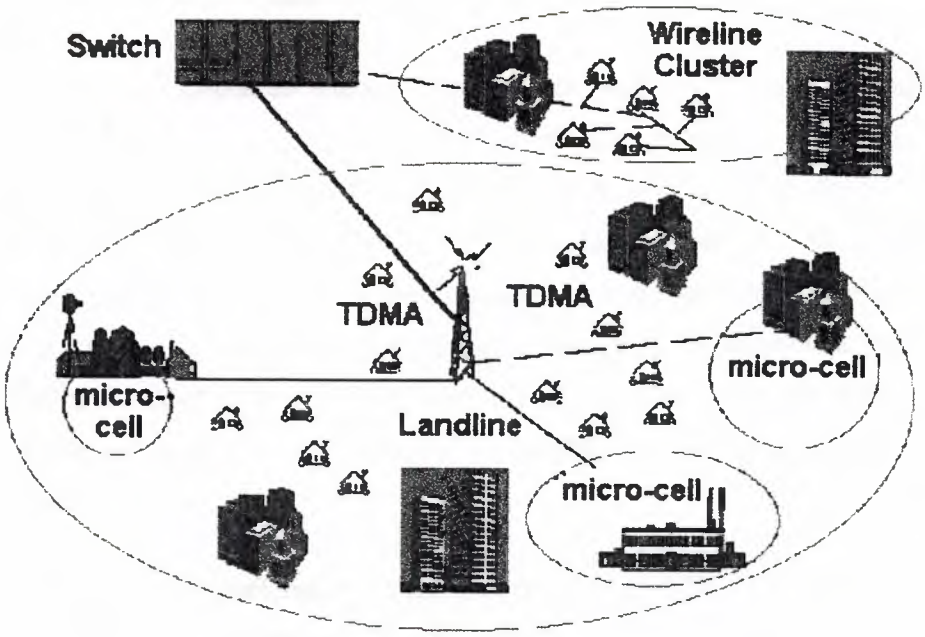

Figure 1.4 Fixed Wireless Access

1.10 Personal Communications Service (PCS)

The future of telecommunications includes PCS. PCS at 1900 MHz (PCS 1900) is the North American implementation of digital cellular system (DCS) 1800 (GSM). Trial networks were operational in the United States by 1993, and in 1994 the Federal Communications Commission (FCC) began spectrum auctions. As of 1995, the FCC auctioned commercial licenses. In the PCS frequency spectrum, the operator's authorized frequency block contains a definite number of channels. The frequency plan assigns specific channels to specific cells, following a reuse pattern that restarts with each *n*th cell. The uplink and downlink bands are paired mirror images. As with AMPS, a channel number implies one uplink and one downlink frequency (e.g., Channel 512 = 1850.2-MHz uplink paired with 1930.2-MHz downlink).

1.11 Code Division Multiple Access (CDMA)

CDMA is a digital air interface standard, claiming 8 to 15 times the capacity of analog. It employs a commercial adaptation of military, spread-spectrum, single-sideband technology. Based on spread spectrum theory, it is essentially the same as wireline service—the primary difference is that access to the local exchange carrier (LEC) is provided via wireless phone. Because users are isolated by code, they can share the same carrier frequency, eliminating the frequency reuse problem encountered in AMPS and DAMPS. Every CDMA cell site can use the same 1.25-MHz band, so with respect to clusters, $n = 1$. This greatly simplifies frequency planning in a fully CDMA environment.

CDMA is an interference-limited system. Unlike AMPS/TDMA, CDMA has a soft capacity limit; however, each user is a noise source on the shared channel and the noise contributed by users accumulates. This creates a practical limit to how many users a system will sustain. Mobiles that transmit excessive power increase interference to other mobiles. For CDMA, precise power control of mobiles is critical in maximizing the system's capacity and increasing battery life of the mobiles. The goal is to keep each mobile at the absolute minimum power level that is necessary to ensure acceptable service quality. Ideally, the power received at the base station from each mobile should be the same (minimum signal to interference).

1.12 Cellular System Components

The cellular system offers mobile and portable telephone stations the same service provided fixed stations over conventional wired loops. It has the capacity to serve tens of thousands of subscribers in a major metropolitan area. The cellular communications system consists of the following four major components that work together to provide mobile service to subscribers.

- Public switched telephone network (PSTN)
- Mobile telephone switching office (MTSO)
- Cell site with antenna system
- Mobile subscriber unit (MSU)

1.12.1 PSTN

The PSTN is made up of local networks, the exchange area networks, and the long-haul network that interconnect telephones and other communication devices on a worldwide basis.

1.12.2 Mobile Telephone Switching Office (MTSO)

The MTSO is the central office for mobile switching. It houses the mobile switching center (MSC), field monitoring, and relay stations for switching calls from cell sites to wire line central offices (PSTN). In analog cellular networks, the MSC controls the system operation. The MSC controls calls, tracks billing information, and locates cellular subscribers.

1.12.3 The Cell Site

The term cell site is used to refer to the physical location of radio equipment that provides coverage within a cell. A list of hardware located at a cell site includes power sources, interface equipment, radio frequency transmitters and receivers, and antenna systems.

1.12.4 Mobile Subscriber Units (MSUs)

The mobile subscriber unit consists of a control unit and a transceiver that transmits and receives radio transmissions to and from a cell site. The following three types of MSUs are available:

- The mobile telephone (typical transmit power is 4.0 watts)
- The portable (typical transmit power is 0.6 watts)
- The transportable (typical transmit power is 1.6 watts)

The mobile telephone is installed in the trunk of a car, and the handset is installed in a convenient location to the driver. Portable and transportable telephones are hand-held and can be used anywhere. The use of portable and transportable telephones is limited to the charge life of the internal battery.

CHAPTER TWO

2. ARCHITECTURE OF THE GSM NETWORK

2.1 Architecture of the GSM network

A GSM network is composed of several functional entities, whose functions and interfaces are specified. Figure 2.1 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.

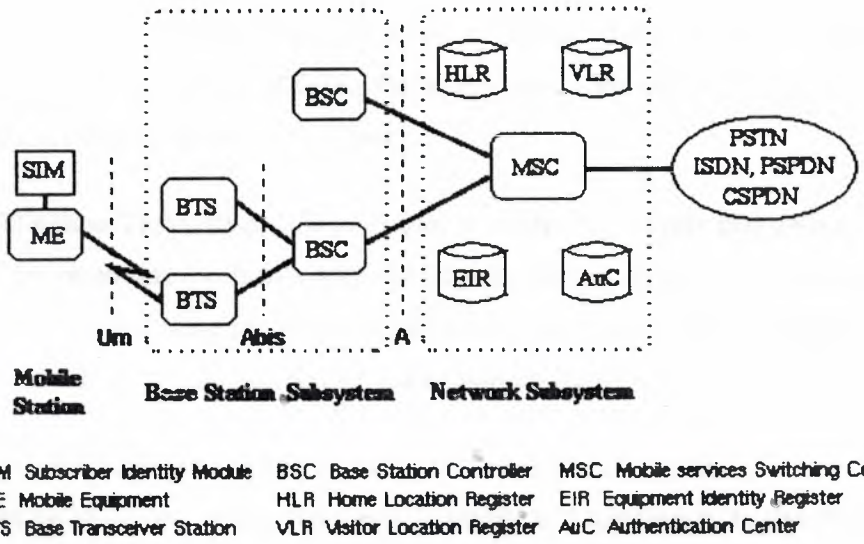

Figure 2.1 General architecture of a GSM network

2.2 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.

2.3 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 tranceivers 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).

2.3.1 The Base Transciever Station

The Base Transciever Station (BTS) is the entity corresponding to one site communicating with the Mobile Stations. Usually, the BTS will have an antenna with several TRXs (radio transcievers) that each communicates on one radio frequency. The link-level signalling on the radio-channels is interpreted in the BTS, whereas most of the higher-level signalling is forwarded to the BSC and MSC. Speech and data-transmissions from the MS is recoded is the BTS from the special encoding used on the radio interface to the standard 64 kbit/s encoding used in telecommunication networks. Like the radio-interface, the Abis interface between the BTS and the BSC is highly standardized, allowing BTSs and BSCs from different manufacturers in one network.

2.3.2 The Base Station Controller

Each Base Station Controller (BSC) control the magnitude of several hundred BTSs. The BSC takes care of a number of different procedures regarding call setup, location update and handover for each MS. The handover control procedures will come especially into focus in this thesis. It is the BSC that decides when handover is necessary. This is accomplished by analyzing the measurement results that are sent from the MS during a call and ordering the MS to perform handover if this is necessary. The continous analyzing of measurements from many MSs requires considerable computational power. This put strong constraints on the design of the BSC.

2.4 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 conjuction 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). Signalling between functional entities in the Network Subsystem uses Signalling System Number 7 (SS7), used for trunk signalling 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 signalling 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 signalling 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.

2.4.1 The Mobile Switching Centre

The Mobile Switching Centre is a normal ISDN-switch with extended functionality to handle mobile subscribers. The basic function of the MSC is to switch speech and data connections between BSCs, other MSCs, other GSM-networks and external non-mobile-networks. The MSC also handles a number of functions assosiated with mobile subscribers, among others registration, location updating and handover.

There will normally exist only a few BSCs per MSC, due to the large number of BTSs connected to the BSC. The MSC and BSCs are connected via the highly standardized A-interface. However, due to the lack of standardization on Operation and Mangement protocols, network providers usually choose BSCs, MSCs and Location Registers from one manufacturer.

2.4.2 The Location Registers

With each MSC, there is associated a Visitors Location Register (VLR). The VLR can be associated with one or several MSCs. The VLR stores data about all customers who are roaming withing the location area of that MSC. This data is updated with the location update procedure initiated from the MS through the MSC, or directly from the subscriber Home Location Register (HLR). The HLR is the home register of the subscriber. Subscribtion information, allowed services, authentication information and localization of the subscriber are at all times stored in the HLR. This information may be obtained by the VLR/MSC when necessary. When the subscriber roams into the location area of another VLR/MSC, the HLR is updated. At mobile terminated calls, the HLR is interrogated to find which MSC the MS is registered with. Because the HLR is a centralized database that need to be accessed during every call setup and data transmission in the GSM network, this entity need to have a very large data transmission capacity. Engineers suggest a scheme for distributing the data in the HLR in order to reduce the load.

The communication between MSC, VLR and HLR is done using the MAP (Mobile Application Part) of the Signalling System 7.

2.5 The Equipment Identity Register

The Equipment Identity Register (EIR) is an optional register. Its purpose is to register IMEIs of mobile stations in use. By implementing the EIR the network provider can blacklist malfunctioning MSs or even receive reports to the operations centre when stolen mobile stations are used to make calls.

2.6 Entities of the GSM System

The GSM system consists of a number of separate entities. These are shown in figure. The entities are connected through interfaces with their own names according to the specifications, these names are shown on the figure. In the following, each of the different entities will be described.

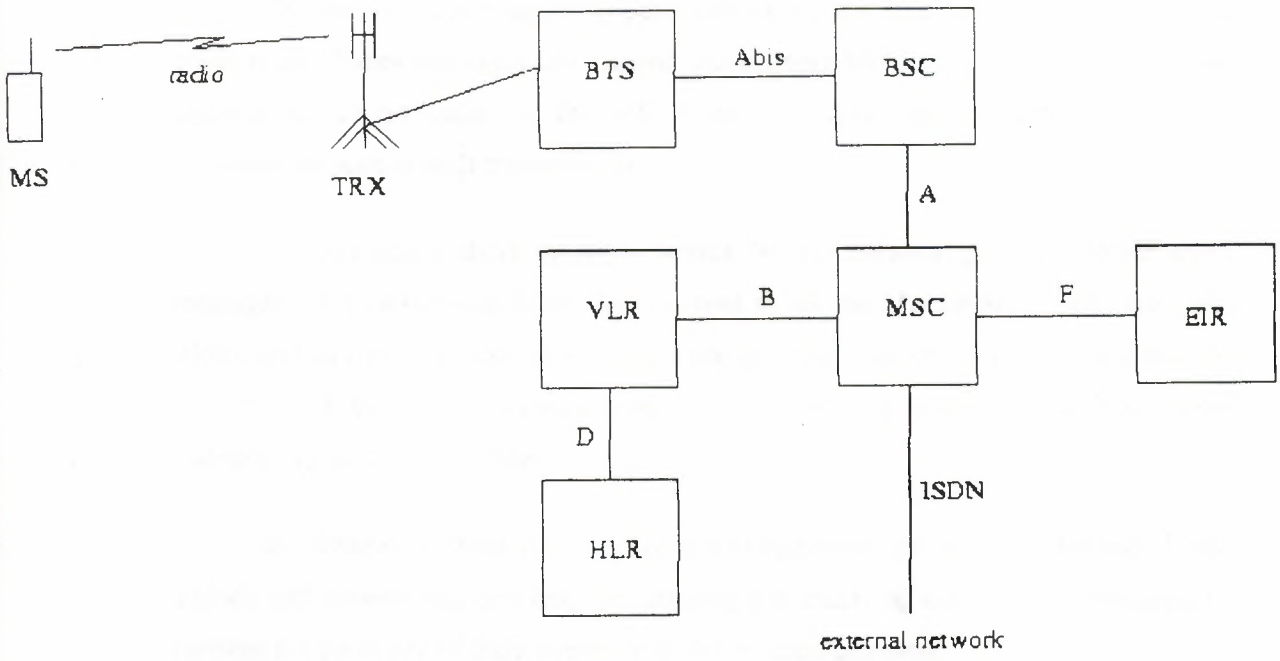

Figure 2.2 Entities of the GSM.

2.7 Services

The services in GSM can be categorized in two main groups:

- Tele services
- Bearer services

The bearer services are parted into nine groups of transparent and non-transparent data-transmission services. Since the data-transmission capabilities of GSM is of little relevance to our problem, it will not be further discussed here.

The tele-services group consists of the basic speech transmission, the point-to-point short message service and the broadcast short message service. The speech transmission resembles normal telephony. Speech is digitalized in the Mobile Station, coded and sent across the radio-channel. In the network, the speech is recoded to the A-law coding used in telephone networks.

The point-to-point short message service let the user send short messages to other users. These messages are relayed via a Short Message Centre (SMC), whose address has to be coded in the MS. Short messages may be sent separately or concurrently with speech transmission.

The broadcast short message service let the network provider define short messages on a cell-by-cell basis that are sent to all the Mobile Stations in that cell. Although this service is not widely used, some providers use it to broadcast information about the cell the MS is currently camping on. As this is position-specific it has some relevance to the MSL problem.

In addition to these services, some supplementary services are defined. These include call forwarding, blocking of outgoing and incoming calls. The supplementary services are generally of little relevance to the location problem.

2.8 Signalling

In order to be able to implement Mobile Station Location (MSL) in a GSM network, it is very important to understand the signalling protocols and procedures used in GSM. In this section, an overview of the signalling protocols and some important signalling sequences will be given.

Figure 2.3 shows an overview of the signalling protocols in the GSM network between the entities MS and MSC. Above the lower layers in the BSS, is the Radio

Resources Protocol (RR). This protocol deals with the allocation, deallocation and parameters.

The radio-channel and is crucial in the setup of all communication with the MS. Above this layer is the Mobility Management (MM) and Circuit Mode Connection Call Protocol (CM or CC). The MM deals with administration of localization and handover. The CM administrates the setup and termination of calls. There also exist protocols between the different entities in the network intended for network internal messages. These are BTS Management protocol (BTSM) across the Abis interface and the BSSAP (BSS Application Part) across the A interface. The BSSAP is divided into BSSMAP (BSS Management Application Part) and DTAP (Direct Transfer Application Part). The lower layers of the A interface are the transport layers of the ITU-T signalling system 7, SCCP and MTP.

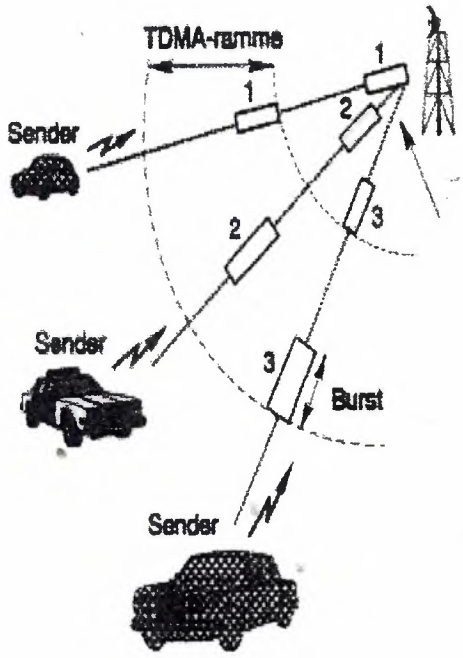

Figure 2.3 Signalling of GSM

2.9 Call setup

To get an idea of the complexity of the signalling procedures and show some of the signals that later will be used, the complete signal-sequence for a mobile-terminated call will be shown here.This shows the signalling sequence between the ISDN network and the GSM network.

CHAPTER THREE

3. RADIO LINK ASPECTS

3.1 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.

3.2 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.

3.2.1 Traffic channels

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multiframe, or group of 26 TDMA frames. The length of a 26-frame multiframe 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 3.1). 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 signalling. In the recommendations, they are called Stand-alone Dedicated Control Channels (SDCCH).

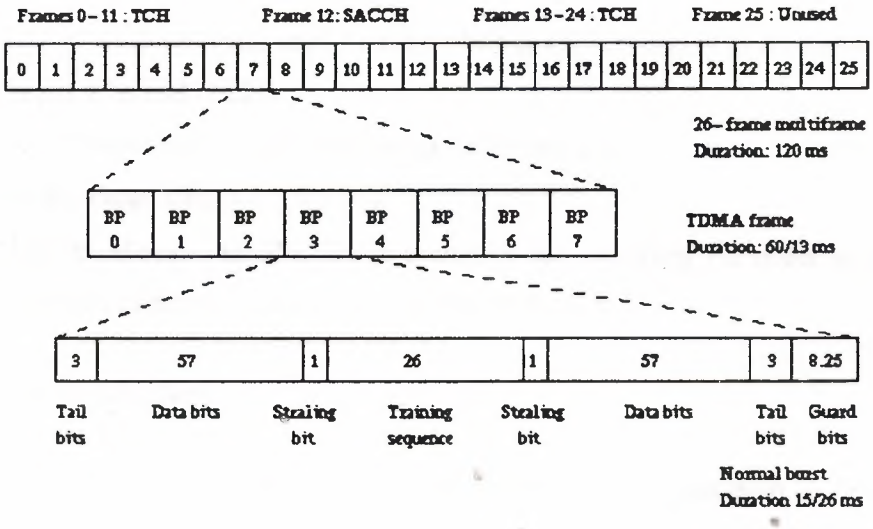

Figure 3.1 Organization of bursts, TDMA frames, and multiframes for speech and data

3.2.2 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 signalling 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 multiframe, so that dedicated mobiles using the 26-frame multiframe 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 Synchronisation Channel (SCH)
  Used to synchronise 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 signalling (in order to obtain a dedicated channel), following a request on the RACH.

3.2.3 Burst structure

There are four different types of bursts used for transmission in GSM. The normal burst is used to carry data and most signalling. 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 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.

3.3 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.

3.4 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 convolutional 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 codec 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 convolutional 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 convolutional 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 convolutional 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).

3.5 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.

3.6 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.

3.7 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.

3.8 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.

3.9 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 alternatingly 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 FOUR

4. NETWORK ASPECTS

4.1 Network aspects

Ensuring the transmission of voice or data of a given quality over the radio link is only part of the function of a cellular mobile network. A GSM mobile can seamlessly roam nationally and internationally, which requires that registration, authentication, call routing and location updating functions exist and are standardized in GSM networks. In addition, the fact that the geographical area covered by the network is divided into cells necessitates the implementation of a handover mechanism. These functions are performed by the Network Subsystem, mainly using the Mobile Application Part (MAP) built on top of the Signalling System No. 7 protocol.

The signalling protocol in GSM is structured into three general layers , depending on the interface, as shown in Figure 3. Layer 1 is the physical layer, which uses the channel structures discussed above over the air interface. Layer 2 is the data link layer. Across the Um interface, the data link layer is a modified version of the LAPD protocol used in ISDN, called LAPDm. Across the A interface, the Message Transfer Part layer 2 of Signalling System Number 7 is used. Layer 3 of the GSM signalling protocol is itself divided into 3 sublayers

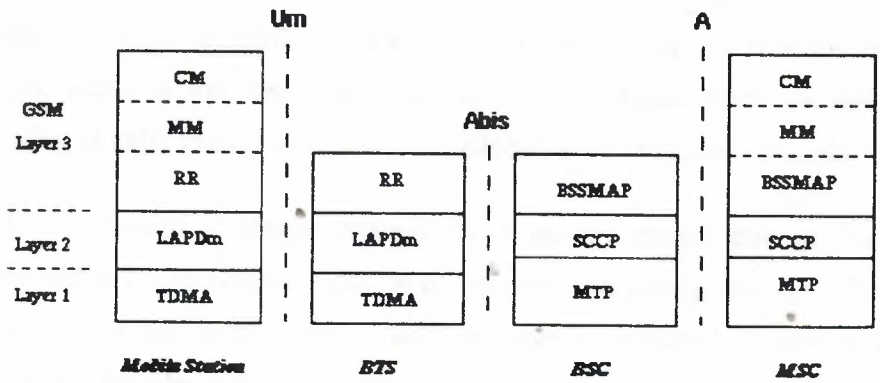

Figure 4.1 Signalling protocol structure in GSM

. **Radio Resources Management**

- Controls the setup, maintenance, and termination of radio and fixed channels, including handovers.

- Mobility Management

  Manages the location updating and registration procedures, as well as security and authentication.

- Connection Management

  Handles general call control, similar to CCITT Recommendation Q.931, and manages Supplementary Services and the Short Message Service.

Signalling between the different entities in the fixed part of the network, such as between the HLR and VLR, is accomplished throught the Mobile Application Part (MAP). MAP is built on top of the Transaction Capabilities Application Part (TCAP, the top layer of Signalling System Number 7. The specification of the MAP is quite complex, and at over 500 pages, it is one of the longest documents in the GSM recommendations .

4.2 Radio resources management

The radio resources management (RR) layer oversees the establishment of a link, both radio and fixed, between the mobile station and the MSC. The main functional components involved are the mobile station, and the Base Station Subsystem, as well as the MSC. The RR layer is concerned with the management of an RR-session, which is the time that a mobile is in dedicated mode, as well as the configuration of radio channels including the allocation of dedicated channels.

An RR-session is always initiated by a mobile station through the access procedure, either for an outgoing call, or in response to a paging message. The details of the access and paging procedures, such as when a dedicated channel is actually assigned to the mobile, and the paging sub-channel structure, are handled in the RR layer. In addition, it handles the management of radio features such as power control, discontinuous transmission and reception, and timing advance.

4.2.1 Handover

In a cellular network, the radio and fixed links required are not permanently allocated for the duration of a call. Handover, or handoff as it is called in North America, is the switching of an on-going call to a different channel or cell. The execution and measurements required for handover form one of basic functions of the RR layer.

There are four different types of handover in the GSM system, which involve transferring a call between:

- Channels (time slots) in the same cell
- Cells (Base Transceiver Stations) under the control of the same Base Station Controller (BSC),
- Cells under the control of different BSCs, but belonging to the same Mobile services Switching Center (MSC), and
- Cells under the control of different MSCs.

The first two types of handover, called internal handovers, involve only one Base Station Controller (BSC). To save signalling bandwidth, they are managed by the BSC without involving the Mobile services Switching Center (MSC), except to notify it at the completion of the handover. The last two types of handover, called external handovers, are handled by the MSCs involved. An important aspect of GSM is that the original MSC, the *anchor MSC*, remains responsible for most call-related functions, with the exception of subsequent inter-BSC handovers under the control of the new MSC, called the *relay MSC*.

Handovers can be initiated by either the mobile or the MSC (as a means of traffic load balancing). During its idle time slots, the mobile scans the Broadcast Control Channel of up to 16 neighboring cells, and forms a list of the six best candidates for possible handover, based on the received signal strength. This information is passed to the BSC and MSC, at least once per second, and is used by the handover algorithm.

The algorithm for when a handover decision should be taken is not specified in the GSM recommendations. There are two basic algorithms used, both closely tied in with power control. This is because the BSC usually does not know whether the poor signal quality is due to multipath fading or to the mobile having moved to another cell. This is especially true in small urban cells.

The 'minimum acceptable performance' algorithm gives precedence to power control over handover, so that when the signal degrades beyond a certain point, the power level of the mobile is increased. If further power increases do not improve the signal, then a handover is considered. This is the simpler and more common method, but it creates 'smeared' cell boundaries when a mobile transmitting at peak power goes some distance beyond its original cell boundaries into another cell.

The 'power budget' method uses handover to try to maintain or improve a certain level of signal quality at the same or lower power level. It thus gives precedence to handover over power control. It avoids the 'smeared' cell boundary problem and reduces co-channel interference, but it is quite complicated.

4.3 Mobility management

The Mobility Management layer (MM) is built on top of the RR layer, and handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects. Location management is concerned with the procedures that enable the system to know the current location of a powered-on mobile station so that incoming call routing can be completed.

4.3.1 Location updating

A powered-on mobile is informed of an incoming call by a paging message sent over the PAGCH channel of a cell. One extreme would be to page every cell in the network for each call, which is obviously a waste of radio bandwidth. The other extreme would be for the mobile to notify the system, via location updating messages, of its current location at the individual cell level. This would require paging messages to be sent to exactly one cell, but would be very wasteful due to the large number of

location updating messages. A compromise solution used in GSM is to group cells into *location areas*. Updating messages are required when moving between location areas, and mobile stations are paged in the cells of their current location area.

The location updating procedures, and subsequent call routing, use the MSC and two location registers: the Home Location Register (HLR) and the Visitor Location Register (VLR). When a mobile station is switched on in a new location area, or it moves to a new location area or different operator's PLMN, it must register with the network to indicate its current location. In the normal case, a location update message is sent to the new MSC/VLR, which records the location area information, and then sends the location information to the subscriber's HLR. The information sent to the HLR is normally the SS7 address of the new VLR, although it may be a routing number. The reason a routing number is not normally assigned, even though it would reduce signalling, is that there is only a limited number of routing numbers available in the new MSC/VLR and they are allocated on demand for incoming calls. If the subscriber is entitled to service, the HLR sends a subset of the subscriber information, needed for call control, to the new MSC/VLR, and sends a message to the old MSC/VLR to cancel the old registration.

For reliability reasons, GSM also has a periodic location updating procedure. If an HLR or MSC/VLR fails, to have each mobile register simultaneously to bring the database up to date would cause overloading. Therefore, the database is updated as location updating events occur. The enabling of periodic updating, and the time period between periodic updates, is controlled by the operator, and is a trade-off between signalling traffic and speed of recovery. If a mobile does not register after the updating time period, it is deregistered.

A procedure related to location updating is the IMSI attach and detach. A detach lets the network know that the mobile station is unreachable, and avoids having to needlessly allocate channels and send paging messages. An attach is similar to a location update, and informs the system that the mobile is reachable again. The activation of IMSI attach/detach is up to the operator on an individual cell basis.

4.3.2 Authentication and security

Since the radio medium can be accessed by anyone, authentication of users to prove that they are who they claim to be, is a very important element of a mobile network. Authentication involves two functional entities, the SIM card in the mobile, and the Authentication Center (AuC). Each subscriber is given a secret key, one copy of which is stored in the SIM card and the other in the AuC. During authentication, the AuC generates a random number that it sends to the mobile. Both the mobile and the AuC then use the random number, in conjuction with the subscriber's secret key and a ciphering algorithm called A3, to generate a signed response (SRES) that is sent back to the AuC. If the number sent by the mobile is the same as the one calculated by the AuC, the subscriber is authenticated

The same initial random number and subscriber key are also used to compute the ciphering key using an algorithm called A8. This ciphering key, together with the TDMA frame number, use the A5 algorithm to create a 114 bit sequence that is XORed with the 114 bits of a burst (the two 57 bit blocks). Enciphering is an option for the fairly paranoid, since the signal is already coded, interleaved, and transmitted in a TDMA manner, thus providing protection from all but the most persistent and dedicated eavesdroppers.

Another level of security is performed on the mobile equipment itself, as opposed to the mobile subscriber. As mentioned earlier, each GSM terminal is identified by a unique International Mobile Equipment Identity (IMEI) number. A list of IMEIs in the network is stored in the Equipment Identity Register (EIR). The status returned in response to an IMEI query to the EIR is one of the following:

White-listed

The terminal is allowed to connect to the network.

Grey-listed

The terminal is under observation from the network for possible problems.

Black-listed

The terminal has either been reported stolen, or is not type approved (the correct type of terminal for a GSM network). The terminal is not allowed to connect to the network.

4.4 Communication management

The Communication Management layer (CM) is responsible for Call Control (CC), supplementary service management, and short message service management. Each of these may be considered as a separate sublayer within the CM layer. Call control attempts to follow the ISDN procedures specified in Q.931, although routing to a roaming mobile subscriber is obviously unique to GSM. Other functions of the CC sublayer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

4.4.1 Call routing

Unlike routing in the fixed network, where a terminal is semi-permanently wired to a central office, a GSM user can roam nationally and even internationally. The directory number dialed to reach a mobile subscriber is called the Mobile Subscriber ISDN (MSISDN), which is defined by the E.164 numbering plan. This number includes a country code and a National Destination Code which identifies the subscriber's operator. The first few digits of the remaining subscriber number may identify the subscriber's HLR within the home PLMN.

An incoming mobile terminating call is directed to the Gateway MSC (GMSC) function. The GMSC is basically a switch which is able to interrogate the subscriber's HLR to obtain routing information, and thus contains a table linking MSISDNs to their corresponding HLR. A simplification is to have a GSMC handle one specific PLMN. It should be noted that the GMSC function is distinct from the MSC function, but is usually implemented in an MSC.

The routing information that is returned to the GMSC is the Mobile Station Roaming Number (MSRN), which is also defined by the E.164 numbering plan. MSRNs are related to the geographical numbering plan, and not assigned to subscribers, nor are they visible to subscribers.

The most general routing procedure begins with the GMSC querying the called subscriber's HLR for an MSRN. The HLR typically stores only the SS7 address of the

subscriber's current VLR, and does not have the MSRN (see the location updating section). The HLR must therefore query the subscriber's current VLR, which will temporarily allocate an MSRN from its pool for the call. This MSRN is returned to the HLR and back to the GMSC, which can then route the call to the new MSC. At the new MSC, the IMSI corresponding to the MSRN is looked up, and the mobile is paged in its current location area.

CHAPTER FIVE

5. MANAGEMENT METHOD FOR MOBILES

5.1 Management methods for mobiles

In today's digital cellular mobile radio networks, features like power control and handover are related to periodic measurements of level and quality at the mobile (downlink/forward) and at the base station (uplink/reverse) receiver. The measurements values and corresponding signaling events of all customer's calls in a specific cell under investigation could be observed by the network operator at the protocol interface between base station controller unit. Statistical evaluation of such mass data produced by customer calls and collected at the protocol interface is an important aid to optimize the base station subsystem parameters in an operating network. The almost only drawback is that there is no exact information available about the position of the mobile. Position determination is limited to the statement "lies in" or "lies out" of the coverage boundaries - which are known only roughly - of the cell under investigation.

From all these observations, location management plays an important role in GSM mobile system. Location management methods for mobile systems have been introduced by Sami Tabbane, ESPTT. Several proposals have been made in the past addressing the problems associated with the cost of location management. Overview about these contributions will be studied first, and then the new location management methods will be introduced.

Location management schemes are essentially based on users' mobility and incoming call rate characteristics. The network mobility process has to face strong antagonism between its two basic procedures: location and paging. The location procedure allows the system to keep the user's location knowledge, more or less accurately, in order to be able to find him, in case of a coming call, for example. Location registration is also used to bring the user's service profile near its location and allows the network provide him rapidly with his services. The paging process achieved by the system consisting of sending paging messages in all cells where the mobile terminal could be located. Therefore, if the location cost is high (and thus the user

location knowledge is accurate), the paging cost will be low (paging messages will be only be transmitted over a small area) and vice versa.

5.2 Present Location Management Methods

5.2.1 No Location Management

In early wide area wireless system (not yet cellular), human operators had to process the calls and the users' locations were not managed by the system. A user was able to generate a call through any base station (BS), and paging messages addressed to the called mobiles were transmitted through all BSs. The main characteristics of these systems were very large cells, and lower user population and call rates.

Small-capacity cellular systems (with a few tens of BSs serving a few thousand users) may also not use a location management method, even when the standard allows it. if subscriber number and calling rates do not require it, the location management method is not activated; resource consumption for finding users is not so important that its reduction is mandatory.

This level 0 method is therefore as simple as could be: no location management is realized; the system does not track the mobiles. A search for a called user must therefore be done over complete radio coverage area and within a limited time. This method is usually referred to as flooding algorithm.

It is used in paging systems because of the lack of an uplink channel allowing a mobile to inform the network of its whereabouts. It is also used in the small private mobile networks because of their small coverage area and user populations.

The main advantage of not locating the mobile terminals is obviously simplicity; in particular, there is no need to implement special databases. Unfortunately, it does not fit large networks dealing with high numbers of users and high incoming call rates.

5.2.2 Manual Registration

This method requires the user to locate himself by achieving a special procedure if he wishes to receive his incoming calls. From the network site, this method is relatively simple to manage because it just requires the management of an indicator,

which stores the current location of the user. The mobile is also relatively simple; its task is just limited to scanning the channels to detect paging messages.

This method is currently used in telepoint cordless systems (such as CT2). The user has to register itself each time he moves to a new island of CT2 beacons. To page a user, the network first transmits messages through the beacon with which he registered and, if the mobile dose not answer, extends the paging to neighboring beacons.

The main drawback of this method is the constraint for a user to register each time he moves. Nevertheless, this low ergonomic can be balanced by the low equipment and management costs of the network, which allow the operator to offer users attractive fees.

5.2.3 Use Of Location Areas For Automatic Location Management

Presently, the location method most widely implemented in the first- and second-generation cellular system (NMT, GSM, IS-95, etc.) makes use of location areas (LAs) (figure5.1). In these wide-area radio networks, location management is done automatically.

Location areas allow the system to track the mobiles during their roaming in the networks: subscriber location is known if the system knows the LA in which the subscriber is located. When the system must establish a communication with the mobile, the paging only occurs in the current user L. Thus, resource consumption is limited to this LA; paging messages are only transmitted in the cells of this particular LA.

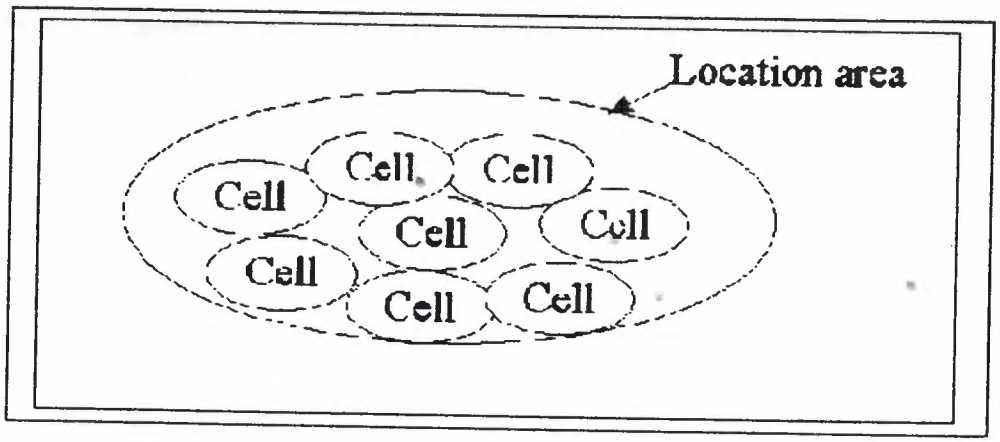

Figure 5.1 Location Area

5.2.4 Periodic location updating

Implementing LA-based methods requires the use of databases. Generally, a home database and several visitor databases are included in the network architecture. There are also several locations updating methods that can be implemented based on LA structuring.

This method is simplest because it just requires the mobile to periodically transmit its identity to the network. Its drawback is its resource consumption, which is user_dependent and can be unnecessary if the user does not move from a LA for several hours. Generally, this method is combined with the next one. Location updating on LA crossing

This method (figure 3) first requires each BS to periodically broadcast the identity of its LA. Second, the mobile is required to permanently listen to network broadcast information (on the broadcast channel) and to store the current LA identity. Of the received LA number differs from the stored one, a location update (LU) procedure is automatically triggered by the mobile.

The advantage of this method is that it only requires LUs when the mobile actually moves. A highly mobile user will generate a lot of LUs; a low mobility user will only trigger a few.A hybrid method which combines the two previous ones can also be implemented.

The mobile generates its LUs each time it detects a LA crossing. Nevertheless, if no communication (related to a LU or a call) has occurred between the mobile (in idle mode, ie., powered on but not communicating) and the network for a fixed period, the mobile generates a LU. This periodic LU typically allows the system to recover user location data in case of a database failure.

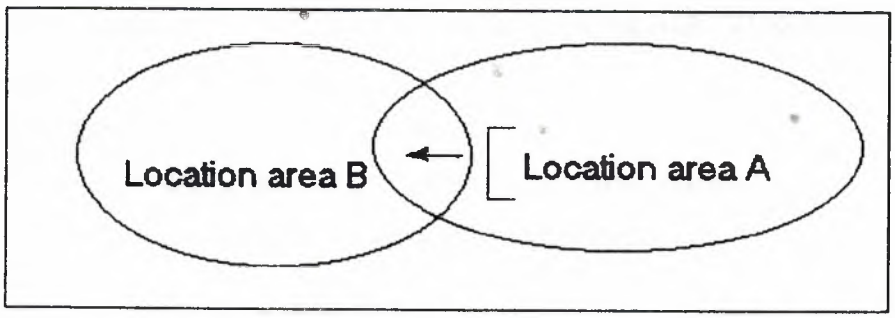

Figure 5.2 Location updating on LA crossing

5.3 GSM Example

The GSM standard defines a database structure based on:

- An HLR (Home Location Register) where all subscriber related information is stored (access right, user location, etc.). Security parameters and algorithms are managed by the authentication center (AuC) which is often considered part of the HLR.
- Several VLRs. Each VLR stores part of the data regarding the users located in its related LAs.

The location management method defined in GSM combines the periodic LU method and the LU on the border crossing. The VLR stores the LA identifier, and the HLR stores the VLR identifier.

This consists of three main types of LU procedures: The intra-VLR LU, the inter_VLR LU using TMSI (temporary mobile subscriber identity), and the inter_VLR LU using IMSI (international mobile subscriber identity). A fourth one, the IMSI attach procedure, is triggered when the mobile is powered on in the LA where it was powered off.

In the following, we present the most complete LU, which is inter_VLR using MISI. This procedure mainly consists of the following steps:

- A signaling channel is allocated to the MS, and a LU is requested.
- The MS provides the network with its IMSI, which allows the new VLR (VKR2) to load authentication data from the HLR/AuC, mainly the triplets for the authentication and the ciphering procedures.
- The VLR is then able to authenticate the MS; if this step succeeds, it updates the location at the HLR. The HLR informs the old HLR (VLR1) to remove the user's data stored in VLR1.
- Ciphering may be required id available.
- · A new TMSI is allocated to the MS, and , after acknowledgment of its LU request (first message sent by the MS), the channel finally released

5.4 Limits Of Present Location Management Methods

The LA-based location management methods are the most adapted and widely used in current cellular (GSM, IS-54 and IS-95...), in trunk systems such as trans_European trunk radio (TETRA), in cordless systems like Digital European Cordless Telecommunication (DECT), Personal Access Communication System (PACS), Personal Handyphone systems (PHS), and so on. Nevertheless, the traffic and processing generated may lead to congestion problems in high-density systems. One of the main concerns of the system designers is therefore to define methods allowing the system to reduce the overhead traffic as much as possible.

Several location management methods proposed within these last years, which attempt to reduce the overhead traffic. Followings are location management methods for third_generation system written by Sami Tabbane who presently teaches and performs research at ESPTT. His research topics of interest are location management techniques, handover procedures, and cellular networking planning.

5.5 Location Management Methods For Third-Generation Systems

He classifies the location management methods into two major groups (figure 5). In the first, he concludes all methods based on algorithms and network architecture, mainly on the processing capabilities of the system. The second group gathers the methods based on learning processes, which require the collection of statistics on users' mobility behavior, for instance. The second method emphasizes the information capabilities of the network.

5.6 Memoryless Methods

5.6.1 Database architecture

This divides into three cases:

- Centralized database architecture: presents an architecture where a unique centralized database is used. This is well suited to small and medium networks, typically based on a star topology.

- Distributed database architecture: uses several independent databases according to geographical proximity or service providers. It is best suited to large

networks including subnetworks managed by different operators and service providers. The GSM worldwide network, defined as the network made up of all interconnected GSM networks in the world, can be such an example of a large network. The main drawbacks of this architecture are clearly the cost of database system acquisition, implementation, and management.

- Hybrid database architecture: combines the centralized and distributed architectures. In this case, a central database (HLR-like) is used to store all user information. Other small databases (VLR-like) are distributed all over the

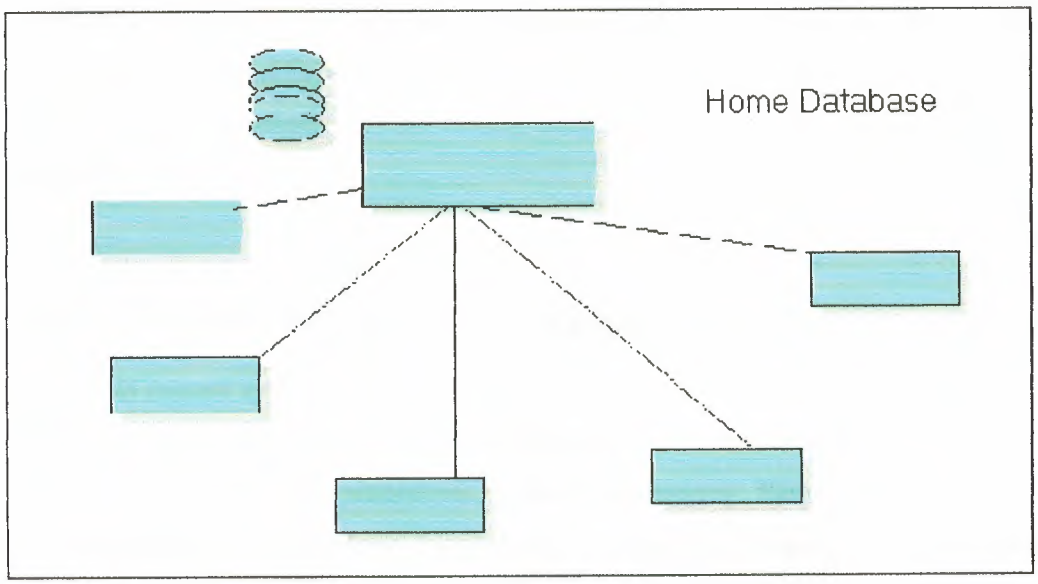

Figure 5.3 Centralized data base architecture.

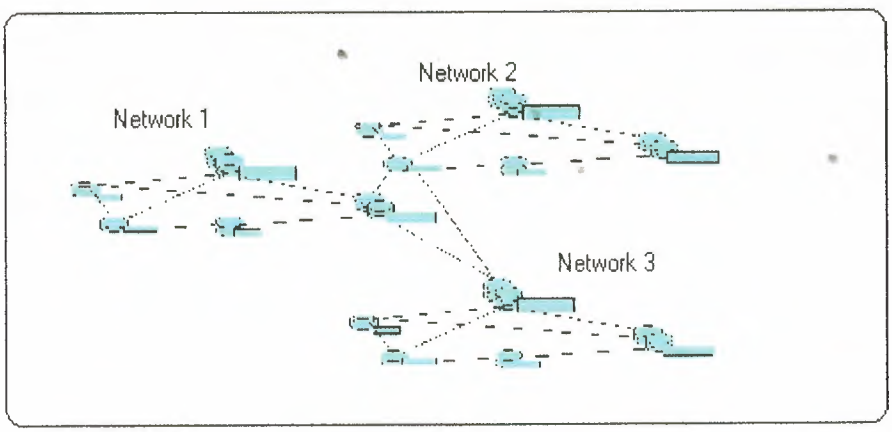

Figure 5.4 Distributed Data base Architecture

- network. These VLR databases store portions of HLR user records. A single GSM network is an example of such architecture.

5.6.2 Optimizing fixed network architecture

In second-generation cellular networks and third-generation systems, signaling is managed by the intelligent network (IN). Appropriately organizing mobility functions and entities can help reduce the signaling burden at the network site. The main advantage of these propositions is that they allow us to reduce the network mobility costs independent of the radio interface and LA organization. For example, it is proposed to use different degrees of decentralization of the control functions. Thus, using adapted signaling network nodes, interconnection allows mobility costs to be reduced.

5.6.3 Combining location areas and paging areas

In current systems, a LA is defined as both an area in which to locate a user and an area in which to page him. LA size optimization is therefore achieved by taking into account two antagonistic procedures, locating and paging. Based on this observation, several proposals have defined location management procedures, which make use of LAs and paging areas (PAs) of different sizes. One method often considered consists of splitting an LA into several PAs (figure 5.3)

An MS registers only once, that is, when it enters the LA. It does not register when moving between different PAs of the same LA. For an incoming call, paging messages will broadcast in the PAs according to a sequence determined by different strategies. For example, the first PA of the sequence can be the one where the MS was last detected by the network. The drawback of this method is the possible delay increase due to large LAs

5.6.4 Multilayer LAs

In present location management methods, LU traffic is mainly concentrated in the cells of the LA border. Based on this observation and to overcome this problem, Okasaka has introduced the multilayer concept. In his method, each MS is assigned to a given group, and each group is assigned one or several layers of LAs

According to figure 5.5, it is clear that group 1 and group 2 MSs will not generate Lus in the same cells, thus allowing the LU traffic load to be distributed over the cells. Nevertheless, this location updating method, although it may help channel congestion, does not help reduce the overall signaling load generated by LUs.

5.7 Memory-Based Methods

The design of memory-based location management methods has been motivated by the fact that systems do a lot of repetitive actions, which can be avoided if predicted. This is particularly the case for LUs. Indeed, present cellular systems achieved everyday, at the same peak hours, almost the same LU processing. Systems act as memoryless processes. Short-term and long-term memory processes can help the system avoid these repetitive actions. Some methods have thus been proposed that be based on user and system behavior observation and statistics.

5.7.1 Short-term observation for dynamic LA and PA size

In current systems, the size of LAs is optimized according to mean parameter values, which in practical situations vary over a wide range during the day and from one user to another.

Based on this observation, it is proposed to manage user location by defining multilevel Lass in a hierarchical cellular structure. At each level the LA size is different, and a cell belongs to different LAs of different sizes. According to past and present MS mobility behavior, the scheme dynamically changes the hierarchical level of the LA to which the MS register. LU savings can thus be obtained.

A variant of this strategy requires from mobiles to register in the cells where they are camped on. Registrations involve a periodic timer which value has to be optimized. Thus rather than paging a mobile in all cells of a LA, the mobile will be

paged only in the cells visited during the last period: these are cells the mobile camped on during its traversal of the LA.

In figure 5.5, high coming call rate and low-mobility users are directed to small LAs, medium-mobility users are directed to medium-sized LAs, and high-velocity and low coming call rate users are directed to large LAs.

Adapting the LA size to each user parameter values may be difficult to manage in practical situations. This led to definition of a method where the LAs sizes are dynamically adjusted for the whole population, not per user as in the previous method. Statistical information about users and mobility in the network is collected in databases and computed. Networks characteristics in function of time, place, density, and so on are thus evaluated. Results of this computation allow the network to dynamically (daily, weekly, monthly, yearly.) adjust LAs sizes. For instance, during the day, when call rates are high, it is preferable to deal with small LAs. Conversely, at night the call rate is much lower, and therefore larger LAs are better.

5.7.2 Individual user patterns

Observing that users show repetitive mobility patterns, the alternative strategy (AS) is defined; its main goal is to reduce the traffic related to mobility management - thus reduce the LUs - by taking advantage of users' highly predictable patterns. In AS, the system handles a profile recording the most probable mobility patterns of each user. The profile of the user can be provided and updated manually by the subscriber himself or determined automatically by monitoring the subscriber's movements over period of time.

The main savings allowed by this method are due to the non-triggered LUs when the user keeps moving inside his profile LAs. So, the more predictable the users' mobility, the lower the mobility management cost.

A variant of this method, called the Two-Location Algorithm (TLA), is proposed and studied. In this strategy, a mobile stores the two most recently visited LA addresses. The same is done at the HLR level. Obviously, the main advantage of this method relies on the reduction of LUs when a mobile goes back and forth between two LAs.

5.7.3 Predicting short-term movements of the subscriber

The method uses a process, which predicts the movements of the MS according to its direction, velocity, and so on. Processing and prediction are made at both the MS and the HLR. When actual movements of the MS do not fit with those predicted, a registration is triggered by the mobile to inform the network of its actual location. Otherwise, no exchange is required, which allows savings in LU processing and signaling.

5.7.4 Mobility statistics

A mobility management method similar to AS is defined. It is called Statistical Paging Area Selection (SPAS) and is based on location statistics collected by each MS, which periodically reports them to the network. These statistics consist of a list of the average duration the MS had been located in each LA. A priority rule is determined to settle the sequence of LAs visited by the mobile. If this sequence id different from the last one reported to the network, the MS transmits it; otherwise, nothing is done. The paging process is achieved in the same way as in AS. When the MS moves to an area that is not on the reported list, it has to process a temporary location registration to the network.

In " A Predictive Mobility Management Algorithm for Wireless Mobile Computing and Communications ', G. Y. Liu and G. Q. Maguire proposed the method provide a means of allowing preconnection and pre-assignment of data or services at the location before the user moves into it, so he can immediately receive service or data. This method clearly applies to location management. Just as are the previous two methods, it is based on users' movement history patterns. Called Mobile Motion Prediction (MMP), it allows the system to predict the future location of the user. Schematically, the MMP combines two movement models: Movement circle (MC), based on a closed-circuit model of user movement behavior, and Movement Track, used to predict routine movements. MC is used to predict long-term regular movements.

The author, finally, mentions the method proposed in " Comparing the PCSS Location Tracking Strategies" by Y. B. Lin and S. Y. Hwang. The method makes use of a cache memory for reducing the search cost. The proposal is to store the location of the frequently called mobiles in a local database (i.e. cache). This scheme allows the number of queries to the HLR to be reduced; thus reducing the signaling traffic at he fixed network side between the local database and the HLR.

CHAPTER SIX

6. INTRODUCTION TO WAP

6.1 Introduction

WAP bridges the gap between the mobile world and the Internet as well as corporate intranets and offers the ability to deliver an unlimited range of mobile value-added services to subscribers—independent of their network, bearer, and terminal. Mobile subscribers can access the same wealth of information from a pocket-sized device as they can from the desktop.

WAP is a global standard and is not controlled by any single company. Ericsson, Nokia, Motorola, and Unwired Planet founded the WAP Forum in the summer of 1997 with the initial purpose of defining an industry-wide specification for developing applications over wireless communications networks. The WAP specifications define a set of protocols in application, session, transaction, security, and transport layers, which enable operators, manufacturers, and applications providers to meet the challenges in advanced wireless service differentiation and fast/flexible service creation. There are now over one hundred members representing terminal and infrastructure manufacturers, operators, carriers, service providers, software houses, content providers, and companies developing services and applications for mobile devices.

WAP also defines a wireless application environment (WAE) aimed at enabling operators, manufacturers, and content developers to develop advanced differentiating services and applications including a microbrowser, scripting facilities, e-mail, World Wide Web (WWW)–to-mobile-handset messaging, and mobile-to-telefax access.

The WAP specifications continue to be developed by contributing members, who, through interoperability testing, have brought WAP into the limelight of the mobile data marketplace with fully functional WAP–enabled devices.

6.1 Why WAP

WAP provides mobile to internet connectivity. In theory WAP enabled devices like Mobile Phones, PDA's and other hand-held devices should be able to access web content as desktops do. But since minimal web content is html content and small devices have limitation for rendering this type of content, a different language called Wireless Markup Language (WML) has been adopted for use. WML is designed keeping in mind small display area of hand-held devices like mobile phones. Besides this problem, mobile devices have some other limitations too, which make WAP important. Here is a list of a few.

- **Less powerful CPUs**
- **Less memory (ROM and RAM)**
- **Restricted power consumption**
- **Smaller displays**
- **Different input devices (eg, a phone keypad)**

It is not only the limitations of mobile devices but problems in wireless data networks too had the impact on designing Wireless Application Protocol. Issues with wireless data networks are

- **Less bandwidth** : The GSM network user has maximum bandwidth of 9.6 kbps available to him/her. **GPRS** (General Packet Radio Service) will incraese the bandwidth allocated per user to 160 kbps.
- More latency
- Less connection stability
- Less predictable availability

6.2 WAP Model

This diagram shows how the WAP model works. WAP Client sends an encoded request to the WAP server. WAP client can be a mobile phone, Personal digital assistant or any other WAP enabled device. The request is encoded in a compact form because of the limitations of the wireless data networks. WAP gateway decodes this request to HTTP request and sends this to the web server. The web server

responds with the wml content. WAP gateway prepares encoded response and sends it to client server.the figure 6.1 shows how wap works.

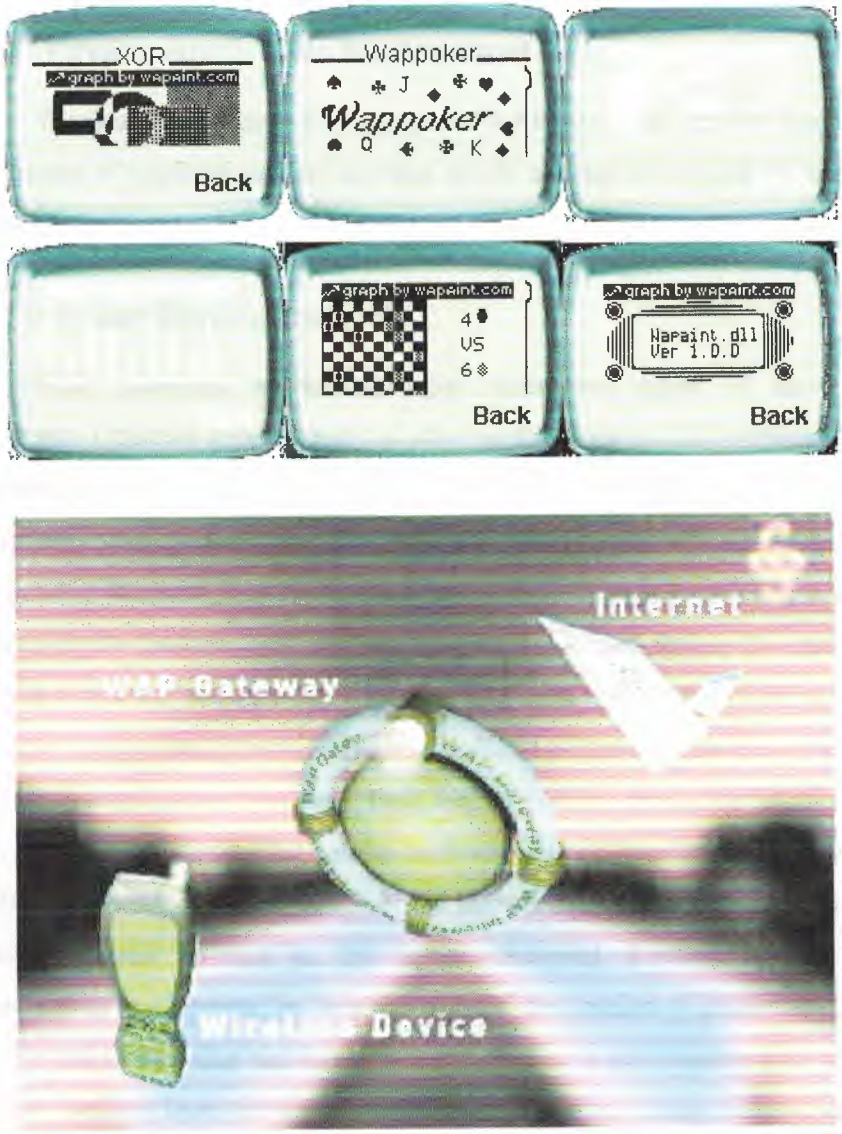

Figure 6.1 Wireless Devices

6.3 WAP Architecture

WAP has a layered architecture. The entire protocol stack consists of five layers.

- Wireless Application Envireonment
- Wireless Session Protocol

- Wireless Transaction Protocol
- Wireless Transport Layer Security
- Wireless Datagram Protocol

6.3.1 Wireless Application Environment

Wireless Application Environment (WAE) provides the environment for the develoment of applications and services which operate over wireless communication networks.

6.3.2 Wireless Session Protocol

WSP provides application layer with two types of services. First is Connection-Oriented service and the other is Connection-Less service. Connection-Oriented service operates above WTP layer. This mode of service provides facilities like Session Management, Method Invocation, Confirmed Push, Non-Confirmed Push and Suspend Resume. Session Management allows a client to connect to a server and to agree on the facilities and protocol options to be used during the session. Session provides a context between the client and the server. Both the client and server can terminate this session. Method Invocation allows a client to ask the server to execute an operation and return the result. Push facility permits the server to send unsolicited information to the client. This can be confirmed or non-confirmed. In confirmed push the client acknowledges the receipt of the information, but in non-confirmed push no acknowledgement is sent to the server. Suspend Resume facility allows the suspension of the session, so that the state of the session is preserved. In this state both the peers know that the further communication is not possible until the session is resumed. Session layer provides the functionality of encoding and decoding of data. Using these encoding techniques, the size of the data over the wireless network is reduced.

6.3.3 Wireless Transaction Protocol

WTP runs on top of a data gram service and optionally a security service. WTP has been defined as a lightweight transaction oriented protocol that is suitable

for implementation in "thin" clients (mobile stations) and operates efficiently over wireless data gram networks. The benefits of using WTP include:

1. Improved reliability over data gram services. WTP relieves the upper layer from re-transmissions and acknowledgements, which are necessary if data gram services are used.
2. Improved efficiency over connection oriented services. WTP has no explicit connection set up or teardown phases.
3. WTP is message oriented and designed for services oriented towards transactions, such as "browsing".

WTP provides three classses of transactions.

- **Class 0** Unreliable one way requests. Request from one peer to another is not followed by an acknowlegement of the receipt of request.

- **Class 1** Reliable one way requests. Request from one peer to another is followed by an acknowlegement of the receipt of request.

- **Class 2** Reliable two way request-reply transactions. Request from one peer is acknowledged by the other, which is followed by a reply and that is also acknowledged.

6.3.4 Wireless Transport Layer Security

The Security layer protocol in the WAP architecture is called the Wireless Transport Layer Security, WTLS. The WTLS layer operates above the transport protocol layer. The WTLS layer is modular and it depends on the required security level of the given application whether it is used or not. WTLS provides the upper-level layer of WAP with a secure transport service interface that preserves the transport service interface below it. In addition, WTLS provides an interface for managing (eg, creating and terminating) secure connections.The primary goal of the WTLS layer is to provide privacy, data integrity and authentication between two communicating applications.The WTLS protocol is optimised for low-bandwidth bearer networks with relatively long latency.

6.3.5 Wireless Datagram Protocol

The WDP layer operates above the data capable bearer services supported by the various network types. As a general datagram service, WDP offers a consistent service to the upper layer protocol (Security, Transaction and Session) of WAP and communicate transparently over one of the available bearer services. Since the WDP protocols provide a common interface to the upper layer protocols the Security, Session and Application layers are able to function independently of the underlying wireless network. This is accomplished by adapting the transport layer to specific features of the underlying bearer. By keeping the transport layer interface and the basic features consistent, global interoperability can be achieved using mediating gateways.

CONCLUSION

In this project I have tried to give an overview of the GSM system. As with any overview, and especially one covering a standard 6000 words long, there are many details missing. I believe, however, that I gave the general flavor of GSM and the philosophy behind its design. It was a monumental task that the original GSM committee undertook, and one that has proven a success, showing that international cooperation on such projects between academia, industry, and government can succeed. It is a standard that ensures interoperability without stifling competition and innovation among suppliers, to the benefit of the public both in terms of cost and service quality. For example, by using Very Large Scale Integration (VLSI) microprocessor technology, many function s of the mobile station can be built on one chipset, resulting in lighter, more compact, and more energy-efficient terminals.

Telecommunications are evolving towards personal communication networks, whose objective can be stated as the availability of all communication services anytime, anywhere, to anyone, by a single identity number and a pocketable communication terminal. Having a multitude of incompatible systems throughout the world moves us farther away from this ideal. The economies of scale created by a unified system are enough to justify its implementation, not to mention the convenience to people of carrying just one communication terminal anywhere they go, regardless of national boundaries.

The GSM system, and its sibling systems operating at 1.8 GHz (called DCS1800) and 1.9 GHz (called GSM1900 or PCS1900, and operating in North America), are a first approach at a true personal communication system. The SIM card is a novel approach that implements personal mobility in addition to terminal mobility. Together with international roaming, and support for a variety of services such as telephony, data transfer, fax, Short Message Service, and supplementary services, GSM comes close to fulfilling t he requirements for a personal communication system: close enough that it is being used as a basis for the next generation of mobile communication technology in Europe, the Universal Mobile Telecommunication System (UMTS).

Another point where GSM has shown its commitment to openness, standards and interoperability is the compatibility with the Integrated Services Digital Network (ISDN) that is evolving in most industrialized countries, and Europe in particular (the so-called Euro-ISDN). GSM is also the first system to make extensive use of the Intelligent Networking concept, in in which services like 800 numbers are concentrated and handled from a few centralized service centers, instead of being distributed over every switch in the country. This is the concept behind the use of the various registers such as the HLR. In addition, the signalling between these functional entities uses Signalling System Number 7, an international standard already deployed in many countries and specified as the backbone signalling network for ISDN.

GSM is a very complex standard, but that is probably the price that must be paid to achieve the level of integrated service and quality offered while subject to the rather severe restrictions imposed by the radio environment.

References

Refrences to Books

[1] Jan A. Audestad. Network aspects of the GSM system. In *EUROCON 88*, June 1988.

[2] D. M. Balston. The pan-European system: GSM. In D. M. Balston and R.C.V. Macario, editors, *Cellular Radio Systems*. Artech House, Boston, 1993.

[3] David M. Balston. The pan-European cellular technology. In R.C.V. Macario, editor, *Personal and Mobile Radio Systems*. Peter Peregrinus, London, 1991.

[4] M. Bezler et al. GSM base station system. *Electrical Communication*, 2nd Quarter 1993.

[5] David Cheeseman. The pan-European cellular mobile radio system. In R.C.V. Macario, editor, *Personal and Mobile Radio Systems*. Peter Peregrinus, London, 1991.

[6] C. Déchaux and R. Scheller. What are GSM and DCS. *Electrical Communication*, 2nd Quarter 1993.

[7] M. Feldmann and J. P. Rissen. GSM network systems and overall system integration. *Electrical Communication*, 2nd Quarter 1993.

[8] John M. Griffiths. *ISDN Explained: Worldwide Network and Applications Technology*. John Wiley &Sons, Chichester, 2nd edition, 1992.

[9] Harris. Data in the GSM cellular network. In D. M. Balston and R.C.V. Macario, editors, *Cellular Radio Systems*. Artech House, Boston, 1993.

[10] Harris. Facsimile over cellular radio. In D. M. Balston and R.C.V. Macario, editors, *Cellular Radio Systems*. Artech House, Boston, 1993.

[11] Thomas Haug. Overview of the GSM project. In *EUROCON 88*, June 1988.

[12] Josef-Franz Huber. Advanced equipment for an advanced network. *Telcom Report International*, 15(3-4), 1992.

[13] Hans Lobensommer and Helmut Mahner. GSM - a European mobile radio standard for the world market. *Telcom Report International*, 15(3-4), 1992.

[13] Bernard J. T. Mallinder. Specification methodology applied to the GSM system. In *EUROCON 88*, June 1988.