NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

MOBILE PHONE AND BASE STATION

Graduation Project

EE- 400

NAME: MOHAMMAD SHANABLEH (20033300)

SUBMITTED TO: Mr. Jamal Abu Hasna

Nicosia - 2007

ACKNOWLEDGMENTS

IN THE NAME OF ALLAH, MOST GRACIOUS, MOST MERCIFUL.

I wish to express my deepest appreciation to my god who stood beside me all the time,who supported me in all my achievements and who has given me the power and patience to finish my college studies successfully.

I am vary grateful to my teachers from in school and my lecturers who have brightened my mind with knowledge that i will need to have the finest life.

I would like to thank my supervisor Mr. Jamal Abu Hasna Under his guidance, I successfully overcome many difficulties and learn a lot about Mobile Phones And Base Station, I asked him many questions in Communications,Telecommunication and GSM, he explained my questions patiently.

I would like to express my gratitude to Prof. Dr. Şenol Bektaş and my uncle Mr. Tayseer Al-Shanableh and his family, because they helped to me at each stage of my Undergraduate Education in Near East University.

I also wish to thank my advisor Mr.Ozgur Ozdarem at my Undergraduate Education for his invaluable advices, for his help and for his patience also for his support.

Last but not least I want to thank Bilal Al-Kilany, Mahmoud Masoud, Yamen Al-Batarseh, and group of 2003 who provided me the encouragement and assistance that have made the completion of this work possible and I hope them success and happiness in life.

Finally, I dedicate my work and my success to my family,especially my parents without their endless support, I could never have prepared this thesis without the encouragement and support of my family, and cousines.

TABLE OF CONTENTS

INTRODUCTION

GSM (Global System for Mobile Communications) is a European digital communications standard which provides full duplex data traffic to any device fitted with GSM capability, it can easily interface with other digital communications systems, such as ISDN, and digital devices, such as Group 3 facsimile machines.

Unlike any other service, GSM products such as cellular phones require the use of a Subscriber Identity Module, or SIM card .These small electronic devices are approximately the size of a credit card and record all of the user information in it. This includes data such as programmed telephone numbers and network security features, which identify the user. Without this module, the device will not function. This allows for greater security and also greater easy of use as this card maybe transported from one phone to another, while maintaining the same information available to the user. GSM is also present outside of Europe but known by different names.

The only stands for the operating between these systems in the frequency at which operate . The number of stands for the operating frequency in megahertz . While each system uses the GSM standard, they are not compatible with each other.

1. INTRODUCTION TO GSM

1.1 Overview

GSM (Global System for Mobile Communications) is a European digital communications standard which provides full duplex data traffic to any device fitted with GSM capability, such as a phone, fax, or pager, at a rate of 9600 bps using the TDMA communications scheme. Since GSM is purely digital, it can easily interface with other digital communications systems, such as ISDN, and digital devices, such as Group 3 facsimile machines.

Unlike any other service, GSM products such as cellular phones require the use of a Subscriber Identity Module, or SIM card. These small electronic devices are approximately the size of a credit card and record all of the user information it. This includes data such as programmed telephone numbers and network security features, which identify the user. Without this module, the device will not function. This allows for greater security and also greater ease of use as this card may be transported from one phone to another, while maintaining the same information available to the user. GSM is also present outside of Europe but known by different names.

In North America it is known as PCS 1900 and elsewhere are DCS 1800 (also known as PCS). The only difference between these systems is the frequency at which operate. The number stands for the operating frequency in megahertz. While each system uses the GSM standard, they are not compatible with each other. Figure 1.1 shows the evolution of the Mobile.

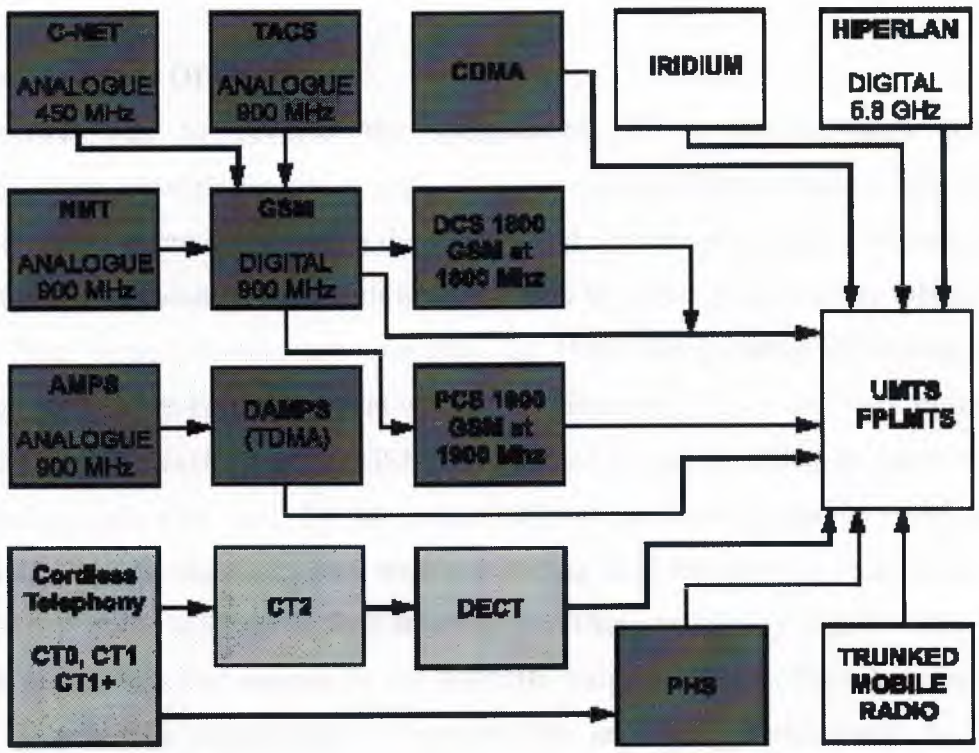

Figure 1.1 The Mobile Evolution

1.2 History Of GSM

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. In the Nordic and Benelux countries the NMT 450 was developed, TACS in the UK and C-Netz in West Germany. The Radio com 2000 was in France and RTMI/RTMS in Italy. But each system was incompatible with everyone else's in equipment and operation and as business was becoming increasingly international, the cutting edge of the communications industry focused on exclusively local cellular solutions. These systems were fine if you wanted to call the office if you were in your own home, but not if you were with a client in another country. Also home market revenue simply wouldn't justify sustained programs of investment. As a solution in 1982 CEPT, the Conference des Administrations Europeans des Postes et Telecommunications comprised the telecom administrations of twenty-six European countries, established the Group Special Mobile (GSM).

1.2.1 Developments Of GSM

Its objective was to develop the specification for a pan-European mobile communications network capable of supporting the many millions of subscribers likely to turn to mobile communications in the years ahead. The home market revenue simply wouldn't justify sustained programs of investment so to further progress they lobbied for support from some political heavyweights. In 1985, the growing commitment to resolving the problem became evident when West Germany, France and Italy signed an agreement for the development of GSM. The United Kingdom added its name to the agreement the following year. By this time, CEPTs Group Special Mobile could argue persuasively that the standards they were developing held the key to a technically and economically viable solution as their standard was likely to employ digital rather than analogue technology and operate in the 900MHz frequency band. Digital technology offered an attractive combination of performance and spectral efficiency. In other words, it would provide high quality transmission and enable more callers simultaneously to use the limited radio band available. In addition, such a system would allow the development of advanced features like speech security and data communications. Handsets could be cheaper and smaller. It would also make it possible to introduce the first hand-held terminals - even though in the early days in terms of size and weight these would be practically indistinguishable from a brick. Finally, the digital approach neatly complemented the Integrated Services Digital Network (ISDN), which was being developed by land-based telecommunications systems throughout the world. But the frequencies to be employed by the new standard were being snapped up by the analogue networks. Over-capacity crisis had started to sound alarm bells throughout the European Community. Demand was beginning to outstrip even the most optimistic projections. The Group Special Mobile's advocacy of digital cellular technology was on hand to offer light at the end of the tunnel. The Directive ensured that every Member State would reserve the 900MHz frequency blocks required for the rollout program. Although these were somewhat smaller than the amount advocated by the CEPT, the industry had finally achieved the political support it needed to advance its objectives. The logistical nightmare in the GSM, which followed soon left this achievement as a distant, dream so single, permanent organization at the helm.

In1986 the GSM Permanent Nucleus was formed and its head quarters established in Paris. It was all very well agreeing the technology and standards for this new product. But what about the creation of a market? It was essential to forge a commercial agreement between potential operators who would commit themselves to implementing the standard by a particular date. Without such an agreement there could be no network. Without the network there would be no terminals. Without network and terminals there would be no service. Stephen Temple of the UK's Department of Trade and Industry was charged with the task of drafting the first Memorandum of Understanding (MOU). In September 1987 network operators from thirteen countries signed a MOU in Copenhagen. One of the most important conclusions drawn from the early tests was that the new standard should employ Time Division Multiple Access (TDMA) technology. The strength of its technical performance ensured that narrowband TDMA had the support of major players like Nokia, Ericsson and Siemens. This promised the flexibility inherent in having access to a broad range of suppliers and the potential to get product faster into the marketplace. But as always as soon as one problem was solved other problems looming on the horizon .

In 1989, the UK Department of Trade and Industry published a discussion document called "Phones on the Move". This advocated the introduction of mass-market mobile communications using new technology and operating in the 1800 MHz frequency band. The UK government licensed two operators to run what became known as Personal Communications Networks (PCN). Operating at the higher frequency gave the PCN operators virtually unlimited capacity; where as 900MHz was limited. The next hurdle to over come was that of the deadline. If the 1 July 1991 launch date was not met there was a real danger that confidence in GSM technology would be fatally undermined but moral received a boost when in 1989 the responsibility for specification development passed from the GSM Permanent Nucleus to the newly created European Telecommunications Standards Institute (ETSI). In addition, the UK's PCN turned out to be more of an opportunity than a threat. The new operators decided to utilize the GSM specification - slightly modified because of the higher frequency - and the development of what became known as DCS 1800 was carried out by ETSI in parallel with GSM standardization. In fact, in 1997 DCS 1800 was renamed GSM 1800 to reflect the affinity between the two technologies. With so many manufacturers creating so many products in so many countries, it soon became apparent that it was critical that

each type of terminal was subject to a rigorous approval regime. Rogue terminals could cause untold damage to the new networks. The solution was the introduction of Interim Type Approval (ITA). Essentially, this was a procedure in which only a subset of the approval parameters was tested to ensure that the terminal in question would not create any problems for the networks. In spite of considerable concern expressed by some operators, ITA terminals became widely available in the course of 1992. True hand held terminals hit the market at the end of that year and the GSM bandwagon had finally started to roll. From here the G.S.M became a success story. In 1987, the first of what was to become an annual event devoted to the worldwide promotion of GSM technology was staged by conference organizers IBC Technical Services. The Pan European Digital Cellular Conference . This year it celebrated its tenth anniversary in Cannes, attracting over 2,400 delegates. By the end of 1993, GSM had broken through the 1 million-subscriber barrier with the next million already on the horizon. By June 1995 Phase 2 of standardization came in to play and a demonstration of fax, video and data communication via GSM. When the GSM standard was being drawn up by the CEPT, six separate systems were all considered as the base. There were seven criteria deemed to be of importance when assessing which of the six would be used. Each country developed its own system, which was incompatible with everyone else's in equipment and operation. This was an undesirable situation, because not only was the mobile equipment limited to operation within national boundaries, which in a unified Europe were increasingly unimportant, but there was also a very limited market for each type of equipment, so economies of scale and the subsequent savings could not be realized. The Europeans realized this early on, and in 1982 the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Group Special Mobile (GSM) to study and develop a pan-European public land mobile system. The proposed system had to meet certain criteria. In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase-I of the GSM specifications were published in 1990. Commercial service was started in mid-1991, and by 1993 there were 36 GSM networks in 22 countries with 25 additional countries having already selected or considering GSM. This is not only a European standard - South Africa, Australia, and many Middle and Far East countries have chosen GSM. Although standardized in Europe, GSM is not only a European standard. Over 200 GSM networks (including DCS1800 and PCS1900) are operational in 110 countries around the world. In the beginning of 1994, there were 1.3 million subscribers

worldwide, which had grown to more than 55 million by October 1997. With North America making a delayed entry into the GSM field with a derivative of GSM called PCS1900, GSM systems exist on every continent, and the acronym GSM now aptly stands for Global System for Mobile communications. The developers of GSM chose an unproven (at the time) digital system, as opposed to the then-standard analog cellular systems like AMPS in the United States and TACS in the United Kingdom. They had faith that advancements in compression algorithms and digital signal processors would allow the fulfillment of the original criteria and the continual improvement of the system in terms of quality and cost. The over 8000 pages of GSM recommendations try to allow flexibility and competitive innovation among suppliers, but provide enough standardization to guarantee proper inter-working between the components of the system. This is done by providing functional and interface descriptions for each of the functional entities defined in the system. The development of GSM started in 1982, when the Conference of European Posts and Telegraphs (CEPT) formed a study group called Group Special Mobile (the initial meaning of GSM). The group was to study and develop a pan-European public cellular system in the 900 MHz range, using spectrum that had been previously allocated. At that time, there were many incompatible analog cellular systems in various European countries. Some of the basic criteria for their proposed system were:

- 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, the responsibility for GSM was transferred to the European Telecommunication Standards Institute (ETSI), and the Phase I recommendations were published in 1990. At that time, the United Kingdom requested a specification based on GSM but for higher user densities with low-power mobile stations, and operating at 1.8 GHz. The specifications for this system, called Digital Cellular System (DCS1800) were published 1991. Commercial operation of GSM networks started in mid-1991 in

European countries. By the beginning of 1995, there were 60 countries with operational or planned GSM networks in Europe, the Middle East, the Far East, Australia, Africa, and South America, with a total of over 5.4 million subscribers. As it turned out, none of the six candidates was actually used! The information collected during the tests did enable the GSM (Group Special Mobile) to design the specifications of the current GSM network. The total change to a digital network was one of the fundamental factors of the success of GSM. Digital transmission is easier to decode than analogue due to the limited number of possible input values (0.1), and as ISDN was becoming de facto at the time, it was logical to avail of digital technology. This also ensured that GSM could evolve properly in an increasingly digital world, for example with the introduction of an 8kps speech coder. It is much easier to change channel characteristics digitally than analogously. Finally, the transmission method decided on for the network was TDMA, as opposed to FDMA and CDMA. In 1989, responsibility for the specification was passed from CEPT to the newly formed and now famous European Telecommunications Standards Institute (ETSI). By 1990, the specifications and explanatory notes on the system were documented extensively, producing 138 documents in total, some reaching sizes of several hundred pages in length services.

1.3 Technology

1.3.1 Services Provided By GSM

From the beginning, the planners of GSM wanted ISDN compatibility in terms of the services offered and the control signaling used. However, radio transmission limitations, in terms of bandwidth and cost, do not allow the standard ISDN B-channel bit rate of 64 kbps to be practically achieved. Using the ITU-T definitions, telecommunication services can be divided into bearer services, tele-services, and supplementary services. The digital nature of GSM allows data, both synchronous and asynchronous, to be transported as a bearer service to or from an ISDN terminal. Data can use either the transparent service, which has a fixed delay but no guarantee of data integrity, or a non-transparent service, which guarantees data integrity through an Automatic Repeat Request (ARQ) mechanism, but with a variable delay. The data rates supported by GSM are 300 bps, 600 bps, 1200 bps, 2400 bps, and 9600 bps. The most basic tele-service supported by GSM is telephony. As with all other communications, speech is digitally encoded and transmitted through the GSM network as a digital stream. There is

also an emergency service, where the nearest emergency-service provider is notified by dialing three digits (similar to 911). A variety of data services is offered. GSM users can send and receive data, at rates up to 9600 bps, to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks, and Circuit Switched Public Data Networks using a variety of access methods and protocols, such as X.25 or X.32. Since GSM is a digital network, a modem is not required between the user and GSM network, although an audio modem is required inside the GSM. Network to inter-work with POTS . Other data services include Group 3 facsimile, as described in ITU-T recommendation T.30, which is supported by use of an appropriate fax adaptor. A unique feature of GSM, not found in older analog systems, is the Short Message Service (SMS). SMS is a bi directional service for short alphanumeric (up to 160 bytes) messages. Messages are transported in a store-and-forward fashion. For point-to-point SMS, a message can be sent to another subscriber to the service, and an acknowledgement of receipt is provided to the sender. SMS can also be used in a cell-broadcast mode, for sending messages such as traffic updates or news updates. Messages can also be stored in the SIM card for later retrieval supplementary services are provided on top of tele-services or bearer services. In the current (Phase I) specifications, they include several forms of call forward (such as call forwarding when the mobile subscriber is unreachable by the network), and call barring of outgoing or incoming calls, for example when roaming in another country. Many additional supplementary services will be provided in the Phase 2 specifications, such as caller identification, call waiting, multi-party conversations. GSM was designed having interoperability with ISDN in mind, and the services provided by GSM are a subset of the standard ISDN services. Speech is the most basic, and most important, tele-service provided by GSM. In addition, various data services are supported, with user bit rates up to 9600 bps. Specially equipped GSM terminals can connect with PSTN, ISDN, Packet Switched and Circuit Switched Public Data Networks, through several possible methods, using synchronous or asynchronous transmission. Also supported are Group 3 facsimile service, video-tax, and telexed. Other GSM services include a cell broadcast service, where messages such as traffic reports, are broadcast to users in particular cells. A service unique to GSM, the Short Message Service, allows users to send and receive point-to-point alphanumeric messages up to a few tens of bytes. It is similar to paging services, but much more comprehensive, allowing bi-directional messages, store-and-forward delivery, and acknowledgement of successful delivery.

1.4 The Different GSM-Based Networks

Different frequency bands are used for GSM 900, GSM1800 and GSM 1900 (Table 1.3.). In some countries, an operator applies for the available frequencies. In other countries, e.g. United States, an operator purchases available frequency bands at auctions.

Table 1.3 Frequency Bands for the Different GSM-Based Networks

Network type	Frequency band UL / DL	Implementations
GSM 900	890-915 / 935-960 MHz	GSM 900
GSM1800	1710 – 1785 / 1805 -1880 MHz	GSM 1800
GSM1900	1850-1910 / 1930-1990 MHz	GSM1900

1.4.1 Where Are GSM Frequencies Used?

GSM networks presently operate in three different frequency ranges. These are:

a) GSM 900

(Also called GSM) operates in the 900 MHz frequency range and is the most common in Europe and the world.

b) GSM 1800

(Also called PCN (Personal Communication Network), and DCS 1800) - operates in the 1800 MHz frequency range and is found in a rapidly-increasing number of countries including France, Germany, Switzerland, the UK, and Russia. A European Commission mandate requires European Union members to license at least one DCS 1800 operator before 1998.

c) GSM 1900

(Also called PCS (Personal Communication Services), PCS 1900, and DCS 1900) - the only frequency used in the United States and Canada for GSM. Note that the terms PCS is commonly used to refer to any digital cellular network operating in the1900 MHz frequency range, not just GSM.

1.5 Summary

This chapter represents Introduction to GSM, History Of GSM, Technology and the Different GSM-Based Networks.

2. GSM STRUCTURE

2.1 Services Provided By GSM

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

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

A variety of data services is offered. GSM users can send and receive data, at rates up to 9600 bps, to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks, and Circuit Switched Public Data Networks using a variety of access methods and protocols, such as X.25 or X.32. Since GSM is a digital network, a modem is not required between the user and GSM network, although an audio modem is required inside the GSM network to inter work with POTS.

Other data services include Group 3 facsimile, as described in ITU-T recommendation T.30, which is supported by use of an appropriate fax adaptor. A unique feature of GSM, not found in older analog systems, is the Short Message Service (SMS). SMS is a 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 tale services or bearer services. In the current (Phase I) specifications, they include several forms of call forward (such as call forwarding when the mobile subscriber is unreachable by the network), and call barring of outgoing or incoming calls, for example when roaming in another country. Many additional supplementary services will be provided in the Phase 2 specifications, such as caller identification, call waiting, multi-party conversations.

2.2 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.

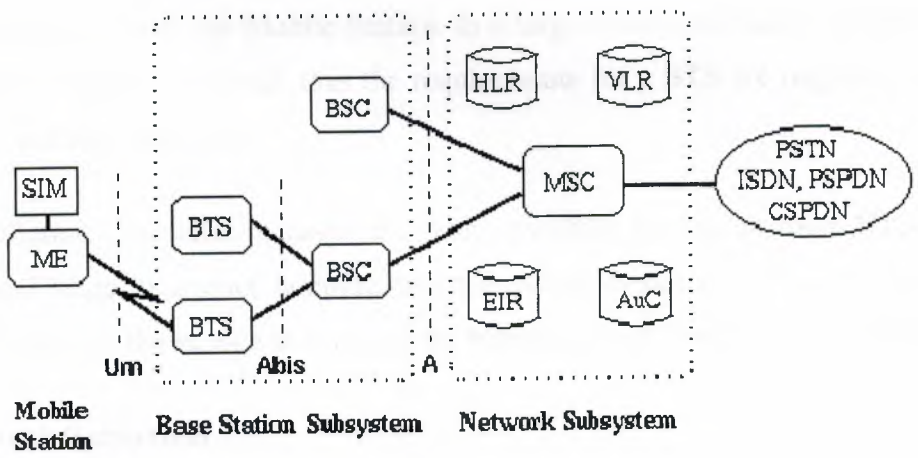

Figure 2.1 General architecture of a GSM network

2.2.1 Mobile Station

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

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

2.2.2 Base Station Subsystem

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

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

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

2.2.3 Network Subsystem

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are

provided in conjunction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the fixed networks (such as the PSTN or ISDN). Signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7), used for trunk signaling in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call-routing and roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The location of the mobile is typically in the form of the signaling address of the VLR associated with the mobile station. The actual routing procedure will be described later. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

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

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

2.3 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.

2.3.1 Multiple Access and Channel Structure

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

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

2.3.1.1 Traffic Channels

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multi frame, or group of 26 TDMA frames. The length of a 26-frame multi frame is 120 ms, which is how the length of a burst period is defined (120 ms divided by 26 frames divided by 8 burst periods per frame). Out of the 26 frames, 24 are used for traffic, 1 is used for the Slow Associated Control Channel (SACCH) and 1 is currently unused (see

Frequency Correction Channel (FCCH) and Synchronization Channel (SCH) Used to synchronies the mobile to the time slot structure of a cell by defining the boundaries of burst periods, and the time slot numbering. Every cell in a GSM network broadcasts exactly one FCCH and one SCH, which are by definition on time slot number 0 (within a TDMA frame).
Random Access Channel (RACH) Slotted Aloha channel used by the mobile to request access to the network.
Paging Channel (PCH) Used to alert the mobile station of an incoming call.
Access Grant Channel (AGCH) Used to allocate an SDCCH to a mobile for signaling (in order to obtain a dedicated channel), following a request on the RACH.

2.3.1.3 Burst Structure

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

2.3.2 Speech Coding

GSM is a digital system, so speech which is inherently analog, has to be digitized. The method employed by ISDN, and by current telephone systems for multiplexing voice lines over high speed trunks and optical fiber lines, is Pulse Coded Modulation (PCM). The output stream from PCM is 64 kbps, too high a rate to be feasible over a radio link. The 64 kbps signal, although simple to implement, contains much redundancy. The GSM group studied several speech coding algorithms on the basis of subjective speech quality and complexity (which is related to cost, processing delay, and power consumption once implemented) before arriving at the choice of a Regular Pulse Excited -- Linear Predictive Coder (RPE--LPC) with a Long Term Predictor loop. Basically, information from previous samples, which does not

change very quickly, is used to predict the current sample. The coefficients of the linear combination of the previous samples, plus an encoded form of the residual, the difference between the predicted and actual sample, represent the signal. Speech is divided into 20 millisecond samples, each of which is encoded as 260 bits, giving a total bit rate of 13 kbps. This is the so-called Full-Rate speech coding. Recently, an Enhanced Full-Rate (EFR) speech coding algorithm has been implemented by some North American GSM1900 operators. This is said to provide improved speech quality using the existing 13 kbps bit rate.

2.3.3 Channel Coding and Modulation

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

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

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

slot burst can carry two 57 bit blocks, each burst carries traffic from two different speech samples.

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

2.3.4 Multi Path 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 multi path 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.

2.3.5 Frequency Hopping

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

2.3.6 Discontinuous Transmission

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

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

2.3.7 Discontinuous Reception

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

2.3.8 Power Control

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

The mobile station measures the signal strength or signal quality (based on the Bit Error Ratio), and passes the information to the Base Station Controller, which ultimately decides if and when the power level should be changed. Power control should be handled carefully, since there is the possibility of instability. This arises from having mobiles in co-channel cells alternating increase their power in response to increased co-channel interference caused by the other mobile increasing its power. This in unlikely to occur in practice but it is (or was as of 1991) under study.

2.4 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 Signaling System No. 7 protocol.

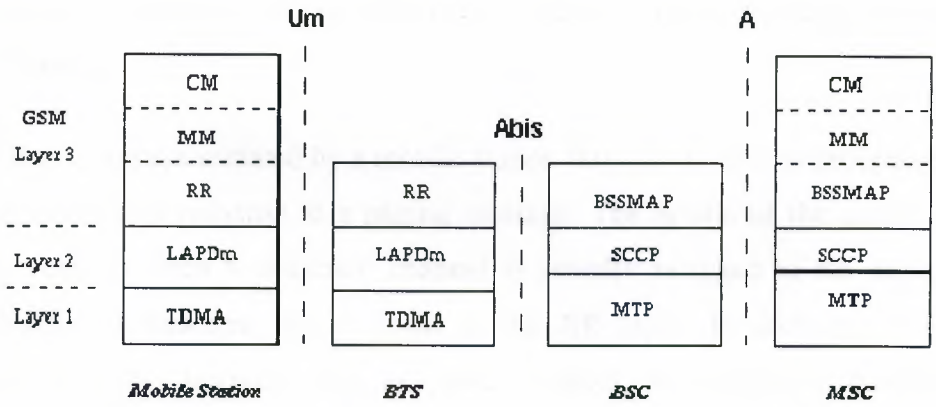

Figure 2.3 Signaling protocol structure in GSM

The signaling protocol in GSM is structured into three general layers, depending on the interface, as shown in Figure 2.3 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 Signaling System Number 7 is used. Layer 3 of the GSM signaling protocol is itself divided into 3 sub layers.

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.
Signaling between the different entities in the fixed part of the network, such as between the HLR and VLR, is accomplished thought the Mobile Application Part (MAP). MAP is built on top of the Transaction Capabilities Application Part (TCAP, the top layer of Signaling 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.

2.4.1 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.

2.4.1.1 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 signaling 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 multi path 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.

2.4.2 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.

2.4.2.1 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 signaling, 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 signaling 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.

2.4.2.2 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 conjunction 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.

2.4.3 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 sub layer 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 sub layer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

2.4.3.1 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 (see Figure 2.4).

3. MOBILE PHONES

3.1 Overview

Mobile phones may be thought of as cordless phones with elaborate portable and base units. High-power transmitters and elevated antennas that provide the radio carrier link over an area within 20 to 30 miles from the base station antenna, as well as the multiplexing, detecting, sorting and selecting features required to simultaneously service 60 subscribers per base station, are the major differences between cordless phones and mobile phones.

3.2 Base Unit

The base station can transmit and receive on several different frequencies simultaneously to provide individual channels for use at the same time. The radio base station transmitter output power is typically 200-250 watts and the radiated power can be as high as 500 watts if the transmitting antenna gain is included. It covers a circular area of up to 30 miles in radius for clear reliable communications, but transmitters with the same frequency are not spaced closer than about 60 to 100 miles because of the noise interference levels.

The receiver contains filters, high-gain amplifiers, and demodulators to provide a usable voice signal to the phone line. The control terminal contains the necessary detector and timing and logic circuits to control the transmission link between the base unit and the mobile units. As a result, phone calls are coupled to and from the standard phone system just like calls that are carried completely over wired facilities. The control terminal has the necessary interface circuits so that a call initiated at a mobile unit is interconnected through the national or international phone system to the called party just as any other phone call.

The national and international phone system facilities are owned by the respective phone companies. The base units and mobile units may be owned by the phone company or by a separate company called a radio common carrier (RCC). When the mobile system is run

by a RCC, the RCC is charged by the telephone company for the use of the standard phone system just like any other customer.

The cost is then included in the charge by the RCC to the eventual user of the mobile units.

To subscribe to mobile phone service, a user has only to apply, and be accepted by the RCC or the phone company operating the system. When the application is accepted, the user can lease or purchase the mobile equipment.

3.3 Mobile Unit

The mobile unit in the user's vehicle consists of a receiver containing amplifiers, a mixer and a demodulator; a transmitter containing a modulator, carrier oscillators and amplifiers; the necessary control logic; a control unit with microphone, speaker, keypad and switches; antennas and the interconnecting cables. The control unit performs all of the functions associated with normal phone use. A modern control head with automatic functions is illustrated.

The mobile phone user with automatic control places and receives calls in the same manner as with an ordinary phone. When the handset is lifted to place a call, the radio unit automatically selects an available channel. If no channel is available, the busy light comes on, if a channel is found, the user hears the normal dial tone from the phone system, and can then dial the number and proceed as if the phone were direct wired. An incoming call to the mobile unit is signaled by a ringing tone and is answered simply by lifting the handset and talking. Thus, the automatic mobile phone is as easily used as a phone. The mobile phone combines the mobility of the radio link and the world-wide switched network of the existing phone system to provide a communication link to any other phone in the world.

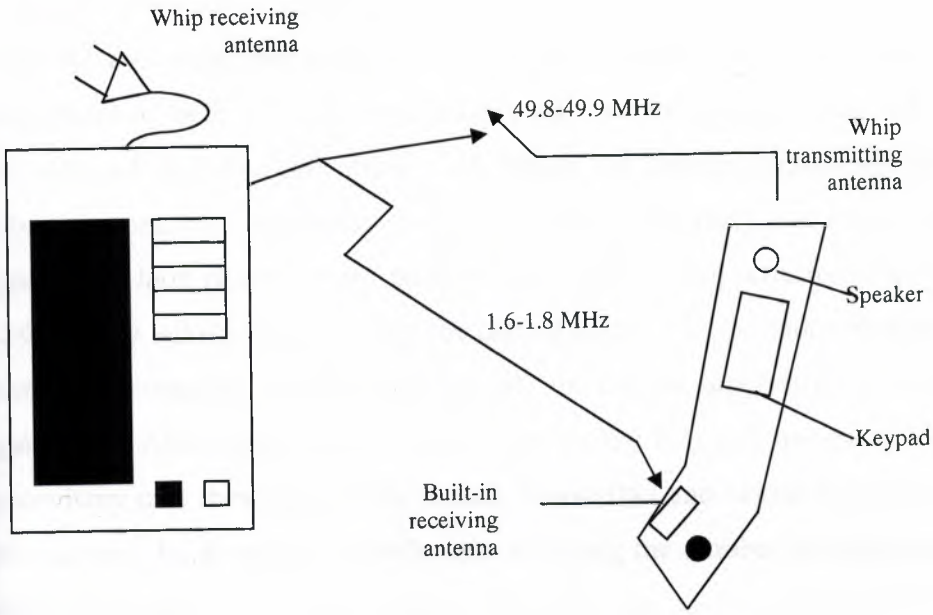

Figure 3.1 Mobile Unit

3.4 Detailed Operation

Different signaling techniques have to use in a mobile phone system in contrast with a wired facility. Since there are no wires connecting the telephone to the network, both speech and signaling must be transmitted via radio. For wireless operation, tones are used for those signaling functions, which are otherwise performed by voltage and current in hard-wired systems. This is accomplished by the use of special tones rather than applying a voltage level or detecting a current. The proper tone transmitted to the mobile unit will, for example, ring the mobile phone to indicate and incoming call just as with a standard phone different tone is used to indicate off-hook, busy, etc. The Improved Mobile Telephone System (IMTS) uses in band signaling tones from 1300 Hz to 2200 Hz. The older Mobile Phone system (MTs) had in band signaling tones in the 600 HZ to 1500 Hz range. Some systems use 2805 Hz as manual operation channel. When the mobile unit receives its correct seven-digit address, the mobile supervisory unit turns on the mobile transmitter and sends the acknowledgement signal Ack (5) using the 2150 Hz guard-tone, back to the control terminal. If this acknowledgement is not received by the control

terminal within 3 seconds after out pulsing the address, seize tone is removed and the call is abandoned However, upon receipt of the mobile acknowledgement signal, the terminal sends standard repetitive ringing at a cycle of 2 seconds on, 4 seconds off, using idle and seize tones as before. If the mobile does not answer within 45 seconds, ringing (6), is discontinued and the call abandoned. When the mobile subscriber goes off-hook to answer, the mobile supervisory unit sends a burst of connect tone (1633 Hz) as an answer signal (8). Upon receipt of the answer signal, the control terminal stops the ringing and establishes a talking path between the calling circuit and the radio channel (7). When the subscriber hangs-up (8). At the end of call, the mobile supervisory unit sends disconnect signal (12). Alternating the disconnect tone (1336 Hz) and the guard tone. The mobile supervisory unit then turns of the mobile transmitter and begins searching for the market idle channel. Each on-hook mobile unit receiving the number transmission compares the received number to its unit number. Only the one mobile unit with a number match remains locked on that channel.

3.5 Outgoing Call

The sequence for a call originated by a mobile subscriber is illustrated. When the subscriber goes off-hook to place the call, the mobile unit must be locked on the marked-idle channel. If not, the hand set will be inoperative and the bust lamp on the control unit will light, indicating to the subscriber that no channel is available. If the mobile unit will light, indicating to the subscriber that no channel is available. If the mobile unit is locked on the marked idle channel, the mobile supervisory unit will turn on the mobile transmitter to initiate the acknowledgement or handshake sequence.

Then mobile unit transmits its own number so the control terminal can identify if as a subscriber and can charge the call to the number. The roaming functions, are similar to those.

When a call is originated from the field, the mobile unit finds a marked idle channel and broadcasts an acknowledgement to the base by sending its identification. The mobile unit than completes a call in the usual manner by receiving a dial tone, then dialing the number and waiting for the called party to answer. Figure 3.3 shows the Outgoing Call.

3.6 Mobile Station

A Mobile station consists of two main elements: The Mobile Terminal (MT) and the Subscriber Identity Module (SIM). There are different types of terminals distinguished principally by their power and application. The fixed terminals are the ones installed in cars. Their maximum allowed output power is 20 W. The handheld terminals have experienced the biggest success thanks to their weight and volume, which are continuously decreasing. These terminals can emit up to 2 W. The evolution of technologies allows decreasing the maximum allowed power to 0.8 W.

3.7 Mobile Internal Call (MIC)

The MSI sends the call setup information dialed by the mobile subscriber (MSISDN) to the MSI (1). The MSC request information about the calling mobile subscriber MS2 from the VLR (2). The MSI used the dialing information (MSISDN) to establish the HLR and sets up signaling connection to it (3). The HLR sends a request to the VLR in whose are the called mobile subscribers MS2 is currently roaming (4). The VLR sends the request MSRN back to the HLR. The HLR forwards the MSRN to the MSC (5). Steps (6) to (9) are the same as steps (6) to (9) traditional silicon in photovoltaic cells in space because of its superior yielding about one-third more power for comparable cell areas.

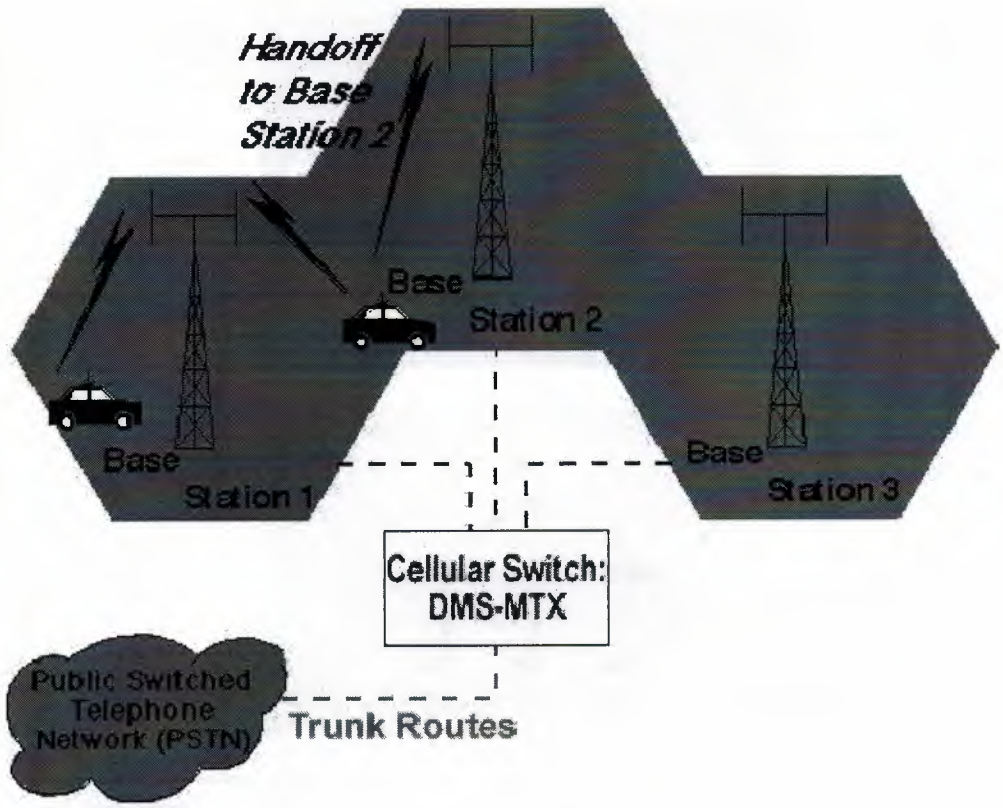

Figure 3.2 Mobile Internal Calls

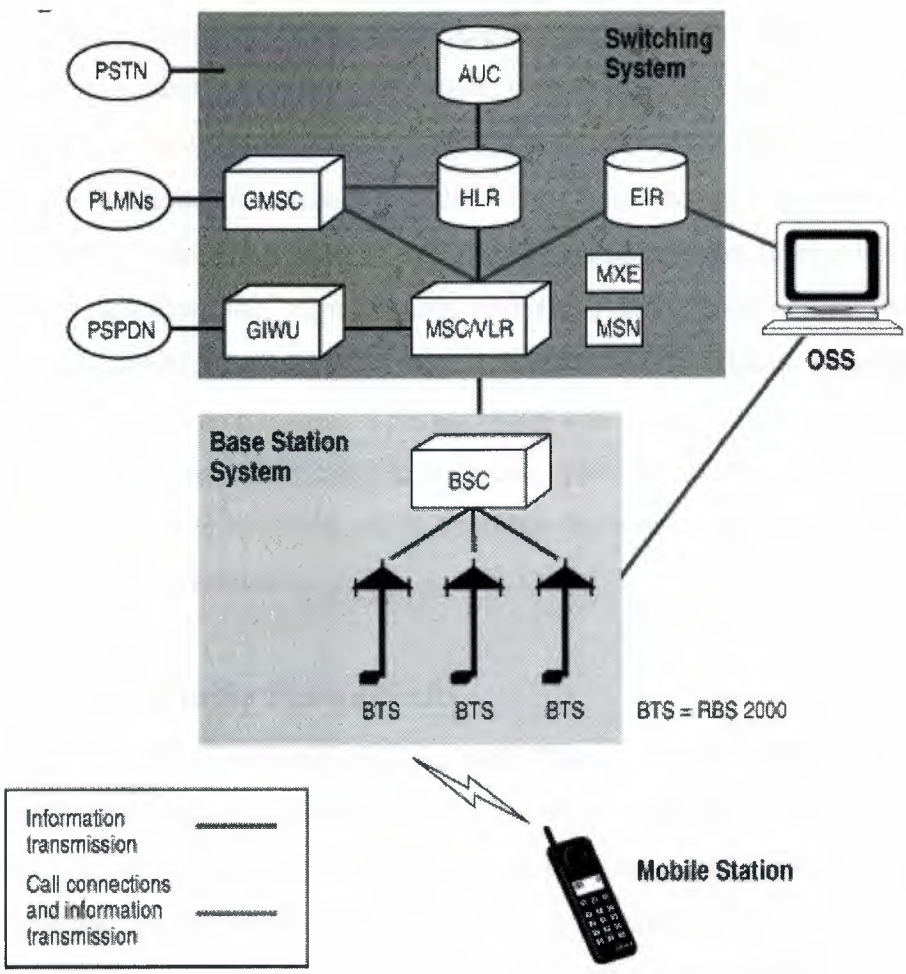

Figure 3.3 Outgoing Call

A trio of phased-away antennas extends and points earthward to establish direct links over the 1.610-1.625-GHz band to Iridium subscribers. The Iridium constellation, with a company-project price tag of $3.4 billion, is one of the most costly concepts ever devised for providing mobile communication services. Each satellite in the Iridium constellation will send out 48 pencil-thin spot-beams each of which can handle 230 simultaneous duplex conversations. Iridium satellites are distributed among six evenly spaced, near-polar orbits (86.4 degrees inclination) 780 Km above the earth, sixty of the satellites

provide overlapping global coverage, Polar Regions included. The other six are in-orbit spares. Iridium subscriber equipment offer voice, data, paging, and facsimile services.
Used instead the satellite-to-satellite cross links, the satellite-to-Iridium gateway stations and downlinks connecting the iridium satellites with their ground-based system control stations are provided using Ka-band at 20 GHz. The transmission links connecting the hand-held communicator, the paging units, and the remote area phones will all be handled with the L-band frequencies between 1.5 and 1.6 GHz. Iridium employs CDMA modulations and TDMA architecture. This approach will require that a dedicated portion of the frequency spectrum be allocated to Iridium to provide interference-free operation. Iridium's transmission rate has been set at 4800 bps for voice, and both 4800 and 2400 bps for digital data transmission.

3.8 Mobile and Portable Phone Units

Mobile and portable units are essentially the same things. The only difference is that the portable units have a lower output power and a less efficient antenna. Each mobile phone unit consists of a control unit, a radio transceiver, a logic unit, and a mobile antenna. The control unit house all the user interfaces, including a handset. The transceiver uses a frequency synthesizer to tune into any designated cellular system channel. The logic unit interrupts subscriber actions and system commands and manages the transceiver and control units.

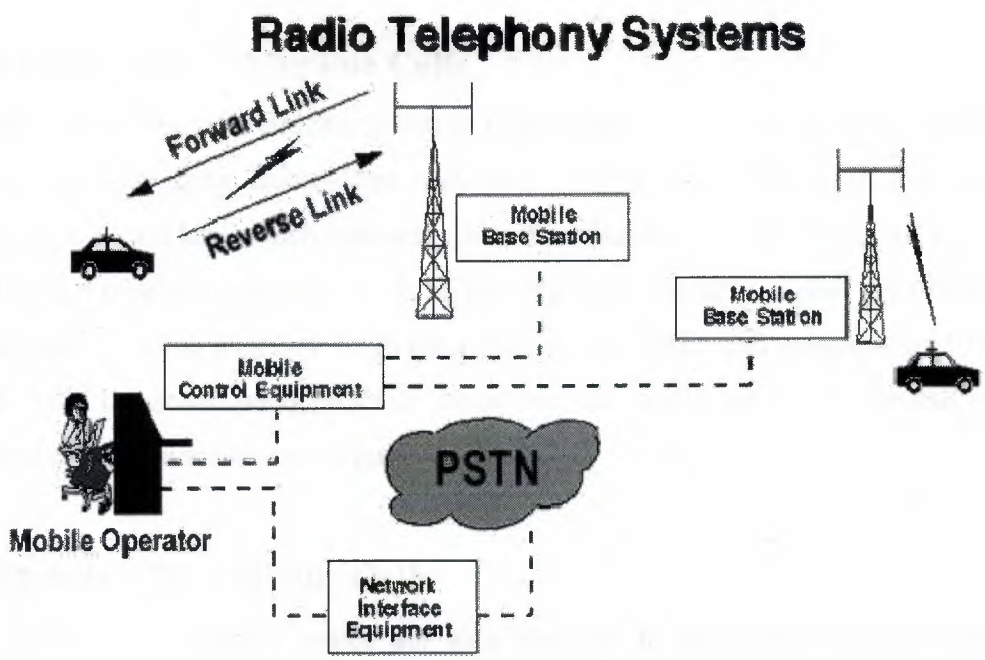

Figure 3.4 Portable Units of Mobile Phones

3.9 Wire line-To-Mobile Calls

The cellular system's switching centre receives a from a wire line party through a dedicated interconnect line from the public switched phone network. The switch translates the received dialing digits and determines whether the mobile unit to which the call is destined is on or off hook (busy). If the mobile unit is available, the switch pages the mobile subscriber. Following a page response from the mobile unit, the switch assigns an idle channel and instructs the mobile unit to time into that channel. The mobile unit sends a verification of channel tuning the controller in the cell site and then sends an audible call progress tone to the subscriber's mobile phone. Causing it to ring the switch terminates the call progress tones when it receives positive indication that the subscriber has answered the phone the conversation between the two parties has begun.

3.10 Mobile – To – Wire line Calls

A mobile subscriber who desires to call wire line party first enters the calls number into the unit's memory using Touch-Tone buttons or a dial on the phone unit. The subscriber then presses a send key, which transmits the called number as well as mobile subscriber's identification number to the switch. If the identification number is valid, the switch routes the call over a leased wire line interconnection to the public call progress tone from the switch. After the called party picks up the phone, the switch terminates the call progress tones and the conversation can begin.

3.11 Mobile – To – Mobile Calls

Calls between two mobile unites are also possible in the cellular radio system. To originate a call to another mobile unit, the calling party enters the called number into the unit's memory via the touchpad on the telephone set and the called number and then determines if the called unit is free to receive a call. The switch sends a page command to all cell-site controllers, and the called party (who may be anywhere in the service area) receives a page. Following a positive page from the called party, the switch assigns each party an idle user channel and instructs each party to tune into the respective user channel. Then the called party's phone rings. When the system receives notice that the called party has answered the phone, the switch terminates the call progress tone, and the conversation may begin between the two mobile units. If a mobile subscriber wished to initiate a call and all user channels are busy, the switch sends a directed retry command instructing the subscriber to reattempt the call through a neighboring cell. If the system cannot allocated as user channel through the neighboring cell, the switch transmits a intercept message to the calling mobile unit over the control channel. Whenever the called party is off look, the calling party receives busy signal. Also, if the called is invalid, the system either a record message via the control channel or provides and an announcement that the call cannot be processed.

3.12 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 (Figure 3.5):

1. Public switched telephone network (PSTN)
2. Mobile telephone switching office (MTSO)
3. Cell site with antenna system
4. Mobile subscriber unit (MSU)

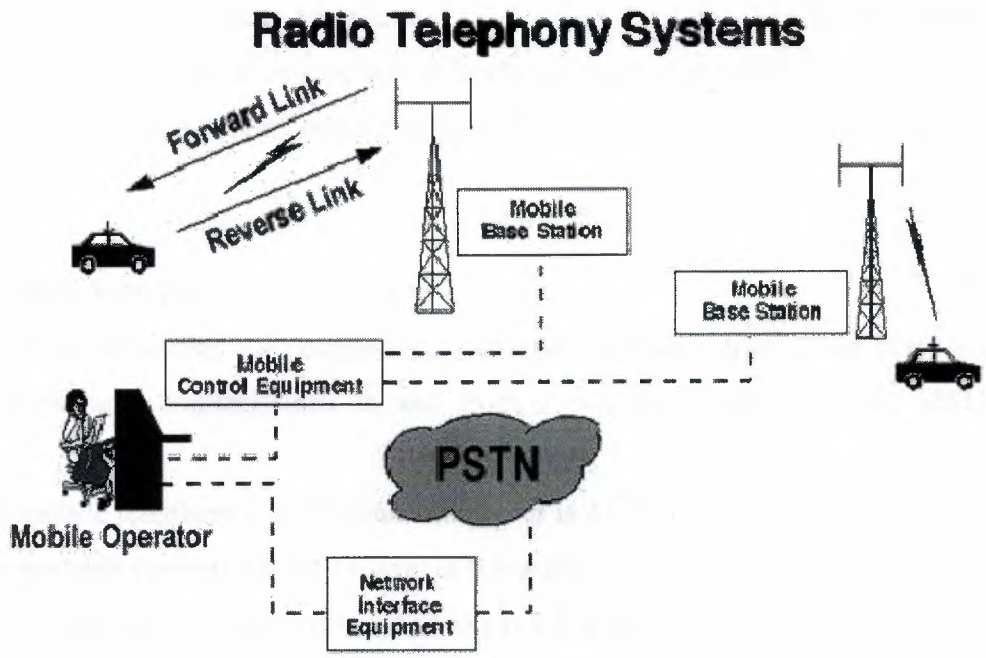

Figure 3.5: Cellular System Components

3.12.1 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.

3.12.2 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.

3.12.3 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.

3.12.4 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. Three types of MSUs are available:

1. The mobile telephone (typical transmit power is 4.0 watts)
2. The portable (typical transmit power is 0.6 watts)
3. 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.

3.13 Mobile Telephone System Using the Cellular Concept

Interference problems caused by mobile units using the same channel in adjacent areas proved that all channels could not be reused in every cell. Areas had to be skipped before the same channel could be reused. Even though this affected the efficiency of the original concept, frequency reuse was still a viable solution to the problems of mobile telephony systems.

Engineers discovered that the interference effects were not due to the distance between areas, but to the ratio of the distance between areas to the transmitter power (radius) of the areas. By reducing the radius of an area by fifty percent, service providers could increase the number of potential customers in an area fourfold. Systems based on areas with a one-kilometer radius would have one hundred times more channels than systems with areas ten kilometers in radius. Speculation led to the conclusion that by reducing the radius of areas to a few hundred meters, millions of calls could be served.

The cellular concept employs variable low-power levels, which allows cells to be sized according to the subscriber density and demand of a given area. As the population grows, cells can be added to accommodate that growth. Frequencies used in one cell cluster can be reused in other cells. Conversations can be handed off from cell to cell to maintain constant phone service as the user moves between cells (Figure3.6).

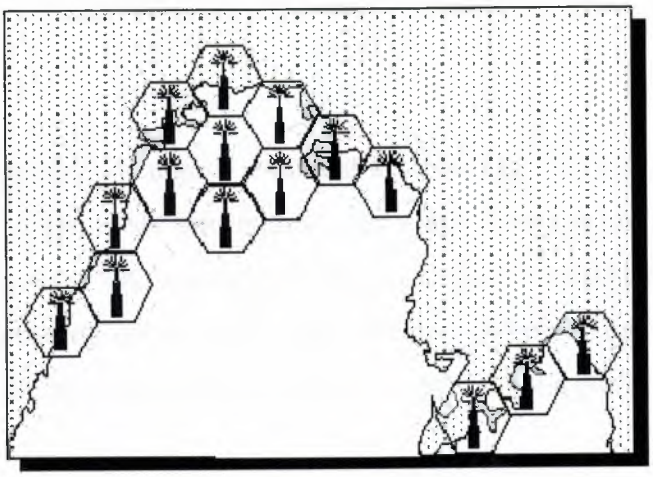

Figure 3.6: Mobile Telephone System Using a Cellular Architecture

The cellular radio equipment (base station) can communicate with mobiles as long as they are within range. Radio energy dissipates over distance, so the mobiles must be within the operating range of the base station. Like the early mobile radio system, the base station communicates with mobiles via a channel. The channel is made of two frequencies, one for transmitting to the base station and one to receive information from the base station.

3.14Cellular System Architecture

Increases in demand and the poor quality of existing service led mobile service providers to research ways to improve the quality of service and to support more users in their systems. Because the amount of frequency spectrum available for mobile cellular use was limited, efficient use of the required frequencies was needed for mobile cellular coverage. In modern cellular telephony, rural and urban regions are divided into areas according to specific provisioning guidelines. Engineers experienced in cellular system architecture determine deployment parameters, such as amount of cell-splitting and cell sizes.

Provisioning for each region is planned according to an engineering plan that includes cells, clusters, frequency reuse, and handovers.

3.14.1Cells

A cell is the basic geographic unit of a cellular system. The term *cellular* comes from the honeycomb shape of the areas into which a coverage region is divided. Cells are base stations transmitting over small geographic areas that are represented as hexagons. Each cell size varies depending on the landscape. Because of constraints imposed by natural terrain and man-made structures, the true shape of cells is not a perfect hexagon.

3.14.2Clusters

A cluster is a group of cells. No channels are reused within a cluster. (Figure3.7) illustrates a seven-cell cluster.

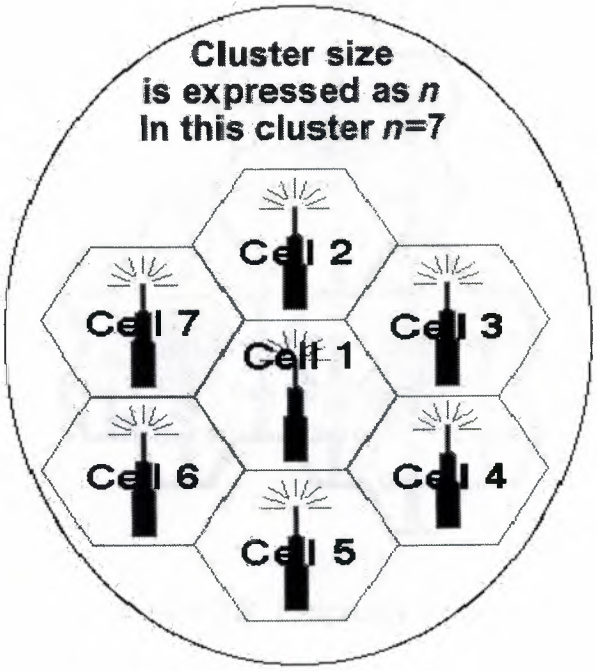

Figure3.7: A Seven-Cell Cluster

3.14.3Frequency Reuse

Because only a small number of radio channel frequencies were available for mobile systems, engineers had to find a way to reuse radio channels in order to carry more than one conversation at a time. The solution the industry adopted was called frequency planning or frequency reuse. Frequency reuse was implemented by restructuring the mobile telephone system architecture into the cellular concept.

The concept of frequency reuse is based on assigning to each cell a group of radio channels used within a small geographic area. Cells are assigned a group of channels that is completely different from neighboring cells. The coverage area of cells is called the footprint. This footprint is limited by a boundary so that the same group of channels can be used in different cells that are far enough away from each other so that their frequencies do not interfere (Figure 3.8).

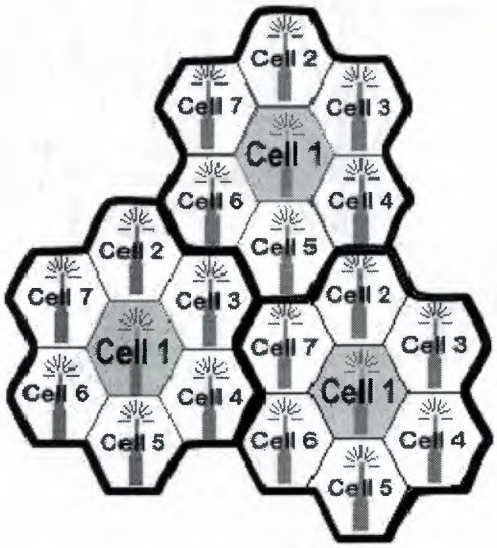

Figure 3.8: Frequency Reuse

Cells with the same number have the same set of frequencies. Here, because the number of available frequencies is 7, the frequency reuse factor is 1/7. That is, each cell is using 1/7 of available cellular channels.

3.14.4Cell Splitting

Unfortunately, economic considerations made the concept of creating full systems with many small areas impractical. To overcome this difficulty, system operators developed the idea of cell splitting. As a service area becomes full of users, this approach is used to split a single area into smaller ones. In this way, urban centers can be split into as many areas as necessary in order to provide acceptable service levels in heavy-traffic regions, while larger, less expensive cells can be used to cover remote rural regions (Figure 3.9).

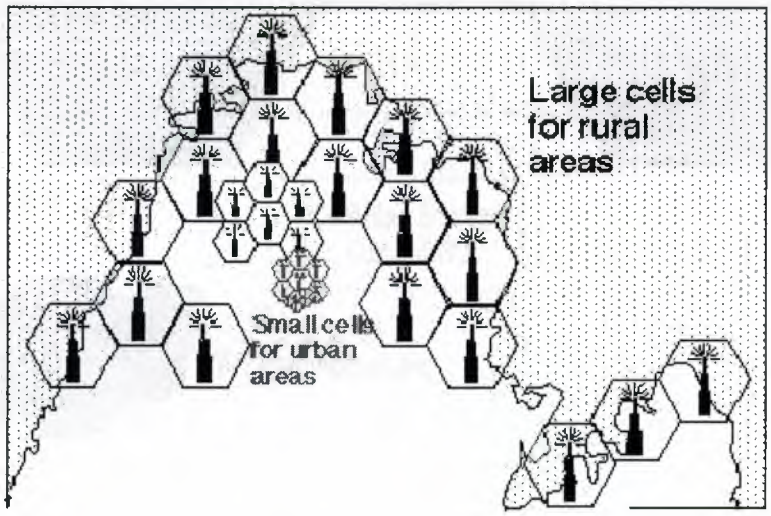

Figure3.8: Cell Splitting

3.14.5Handoff

The final obstacle in the development of the cellular network involved the problem created when a mobile subscriber traveled from one cell to another during a call. As adjacent areas do not use the same radio channels, a call must either be dropped or transferred from one radio channel to another when a user crosses the line between adjacent cells. Because dropping the call is unacceptable, the process of handoff was

created. Handoff occurs when the mobile telephone network automatically transfers a call from radio channel to radio channel as mobile crosses adjacent cells (Figure 3.10).

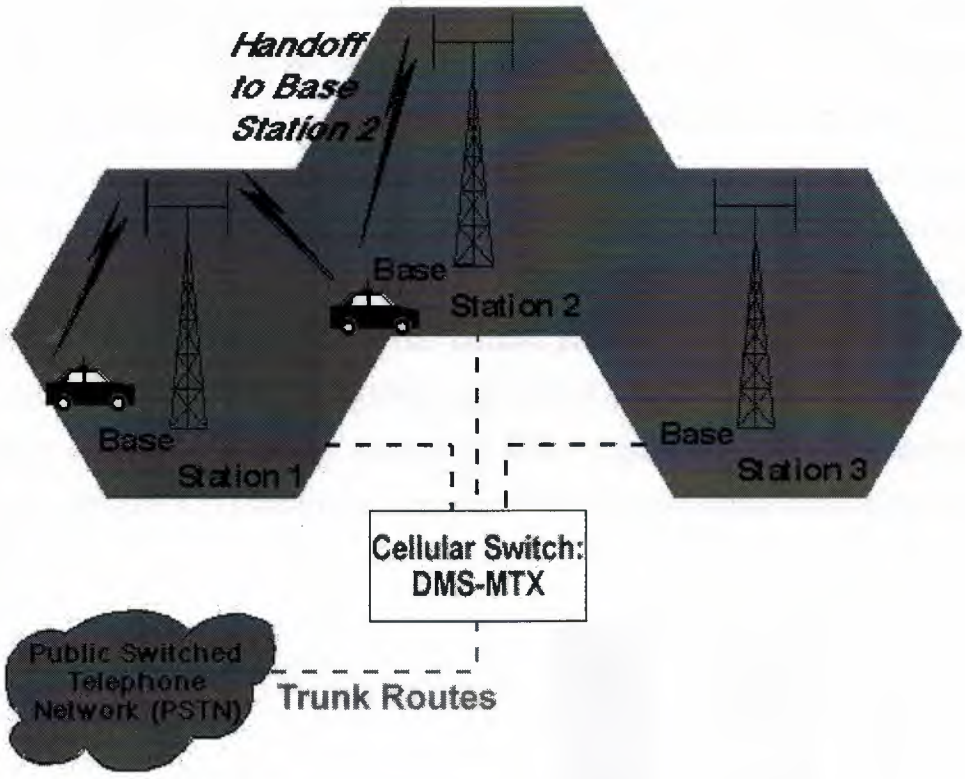

Figure 3.10: Handoff between Adjacent Cells

During a call, two parties are on one voice channel. When the mobile unit moves out of the coverage area of a given cell site, the reception becomes weak. At this point, the cell site in use requests a handoff. The system switches the call to a stronger-frequency channel in a new site without interrupting the call or alerting the user. The call continues as long as the user is talking, and the user does not notice the handoff at all.

3.15 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 ten minutes, mobile calls usually run ninety seconds. Engineers who expected to assign fifty 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 TDMA, GSM, PCS1900, and CDMA promise to significantly increase the efficiency of cellular telephone systems to allow a greater number of simultaneous conversations. (Figure 3.11) shows the components of a typical digital cellular system.

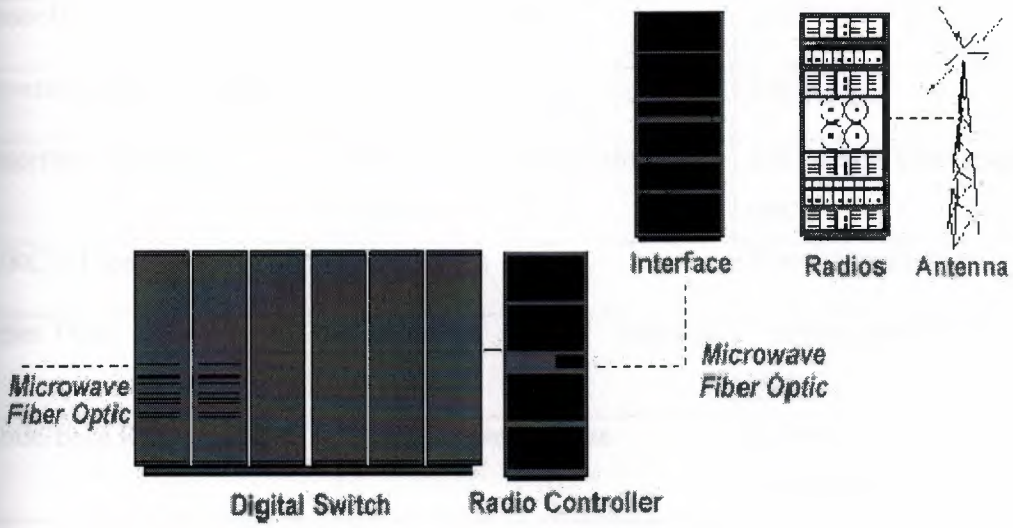

Figure 3.11: Digital Cellular System

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 DAMPS by overlaying their existing networks with TDMA architectures.

Table 3.1: AMPS/DAMPS Comparison

	Analog	Digital
Standard	EIA-533 (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 Relation ship	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)

3.15.1 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. Uses many blocks of spectrum in 800 MHz and 1900 MHz
5. All transmissions are digital
6. TDMA/FDMA application 7.3 callers per radio carrier (6 callers on half rate later), providing three 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.

3.15.2 Extended Time Division Multiple Access (E– TDMA)

The extended TDMA (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.

3.15.3 Fixed Wireless Access (FWA)

Fixed wireless access (FWA) is a radio-based local exchange service in which telephone service is provided by common carriers (Figure 3.12). 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 wire line 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.

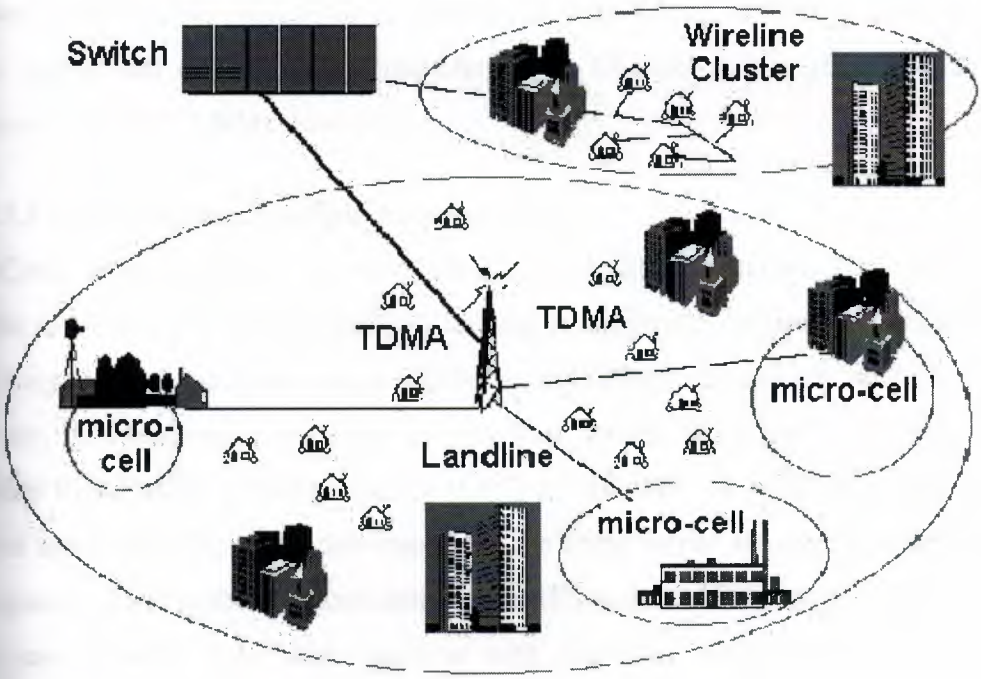

Figure 3.12: Fixed Wireless Access

3.15.4 Personal Communications Services (PCS)

The future of telecommunications includes personal communications services. PCS at 1900 MHz (PCS1900) is the North American implementation of DCS1800 (Global System for Mobile communications, or 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, which 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.

3.15.5 Code Division Multiple Access (CDMA)

Code division multiple access (CDMA) is a digital air interface standard, claiming eight to fifteen 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 wire line 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).

3.16 Advanced Mobile Phone Service

Lyn the AMPS system, the interface between the land phone network and the radio paths to the mobiles occurs at the cell sites. In addition to performing unction needed for trunk termination and for radio transmission and reception, the cell site handles many semiautonomous functions under the general direction of the Mobile Phone Switching Office (MTSO).

Cell sites have facilities to:

Provide RF radiation, reception, and distribution.

Provide data communications with the MTSO and mobiles.

Locate mobiles.

Perform remotely ordered equipment testing.

Perform equipment control and reconfiguration functions.

Perform voice-processing functions.

Perform, call setup, call supervision, and call termination.

Handoff or receive from another cell site any mobile which has moved out of the normal service area of the cell site carrying the call. Programmable controllers control cell-site operations partially by wired logic and partially. Control functions are redundant and can be a configured as needed to overcome a loalised failure. A battery plant assures maintenance of service in case of commercial power outage.

Facilities dependent upon traffic requirements in each cell coverage area are modular so those additional units may be installed as needed to match busy-hour traffic levels. This will ensure that plant investment can grow sensibly as a function of anticipated revenues 48 voice channels. The precise number if a frame at each site is a function of the voice channels requirements for that site. There are four frame codes, and the smallest size cell site requires one of each code. Each radio frame has a maximum capacity of 16 radiuses. When the number of voice radius grows beyond 16, another radio frame must be added. Each line supervision frame (LSF) can handle 48 voice channels and, when this number is exceeded, another LSF is added. A single data frame (DF) and a single maintenance test frame (MTF) are necessary regardless if the number of voice radius in the cell site. The maximum size of all cell site is 144 voice radius, which would require a total of 14 frames; nine radio frames, three line supervision frames, one data frame, and one maintenance test frame.

Cell-Site Hardware

The hardware facilities of the AMPS cell-site connect the mobile radio customer to the land phone network and perform actions necessary for RF radiation, caption, and distribution, voice and data communications and processing, equipment easting, control, and reconfiguration, and call set-up, supervision, and termination. Cell-site operational control is achieved partially through wired logic and partially through programmable controllers. This part describes the cell-site functional groups, their physical characteristics and designed, and the ways they inter/ace with the rest of the AMPS system.

3.17 Data Frame

The date frame contains the equipment for major cell-site control functions, which include communication with the MTSO, control of voice and data communication with mobiles, and communication with the controller in the maintenance test frame communication between controllers is necessary for requesting performance of specific tests and for receiving results. The DF contains both hardware logic and programmable controllers. Only one set of hardware logic and one controller is needed per cell site regardless of the number if voice radius. Because of the critical functions performed in the DF, redundancy if all subassemblies is provided to assure continuation of service in the presence of a failure. The OF can reconfigure itself under the direction of the MTSO, which maintains service by permitting any malfunctioning subassembly to be replaced with an off-line redundant unit. The data frame contains five major subsystems.

3.18 Central Control and Monitoring Site

Illustrates the system design of the CCM, which is based on an pH 2100 microprocessor data-acquisition system. Through software, it emulates radio plan control functions performed by an less, supervises data gathering and recording and automatically calibrated and monitors the performance of all the Cellular Test Bed's land-based radio components. The CCM interrogates and instructs the mobile unit via telemetry link and the cell sties via specially, conditioned landlines. Operator intervention, if needed is also available. The cell site control message formats, as in the AMPS design, include seven parity bits to ensure high reliability of data

transmission. The CCM software requests data retransmission whenever errors occur. The CCM also contains the calibrated audio facilities necessary to conduct voice quality tests.

3.19 The Telemetry Site

The telemetry site ™ incorporates the radio transceiver facilities, which permit the CCM to reliably instruct and interrogate the MCL. Anywhere within the CTB test probe area. To meet the TM site is centrally located within the probe area and used a high-gain transmits and diversity-receive antenna system elevated 230 feet above the local street surface. The TM site also incnipcirates voice communication facilities to administer test operations.

3.20 Mobile Communications Laboratory

The interior of the MCL. Contains radio, logic. Mini processor and data-recording facilities. The RF/analog subsystem which consists of five measurement channels driven by two electronically selectable RF preamplifiers fed from two receive antennas appropriately paced for diversity reception, is illustrated. The same antennas and preamplifiers also feed the AMPS mobile radio used to evaluate the performance of the voice and signaling subsystems.

The main measurement receiver used a computer-controller agile local oscillator, which mixes the RF signals down to three intermediate frequencies. Each of these frequencies feeds into two highly selective channels that use logarithmic detector. Two channels (one high-gain, one low-gain) service each IF signal to achieve an instantaneous dynamic range that is linear from – 150 to – 30 dBm. The two channels are adjusted to maintain a 20-dB overlap centered at -90 dBm. The measurements for calculating real-time average values are selected using either the high-gain measurement or by, accepting the low-gain result it exceeds a threshold approximately in the middle of the Overlap region.

Environmental noise is monitored on one antenna by a single logia-rhythmic detector with a linear range from – 150 to – 10 dBm. The output of the diversity switch in the mobile radio is measured by an eighth logarithmic detector having a linear range from – 120 to – 40 dBm, with the useful range extending nearly 10 dB more at each end.

Instantaneous data sampled from these receivers are processed to obtain a true incident power by a stored program reference tabulation, this processing translated the output from a 10- bit analog-to-digital converter to a number proportional to the corresponding instantaneous input signal power. The instantaneous signal power samples are summed over one-half second of real-time to calculate average values.

The MCL is also equipped with a gyroscopic-bearing and distance-tracking system so that all system status and measurement information recorded each one-half second are tagged with true vehicle position.

3.21 CTB Calibration and Performance Monitoring

The calibration and performance-monitoring equipment in the CTB's hardware and software designs and the subsequent off-line statistical processing of the measurement data can precisely control and qualify the field experiments to obtain results comparable in resolution and reliability to those achieved in the laboratory. Examples of the call- ration and performance monitoring subsystems incorporated within the central and interferer cell sited the MCL used a similar calibration and monitoring system.

The cell sites transmit calibration and monitoring subsystem monitors, via precision coupler and temperature-compensated detection circuits the RF power incident to and reflected from each antenna/cable assembly. The detected voltages, sampled and processed by the PROCON, are sent to the CCM, where they are monitored and recorded (on-line) to insure the integrity of the cell site transmit function.

The type of calibration and monitoring subsystem used in the cell sitter receivers is illustrated. In practice, the test generator is set, under CCM control, to a reference power level. The CCM then (via land lines and the PROCON) automatically steps a programmable, precision attenuator to supply the input reference signals necessary to calibrate the cell site instrument level, 1000 samples are taken and averaged to generate stored program reference tabulation which, during real-time data acquisition, re used to determine the true instantaneous signal strength incident at the terminals of the receive antenna. The test generator also furnishes a reference signal to each antenna and cable subsystem. The instrumentation receiver monitors the forward and reflected power to ensure that antenna system returns requirements are met. As shown, the test generator subsystem also furnishes the reference signal necessary to

establish the FM quieting performance of the AMPS radius. Calibration of the CTB's transmit-and- receive subsystems is maintained within + 1/2 dB during each field evaluation sequence. The calibrations are performed at least before and after each test sequence and are hardcopies as part of the data package.

3.22 Control/Recording Architecture

This section describes the system control and data- recording structures of the CTB that perform the AMPS emulation and data-acquisition functions. As noted previously and extensive data of transmission parameters is established at the CCM every data frame. The algorithmic software module accesses the appropriate cell site transmission data are communicated to cell site and implemented by the operating system. The following paragraphs discuss the communication, control, measurement, and data-recording aspects CTB operation.

3.23 CTB Data Communication

As described earlier, the CTB, which is linked with cell, sites by data lines and to the MCL by a full-duplex telemetry channel. These interconnections, together with powerful processing capability at each remote site, form a comprehensive data communications structure.

Basically, three types of message are used for are used for data communications within this field configuration: First, control messages, such as signaling requests to cell sites, this field configuration: First, control messages, such as signaling requests to cell sites, permit the execution of system-level operations. Second special data acquisition requests and data messages to and from cell site and the MCL permit the acquisition of data at the CCM.

Third, CTB operational-control messages permit the automatic calibration of cell sites, synchronize the data-acquisition frame at each cell site status information on the proper performance of the system. The last category of messages allows direct CCM instructions to the mobile logic unit via telemetry link and also permits the MCL and CCM operators to request test pauses.

The land-line messages are transmitted at a rate of 2400 b/s, while the MCL data transfer rate is 1800 b/s. All messages are formatted into 32-bit blocks with seven bits devoted to error control. The data are encoded in a shortened (127.120) Bose-

Chaudhuri-Hocquenghem (BCH) code, which is used in an error-detection mode with retransmission.

a) System Control

The CTB configuration must be properly initialized to start data acquisition. First, the interfered transmitters and the main cell site instrumentation receivers must be tuned to the serving channel. Then the test can start by synchronizing the data-acquisition frames at each cell site and the MCL with the CCM system clock. From that point on microscopic data measurement at the MCL and cell sites depend on their local clocks. The CCM data-collection subsystem initiates each frame with "request-for-data" messages to the cell sites and the MCL. The data received are checked and formatted by a CCM software module and placed in a buffer to the system-control algorithmic module. This module is coded so that is can access data variable to the AMPS control algorithms only at the proper time interval. The output of the module by requires a system reconfiguration, which is accomplished by the CCM with appropriate data-link messages. All system decision, requests for action, and actions, are recorded with the underlying data for later analysis.

3.24 Measurement of RF Transmission Parameters

Radio transmissions parameters are measured at each of the cell sites and at the MCL. Each cell site instrumentation receiver switches sequentially to each of eight RF channels for sampling the mobile carrier level as received on each of two omni directional and three pairs of directional antennas. The data-sampling rate is 512 Hz enabling the acquisition system to make 64 measurements per channels each data frame. The samples are processed through a calibration stored-program reference tabulation to generate quantities proportional to the RS signal as receiver at the antenna terminals.

The cell site programmable controller than forms eight averages from these samples every data frame. If we assume an underlying Rayleigh distribution, these averages estimate the local means within a 95% confidence interval of approximately 1 dB. They are eight averages together with the final eight instantaneous samples from the RF parameter list, which is transmitted to the CCM,. Every data frame and recorded on digital tape in the formatted.

b) MCL activities

The MCL is a highly sophisticated data acquisition facility. Its five basic measurement channels are alternately switched to two diversity- receiving antennas. Further, measurements are made on both the high-and-low-gain if channels with the MCL computer selecting the proper value in real-time. Measurements are made on setup, voice, interferer and noise channels. In addition, the AMPS diversity signal and peak-noise distributions are measures.

3.25 ROAMING IN GSM SYSTEMS

3.25.1 What is Roaming?

Roaming is defined as the ability for a cellular customer to automatically make & receive voice calls, send & receive data, or access other services when traveling outside the geographical coverage area of the home network, by means of using a visited network. It is a general term in wireless telecommunications that refers to the extending of connectivity service in a location that is different from the home location where the service was registered. Roaming occurs when a subscriber of one wireless service provider uses the facilities of another wireless service provider. This second provider has no direct pre-existing financial or service agreement with this subscriber to send or receive information. A device will usually indicate when it is roaming.

The quintessential example of "roaming" is the case of cellular phones when a phone is in a location where its wireless service provider does not provide coverage (for example, another country). In some cases, roaming occurs in a phone's designated home area when it transmits via a different provider's tower (sometimes at a higher price). This is likely to occur when the service provider's signal is too weak or if the volume of callers is too high. In order for a mobile device to use a different carrier's service, the phone's service provider must have a roaming agreement with that carrier.

Roaming is technically supported by mobility management, authentication and billing procedures. Establishing roaming between network operators is based on - and the

commercial terms are contained in - Roaming Agreements. If the visited network is in the same country as the home network, this is known as National Roaming. If the visited network is outside the home country, this is known as International Roaming (the term Global Roaming has also been used). If the visited network operates on a different technical standard than the home network, this is known as Inter-standard roaming.

GSM Roaming, which involves roaming between GSM networks, offers the convenience of a single number, a single bill and a single phone with worldwide access to over 210 countries. The convenience of GSM Roaming has been a key driver behind the global success of the GSM Platform. GSM coverage map is a unique resource containing information supplied and approved by the members of the GSM Association. Network, Services and Roaming information are continually updated to reflect the evolving situation worldwide. Interactive coverage maps, updated quarterly, allow you to navigate to see where exactly you can use your phone.

3.25.2 How does Roaming work?

The user needs to check with the operator that his mobile subscription allows him to use his phone abroad and which services are available in his destination country. A simple phone call is all that is normally required. The user should also check that his operator has a 'roaming agreement' with an operator in the country that he is visiting. The operator will be able to provide a list of all of the countries that the user can roam to. Finally, he should check that his mobile phone supports the radio frequency employed in that region of the world. GSM services are provided in a number of bands (e.g. 850, 900, 1800 and 1900 MHz). Most modern phones are multi-band, but travelers from Europe to North America, for example, should check that their phones will operate in the 850 and/or 1900 MHz bands.

When the user travels to a different country with his mobile phone, his home operator may not have coverage in the place that the user has traveled to. However, he is still able to make and receive calls because his mobile phone can 'roam' onto another operator's network, in the visited country. This is possible because the user's home operator has a 'roaming agreement' with an operator in the visited country that

enables him to use its network. So when he switch on his phone in the foreign country, his mobile phone picks up the radio signals of one of the operators in that country. This local operator will then 'authenticate' his mobile phone with the home operator. If the home operator responds with a positive authentication, the mobile phone is ready for use. Operators have done a lot of work behind the scenes to make this process completely automatic and it typically takes only a few minutes to log on to the local network.

When the user is making a call and roaming, the operator in the visited country analyses the dialed number, and decides how best to route the call. If the user is calling back home then the visited operator will connect the call back to the home country. Note that he should type in the international access code and the correct country code omitting the zeroes.

For example, to dial the UK mobile number 07903 XXX XXX from another country, you dial +44 7903 XXX XXX. If you are calling a landline, you may need to include an area code. If you are calling a local number in the visited country, the visited operator will usually connect the call directly to the party within the country you are in. When someone calls you on your mobile, the call will usually be routed to your home country and your home operator. Your home operator knows where you are roaming, and will then forward the call to the operator whose network you are using in the visited country. The visited network will then connect the call to you. This initial routing back to your home operator happens regardless of where the call originates, as only your home operator has the information about your location. Note that when roaming you have to pay both for calls that you make and receive.

Also when using the phone while roaming (both making and receiving calls), the visited operator will keep a record of the calls. It will send these records, along with the corresponding charges, to the home operator. The home operator then, will aggregate these call charges, and reflect them in the next bill. All charges will appear in the home currency – the home operator should convert the foreign operator charges automatically. It can take some time for the call charges to be sent to the home operator by the visited operator.

3.26 Types of Roaming

3.26.1 Regional roaming:

This type of roaming refers to the ability of moving from one region to another region inside national coverage of the mobile operator. Initially, operators often made commercial offers restricted to a region (sometimes to a town). Due to the success of GSM and the decrease in cost, regional roaming is rarely offered to clients except in nations with wide geographic areas like the USA, Russia, India, etc., in which there are a number of regional operators.

3.26.2 National roaming:

This type of roaming refers to the ability to move from one mobile operator to another in the same country. For example, a subscriber of T-Mobile USA who is allowed to roam on Consular Wireless's service would have national roaming rights. For commercial and license reasons, this type of roaming is not allowed unless under very specific circumstances and under regulatory scrutiny. This has often taken place when a new company is assigned a mobile telephony license, to create a more competitive market by allowing the new entrant to offer coverage comparable to that of established operators (by requiring the existing operators to allow roaming while the new entrant has time to build up its own network).

3.26.3 International roaming:

This type of roaming refers to the ability to move to a foreign service provider's network. It is, consequently, of particular interest to international tourists and business travelers. Broadly speaking, international roaming is easiest using the GSM standard, as it is used by over 80% of the world's mobile operators. However, even then, there may be problems, since countries have allocated different frequency bands for GSM communications (there are two groups of countries: most GSM countries use 900/1800 MHz, but the United States and some other countries in the Americas have allocated 850/1900 MHz): for a phone to work in a country with a different frequency allocation, it must support one or both of that country's frequencies, and thus be tri- or quad-band.

3.27 Roaming Process

3.27.1 Basic Steps of Roaming

The details of the roaming process differ among types of cellular networks, but in general, the process resembles the following:

1. When the mobile device is turned on or is transferred via a handover to the network, this new "visited" network sees the device, notices that it is not registered with its own system, and attempts to identify its home network. If there is no roaming agreement between the two networks, maintenance of service is impossible, and service is denied by the visited network.

2. The visited network contacts the home network and requests service information (including whether or not the mobile should be allowed to roam) about the roaming device using the its IMSI number.

3. If successful, the visited network begins to maintain a temporary subscriber record for the device. Likewise, the home network updates its information to indicate that the mobile is on the host network so that any information sent to that device can be correctly routed.

3.27.2 Explanation on the Roaming Process

If a call is made to a roaming mobile, the public telephone network routes the call to the phones registered service provider, who then must route it to the visited network. That network must then provide an internal temporary phone number to the mobile. Once this number is defined, the home network forwards the incoming call to the temporary phone number, which terminates at the host network and is forwarded to the mobile. In order that a subscriber is able to "latch" on to a visited network, a roaming agreement needs to be in place between the visited network and the home network. This agreement is established after a series of testing processes called IREG and TADIG. While the IREG testing is to test the proper functioning of the established communication links, the TADIG testing is to check the billability of the calls.

The usage by a subscriber in a visited network is captured in a file called the TAP (Transferred Account Procedure) for GSM / CIBER (Cellular Intercarrier Billing Exchange Roamer) for CDMA, AMPS etc... file and is transferred to the home network. A TAP/CIBER file contains details of the calls made by the subscriber viz. location, calling party, called party, time of call and duration, etc. The TAP/CIBER files are rated as per the tariffs charged by the visited operator. The home operator then bills these calls to its subscribers and may charge a mark-up/tax applicable locally.

3.27.3 Tariffs

Roaming fees are traditionally charged on a per-minute basis and they are typically determined by the service provider's pricing plan. Several carriers in the United States have eliminated these fees in their nationwide pricing plans. All of the major carriers now offer pricing plans that allow consumers to purchase nationwide roaming-free minutes. However, carriers define "nationwide" in different ways. For example, some carriers define "nationwide" as anywhere in the U.S., whereas others define it as anywhere within the carrier's network.

An operator intending to provide roaming services to visitors publishes the tariffs that would be charged in his network at least sixty days prior to its implementation under normal situations. The visited operator tariffs may include tax, discounts etc and would be based on duration in case of voice calls. For data calls, the charging may be based on the data volume sent and received. Some operators also charge a separate fee for call setup i.e. for the establishment of a call. This charge is called a Flag fall charge.

3.28 Summary

This chapter represents Mobile phones, Base Unit, Mobile Unit, Detailed Operation, Outgoing Call, Mobile Station, Mobile Internal Call (MIC), Mobile and Portable Phone Units, Wire line-To-Mobile Calls, Mobile – To – Wire line Calls, Mobile – To – Mobile Calls, Advanced Mobile Phone Service, Cell-Site Hardware, Data Frame, Central Control and Monitoring Site, The Telemetry Site, Mobile Communications Laboratory, CTB Calibration and Performance Monitoring, Control/Recording Architecture, CTB Data Communication and Measurement of RF Transmission Parameters.

4. THE MOBILE STATION AND THE SUBSCRIBER IDENTITY MODULE

4.1 Overview

The GSM telephone set and the SIM are the only system elements with which most users of GSM have direct contact. The GSM telephone set and the SIM form an almost complete GSM system within themselves with all the functionality, from ciphering to the HLR. Figure 4.1 shows a block diagram of a mobile station with a SIM slot.

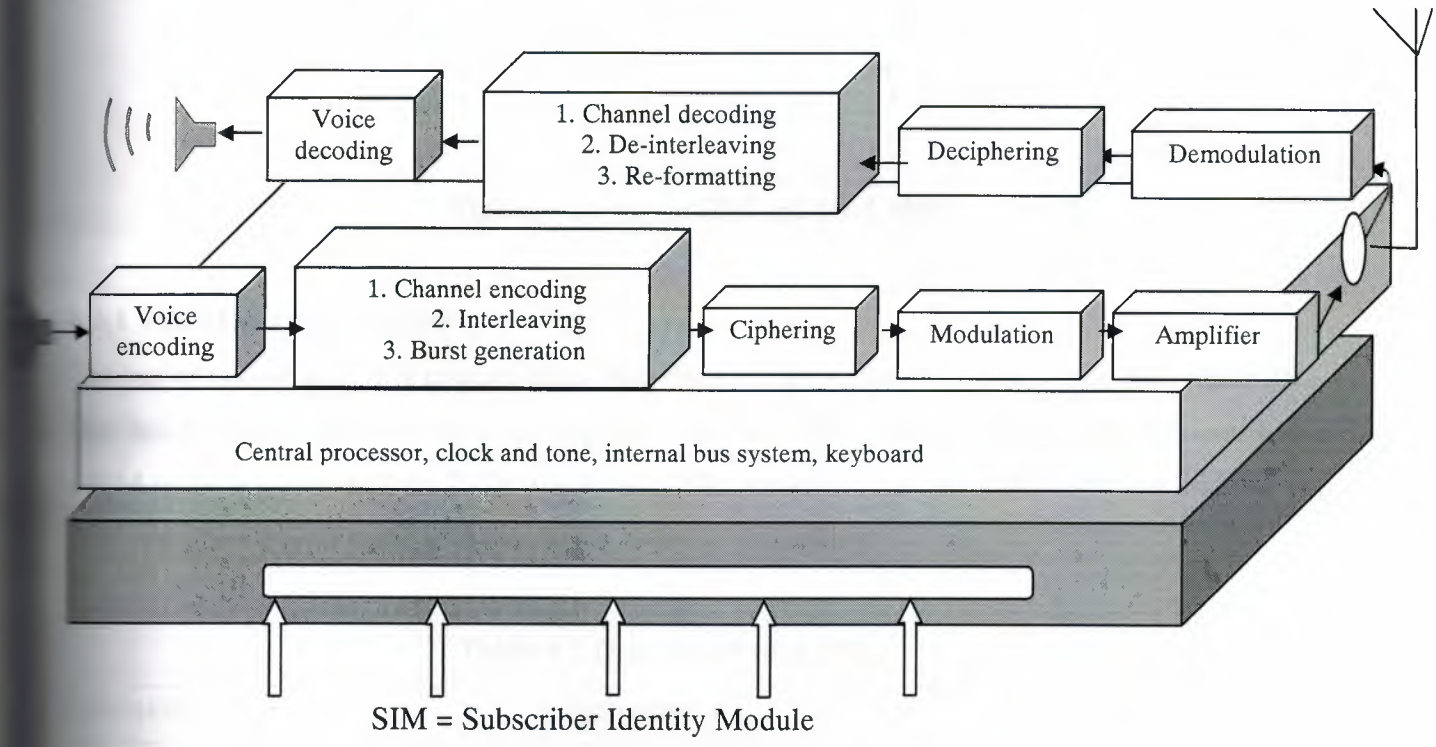

Figure 4.1 Block Diagram of a GSM MS.

4.2 Subscriber Identity Module

The SIM is a microchip that is planted on either a check card (ID-1 SIM) or a plastic piece about 1 cm square (plug-in SIM). Figure 4.2 shows both variants. Except for emergency calls, a GSM mobile phone cannot be used without the SIM. The GSM terminology distinguishes between a mobile station and mobile equipment. The mobile equipment becomes a mobile station when the SIM is inserted. There is no difference in functionality between the ID-1 SIM and the plug-in

SIM, except for size, which is an advantage for the plug-in SIM when used in a small handheld telephone. Today, many network operators offer (at an additional cost) identical pairs of ID-1 SIM/plug-in SIM, so the same SIM can be used in a car phone and in a handheld telephone.

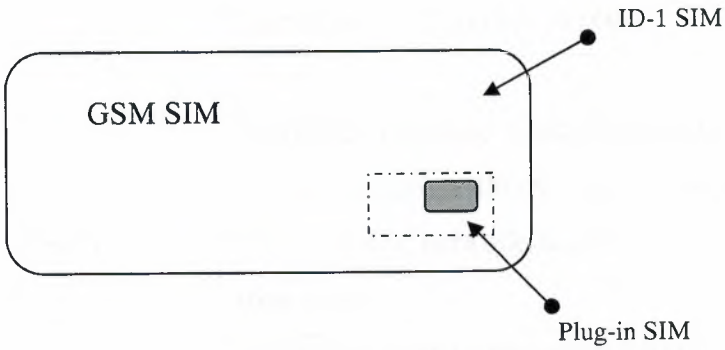

Figure 4.2 Plug-in SIM and ID-1 SIM

4.2.1 The SIM as a Database

The major task of a SIM is to store data. That does not mean that the data is only subscriber data. One has to differentiate between data types for various tasks. The most important parameters that a SIM holds are presented in Table 4.1. It should be noted that the list is not complete and that the SIM can also be used to store, for example, telephone numbers.

Table 4.1 Data Stored on a SIM

Parameter	**Remarks**
Administrative data	
PIN/PIN2 (m/v)	Personal identification number; requested at every power up (PIN or PIN2)
PUK/PUK2 (m/f)	PIN unblocking key; required to unlock a SIM
SIM service table(m/f)	List of the optional functionality of the SIM
Last dialed number (o/v)	Radial
Charging meter (o/v)	Charges and time increments can be set
Languages(m/v)	Determines the language for prompts by the mobile station
Security related data	

Algorithm A3 *and* AS (m/f)	Required for authentication and to determine Kc.
Key Ki (m/fl)	Individual value: known only on SIM and the HLR.
Key Kc (m/v)	Result of A8, Ki, and random number (RAND).
CKSN (m/v)	Ciphering key sequence number.
Subscriber data	
IMSI (m/f)	International mobile subscriber identity.
MSISDN (m/f)	Mobile subscriber ISDN; directory number of a subscriber.
Access control class(es)(m/f)	For control of network access.
Roaming data	**Remarks**
TMSI (m/v)	Temporary mobile subscriber identity
Value of T3212 (m/v)	For location updating
Location updating status	Is a location update required?
LAI (m/v)	Location area information
Network color codes(NCCs) of restricted PLMNs(m/v)	Maximum of 4 PLMNs can be entered on a SIM after unsuccessful Locations update; cause "PLMN not allowed." Oldest entry deleted when more than 4 restricted PLMNs are found.
NCCs of preferred PLMNs (o/v)	What PLMN should the MS select, it there is more than one to choose from and the home PLMN is not available?
PLMN data	**Remarks**
NCC, mobile country code (MCC), and mobile network code (MNC) of the home PLMN (m/f).	Network identifier
Absolute radio frequency channel numbers (ARFCNs) of home PLMN (m/f).	Frequencies for which the home PLMN is licensed

Legend : m =mandatory ;f = fixed, unchangeable value; v = changeable

4.2.2 Advantage for the Subscriber

The SIM is one of the most interesting features for a user of GSM, because it permits separation of GSM telephone equipment and the related database. In other words, the subscriber to a GSM system is not determined by the identity of the mobile equipment but by the SIM, which always has to be inserted into the equipment before it can be used. This is the basis for personal mobility. Because of the SIM, a GSM customer can use different telephones (e.g., a car phone and a handheld phone) and still be reachable under the same directory number. Even in case of a defect in the user's GSM telephone, any other GSM telephone can be used instead, simply by changing the SIM.

4.3 Mobile Station

A GSM terminal is, even for experts, a technical marvel. (Consider the rate at which prices have fallen, the complexity of the devices, and the large number of different types of equipment available. All the functionality known from the BTS transmitter/receiver (TRX), like Gaussian minimum shift keying (GMSK) modulation/demodulation up to channel coding/decoding, also needs to he implemented in an MS.

Other MS-specific functionalities need to be mentioned, like dual-tone multifrequency (DTMF) generation and the most important issue, the economical use of battery power.

From the perspective of the protocol, the MS is not only a peer of the BTS hut communicates directly with the MSC and the VLR, via the mobility management (MM) and call control (CC). Furthermore, the MS has to be able to provide a transparent interface (terminal adaptation function, or TAF) for data and fax connections to external devices.

4.3.1 Types of Mobile Stations

The most common way to distinguish among GSM mobile equipment is by the power class ratings, in which the value specifies the maximum transmission power of an MS. When GSM was introduced, five power classes were defined for GSM 900, of which the most powerful class allowed for a 20W output. That class is no longer supported; currently, the most powerful rating is 8W. The power emission of DCZS 1800 and PCS 1900 mobiles is generally lower.

4.3.2 Functionality

GSM Recommendation 02.07 describes in detail what functionality mobile equipment has to support and what features are optional. The most important and mandatory features are:

- DTMF capability;
- Short-message service (SMS) capability;
- Availability of the ciphering algorithms A5/1 and A5/2;
- Display capability for short messages; dialed numbers, and available PLMN;
- Support of emergency calls, even without the SIM inserted;
- "Burned-in" IMEI.

4.3.3 Mobile Stations as Test Equipment

An MS is a useful test tool for the laboratory testing of a new network function.

Several manufacturers offer, for that purpose, a semi stationary MS, which Allows manipulation of specific system parameters, to test the behavior of new software or hardware.

Besides those complex and expensive pieces of equipment used mainly in laboratories, a number of standard mobile telephones exist, which can easily be modified with additional packages to act as mobile test equipment. Such equipment is connected to a personal computer and uses standard functionality to monitor signaling between the network and the MS. Usually, it is also able to represent the test results in tabular or graphical form.

Despite those advantages, the test mobile stations seldom are used for protocol and error analysis, because the results are not representative from a statistical point of view and can be gathered only with substantial effort and time.

Nonetheless, special test mobiles are necessary tools for network operators monitor coverage and evaluate the behavior of handover as a customer would experience it.

4.4 The Base Station Subsystem

Via the Air-interface, the BSS provides a connection between the MSs of a limited area and the network switching subsystem (NSS). The BSS consists of the following elements:

- One or more BTSs (base tranceiver station);
- One BSC (base station controller);
- One TRAU (transcoding rare and adaptation unit).

The tasks and the structure of those elements or modules are described in this chapter.

4.4.1 Base Transceiver Station

The BTS provides the physical connection of an MS to the network in form of the Air-interface. On the other side, toward the NSS, the BTS is connected to the BSC via the Abis-interface.

The manufacturers of BTS equipment have been able to reduce its size substantially. The typical size in 1991 was that of an armoire; today the size is comparable to that of a mailbox. The basic structure of the BTS, however, has not changed. The block diagram and the signal flow of a BTS with one TRX are shown in Figure 4.3. The GSM Recommendations allow for one BTS to host up to 16 TRXs. In the field, the majority of the BTSs host between one and four TRXs.

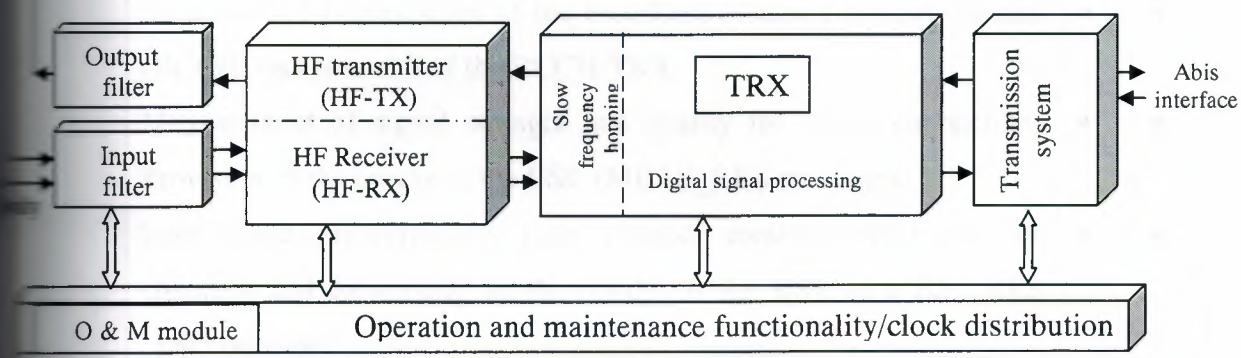

Figure 4.3 Block Diagram of a BTS With One TRX

4.4.2 Architecture and Functionality of a Base Transceiver Station

4.4.2.1 Transmitter/Receiver Module

The TRX module is, from the perspective of-signal processing, the most important part of a BTS. The TRX consists of a low—frequency part for digital signal processing and a high—frequency part for GMSK modulation and demodulation. Both parts are connected via a separate or an integrated frequency hopping unit. All other parts of the BTS are more or less associated with the TRXs and perform auxiliary or administrative tasks.

A TRX with integrated frequency hopping serves the tasks listed Table 2.2.

Table 4.2 Tasks of a TRX with Integrated Frequency Hopping

Function	**LF**	**HF**
Channel coding and decoding.	●	
Interleaving and ordering again.	●	
Encryption and decryption (ciphering).	●	
Slow frequency hopping.	●	
Burst formatting.	●	
TRAU frame formatting and conversion in direction to/from the BSC,setup of the LAPD connection to the BSC.	●	
GMSK modulation of all downlink data.	●	●
GSMK demodulation of all received MS signals.	●	●
Creation and transmission of the broadcast common control channel (BCCH) on channel 0 of the BCCH-TRX.	●	●
Measurement of signal strength and quality for active connections Provision of the results to the BSC (MEAS_RES message).	●	●
Interference measurements (idle channel measurements) on free channels and forwarding of the results to the BSC in a RF _RES _IND message.	●	●

LF=low frequency part of the TRX; HF = high frequency part of the TRX.

4.4.2.2 Operations and Maintenance Module

The operations and maintenance (O&M) module consists of at last one central unit, which administers all other parts of the BTS. For those purposes, connected directly to the BSC by means of a specifically assigned O&M channel. That allows the O&M module to process the commands from the BSC or the MSC directly into the BTS and to report the results. Typically, the central unit also contains the system and operations software of the TRXs. That allows it to be reloaded when necessary, without the need to consult the BSC Furthermore, the O&M module provides a human-machine interface (HMI), which allows for local control of the BTS.

4.4.2.3 Clock Module

The modules for clock generation and distribution also are part of the O&M area Although the trend is to derive the reference clock from the PCM signal Abis-interface, a BTS internal clock generation is mandatory. It is especially needed when a BTS has to be tested in a standalone environment, that is, without connection to a BSC or when the PCM clock is not available due to link failure.

Still, there is a cost savings benefit in the approach of deriving the clock from the PCM signal. By doing so, much cheaper internal clock generators can be applied, because they do not require the same long-term stability as an independent clock generator. Besides, there is no need for frequent maintenance check on the clock modules, since they synchronize themselves with the clock coming from the PCM link.

When analyzing errors in call handling, particularly in the area of handover, even minor deviations from the clock have to be considered as possible causes for errors. GSM requires that all the TRXs of a BTS use the same clock signal. The accuracy of the signal has to have a precision of at least 0.05 parts per million (ppm). For example, a clock generator that derives the clock from a 10 MHz signals has to be able to provide a clock with a frequency accuracy of 10MHz ±0.5 Hz (10.10^6 Hz 0.05.10^-6=0.5 Hz).

4.4.2.4 Input and Output Filters

Both input and output filters are used to limit the bandwidth of the received and the transmitted signals. The input filter typically is a nonadjustable wideband filter that lets pass all GSM 900, all DCS 1800, or all PCS 1900 frequencies in the uplink direction. In contrast, remote-controllable filters or wideband filters are used for the downlink direction that limits the bandwidth of the output signal to 200 kHz. When necessary, the 0&M center (OMC) controls the settings of the filters, as in the case of a change in frequency.

4.4.3 Base Transceiver Station Configurations

Different BTS configurations, depending on load, subscriber behavior, and morph structure, have to be considered to provide optimum radio coverage of an area. The most important BTS configurations of a BTS are presented next.

4.4.3.1 Standard Configuration

All BTSs are assigned different cell identities (CIs). A number of BTSs (in some cases, a single BTS) form a location area. Figure 4.4 shows three location areas with one, three, and five BTSs. The systems are usually not fine-synchronized, which prevents synchronized handover between them. That method of implementing BTSs is the one most frequently used. For urban areas with growing traffic density, that may change soon.

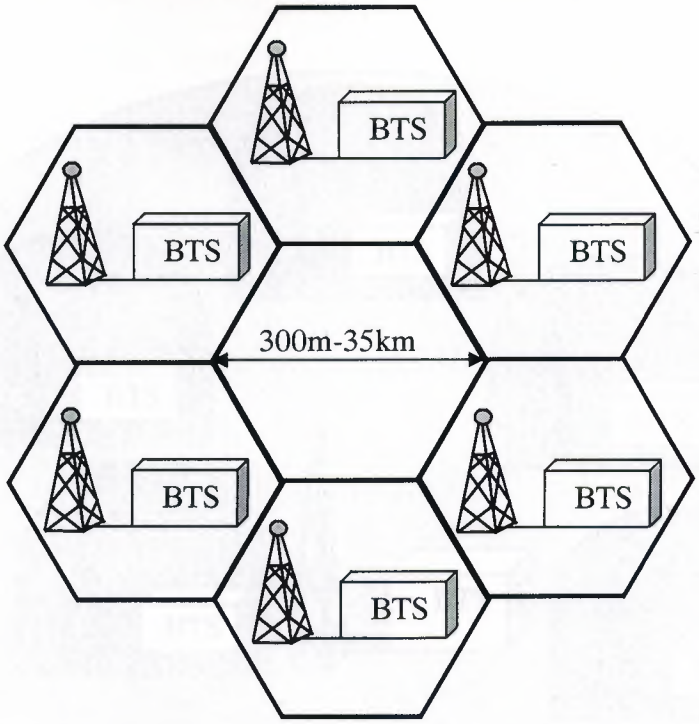

Figure 4.4 BTSs In Standard Configuration

4.4.3.2 Umbrella Cell Configuration

The umbrella cell configuration consists of one BTS with high transmission power and an antenna installed high above the ground that serves as an "umbrella" for a number of BTSs with low transmission power and small diameters (Figure 4.5).

Such a configuration appears to make no sense at first, because the frequency of the umbrella cell can not be reused in all the cells of that area due to interference. Interference even over a large distance was one of the reasons why the high radio and television towers were abandoned as sites for antennas shortly after they were brought into service at the initial network startup.

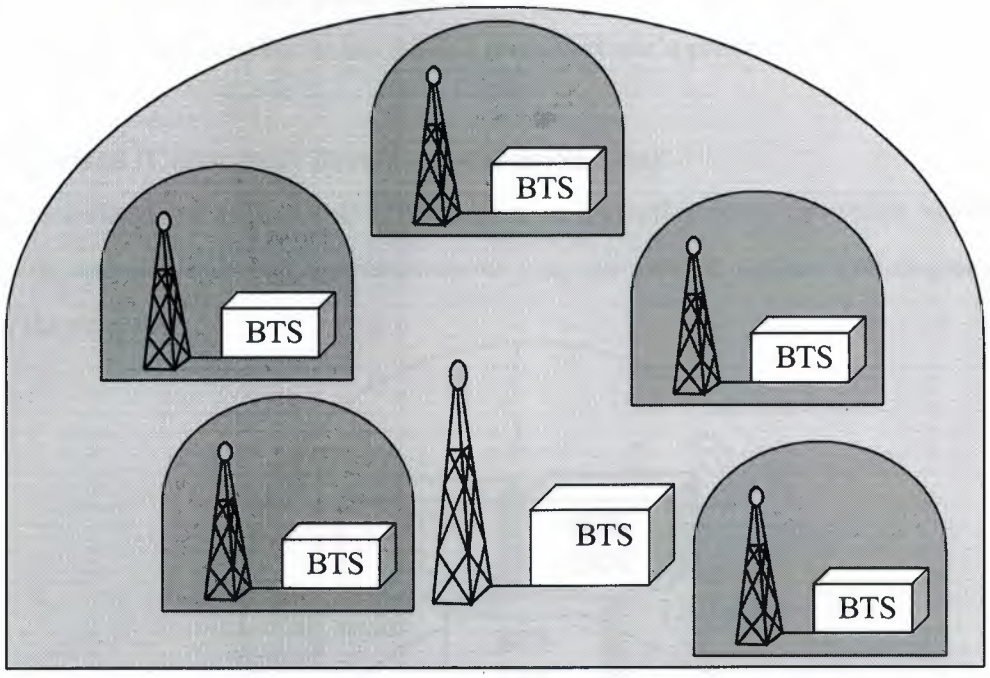

Figure 4.5 Umbrella Cell with Five Smaller Cells

The umbrella cell configuration still has its merits in certain situations and therefore may result in relief from load and an improvement of the network. For example, when cars are moving at rather high speeds through a network of small cells, almost consecutive handovers from one cell to the next are necessary to maintain an active call. This situation is applicable in every urban environment that features city highways. Consequently, the handovers result in a substantial increase of the signalling load for the network as well as in unbearable signal quality degradation for the end user. On the other hand, small cells are required to cope with the coverage demand in an urban environment. The way out of this dilemma is to use both large and small cells at the same time, that is, the umbrella cell configuration. The umbrella cell can be protected from overload when traffic from only fast-moving users is assigned to it. This, on the other hand, reduces the signalling load of the small cells and improves the signal quality for the fast-moving traffic. The speed of a user can be determined to sufficient accuracy by the change of the timing advance (TA) parameter. Its value is updated in the BSC every 480 milliseconds (ms) by means of the data provided in the MEAS_RES message. The BSC decides whether to use the umbrella

cell or one of the small cells. GSM has not specified the umbrella cell configuration, which requires additional functionality in the BSC, a manufacturer's proprietary function.

4.4.3.3 Sectorized (Collocated) Base Transceiver Stations

The term sectorized, or collocated, BTSs refers to a configuration in which several BTSs are collocated at one site but their antennas cover only an area of 120 or 180 degrees. Figure 4.6 illustrates the concept.

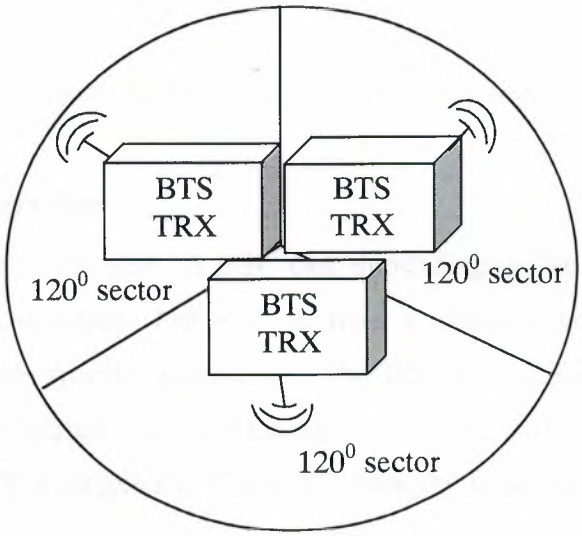

Figure 4.6 Coverage of an Area with Three Sectorized BTSs. Each BTS Covers a Segment of 120^0 degrees.

Typically, it is implemented with BTSs with few TRXs and low transmission power. Like the umbrella cell configuration, this configuration is used mostly in highly populated areas. A peculiarity is that it is fairly easy to fine-synchronize the cells with each other, which allows for synchronized handover between them. Even though in a collocated configuration, one channel per BTS has to be used for the generation of the BCCH, such a configuration has the following advantages:

- Sectorized, or collocated, BTSs are well suited for a serial connection of the Abis-interface. This configuration has the potential to save costs for access lines to the BSC. Otherwise, multiple sites require multiple (leased) lines.

- From the radio perspective, the advantage of using cells with a 120-degree angle is that it allows reuse of frequencies in one sector (one direction), which otherwise would cause interference with neighbor cells if an omni directional cell were used.

- Sectorization eases the demand for frequencies, particularly in an urban environment.

4.5 Base Station Controller

The BSC forms the center of the BSS. A BSC can, depending on the manufacturer, connect to many BTSs over the Abis-interface. The BSC is, from a technical perspective, a small digital exchange with some mobile-specific extensions. The BSC was defined with the intention of removing most of the radio-related load from the MSC. The BSC's architecture and its tasks are a consequence of that goal. For simplicity, Figure 4.7 uses the same hardware for both the Abis-interface and the A-interface, which is not a requirement.

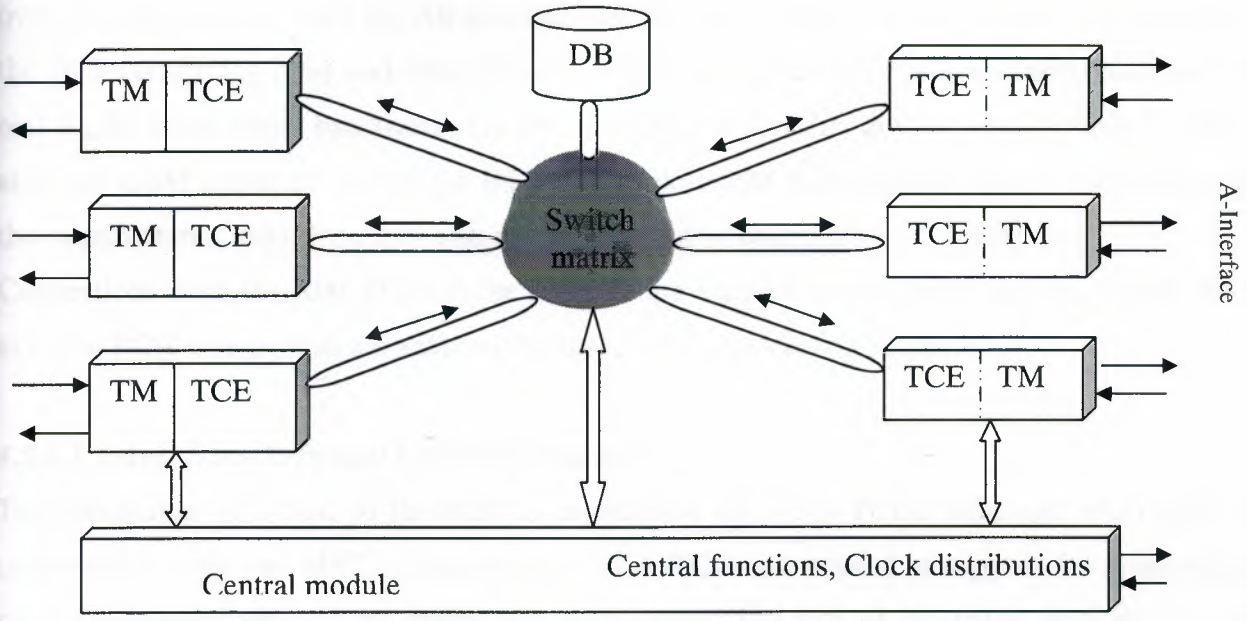

Figure 4.7 Block Diagram of a BSC

4.5.1 Architecture and Tasks of the Base Station Controller

4.5.1.1 Switch Matrix

Because the BSC has the functionality of a small digital exchange, its function is to switch the incoming traffic channel (A-interface from the MSC) to the correct Abis-interface channels. The BSC, therefore, comes with a switch matrix that (1) takes care of the relay functionality and (2) can he used as the internal control bus.

4.5.1.2 Terminal Control Elements of the Abis-interface

The connection to the BTSs is established via the Abis-terminal control elements (TCEs), which, more or less independently from the BSC's central unit, provide the control function for a TRX or a BTS. The number of Abis TCEs that a BSC may contain depends largely on the number of BTSs and on the system manufacturer.

Major tasks of the Abis-TCEs are to set up LAPD connections toward the BTS peers, the transfer of signaling data, and last—but not least—the transparent transfer of payload.

Depending on the manufacturer, the Abis TCEs also may be responsible for the administration of

BTS radio resources. That entails the assignment and release of signaling and traffic channels over the Abis-interface and the Air interface and for the evaluation of measurement results from the BTS concerning busy and idle channels, which are relevant for power control and used in making decisions about handovers. The final control functionality always remains with the BSC, although GSM explicitly allows the BTS to preprocess the measurement results. Depending on the manufacturer, those functions also can be assumed or controlled by a central unit.
Connections from the Abis TCEs to the A-TCEs are realized by the switch matrix. On the other side, the PCM connections are achieved by associated transmission elements.

4.5.1.3 A-Interface Terminal Control Elements

The connection of a BSC to the MSC is established via the A-TCEs. Although every BSC is connected to only one MSC, a large number of A-TCEs are needed to support the A-interface, since all the payload and the major part of the signalling data of the entire BSS have to be conveyed over this interface.
Among the tasks of some, but usually not all A-TCEs is setting up and operating the SS7/SCCP connection toward the MSC. The number of necessary signalling channels depends largely on the predicted traffic load.

4.5.1.4 Database

The BSC is the control center of the BSS. In that capacity, the BSC must maintain a relatively large database in which the maintenance status of the whole BSS, the quality of the radio resources and terrestrial resources, and so on are dynamically administrated. Furthermore, the BSC database contains the complete BTS operations software for all attached BTSs and all BSS specific information, such as assigned frequencies.

4.5.1.5 Central Module

One of the major tasks of the BSC is to decide when a handover should take place. The BSC may decide on intra-BTS handover and intra-BSC handover without needing the MSC. In contrast, for all BSC external handovers, the BSC needs to involve the MSC. Handover decision and power control are main tasks of the central module.

4.5.1.6 Connection to the OMC

Another functionality that many manufacturers have decided the central module should perform is the connection to the OMG. Every BSS is supervised and managed by an OMG via the BSC.

4.5.2 Trans coding Rate and Adaptation Unit

4.5.2.1 Function of the Transcoding Rate and Adaptation Unit

One of the most interesting functions in GSM involves the TRAU, which typically is located between the BSC and the MSC. The task of the TRAU is to compress or decompress speech between the MS and the TRAU. The used method is called regular pulse excitation—long term prediction (RPE-LTP). It is able to compress speech from 64 Kbps to 16 Kbps. in the case of a full rate channel (net bit rate with full rate is 13 Kbps) and to 8 Kbps in the case of a half rate channel (net bit rate with half rate is 6.5 Kbps).

Note that the TRAU is not used for data connections.

4.5.2.2 Site Selection for Transcoding Rate and Adaptation Unit

Although speech compression is intended mainly to save resources over the Air-interface, it also is suitable to save line costs when applied on terrestrial links, as illustrated schematically in Figure 4.8. When the TRAU is installed at the MSC site (see top portion of Figure 4.8), a full rate speech channel uses only 16 Kbps over the link from the BSC to the MSC.

The specifications allow for the installation of the TRAU between the BTS and the BSC. That requires, however, the use of 64-Kbps channels between the BSC and the MSC and hence the use of more links (see bottom portion of Figure 4.8).

This variant is, therefore, used only infrequently. In fact, most of the time, the TRAU is installed at the site of the MSC to get the most benefit from the compression.

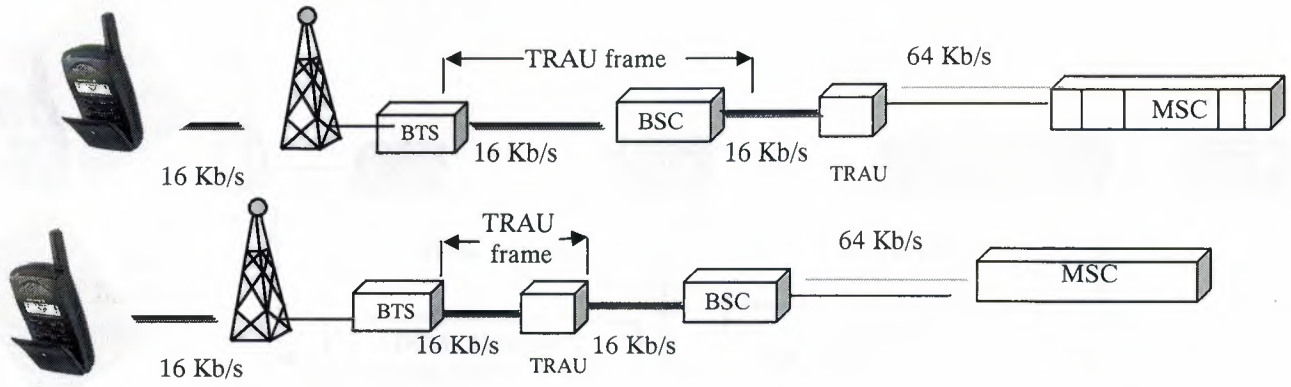

Figure 4.8 Possible Sites for the TRAU in the Signal Chain

4.5.2.3 Relationship between the Transcoding Rate and Adaptation Unit, and Base Station Subsystem

The TRAU is functionally assigned to the BSS, independently of where it actually is located. The reason for that is the following.

Both the BTS and the TRAU have an interface for payload that is transparent for the BSC. The payload is formatted in TRAU frames, and then transparently sent over PCM links between the TRAU and the BTS in cycles of 20 ms.

That applies to both directions. The data contained in the TRAU frames form the input and output values for channel coding.

For data connections, the compression functionality has to be switched off. The type of connection (data/speech) is communicated to the TRAU during the assignment of the traffic channel. As illustrated in Figure 4.9, the BTS starts to transmit TRAU frames in the uplink, immediately after receiving the CHAN_ACT message. Those TRAU frames carry in band signaling, which exchanged between the BTS-TRX (and more precisely the coding unit) and the TRAU, to consolidate the characteristics of a connection. Part of the control information is, in particular, synchronization data, discontinuous transmission (DTX) on/off, and the connection type (halfrate/fullrate).

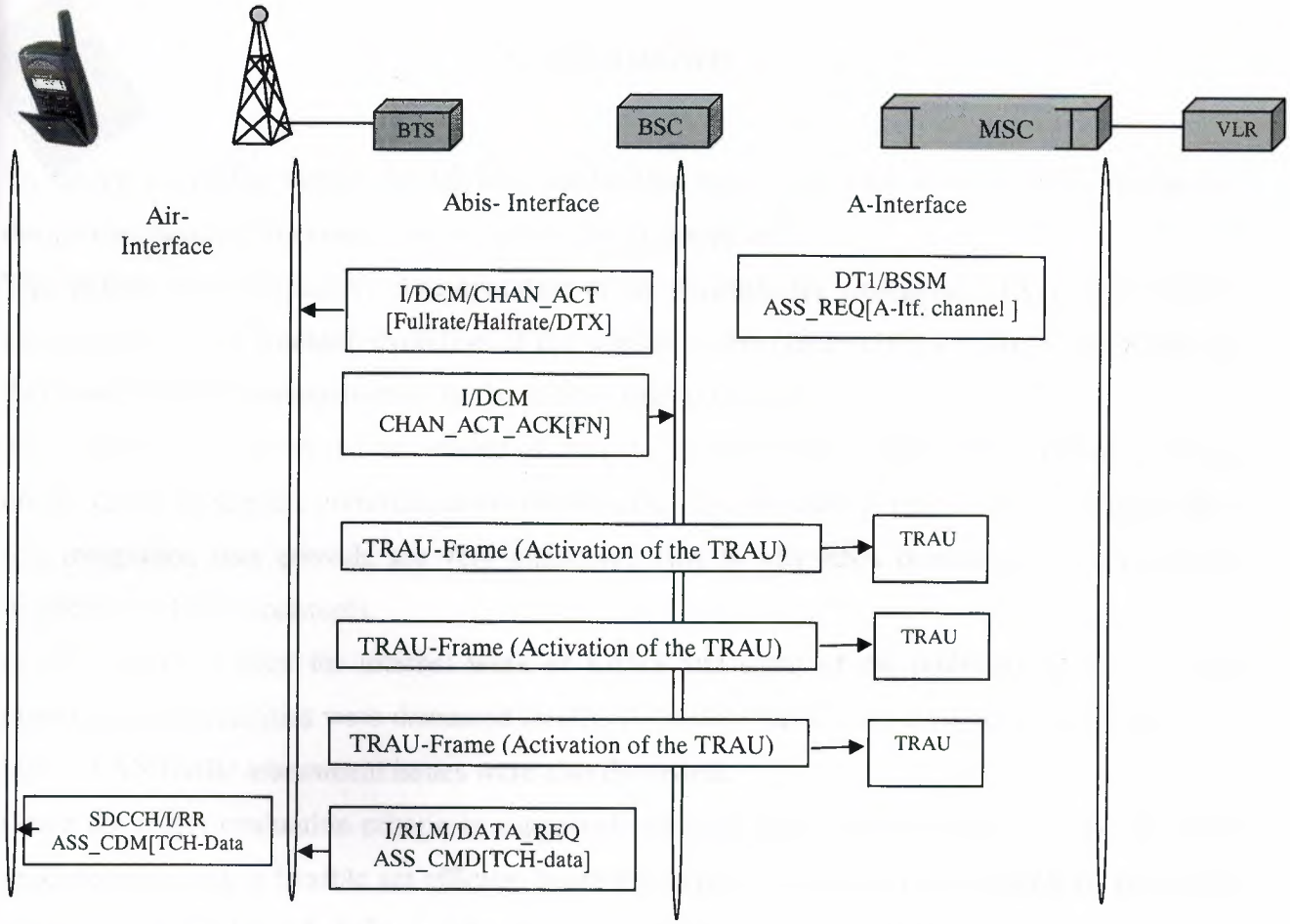

Figure 4.9 Activation of the TRAU during Assignment of a Traffic Channel

Note that TRAU frames are sent over traffic channels and not over the associated control channels and hence are transparent to protocol analysis. The TRAU frames are, nevertheless, very important for error analysis on data connections.

4.6 Summary

This chapter represents The Mobile Station and the Subscriber Identity Module, Subscriber Identity Module, Mobile Station, The Base Station Subsystem and Base Station Controller.

Conclusion

To design a satellite system for tracking application was in the past no more difficult than to design the transmission system whose role it was meant to fulfill

This is now changing rapidly. The evolution of the network, the emergence of very competitive alternative, and the foreseen evolution of the satellite system themselves call for a reappraisal of their role in the implementation of the back bone digital network.

This reappraisal requires the investigate of many system problems which did not use to show up on the tables of satellite communication engineering. The problem is there. But the benefits that this integration may provide are very attractive. This is why ESA is actively studying every implication of these concepts.

In this paper the need for internet work of LANS and some of the problems of the existing interconnection facilities were discussed briefly. A satellite based wide area network concept and inter – LAN traffic assessment issues were also discussed.

Given the major evaluation criteria as suggested earlier in the paper, the conclusion is that such procedures provide a flexible ant efficient space telecommunication network capable of satisfying user requirement. In particle it would provide: minimum transmission delay, user access direct or via ISDN, flexibility in bandwidth – to – service allocation, further extension

REFERENCE

[1] Mamedov F .S, Telecommunication, Lecture notes, Near East University Press, Lefkosa , 2000 .

[2] Vijay K. Garg , Joseph E. Wilkes ,Wireless and Personal Communication System , Feher/Prentice hall Digital and Wireless Communication Series, AT&T Bell labs. Holmdel, New Jersey, 1990.

[3] GSM Specification Series 1.02-1.06,"GSM Overview, Glossary, Abbreviation, Service Phases."

[4] GSM Specification series 3.01-3.88,"GSM PLMN Function, Architecture Numbering and Addressing, Procedure."

[5] Padgett, Jay E.,Gunther ,Christoph G.,Hattori , Takeshi, "overview of Wireless Personal Communication". IEEE Communication magazine, V33, n1, January, 1995:28, 14 pages.

[6] Lee, W .C. Y., Mobile Cellular Telecommunication System, and New York: McGraw-Hill, 1989.

[7] Hans Lobensommer and Hemut Mahner. GSM – a European mobile radio Standard for the world market. Telecom Report International, 15 (3-4), 1992.

[8] Mouly , M and Pouetet,M , "The GSM System for Mobile Communication " , Palaiseau, France , 1992 .

[9] Vijay K. Garg , Willowbrook , Illinois Joseph E.Willkes ," Principle and Applications of GSM " Red Bank , New Jersey , 1999 .

[10] David M.Balston . The Pan-European system : GSM . In David M.Boston and R.C.V Macario , editors , cellular Radio System . Artech House , Boston 1993 .

[11] Javier Gozalvez Sempere Research Engineer in Mobile Communications " An Overview of the GSm System " University of Strothclyde Glasgow, Scotland

[12] John Scourios (University of Waterloo) . " Overview of the Global System for Mobile Communication " http://ccnga.uwaterloo.ca/~jascouria/GSM/gsmreport.html"