NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

ANALOG CELLULAR COMMUNICATIONS AMP SYSTEM

GRADUATION PROJECT
COM-400

Student: Ala Mahamid (980862)

Supervisor: Mr Jamal Fathi

Nicosia - 2003

ACKNOWLEDGEMENTS

First I want to thank Mr Jamal Abu hasna to be my advisor. Under his guidance, I successfully overcome many difficulties and learn a lot about Mobile communication. In each discussion, he explained my questions patiently, and I felt my quick progress from advises. He always helps me a lot either in my study or my life. I asked him many questions in Electronic and Communication and he always answered my questions quickly and in detail.

I also want to thank my friends in NEU being with them make my 4 years in NEU full of fun.

Finally, I want to thank my family, especially my parents, brother and sister. Without their endless support and love for me, I would never achieve my current position. I wish my mother lives happily always, and my father to be proud of me.

TABLE OF CONTENTS

ABSTRACT

The GSM technical specifications define the different entities that form the GSM network by defining their functions and interface requirements.

Each mobile uses a separate, temporary radio channel to talk to the cell site. The cell site talks to many mobiles at once, using one channel per mobile. Channels use a pair of frequencies for communication—one frequency (the forward link) for transmitting from the cell site and one frequency (the reverse link) for the cell site to receive calls from the users. Radio energy dissipates over distance, so mobiles must stay near the base station to maintain communications. The basic structure of mobile networks includes telephone systems and radio services. Where mobile radio service operates in a closed network and has no access to the telephone system, mobile telephone service allows interconnection to the telephone network.

INTRODUCTION

Millions of people around of the world are using cellular phones. They are such great gadgets with a cell phone; you can talk to any one on the planet from just about anywhere.

Since every one agree with the importance of a cell phone, I have prepared this project to be in the hand of student and professional as will, and to make it easy I have put into three chapters.

In the chapter one I briefly present the concept of cellular communication and discuss the first-and second – generation cellular systems used in the United States and Europe. I out line the problems associated with the second –generation –plus PCS system and provide the vision of a third-generation system.

In the chapter two, I present how cell phone works? And I have discussed the cell approach and cell phones codes, and what makes it different from a regular phone?

What do al these confusing terms like PCS, GSM, CDMA and TDMA mean? Also I have described the technology behind call phones.

In the chapter three I present analog cellular communication AMPS systems, I have described the architecture of it, radio transmission which has described physical channel, radiated power, analog signal processing, digital signals, spectrum efficiency and logical channel which has described logical categories, blocks codes, logical channel formats. Also the message that has described what is structure of it and content of it. And also I have put the AMPS protocol summary, and task performed by AMPS terminals which has described the capability of AMPS to move network control message between base stations and mobile station. We have described how AMPS uses these messages to establish and maintain telephone calls, to do so we have four modes operations initialization, idle, access, conversation. And, network operations, which has described mobility management, authentication, and radio resources management. Also Amps status, which has described the capacity of cellular system, network security, non-voice services.

1. HISTROY OF GSM

1.1 Overview

During the early 1980s, analog cellular telephone systems were experiencing rapid growth in Europe, particularly in Scandinavia and the United Kingdom, but also in France and Germany. Each country developed its own system, which was incompatible with everyone else's in equipment and operation. This was an undesirable situation, because not only was the mobile equipment limited to operation within national boundaries, which in a unified Europe were increasingly unimportant, but there was also a very limited market for each type of equipment, so economies of scale and the subsequent savings could not be realized. The Europeans realized this early on, and in 1982 the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Group Special Mobile (GSM) to study and develop a pan-European public land mobile system. The proposed system had to meet certain criteria:

- Good subjective speech quality
- Low terminal and service cost
- Support for international roaming
- Ability to support handheld terminals
- Support for range of new services and facilities
- Spectral efficiency
- ISDN compatibility

In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase I of the GSM specifications were published in 1990. Commercial service was started in mid-1991, and by 1993 there were 36 GSM networks in 22 countries. Although standardized in Europe, GSM is not only a European standard. Over 200 GSM networks (including DCS1800 and PCS1900) are operational in 110 countries around the world. In the beginning of 1994, there were 1.3 million subscribers worldwide, which had grown to more than 55 million by October

1997. With North America making a delayed entry into the GSM field with a derivative of GSM called PCS1900, GSM systems exist on every continent, and the acronym GSM now aptly stands for Global System for Mobile communications.

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

1.2. Services provided by GSM

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

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

A variety of data services is offered. GSM users can send and receive data, at rates up to 9600 bps, to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks, and Circuit Switched Public Data Networks using a variety of access methods and protocols, such as X.25 or X.32. Since GSM is a digital network, a modem is not required between the user and GSM network, although an audio modem is required inside the GSM network to 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 teleservices or bearer services. In the current (Phase I) specifications, they include several forms of call forward (such as call forwarding when the mobile subscriber is unreachable by the network), and call barring of outgoing or incoming calls, for example when roaming in another country. Many additional supplementary services will be provided in the Phase 2 specifications, such as caller identification, call waiting, multi-party conversations.

1.3. Architecture of the GSM network

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

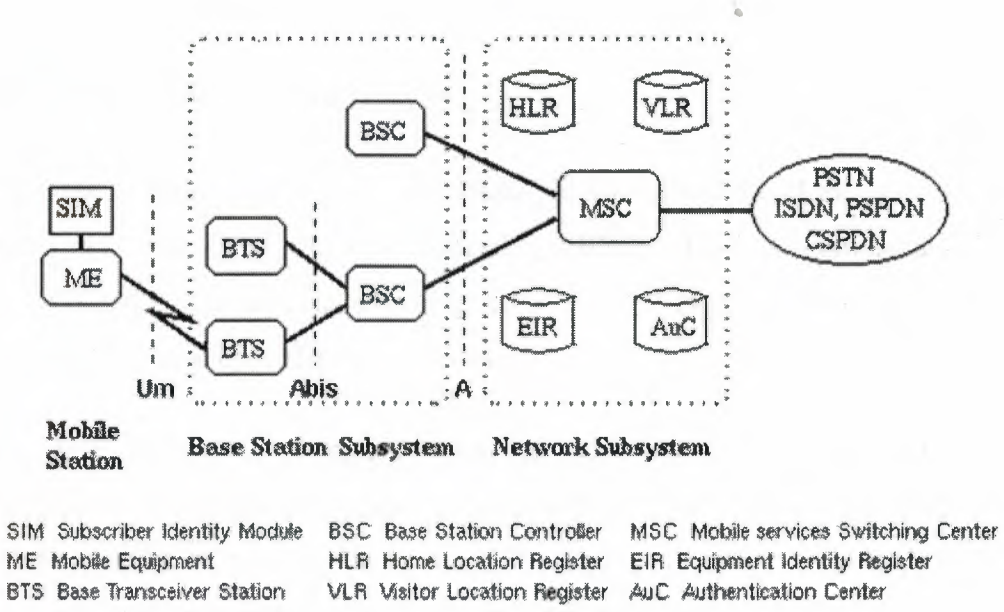


Figure 1.1 General Architecture Of a GSM Network

1.3.1. Mobile Station

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

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

1.3.2. Base Station Subsystem

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

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

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

1.3.3. Network Subsystem

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

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

is typically in the form of the 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 signalling required. Note that the MSC contains no information about particular mobile stations --- this information is stored in the location registers.

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

1.4. Radio Link Aspects

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

1.4.1. Multiple Access and Channel Structure

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

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

1.4.1.1. Traffic Channels

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

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

instead of 13 kbps). Eighth-rate TCHs are also specified, and are used for signaling. In the recommendations, they are called Stand-alone Dedicated Control Channels (SDCCH).

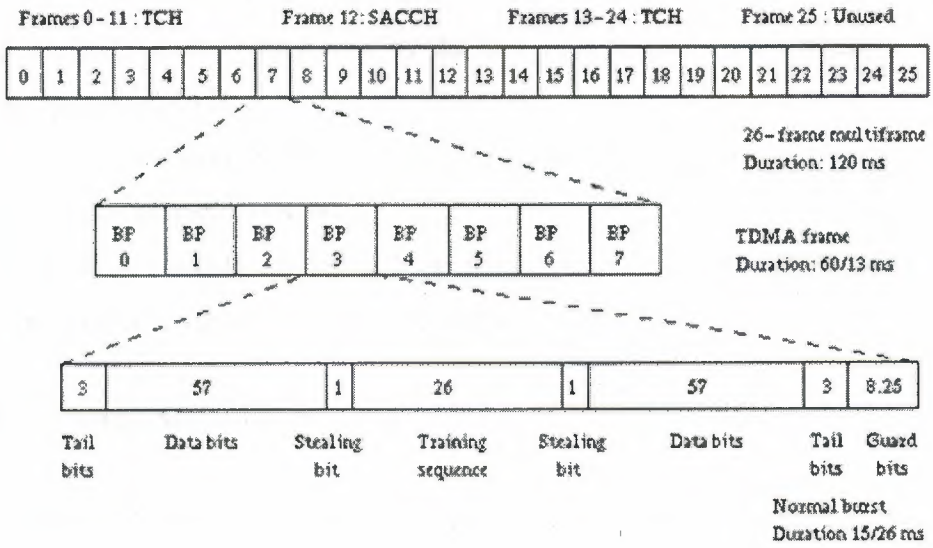


Figure 1.2 Organization of Bursts, TDMA Frames, and Multiframes for Speech and Data

1.4.1.2. Control Channels

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

Broadcast Control Channel (BCCH)

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

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

Used to synchronize the mobile to the time slot structure of a cell by defining the boundaries of burst periods, and the time slot numbering. Every cell in a GSM network broadcasts exactly one FCCH and one SCH, which are by definition on time slot number 0 (within a TDMA frame).

Random Access Channel (RACH)

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

Paging Channel (PCH)

Used to alert the mobile station of an incoming call.

Access Grant Channel (AGCH)

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

1.4.1.3. Burst Structure

There are four different types of bursts used for transmission in GSM. The normal burst is used to carry data and most signalling. It has a total length of 156.25 bits, made up of two 57 bit information bits, a 26 bit training sequence used for equalization, 1 stealing bit for each information block (used for FACCH), 3 tail bits at each end, and an 8.25 bit guard sequence, as shown in Figure 1.2 The 156.25 bits are transmitted in 0.577 ms, giving a gross bit rate of 270.833 kbps.

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

1.4.2. Speech Coding

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

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

1.4.3. Channel Coding and Modulation

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

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

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

Class Ia bits have a 3 bit Cyclic Redundancy Code added for error detection. If an error is detected, the frame is judged too damaged to be comprehensible and it is discarded. It is replaced by a slightly attenuated version of the previous correctly received frame. These 53 bits, together with the 132 Class Ib bits and a 4 bit tail sequence (a total of 189 bits), are input into a 1/2 rate convolution encoder of constraint length 4. Each input bit is encoded as two output bits, based on a combination of the previous 4 input bits. The convolution encoder thus outputs 378 bits, to which are added the 78 remaining Class II

bits, which are unprotected. Thus every 20 ms speech sample is encoded as 456 bits, giving a bit rate of 22.8 kbps.

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

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

1.4.4. Multipath Equalization

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

1.4.5. Frequency Hopping

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

1.4.6. Discontinuous Transmission

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

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

1.4.7. Discontinuous Reception

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

1.4.8. Power Control

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

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

2. The GSM Network

2.1 Architecture of The GSM Network

The GSM technical specifications define the different entities that form the GSM network by defining their functions and interface requirements.

The GSM network can be divided into four main parts:

- The Mobile Station (MS).
- The Base Station Subsystem (BSS).
- The Network and Switching Subsystem (NSS).
- The Operation and Support Subsystem (OSS).

The architecture of the GSM network is presented in figure 2.1.

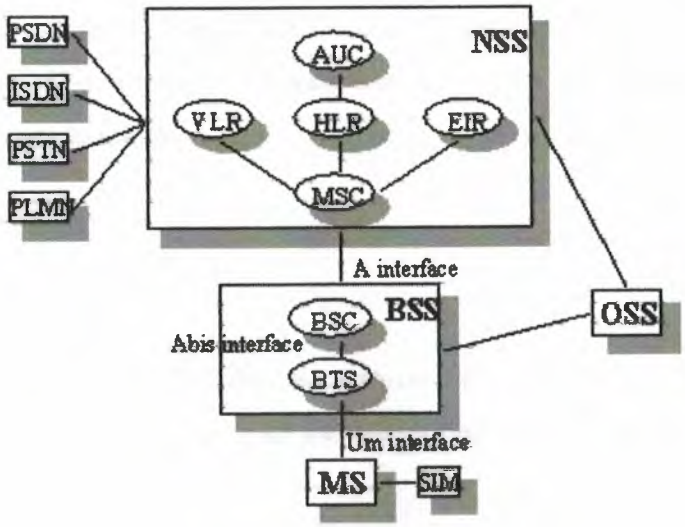


Figure 2.1 Architecture of the GSM network

2.1.1 Mobile Station

A Mobile Station consists of two main elements:

- The mobile equipment or terminal.
- The Subscriber Identity Module (SIM).

2.1.1.1 The Terminal

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 GSM portable terminals can also be installed in vehicles. Their maximum allowed output power is 8W.
- The handhels terminals have experienced the biggest success thanks to thei weight and volume, which are continuously decreasing. These terminals can emit up to 2 W. The evolution of technologies allows to decrease the maximum allowed power to 0.8 W.

2.1.1.2 The SIM

The SIM is a smart card that identifies the terminal. By inserting the SIM card into the terminal, the user can have access to all the subscribed services. Without the SIM card, the terminal is not operational.

The SIM card is protected by a four-digit Personal Identification Number (PIN). In order to identify the subscriber to the system, the SIM card contains some parameters of the user such as its International Mobile Subscriber Identity (IMSI).

Another advantage of the SIM card is the mobility of the users. In fact, the only element that personalizes a terminal is the SIM card. Therefore, the user can have access to its subscribed services in any terminal using its SIM card.

2.1.2 The Base Station Subsystem

The BSS connects the Mobile Station and the NSS. It is in charge of the transmission and reception. The BSS can be divided into two parts:

- The Base Transceiver Station (BTS) or Base Station.
- The Base Station Controller (BSC).

2.1.2.1 The Base Transceiver Station

The BTS corresponds to the transceivers and antennas used in each cell of the network. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell. Each BTS has between one and sixteen transceivers depending on the density of users in the cell.

2.1.2.2 The Base Station Controller

The BSC controls a group of BTS and manages their radio resources. A BSC is principally in charge of handovers, frequency hopping, exchange functions and control of the radio frequency power levels of the BTSs.

2.1.3 The Network and Switching Subsystem

Its main role is to manage the communications between the mobile users and other users, such as mobile users, ISDN users, fixed telephony users, etc. It also includes data bases needed in order to store information about the subscribers and to manage their mobility. The different components of the NSS are described below.

2.1.3.1 The Mobile services Switching Center (MSC)

It is the central component of the NSS. The MSC performs the switching functions of the network. It also provides connection to other networks.

2.1.3.2 The Gateway Mobile services Switching Center (GMSC)

A gateway is a node interconnecting two networks. The GMSC is the interface between the mobile cellular network and the PSTN. It is in charge of routing calls from the fixed network towards a GSM user. The GMSC is often implemented in the same machines as the MSC.

2.1.3.3 Home Location Register (HLR)

The HLR is considered as a very important database that stores information of the suscribers belonging to the covering area of a MSC. It also stores the current location of these subscribers and the services to which they have access. The location of the subscriber corresponds to the SS7 address of the Visitor Location Register (VLR) associated to the terminal.

2.1.3. Visitor Location Register (VLR)

The VLR contains information from a subscriber's HLR necessary in order to provide the subscribed services to visiting users. When a subscriber enters the covering area of a new MSC, the VLR associated to this MSC will request information about the new subscriber to its corresponding HLR. The VLR will then have enough information in order to assure the subscribed services without needing to ask the HLR each time a communication is established.

The VLR is always implemented together with a MSC; so the area under control of the MSC is also the area under control of the VLR.

2.1.3.5 The Authentication Center (AuC)

The AuC register is used for security purposes. It provides the parameters needed for authentication and encryption functions. These parameters help to verify the user's identity.

2.1.3.6 The Equipment Identity Register (EIR)

The EIR is also used for security purposes. It is a register containing information about the mobile equipments. More particularly, it contains a list of all valid terminals. A terminal is identified by its International Mobile Equipment Identity (IMEI). The EIR allows then to forbid calls from stolen or unauthorized terminals (e.g, a terminal which does not respect the specifications concerning the output RF power).

2.1.3.7 The GSM Interworking Unit (GIWU)

The GIWU corresponds to an interface to various networks for data communications. During these communications, the transmission of speech and data can be alternated.

2.1.4 The Operation and Support Subsystem (OSS)

The OSS is connected to the different components of the NSS and to the BSC, in order to control and monitor the GSM system. It is also in charge of controlling the traffic load of the BSS.

However, the increasing number of base stations, due to the development of cellular radio networks, has provoked that some of the maintenance tasks are transferred to the BTS. This transfer decreases considerably the costs of the maintenance of the system.

2.2 The Geographical Areas of the GSM Network

The figure 2.2 presents the different areas that form a GSM network.

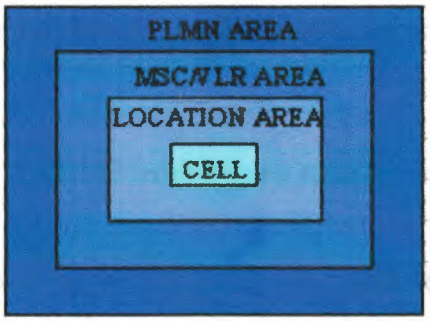


Figure 2.2 GSM Network Areas

As it has already been explained a cell, identified by its Cell Global Identity number (CGI), corresponds to the radio coverage of a base transceiver station. A Location Area (LA), identified by its Location Area Identity (LAI) number, is a group of cells served by a single MSC/VLR. A group of location areas under the control of the same MSC/VLR defines the MSC/VLR area. A Public Land Mobile Network (PLMN) is the area served by one network operator.

2.3 The GSM Functions

In this paragraph, the description of the GSM network is focused on the differents functions to fulfil by the network and not on its physical components. In GSM, five main functions can be defined:

- Transmission.
- Radio Resources management (RR).
- Mobility Management (MM).
- Communication Management (CM).
- Operation, Administration and Maintenance (OAM).

2.3.1 Transmission

The transmission function includes two sub-functions:

- The first one is related to the means needed for the transmission of user information.
- The second one is related to the means needed for the transmission of signaling information.

Not all the components of the GSM network are strongly related with the transmission functions. The MS, the BTS and the BSC, among others, are deeply concerned with transmission. But other components, such as the registers HLR, VLR or EIR, are only concerned with the transmission for their signaling needs with other components of the GSM network.

2.3.2 Radio Resources Management (RR)

The role of the RR function is to establish, maintain and release communication links between mobile stations and the MSC. The elements that are mainly concerned with the RR function are the mobile station and the base station. However, as the RR function is also in charge of maintaining a connection even if the user moves from one cell to another, the MSC, in charge of handovers, is also concerned with the RR functions.

The RR is also responsible for the management of the frequency spectrum and the reaction of the network to changing radio environment conditions. Some of the main RR procedures that assure its responsibilities are:

- Channel assignment, change and release.
- Handover.
- Frequency hopping.
- Power-level control.
- Discontinuous transmission and reception.
- Timing advance.

2.3.2.1 Handover

The user movements can produce the need to change the channel or cell, specially when the quality of the communication is decreasing. This procedure of changing the resources is called handover. Four different types of handovers can be distinguished:

- Handover of channels in the same cell.
- Handover of cells controlled by the same BSC.
- Handover of cells belonging to the same MSC but controlled by different BSCs.
- Handover of cells controlled by different MSCs.

Handovers are mainly controlled by the MSC. However in order to avoid unnecessary signaling information, the first two types of handovers are managed by the concerned BSC (in this case, the MSC is only notified of the handover).

The mobile station is the active participant in this procedure. In order to perform the handover, the mobile station controls continuously its own signal strength and the signal strength of the neighboring cells. The list of cells that must be monitored by the mobile station is given by the base station. The power measurements allow deciding which the best cell is in order to maintain the quality of the communication link. Two basic algorithms are used for the handover:

- The `minimum acceptable performance' algorithm. When the quality of the transmission decreases (i.e the signal is deteriorated), the power level of the mobile is increased. This is done until the increase of the power level has no effect on the quality of the signal. When this happens, a handover is performed.
- The `power budget' algorithm. This algorithm performs a handover, instead of continuously increasing the power level, in order to obtain a good communication quality.

2.3.3 Mobility Management

The MM function is in charge of all the aspects related with the mobility of the user, specially the location management and the authentication and security.

2.3.3.1 Location Management

When a mobile station is powered on, it performs a location update procedure by indicating its IMSI to the network. The first location update procedure is called the IMSI attach procedure.

The mobile station also performs location updating, in order to indicate its current location, when it moves to a new Location Area or a different PLMN. This location updating message is sent to the new MSC/VLR, which gives the location information to the subscriber's HLR. If the mobile station is authorized in the new MSC/VLR, the subscriber's HLR cancels the registration of the mobile station with the old MSC/VLR.

A location updating is also performed periodically. If after the updating time period, the mobile station has not registered, it is then deregistered.

When a mobile station is powered off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected.

2.3.3.2 Authentication and Security

The authentication procedure involves the SIM card and the Authentication Center. A secret key, stored in the SIM card and the AuC, and a ciphering algorithm called A3 are used in order to verify the authenticity of the user. The mobile station and the AuC compute a SRES using the secret key, the algorithm A3 and a random number generated by the AuC. If the two computed SRES are the same, the subscriber is authenticated. The different services to which the subscriber has access are also checked.

Another security procedure is to check the equipment identity. If the IMEI number of the mobile is authorized in the EIR, the mobile station is allowed to connect the network.

In order to assure user confidentiality, the user is registered with a Temporary Mobile Subscriber Identity (TMSI) after its first location update procedure.

Enciphering is another option to guarantee a very strong security but this procedure is going to be described in section 5.

2.3.4 Communication Management (CM)

The CM function is responsible for:

- Call control.
- Supplementary Services management.
- Short Message Services management.

2.3.4.1 Call Control (CC)

The CC is responsible for call establishing, maintaining and releasing as well as for selecting the type of service. One of the most important functions of the CC is the call routing. In order to reach a mobile subscriber, a user dials the Mobile Subscriber ISDN (MSISDN) number which includes:

- a country code
- a national destination code identifying the subscriber's operator
- a code corresponding to the subscriber's HLR

The call is then passed to the GMSC (if the call is originated from a fixed network) which knows the HLR corresponding to a certain MISDN number. The GMSC asks the HLR for information helping to the call routing. The HLR requests this information from the subscriber's current VLR. This VLR allocates temporarily a Mobile Station Roaming Number (MSRN) for the call. The MSRN number is the information returned by the HLR

to the GMSC. Thanks to the MSRN number, the call is routed to subscriber's current MSC/VLR. In the subscriber's current LA, the mobile is paged.

2.3.4.2 Supplementary Services management

The mobile station and the HLR are the only components of the GSM network involved with this function.

2.3.4.3 Short Message Services management

In order to support these services, a GSM network is in contact with a Short Message Service Center through the two following interfaces:

- The SMS-GMSC for Mobile Terminating Short Messages (SMS-MT/PP). It has the same role as the GMSC.
- The SMS-IWMSC for Mobile Originating Short Messages (SMS-MO/PP).

2.3.5 Operation, Administration and Maintenance (OAM)

The OAM function allows the operator to monitor and control the system as well as to modify the configuration of the elements of the system. Not only the OSS is part of the OAM, also the BSS and NSS participate in its functions as it is shown in the following examples:

- The components of the BSS and NSS provide the operator with all the information it needs. This information is then passed to the OSS which is in charge of analyze it and control the network.
- The self test tasks, usually incorporated in the components of the BSS and NSS, also contribute to the OAM functions.
- The BSC, in charge of controlling several BTSs, is another example of an OAM function performed outside the OSS.

2.4 The GSM Radio Interface

The radio interface is the interface between the mobile stations and the fixed infrastructure. It is one of the most important interfaces of the GSM system.

One of the main objectives of GSM is roaming. Therefore, in order to obtain a complete compatibility between mobile stations and networks of different manufacturers and operators, the radio interface must be completely defined.

The spectrum efficiency depends on the radio interface and the transmission, more particularly in aspects such as the capacity of the system and the techniques used in order to decrease the interference and to improve the frequency reuse scheme. The specification of the radio interface has then an important influence on the spectrum efficiency.

2.5 Frequency Allocation

Two frequency bands, of 25 Mhz each one, have been allocated for the GSM system:

- The band 890-915 Mhz has been allocated for the uplink direction (transmitting from the mobile station to the base station).
- The band 935-960 Mhz has been allocated for the downlink direction (transmitting from the base station to the mobile station).

But not all the countries can use the whole GSM frequency bands. This is due principally to military reasons and to the existence of previous analog systems using part of the two 25 Mhz frequency bands.

2.6 Multiple Access Scheme

The multiple access scheme defines how different simultaneous communications, between different mobile stations situated in different cells, share the GSM radio spectrum. A mix of Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA), combined with frequency hopping, has been adopted as the multiple access scheme for GSM.

2.6.1 FDMA and TDMA

Using FDMA, a frequency is assigned to a user. So the larger the number of users in a FDMA system, the larger the number of available frequencies must be. The limited available radio spectrum and the fact that a user will not free its assigned frequency until he does not need it anymore, explain why the number of users in a FDMA system can be "quickly" limited.

On the other hand, TDMA allows several users to share the same channel. Each of the users, sharing the common channel, are assigned their own burst within a group of bursts called a frame. Usually TDMA is used with a FDMA structure.

In GSM, a 25 Mhz frequency band is divided, using a FDMA scheme, into 124 carrier frequencies spaced one from each other by a 200 khz frequency band. Normally a 25 Mhz frequency band can provide 125 carrier frequencies but the first carrier frequency is used as a guard band between GSM and other services working on lower frequencies. Each carrier frequency is then divided in time using a TDMA scheme. This scheme splits the radio channel, with a width of 200 khz, into 8 bursts. A burst is the unit of time in a TDMA system, and it lasts approximately 0.577 ms. A TDMA frame is formed with 8 bursts and lasts, consequently, 4.615 ms. Each of the eight bursts, that form a TDMA frame, are then assigned to a single user.

2.6.2 Channel Structure

A channel corresponds to the recurrence of one burst every frame. It is defined by its frequency and the position of its corresponding burst within a TDMA frame. In GSM there are two types of channels:

- The traffic channels used to transport speech and data information.
- The control channels used for network management messages and some channel maintenance tasks.

2.6.2.1 Traffic Channels (TCH)

Full-rate traffic channels (TCH/F) are defined using a group of 26 TDMA frames called a 26-Multiframe. The 26-Multiframe lasts consequently 120 ms. In this 26-Multiframe structure, the traffic channels for the downlink and uplink are separated by 3 bursts. As a consequence, the mobiles will not need to transmit and receive at the same time which simplifies considerably the electronics of the system.

The frames that form the 26-Multiframe structure have different functions:

- 24 frames are reserved to traffic.
- 1 frame is used for the Slow Associated Control Channel (SACCH).
- The last frame is unused. This idle frame allows the mobile station to perform other functions, such as measuring the signal strength of neighboring cells.

Half-rate traffic channels (TCH/H), which double the capacity of the system, are also grouped in a 26-Multiframe but the internal structure is different.

2.6.2.2 Control Channels

According to their functions, four different classes of control channels are defined:

- Broadcast channels.
- Common control channels.
- Dedicated control channels.
- Associated control channels.

2.6.2.2.1 Broadcast channels (BCH)

The BCH channels are used, by the base station, to provide the mobile station with the sufficient information it needs to synchronize with the network. Three different types of BCHs can be distinguished:

- The Broadcast Control Channel (BCCH), which gives to the mobile station the parameters needed in order to identify and access the network
- The Synchronization Channel (SCH), which gives to the mobile station the training sequence needed in order to demodulate the information transmitted by the base station
- The Frequency-Correction Channel (FCCH), which supplies the mobile station with the frequency reference of the system in order to synchronize it with the network

2.6.2.2.2 Common Control Channels (CCCH)

The CCCH channels help to establish the calls from the mobile station or the network. Three different types of CCCH can be defined:

- The Paging Channel (PCH). It is used to alert the mobile station of an incoming cal
- The Random Access Channel (RACH), which is used by the mobile station to request access to the network

- The Access Grant Channel (AGCH). It is used, by the base station, to inform the mobile station about which channel it should use. This channel is the answer of a base station to a RACH from the mobile station

2.6.2.2.3 Dedicated Control Channels (DCCH)

The DCCH channels are used for message exchange between several mobiles or a mobile and the network. Two different types of DCCH can be defined:

- The Standalone Dedicated Control Channel (SDCCH), which is used in order to exchange signaling information in the downlink and uplink directions.
- The Slow Associated Control Channel (SACCH). It is used for channel maintenance and channel control.

2.6.2.2.4 Associated Control Channels

The Fast Associated Control Channels (FACCH) replace all or part of a traffic channel when urgent signaling information must be transmitted. The FACCH channels carry the same information as the SDCCH channels.

2.6.3 Burst structure

As it has been stated before, the burst is the unit in time of a TDMA system. Four different types of bursts can be distinguished in GSM:

- The frequency-correction burst is used on the FCCH. It has the same length as the normal burst but a different structure.
- The synchronization burst is used on the SCH. It has the same length as the normal burst but a different structure.
- The random access burst is used on the RACH and is shorter than the normal burst.

- The normal burst is used to carry speech or data information. It lasts approximately 0.577 ms and has a length of 156.25 bits. Its structure is presented in figure 2.3

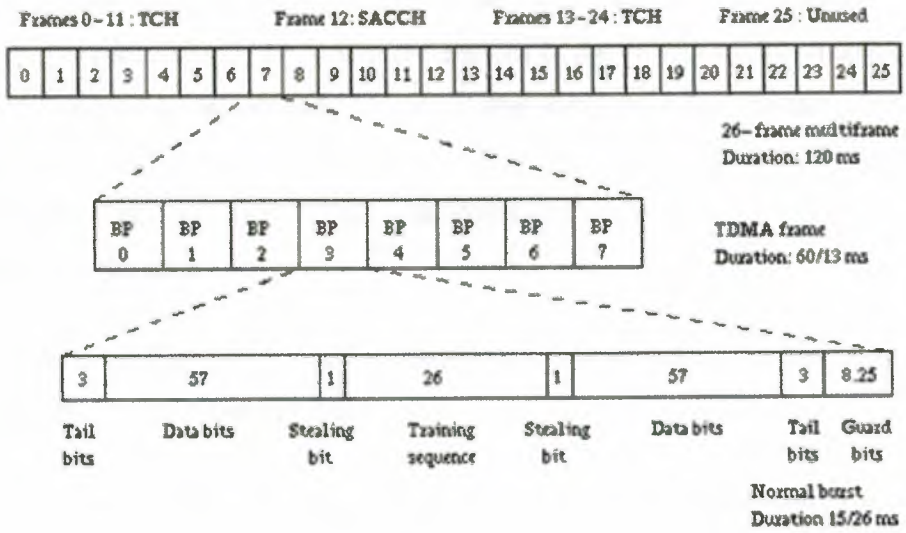


Figure 2.3: Structure of the 26-Multiframe, the TDMA frame and the normal burst

The tail bits (T) are a group of three bits set to zero and placed at the beginning and the end of a burst. They are used to cover the periods of ramping up and down of the mobile's power.

The coded data bits corresponds to two groups, of 57 bits each, containing signaling or user data.

The stealing flags (S) indicate, to the receiver, whether the information carried by a burst corresponds to traffic or signaling data.

The training sequence has a length of 26 bits. It is used to synchronize the receiver with the incoming information, avoiding then the negative effects produced by a multipath propagation.

The guard period (GP), with a length of 8.25 bits, is used to avoid a possible overlap of two mobiles during the ramping time.

2.6.4 Frequency Hopping

The propagation conditions and therefore the multi-path fading depend on the radio frequency. In order to avoid important differences in the quality of the channels, the slow frequency hopping is introduced. The slow frequency hopping changes the frequency with every TDMA frame. A fast frequency hopping changes the frequency many times per frame but it is not used in GSM. The frequency hopping also reduces the effects of co-channel interference.

There are different types of frequency hopping algorithms. The algorithm selected is sent through the Broadcast Control Channels.

Even if frequency hopping can be very useful for the system, a base station does not have to support it necessarily on the other hand, a mobile station has to accept frequency hopping when a base station decides to use it.

2.7 From source information to radio waves

The figure 2.2 presents the different operations that have to be performed in order to pass from the speech source to radio waves and vice versa.
If the source of information is data and not speech, the speech coding will not be performed.

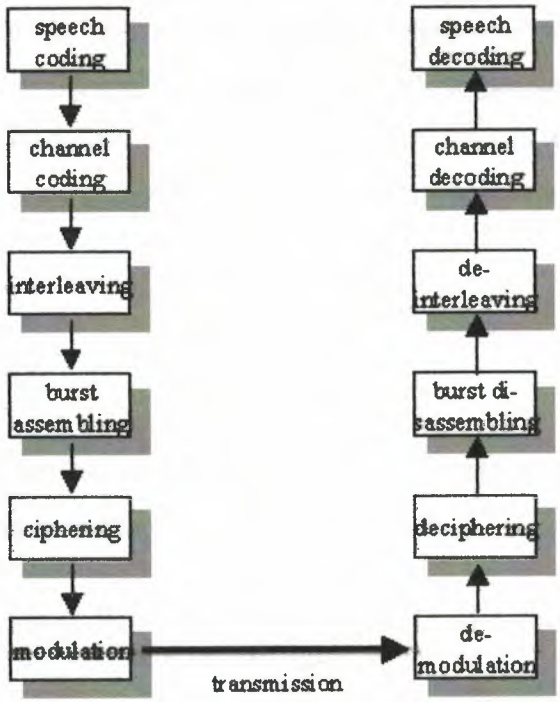


Figure 2.4: From speech source to radio waves

2.7.1 Speech Coding

The transmission of speech is, at the moment, the most important service of a mobile cellular system. The GSM speech code, which will transform the analog signal (voice) into a digital representation, has to meet the following criteria's:

- A good speech quality, at least as good as the one obtained with previous cellular systems.
- To reduce the redundancy in the sounds of the voice. This reduction is essential due to the limited capacity of transmission of a radio channel.
- The speech code must not be very complex because complexity is equivalent to high costs.

The final choice for the GSM speech code is a code named RPE-LTP (Regular Pulse Excitation Long-Term Prediction). This code uses the information from previous samples (this information does not change very quickly) in order to predict the current sample. The speech signal is divided into blocks of 20 ms. These blocks are then passed to the speech code, which has a rate of 13 kbps, in order to obtain blocks of 260 bits.

2.7.2 Channel Coding

Channel coding adds redundancy bits to the original information in order to detect and correct, if possible, errors occurred during the transmission.

2.7.2.1 Channel Coding For The GSM Data TCH Channels

The channel coding is performed using two codes: a block code and a convolution code.

The block code corresponds to the block code defined in the GSM Recommendations 05.03. The block code receives an input block of 240 bits and adds four zero tail bits at the end of the input block. The output of the block code is consequently a block of 244 bits.

A convolution code adds redundancy bits in order to protect the information. A convolution encoder contains memory. This property differentiates a convolution code from a block code. A convolution code can be defined by three variables: n, k and K. The value n corresponds to the number of bits at the output of the encoder, k to the number of bits at the input of the block and K to the memory of the encoder. The ratio, R, of the code is defined as follows: R = k/n. Let's consider a convolution code with the following values: k is equal to 1, n to 2 and K to 5. This convolution code uses then a rate of R = 1/2 and a delay of K = 5, which means that it will add a redundant bit for each input bit. The convolution code uses 5 consecutive bits in order to compute the redundancy bit. As the convolution code is a 1/2 rate convolution code, a block of 488 bits is generated.

These 488 bits are punctured in order to produce a block of 456 bits. Thirty two bits, obtained as follows, are not transmitted:

$$C(11 + 15j) \text{ for } j = 0, 1, ..., 31 \quad (2.1)$$

The block of 456 bits produced by the convolution code is then passed to the inter leaver.

2.7.2.2 Channel Coding For the GSM Speech Channels

Before applying the channel coding, the 260 bits of a GSM speech frame are divided in three different classes according to their function and importance. The most important class is the class Ia containing 50 bits. Next in importance is the class Ib, which contains 132 bits. The least important is the class II, which contains the remaining 78 bits. The different classes are coded differently. First of all, the class Ia bits are block-coded. Three parity bits, used for error detection, are added to the 50 class Ia bits. The resultant 53 bits are added to the class Ib bits. Four zero bits are added to this block of 185 bits (50+3+132). A convolution code, with r = 1/2 and K = 5, is then applied, obtaining an output block of 378 bits. The class II bits are added, without any protection, to the output block of the convolution coder. An output block of 456 bits is finally obtained.

2.7.2.3 Channel Coding For the GSM Control Channels

In GSM the signaling information is just contained in 184 bits. Forty parity bits, obtained using a fire code, and four zero bits are added to the 184 bits before applying the convolution code (r = 1/2 and K = 5). The output of the convolution code is then a block of 456 bits, which does not need to be punctured.

2.7.3 Interleaving

An interleaving rearranges a group of bits in a particular way. It is used in combination with FEC codes in order to improve the performance of the error correction mechanisms. The interleaving decreases the possibility of losing whole bursts during the transmission, by dispersing the errors. Being the errors less concentrated, it is then easier to correct them.

2.7.3.1 Interleaving For the GSM Control Channels

A burst in GSM transmits two blocks of 57 data bits each. Therefore the 456 bits corresponding to the output of the channel coder fit into four bursts (4*114 = 456). The 456 bits are divided into eight blocks of 57 bits. The first block of 57 bits contains the bit numbers (0, 8, 16, ...448), the second one the bit numbers (1, 9, 17, ...449), etc. The last block of 57 bits will then contain the bit numbers (7, 15, ...455). The first four blocks of 57 bits are placed in the even-numbered bits of four bursts. The other four blocks of 57 bits are placed in the odd-numbered bits of the same four bursts. Therefore the interleaving depth of the GSM interleaving for control channels is four and a new data block starts every four bursts. The inter leaver for control channels is called a block rectangular inter leaver.

2.7.3.2 Interleaving For the GSM Speech Channels

The block of 456 bits, obtained after the channel coding, is then divided in eight blocks of 57 bits in the same way as it is explained in the previous paragraph. But these eight blocks of 57 bits are distributed differently. The first four blocks of 57 bits are placed in the even-numbered bits of four consecutive bursts. The other four blocks of 57 bits are placed in the odd-numbered bits of the next four bursts. The interleaving depth of the GSM interleaving for speech channels is then eight. A new data block also starts every four bursts. The inter leaver for speech channels is called a block diagonal inter leaver.

2.7.3.3 Interleaving For the GSM Data TCH Channels

A particular interleaving scheme, with an interleaving depth equal to 22, is applied to the block of 456 bits obtained after the channel coding. The block is divided into 16 blocks of 24 bits each, 2 blocks of 18 bits each, 2 blocks of 12 bits each and 2 blocks of 6 bits each. It is spread over 22 bursts in the following way:

- the first and the twenty-second bursts carry one block of 6 bits each
- the second and the twenty-first bursts carry one block of 12 bits each
- the third and the twentieth bursts carry one block of 18 bits each
- from the fourth to the nineteenth burst, a block of 24 bits is placed in each burst

A burst will then carry information from five or six consecutive data blocks. The data blocks are said to be interleaved diagonally. A new data block starts every four bursts.

2.7.4 Ciphering

Ciphering is used to protect signaling and user data. First of all, a ciphering key is computed using the algorithm A8 stored on the SIM card, the subscriber key and a random number delivered by the network (this random number is the same as the one used for the authentication procedure). Secondly, a 114 bit sequence is produced using the ciphering key, an algorithm called A5 and the burst numbers. This bit sequence is then XORed with the two 57 bit blocks of data included in a normal burst.

In order to decipher correctly, the receiver has to use the same algorithm A5 for the deciphering procedure.

2.7.5 Modulation

The modulation chosen for the GSM system is the Gaussian Minimum Shift Keying (GMSK).

The aim of this section is not to describe precisely the GMSK modulation as it is too long and it implies the presentation of too many mathematical concepts. Therefore, only brief aspects of the GMSK modulation are presented in this section.

The GMSK modulation has been chosen as a compromise between spectrum efficiency, complexity and low spurious radiations (that reduce the possibilities of adjacent channel interference). The GMSK modulation has a rate of 270 5/6 kbauds and a BT product equal to 0.3. Figure 5 presents the principle of a GMSK modulator.

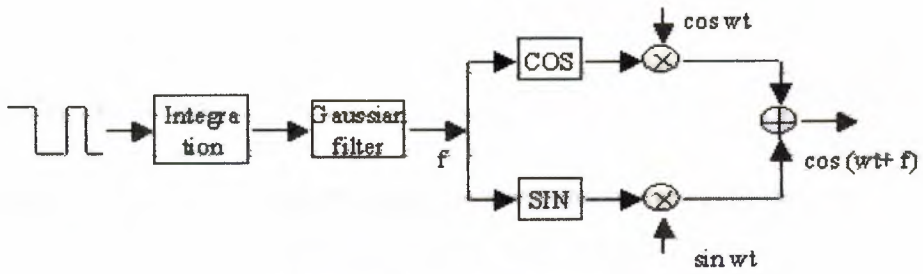


Figure 2.5: GMSK Modulator

2.8 Discontinuous Transmission (DTX)

This is another aspect of GSM that could have been included as one of the requirements of the GSM speech codes. The function of the DTX is to suspend the radio transmission during the silence periods. This can become quite interesting if we take into consideration the fact that a person speaks less than 40 or 50 percent during a conversation. The DTX helps then to reduce interference between different cells and to increase the capacity of

the system. It also extends the life of a mobile's battery. The DTX function is performed thanks to two main features:

- The Voice Activity Detection (VAD), which has to determine whether the sound represents speech or noise, even if the background noise is very important. If the voice signal is considered as noise, the transmitter is turned off producing then, an unpleasant effect called clipping.
- The comfort noise. An inconvenient of the DTX function is that when the signal is considered as noise, the transmitter is turned off and therefore, a total silence is heard at the receiver. This can be very annoying to the user at the reception because it seems that the connection is dead. In order to overcome this problem, the receiver creates a minimum of background noise called comfort noise. The comfort noise eliminates the impression that the connection is dead.

2.9 Timing Advance

The timing of the bursts transmissions is very important. Mobiles are at different distances from the base stations. Their delay depends, consequently, on their distance. The aim of the timing advance is that the signals coming from the different mobile stations arrive to the base station at the right time. The base station measures the timing delay of the mobile stations. If the bursts corresponding to a mobile station arrive too late and overlap with other bursts, the base station tells, this mobile, to advance the transmission of its bursts.

2.10 Power Control

At the same time the base stations perform the timing measurements, they also perform measurements on the power level of the different mobile stations. These power levels are adjusted so that the power is nearly the same for each burst.

A base station also controls its power level. The mobile station measures the strength and the quality of the signal between itself and the base station. If the mobile station does not receive correctly the signal, the base station changes its power level.

2.11 Discontinuous Reception

It is a method used to conserve the mobile station's power. The paging channel is divided into sub channels corresponding to single mobile stations. Each mobile station will then only 'listen' to its sub channel and will stay in the sleep mode during the other sub channels of the paging channel.

2.12 Multipart and Equalization

At the GSM frequency bands, radio waves reflect from buildings, cars, hills, etc. So not only the 'right' signal (the output signal of the emitter) is received by an antenna, but also many reflected signals, which corrupt the information, with different phases.

An equalizer is in charge of extracting the 'right' signal from the received signal. It estimates the channel impulse response of the GSM system and then constructs an inverse filter. The receiver knows which training sequence it must wait for. The equalizer will then, comparing the received training sequence with the training sequence it was expecting, compute the coefficients of the channel impulse response. In order to extract the 'right' signal, the received signal is passed through the inverse filter.

3. CELLULAR COMMUNICATIONS

3.1. Definition

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

3.2. Overview

This tutorial discusses the basics of radio telephony systems, including both analog and digital systems. Upon completion of this tutorial, you should be able to describe the basic components of a cellular system and identify digital wireless technologies.

3.3. Mobile Communications Principles

Each mobile uses a separate, temporary radio channel to talk to the cell site. The cell site talks to many mobiles at once, using one channel per mobile. Channels use a pair of frequencies for communication—one frequency (the forward link) for transmitting from the cell site and one frequency (the reverse link) for the cell site to receive calls from the users. Radio energy dissipates over distance, so mobiles must stay near the base station to maintain communications. The basic structure of mobile networks includes telephone systems and radio services. Where mobile radio service operates in a closed network and has no access to the telephone system, mobile telephone service allows interconnection to the telephone network.

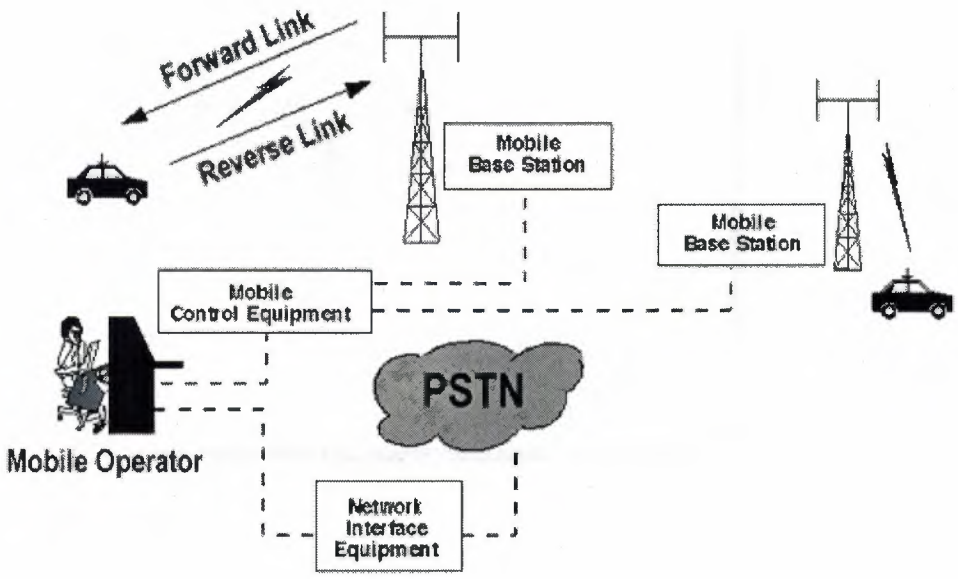


Figure 3.1 Basic Mobile Telephone Service Network

3.4. Early Mobile Telephone System Architecture

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

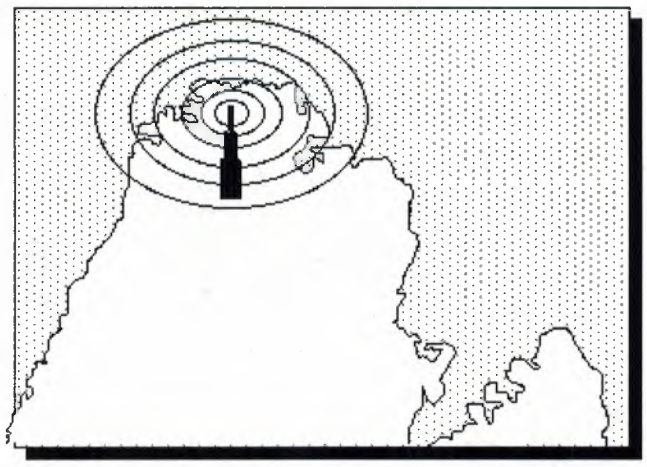


Figure 3.2. Early Mobile Telephone System Architecture

3.5. 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 50 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 10 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 allow 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 h anded off from cell to cell to maintain constant phone service as the user moves between cells.

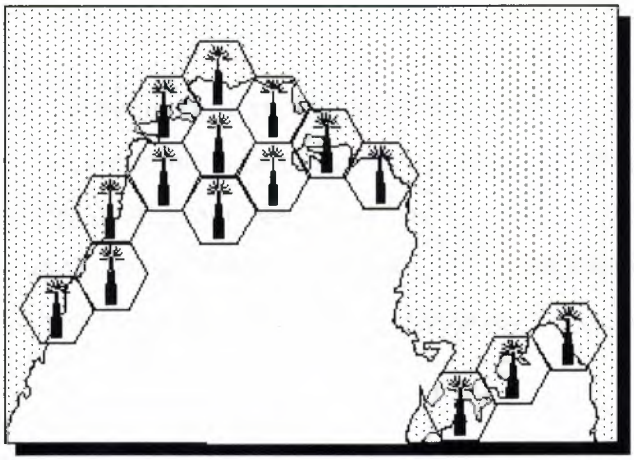


Figure 3.3. Mobile Telephone System Using a Cellular Architecture

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.

3.6. Cellular 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. Deployment parameters, such as amount of cell- splitting and cell sizes, are determined by engineers experienced in cellular system architecture.

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

3.6.1. Cells

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.

3.6.2. Clusters

A cluster is a group of cells. No channels are reused within a cluster. Figure 3.4 illustrates a seven-cell cluster.

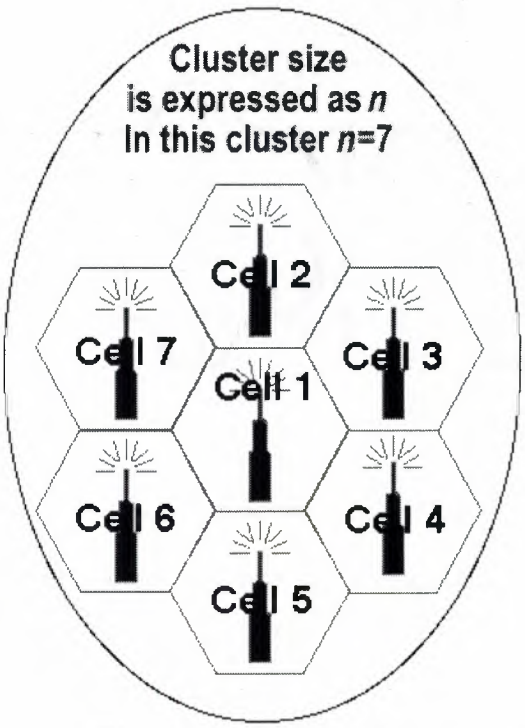


Figure 3.4. A Seven-Cell Cluster

3.6.3. Frequency 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 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.

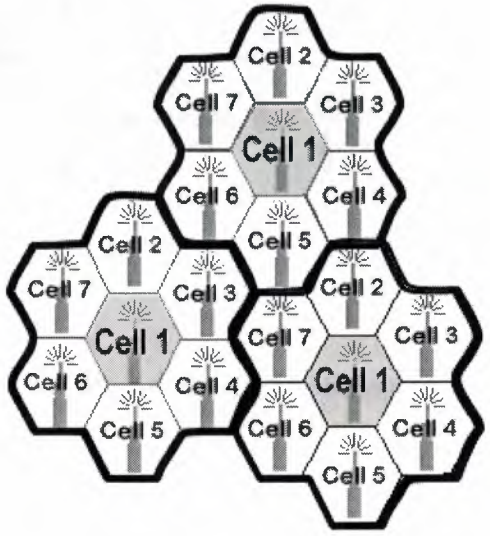


Figure 3.5. Frequency Reuse

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.

3.6.4. Cell 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 to provide acceptable service levels in heavy-traffic regions, while larger, less expensive cells can be used to cover remote rural regions.

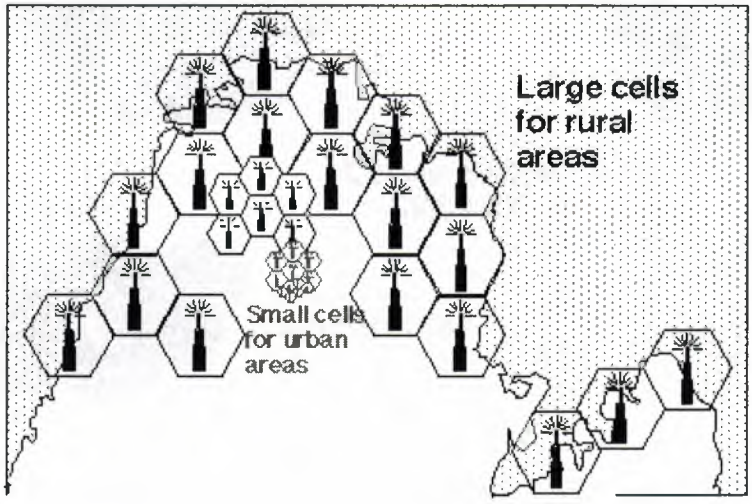


Figure 3.6 Cell Splitting

3.6.5. Handoff

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 a mobile crosses adjacent cells .

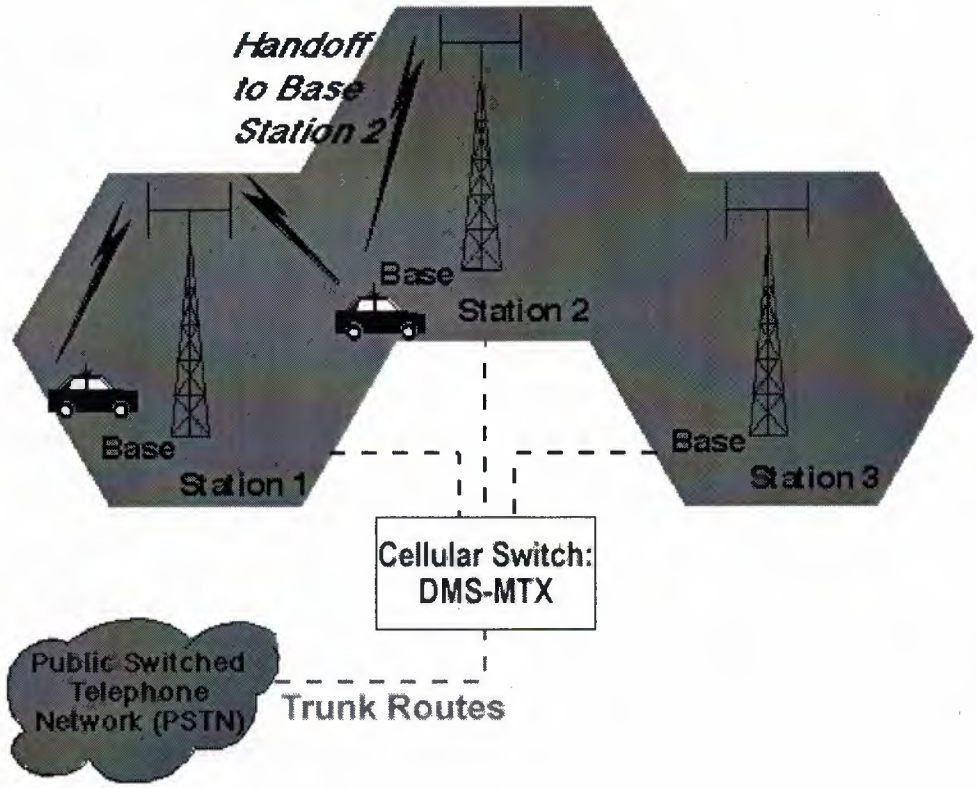


Figure 3.7. Handoff between Adjacent Cells

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.

3.7. North American Analog Cellular Systems

Originally devised in the late 1970s to early 1980s, analog systems have been revised somewhat since that time and operate in the 800-MHz range. A group of government, telco, and equipment manufacturers worked together as a committee to develop a set of rules (protocols) that govern how cellular subscriber units (mobiles) communicate with the cellular system. System development takes into consideration many different, and often opposing, requirements for the system, and often a compromise between conflictin g requirements results. Cellular development involves the following basic topics:

- frequency and channel assignments
- type of radio modulation
- maximum power levels
- modulation parameters
- messaging protocols
- call-processing sequences

3.7.1. The Advanced Mobile Phone Service (AMPS)

AMPS was released in 1983 using the 800 -MHz to 900-MHz frequency band and the 30-kHz bandwidth for each channel as a fully automated mobile telephone service. It was the first standardized cellular service in the world and is currently the most widely used standard for cellular communications. Designed for use in cities, AMPS later expanded to rural areas. It maximized the cellular concept of frequency reuse by reducing radio power output. The AMPS telephones (or handsets) have the familiar telephone-style user interface and are compatible with any AMPS base station. This makes mobility between service providers (roaming) simpler for subscribers. Limitations associated with AMPS include the following:

- low calling capacity
- limited spectrum
- no room for spectrum growth
- poor data communications

- minimal privacy
- inadequate fraud protection

AMPS is used throughout the world and is particularly popular in the United States, South America, China, and Australia. AMPS uses frequency modulation (FM) for radio transmission. In the United States, transmissions from mobile to cell site use separate frequencies from the base station to the mobile subscriber.

3.7.2. Narrowband Analog Mobile Phone Service (NAMPS)

Since analog cellular was developed, systems have been implemented extensively throughout the world as first-generation cellular technology. In the second generation of analog cellular systems, NAMPS was designed to solve the problem of low calling capacity. NAMPS is now operational in 35 U.S. and overseas markets, and NAMPS was introduced as an interim solution to capacity problems. NAMPS is a U.S. cellular radio system that combines existing voice processing with digital signaling, tripling the capacity of today's AMPS systems. The NAMPS concept uses frequency division to get 3 channels in the AMPS 30-kHz single channel bandwidth. NAMPS provides 3 users in an AMPS channel by dividing the 30-kHz AMPS bandwidth into 3 10-kHz channels. This increases the possibility of interference because channel bandwidth is reduced.

3.8. Cellular System Components

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

- public switched telephone network (PSTN)
- mobile telephone switching office (MTSO)
- cell site with antenna system
- mobile subscriber unit (MSU)

3.8.1. 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.

3.8.2. 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 wireline central offices (PSTN). In analog cellular networks, the MSC controls the system operation. The MSC controls calls, tracks billing information, and locates cellular subscribers.

3.8.3. The Cell Site

The term *cell site* is used to refer to the physical location of radi o 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.

3.8.4. Mobile Subscriber Units (MSUs)

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

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

The mobile telephone is installed in the trunk of a car, and the handset is installed in a convenient location to the driver. Portable and transportable telephones are hand-held and

can be used anywhere. The use of portable and transportable telephones is limited to the charge life of the internal battery.

3.9. Digital Systems

As demand for mobile telephone service has increased, service providers found that basic engineering assumptions borrowed from wireline (landline) networks did not hold true in mobile systems. While the average landline phone call lasts at least 10 minutes, mobile calls usually run 90 seconds. Engineers who expected to assign 50 or more mob ile phones to the same radio channel found that by doing so they increased the probability that a user would not get dial tone—this is known as call-blocking probability. As a consequence, the early systems quickly became saturated, and the quality of service decreased rapidly. The critical problem was capacity. The general characteristics of time division multiple access (TDMA), Global System for Mobile Communications (GSM), personal communications service (PCS) 1900, and code division multiple access (CDMA) promise to significantly increase the efficiency of cellular telephone systems to allow a greater number of simultaneous conversations. Figure 8 shows the components of a typical digital cellular system.

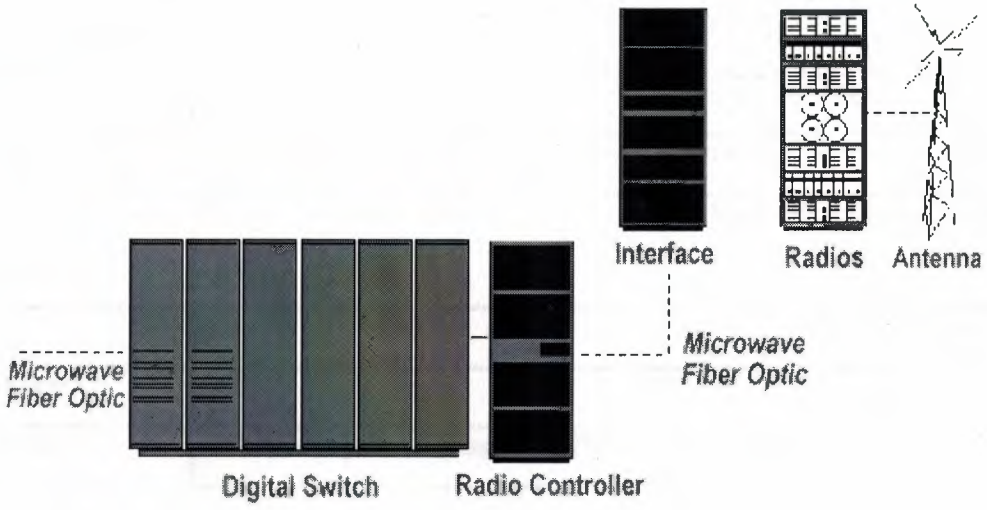


Figure 3.8 Digital Cellular System

The advantages of digital cellular technologies over analog cellular networks include increased capacity and security. Technology options such as TDMA and CDMA offer more channels in the same analog cellular bandwidth and encrypted voice and data. Because of the enormous amount of money that service providers have invested in AMPS hardware and software, providers look for a migration from AMPS to digital analog mobile phone service (DAMPS) by overlaying their existing networks with TDMA architectures.

Table 3.1. AMPS/DAMPS Comparison

	Analog	**Digital**
standard	EIA–553 (AMPS)	IS–54 (TDMA + AMPS)
spectrum	824 MHz to 891 MHz	824 MHz to 891 MHz
channel bandwidth	30 kHz	30 kHz
channels	21 CC/395 VC	21 CC / 395 VC
conversations per channel	1	3 or 6
subscriber capacity	40 to 50 conversations per cell	125 to 300 conversations per cell
TX/RCV type	continuous	time shared bursts
carrier type	constant phase variable frequency	constant frequency variable phase
mobile/base relationship	mobile slaved to base	authority shared cooperatively
privacy	poor	better—easily scrambled
noise immunity	poor	high
fraud detection	ESN plus optional password (PIN)	ESN plus optional password (PIN)

3.9.1. 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 vo ice channels
2. initial implementation triples the calling capacity of AMPS systems
3. capacity improvements of 6 to 15 times that of AMPS are possible
4. many blocks of spectrum in 800 MHz and 1900 MHz are used
5. all transmissions are digital
6. TDMA/FDMA application 7. 3 callers per radio carrier (6 callers on half rate later), providing 3 times the AMPS capacity

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

3.9.2. Extended Time Division Multiple Acœss (E–TDMA)

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

3.9.3. Fixed Wireless Access (FWA)

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

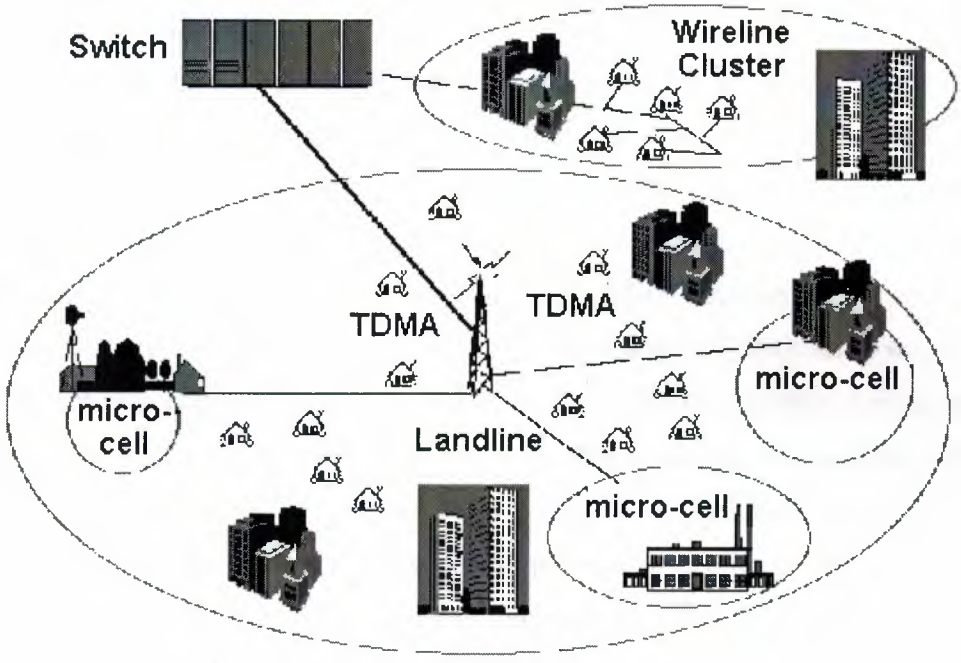


Figure 3.9 Fixed Wireless Access

3.9.4. Personal Communications Service (PCS)

The future of telecommunications includes PCS. PCS at 1900 MHz (PCS 1900) is the North American implementation of digital cellular system (DCS) 1800 (GSM). Trial networks were operational in the United States by 1993, and in 1994 the Federal Communications Commission (FCC) began spectrum auctions. As of 1995, the FCC auctioned commercial licenses. In the PCS frequency spectrum, the operator's authorized frequency block contains a definite number of channels. The frequency plan assigns

specific channels to specific cells, following a reuse pattern that restarts with each *n*th cell. The uplink and downlink bands are paired mirror images. As with AMPS, a channel number implies one uplink and one downlink frequency (e.g., Channel 512 = 1850.2-MHz uplink paired with 1930.2 -MHz downlink).

3.9.5. Code Division Multiple Access (CDMA)

CDMA is a digital air interface standard, claiming 8 to 15 times the capacity of analog. It employs a commercial adaptation of military, spread-spectrum, single-sideband technology. Based on spread spectrum theory, it is essentially the same as wireline service—the primary difference is that access to the local exchange carrier (LEC) is provided via wireless phone. Because users are isolated by code, they can share the same carrier frequency, eliminating the frequency reuse problem encountered in AMPS and DAMPS. Every CDMA cell site can use the same 1.25- MHz band, so with respect to clusters, $n = 1$. This greatly simplifies frequency planning in a fully CDMA environment. CDMA is an interference-limited system. Unlike AMPS/TDMA, CDMA has a soft capacity limit; however, each user is a noise source on the shared channel and the noise contributed by users accumulates. This creates a practical limit to how many users a system will sustain. Mobiles that transmit excessive power increase interference to other mobiles. For CDMA, precise power control of mobiles is critical in maximizing the system's capacity and increasing battery life of the mobiles. The goal is to keep each mobile at the absolute minimum power level that is necessary to ensure acceptable service quality. Ideally, the power received at the base station from each mobile should be the same (minimum signal to interference).

4. ANALOG CELLULAR COMMUNICATIONS AMPS SYSTEM

4.1 Background and Goals:

Compared with 120-year history of telephone, cellular systems are newcomers. Pioneering experiments took place in 1970s in united state (jakes1947). The earliest commercial systems went into service 1980 and 1981 Japan and Scandinavia. The 1980s and 1990s have seen rapid expansion of geographical coverage and subscriber populations in most parts of the world. Cellular communication originated in prosperous industrial countries with advanced telephone networks. Most people already had telephones at home and at work. The original purpose a cellular system was to add motor vehicles to the list of places with telephones. The target customers were a small minority of the population with special needs. Not only have these original aims been fulfilled, they have been surpassed in several way. Cellular telephones are by now familiar parts of popular in the form of small, lightweight, portable units. With its own electronic directory of names and numbers, cellular phone is personal. It belongs to person rather than residence, office, or vehicle. The other surprise of cellular services the mass-market appeal. Even through prices are high compared with conventional telephony, cellular service and equipment are popular are consumer items. In the common with other countries with well-developed cellular services, market penetration in the united sates exceeds 15 percent of the individuals and 30percent of individuals and 30percent of households. In addition to their popularity in industrial countries, cellular telephones have attracted markets in countries at all stages of economic development. The popularity of the original cellular Systems has been a principal Stimulus for the development of the new technologies described in the Chapters following this one. This chapter covers the original, first-generation cellular technology focusing on AMPS (Advanced Mobile Phone System)

[Electronic Industries Association, 1989; Bell System Technical Journal, 19791. AMPS and its first-generation relatives are important as precursors of the newer technology. In addition, the existence in 1997 more than 40 million AMPS subscriber units and supporting infrastructure ensure that AMPS systems will be in service for many years to come regardless of the relative merits of new systems in the fact; the first digital cellular

standards in North America specify "dual mode operation, with each terminal. Capable of both analog and digital voice transmission. An AMP is one of several first-generation cellular systems. All are mutually incompatible in the sense that terminals conforming to one standard cannot operate with base stations conforming to another standard. Prominent differences between systems include operating frequencies and channel bandwidths [Rappaport, 1996: 548; Mehrotra, 1994]. On the other hand, all analog cellular Systems share many characteristics. The most prominent one is voice transmission by means of frequency modulation. . Their network are all similar to AMPS and they have similar signaling systems are in throughout United States and Canada as well as several Latin American and Pacific countries. Referring to the services and design goals of Sections 2.1 and 2.2, AMPS delivers basic telephony and supplementary services of which voice mail and call forwarding are the most popular. Although it is possible to transmit digital data over ANIPS channels, service quality is vulnerable to channel impairments and handoffs. The main design goals of AMP and other first generation Systems were wide area geographical coverage, low probabilities of call blocking and call dropping, high transmission quality; high user mobility', high spectrum efficiency; and early deployment. .

4.2 Architecture

AMPS is an American national standard with title 'mobile station, land station compatibility specification. This is significant, not only for the world s it contain but also for what it omits. The amps standard says nothing about communications between base station and switches. These communications conform the proprietary protocols specific to the individual equipment vendors. This makes it impossible for a service provider to use base stations from one supplier with a switch from a competing supplier. It also inhibits coordination of operations between cellular switches produced by different manufacturers. With limited coordination between switches, cellular communications in the united states begans as a collection of local services. Each subscriber was able to initiate and receive calls within a home subscription area. Roaming services, which make it possible to use a cellular phone outside of subscriber's home area, were spotty and inconsistent from company to company .in the mid-1990s, the American cellular operating industry made major advances toward making cellular national service,

Allowing everyone within range of the base station to initiate and receive phone calls.

4.3.1 Networks Elements

The system architecture displayed with the amps terminology in the figure 4.1 is the one presented in the figures 1.12. The amps specification refers to terminals as mobile stations and to base station. People in the industry often use the terms mobiles for terminals and cell sites for base stations. Although the amps specification does not refer to the cellular switch, this network element play an essential role in all amps communication links between the base stations and switch are labeled landlines, this terminology can be misleading. In the many cases this links are one or more cobber wires or optical fiber carrying digitally multiplexed groups of signals. Leased from local telephony company. In many areas, cellular service providers operate private microwave systems to connect cell site to an MTSO. The connections between the MTSO and public telephone network can also take variety of forms. Usually thee facilities are the property of the local or long-distance telephone company can be in the form of subscriber lines terminating in a central office switch (small MTSO) or trunks terminating In tandem switch (large MTSO)

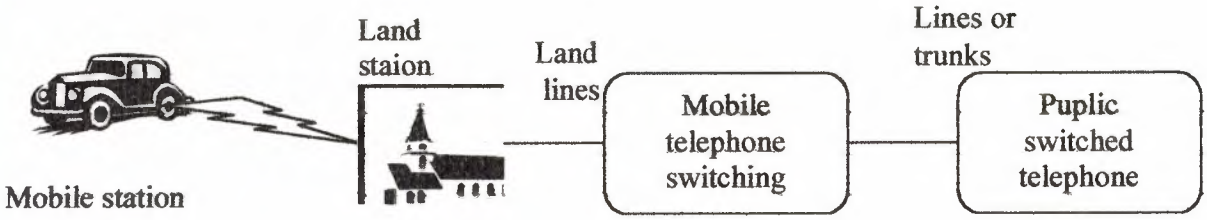


Figure 4.1 AMPS Architecture and Terminology

4.3 Radio Transmission

4.3.1 Frequency Bands and Physical Channels

AMPS operate in the frequency bands shown in the figures 4.2. The original allocation in the United States covered a bandwidth of 40MHz (figure 4.2a). The bandwidth was later extended to 50 MHz (figure4.2b). Frequency division duplex separates signals traveling to a mobile station from signals transmitted by the mobile station .the band for forward transmissions, from cell cite to mobile station, is 870-890MHz.the reverse band, for transmissions by mobiles, 45MHz lower. An Amps channel occupies two 30Khz frequency bands, one for each direction. There are 666 channel in the original Amps spectrum allocation, corresponding to the ratio of entire Amps bandwidth (per direction), to the width of physical channel 20MHZ/30MHz. AMPS channel numbers began with1 t bottom of the original band and continue to666. The carrier frequency corresponding to channel C is

$$F(c)= 825,000 +30\ C\ kHz \qquad (4.1)$$

For transmission in the reverse direction. In the forward direction the carrier frequency is f(c)+45,000Khz.

Soon after amps entered commercial service in the united states and Canada, regulatory authorities respond to the industry requests for additional radio spectrum by adding 10MHz to the original 40MHz allocation.

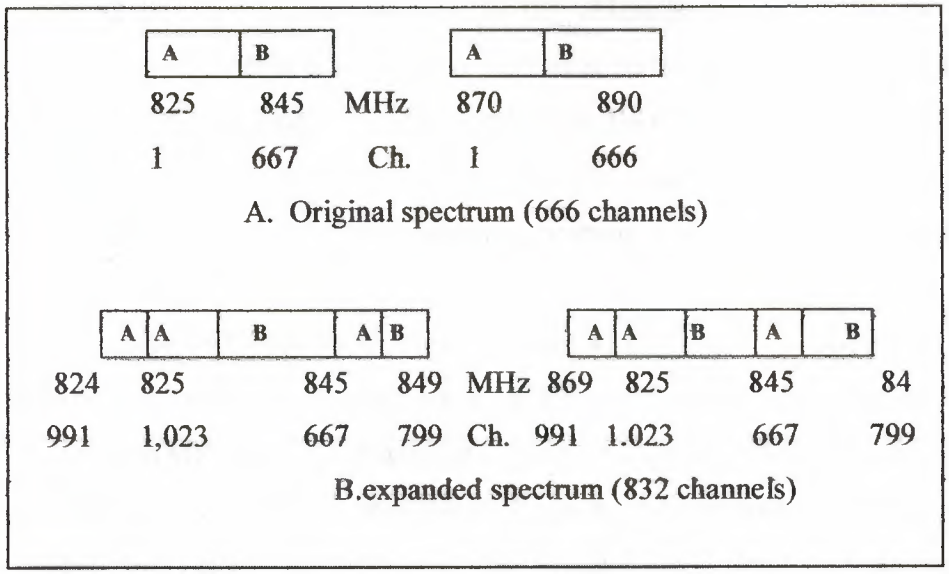


Figure 4.2 AMPS Spectrum And Channel Numbers

For each direction for transmission, the expanded spectrum contains a 1MHz band just below each band of the original spectrum, and a 4MHZ band adjust above each original band. There are 832 channels I the expanded spectrum, with channel numbers 1 to 799 related to carrier frequencies according to equation4.1. The other 33 channels, in the 1MHz band below the original band, have the numbers 991 to 1023. The carrier frequency of one these reverse channels is

$$F(C) = 825{,}000 + 30(C\text{-}1, o23); \text{KHz}; 991<C<1{,}o23 \qquad (4.2)$$

Figure 4.2 divides the AMP spectrum into two (equal, but not contiguous) regions labeled A and B. In the United States, regulators issue two cellular operating licenses in each geographical area. C) One license authorizes a company to operate in the 416 channels of the A-band. The other license applies to the 416 channels in the B-band. There are 1.466 operating licenses in the United States corresponding to two licenses in each of 305 metropolitan statistical areas and 428 rural service areas. The result of this licensing procedure is that each subscriber can choose between two operating companies in any given area. At most locations, a cellular terminal is within the operating range of an A-band cell site and a B-band cell site. The two cell sites have different system identifiers (SIDs). All systems operating in the A-band have odd SIDs

(least significant bit=1). B-band systems have even SIDS. All terminals have access to all 832 AMPS channels (except for the oldest terminals, which can tune only to the original 666 AMPS channels). A particular terminal is programmed with a preference for, or with a restriction to, the band (A or B) in which its home system operates. If it tunes to a control channel at a cell site operating in the other band, the mobile station appears as a roamer in the competing system, even though it is present in the service area of its home system.

Among the 832 AMPS channels, there are 42 channels (21 channels in each band) that carry only system control information. They are channels 313-354, in the center of the original AMPS band. To establish contact with an AMPS system, the receiver at a mobile station tunes to one of these channels. In areas with a high density of cellular subscribers, operating companies may designate additional channels as system control channels.

All other channel (up to 395 channels per operating company) are traffic channels, available to carry user information, which usually takes the form of conversational speech.

4.3.2 Radiated Power

An AMPS terminal is capable of radiating signals at six or eight different power levels depending on the nature of he terminal. A command from the base station don establishes the actual power radiated by the terminal The radiated power levels range from & dBm^{-1} (6 mW) to 36 dBm (4W) in steps 0443) so that each possible power level is 2.5 dnie5 higher than ho next lower one A class III mobile station, usually powered by a vehicle. Battery; has access to an eight power levels A Class ill mobile station, typically handheld, ranges over the six lower levels, to a maximum of 600 mW (The AMPS standard also Class to Class II mobiles with a maximum radiated power of 1.6 W. however there are no commercial product operating at this limit) The radiated power at a base station is typically 25 w per channel, for wide area coverage, and lower in cells with small service areas.

Messages from the base station control the transmitted power level of active terminals some terminals are designed for discontinuous transmission, (DTX). During a conversation, it is possible for these terminals to alternate between two power levels, corresponding to ON and OFF states, under the control of a speech activity detector In

the ON state, when a terminal detects a speech input, it transmits at the power Level commanded by 'be base station. In the OFF state, it transmits at a reduced level to conserve battery power this also reduces the interference to other conversations

Each AMPS channel can carry signals in an analog format for conveying user information or a digital format for system control information. The following paragraphs describe these signal formats that were designed to promote reliable information transfer in the presence of transmission impairments.

4.3.3 Analog Signal Processing

In Figure 4.3 the four operations prior to the modulator serve to maintain High signal quality and to limit *adjacent t ch*annel to transmission in neighboring physical channels. Compression and pre-emphasis are established techniques for audio signal transmission.

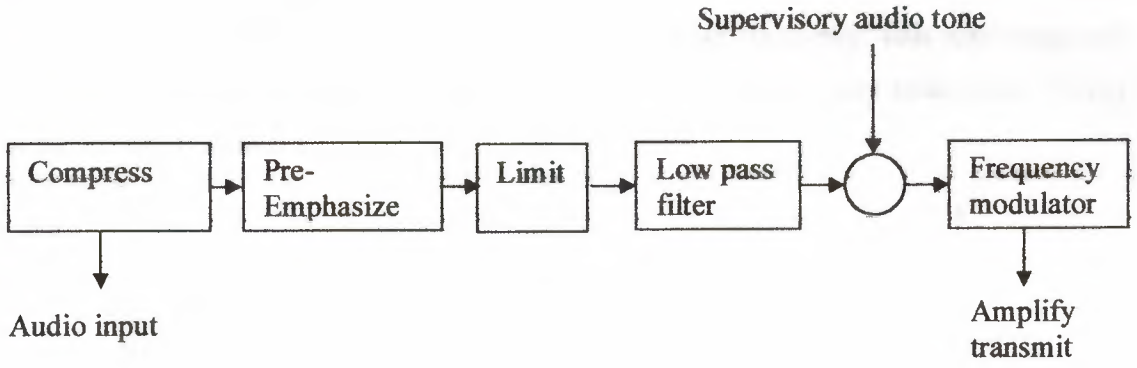


Figure4.3 Analog Signal Processing

The purpose of the compressor and a corresponding expand or the receiver is to raise transmission quality when the input signal exhibits a large range of amplitudes. Human speech has a high dynamic range. For one speaker, the energy in loud sounds (typically vowels) is 16 times (12 dB) stronger than the energy in weak sounds (unvoiced consonants). Magnifying this range of amplitudes is the difference in average sound level between loud speech and quiet speech. This high dynamic range makes a transmission system vulnerable to degradation of strong sounds by nonlinear distortion and, degradation of weak sounds by noise. The Compressor reduces this vulnerability

by compressing the overall Dynamic range (measured in decibels) by a factor of two. At the receiver, the expandor restores the original dynamic range. The result is higher speech quality than there would be without companding.outside of cellular telephony, we experience the benefits Companding when we listen to tape casse4tes with Dolby noise reduction.

The AMPS pre-emphasis filter, with frequency response shown in Figure 4.4and a complementary de-emphasis filter at the receiver, also improves sound qualify; Together they amplify high-frequency sounds (up to 3,000 Hz), which tend to be weaker than low-frequency sounds, prior to transmission, and restore them to their original level after reception An amplitude limiter confines the maximum excursions of the' frequency modulated signal to 12 kHz on either side of the carrier frequency. Finally, the baseband signal goes through a lowpass filter with the transfer function in Figure 4.5. This filter attenuates signal components at frequencies Above 3,000 Hz. It ensures that energy more than 15 kHz away the carrier frequency is attenuated by at least 28 dB. This energy contributes adjacent channel interference to the signal carried in neighboring frequency channe1Note also the notch at 6 kHz relative to the center frequency. This notch removes signal energy at the frequencies associated with the three supervisory audio tones (SAT) of the AMPS system.

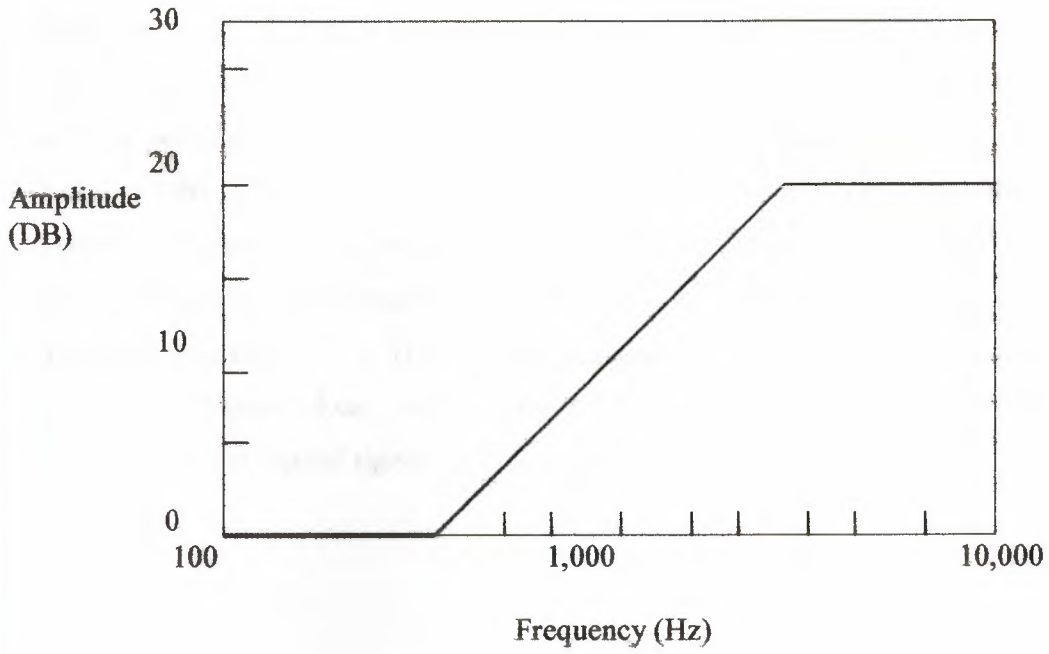


Figure 4.4 Pre-Emphasis Filters.

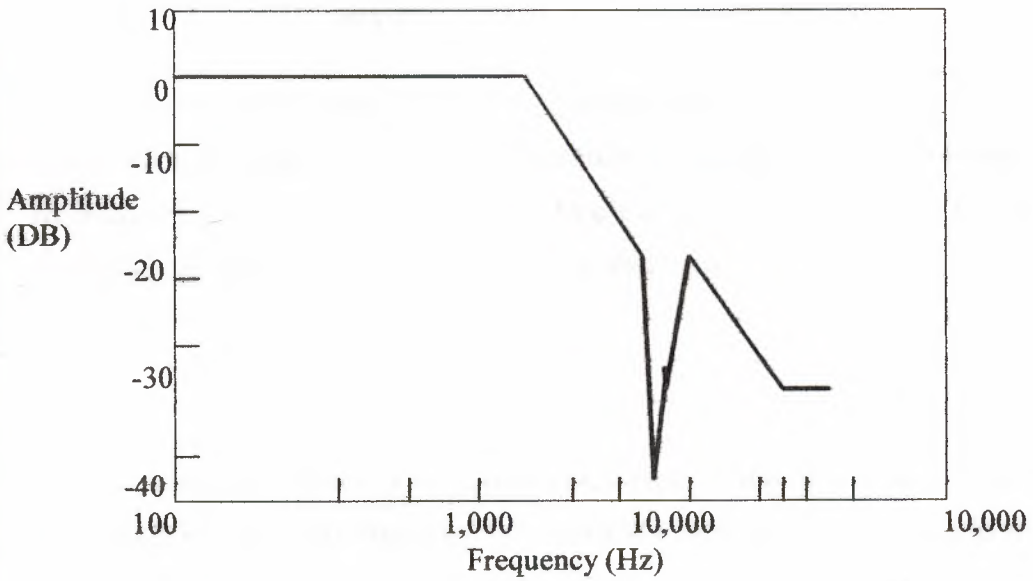


Figure 4.5 Lowpass Filter With A Notch At 6 KHz.

4.3.4 Digital Signals

Although the principal purpose of AMPS is to transport conversational speech to and from mobile stations, it also transmits important network control information in digital form. AMPS digital signals are sine waves either 8 kHz above or 8 kHz below the carrier. The signal format is Manchester coded binary frequency shift keying at a rate of 10 kb/s, or 1 bit per 100. 10^{-6} s. In this format a logical 1 is represented by a transition, in the middle of the 100. 10^{-6} s bit interval, from -8 kHz to +8 kHz relative to the carrier. A logical 0 is represented by the complementary transmission. The Manchester code facilitates receiver synchronization by preventing transmissions at a constant frequency for more than 100. 10^{-6} s. Thus, a long sequence of is results in the frequency pattern shown m Figure 4.6a, while Figure 4.6b shows the pattern corresponding to1010101Q1010 digital signal.

4.3.5 Spectrum Efficiency

Listening tests with juries of potential subscribers have determined that The AMPS transmission technology (frequency modulation in 30 kHz physical channels) requires a received signal-to-interference of at least 18 dB or high-quality production at the receiver in notation of Figure 9.7,the system has to operate with

$$(S/I) > (S/I)_{req} = 18dB. \qquad (4.3)$$

To meet fills requirement with high probability most AMPS operate with reuse factor N =7. This reuse plan is illustrated in figure9.9In these diagrams, two cells that use the same physical channels are labeled with the same number. Along with $(S/I)_{req}$, the nature of the cell site antennas has a strong influence on the reuse factor. To operate with $N = 7$,

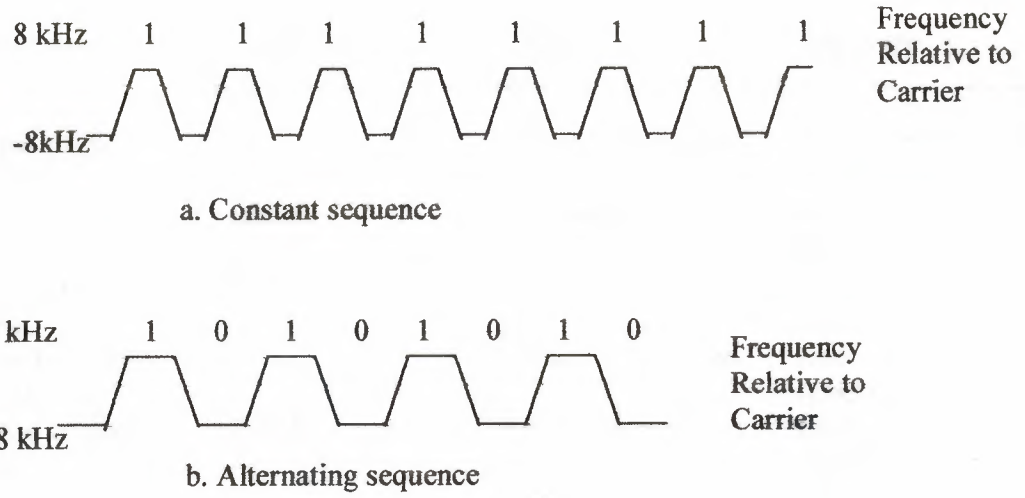


Figure 4.6 Manchester Coded Frequency Shift Keying

AMPS cells require three sets of directional antennas. Each antenna covers 120 degrees. If a system operates with 395 traffic channels, the average number of traffic channels per cell is 56 4/7 with seven-cell reuse. (Recall that of the 416 assigned channels, at least 21 operate as control channels, leaving a maximum of 395 traffic channels. Assigning these channels as equally as possible to seven cells in a Cluster places 56

channels in four cells and 57 channels in the other three cell's.) With the total spectrum assignment totem 25 MHz, the, spectrum efficiency,

$$E = \frac{395}{7*25} = 2.26 \qquad \text{Conversations/cell/N/Hz.} \qquad (4.4)$$

4.4 Logical Channels

This section describes AMPS information formats designed to foster accurate transfer of network control information in the presence of an imperfect physical connection. These information formats appear in the definitions

Table 4.2 AMPS Logical Channel

Channel name	AMPS notation	Purpose	Topology
Reverse traffic channel		User information	Dedicated (One-to-one)
Reverse control channel	RECC	Signaling	Random access (Many-to-one)
Reverse voice channel	RVC	Signaling	Dedicated (One-to-one)
Forward traffic channel		User information	Dedicated (One-to-one)
Forward control channel	FOCC	Signaling	Dedicated (One-to-one)
Forward voice channel	FVC	Signaling	Dedicated (One-to-one)

Of four logical channels. Table 4.2 lists a total of six one-way logical channels. The term *forward* denotes information transfer from base stations to mobile stations. Less formally, this direction is sometimes referred to as the *downlink.* Conversely, reverse (also called *uplink)* channels carry information from mobile stations to base stations. Table 4.2 refers to the pair of channels that carry user information in an analog format (see Section 4.3.3) as traffic *channels.* In addition to the traffic channels, there are four formats for signaling information, as indicated in Table 4.2. The forward and reverse

control channel formats are used on physical channels reserved exclusively for network control information. These logical channels are sometimes referred to as common control *channels* because they are shared by many mobile stations. As discussed in Section 4.3 A, physical channels 354 always carry forward and reverse control channels. In busy systems, operating companies use additional physical channels as forward and reverse control channels. The system uses these control channels to establish calls.

An AMP uses the term *voice channel* to denote the format of system control information carried on a physical channel that also carries user information. A forward voice channel carries system control information from a base station to a terminal when a call is in progress. A reverse voice channel carries system control information from a terminal to a base station when a call is in progress. To transmit information over the forward and reverse voice channels, AMPS uses a technique appropriately referred to as blank-and-burst. To send a Control message over a voice channel, the system interrupts the flow of user information and inserts a control message, typically of duration around 100 ms. the effect is to time-multiplex a physical channel between user information (traffic) and network control (signaling) information.

When the system inserts a signaling burst, the listener hears a click, not especially obtrusive if it occurs infrequently (once or twice per minute). However, frequent transmissions of control information during a call, by causing a lot of clicks, can seriously undermine a conversation. This Impairment limits the amount of AMPS control information that can move between terminals and the system infrastructure during a call.

Owing to the interference and fading on the physical channels, AMPS control signals encounter high binary error rates. Therefore, ANIPS protects its control information with robust error detecting and error-correcting codes.

4.4.1 Logical Channel Categories

Table 4.2 indicates the topologies of the logical channels. A forward control channel (FOCC) carries the same information from one base station to all of the terminals in a particular cell that have their power turned on and do not have a call in progress. Similarly, a reverses control channel (RECC) carries information from many mobiles

that do not have voice channels assigned. To make this possible, AMPS specifies a random access protocol that determines how mobiles contend for the attention of the base station receiver. The forward and reverse voice channels are one-to-one links between a base station and a terminal with a call in progress.

4.4.2 Block Codes

All of the logical channels protect the control information with a concatenated pair of block codes, as indicated in Figure 4.7. This figure contains a considerable amount of information about the codes, expressed in a nomenclature consisting of three integers (n, k; d_{min}), associated with a block code. The second integer, *k*, is the number of information bits carried by each code word. The total number of transmitted bits per code word is *n*. The third quantity, d_{min}, the minimum distance between 'all pairs of code words, is a measure of the block code's ability to detect and/or correct transmission errors. A high value of d_{min} implies a high immunity to transmission impairments. Section 9.4.1 contains a general description of block codes.

(N channel bits, d_{min} minimum distance)

Code rate=k/n

Channel	N	K	M	B/S
RVC	48	36	5	662-703
FVC	48	28	11	271
RECC	48	36	5	1,250-1,442
FOCC	48	28	5	1,215

Figure 4.7 Channels Coding In AMPS.

Figure 4.7 is a summary of the block codes on the four AMPS logical channels. In each channel, the outer code, which is first applied to a control message, is a shortened (63,51; 5) Bose-Chaudhuri-Hocquenghem (BCH) block code [Clark and Cain, 1981: 188494, 394J. The two mobile-to-base channels (RECC and RVC) carry messages divided into code words of length k = 36 bits. The BCH code adds 12 parity check bits to each code word. The result is a transmitted code word with n 48 bits. In the forward direction, the message word length is only k 28 bits and the transmitted code words are n = 40 bits long. In the reverse channels, the outer code is thus a (40,28; 5) block code. To provide even more protection against binary errors, AMPS employs, as an inner coder, a repetition mechanism that transmits each BCH code word at least five times.

On the FVC, the repetition mechanism transmits each word fl times! This extremely robust error-control mechanism is warranted because the FVC carries the handoff command that directs an AMPS terminal to establish communication with a new base station after it crosses a cell boundary. This is a critical communication. When it fails, AMPS drops a call and almost invariably inconveniences and irritates the two people who had been speaking to each other. Not only does the FVC carry critical information, but also it does this under difficult circumstances. The event triggering the handoff is a decline in the quality of the physical Channel that has to carry the handoff message. As a consequence, the FVC transmits

$$nm = 40 * 11 = 440 \text{ bits}$$

To convey 28 information bits.

The receiver generates a bit stream that is first processed by a decoder of the inner (repetition) code, and then by a BCH decoder. The operation of the decoders is not part of the AMPS specification. Each base station and terminal manufacturer can decide whether to operate each decoder to:

(a) Correct two binary errors,

(b) Correct one binary error and detect up to three errors, or

(c) Detect up to four binary errors with no error correction.

One approach is to perform majority logic decoding of the inner code [alternative (a) above] and single-bit error correction of the BCH code [alternative (0)]. With this approach, the inner code decoder examines the detected versions of a bit that was

transmitted five times (11 times in the case of the FVC). It then employs majority logic by deciding 1 was transmitted if it counts more is than Os. After the terminal or base station per-forms this operation $n = 40$ times (forward channels) or $n = 48$ times (reverse channels), the inner code decoder delivers an n-bit code word to the outer decoder. If this code word is identical to, or within 1 bit of, a valid transmitted code word, the decoder delivers the corresponding k-bit code word to the message layer of the controller at the terminal or base station.

4.4.3 Logical Channel Formats

Figures 4.8, 4.10, 4.11, and 4.12 show in detail the four different signaling formats of the logical channels. Each format begins with an alternating binary sequence (101010...) that enables the receiver to establish and maintain bit synchronism. On a radio channel, this sequence produces the pattern of frequency shifts shown in the figure 4.6b with the length of the sequence specific to each logical channel. The bit synchronizing sequence Appearing predictably every 46.3 ms. this makes it an easy matter for a terminal to, Acquire and hold synchronism on the FOCC.on the other three channels, transmission Take place in bursts, which make it necessary for a receiver to acquire synchronism at the start of each message. On the RECC, the bit synchronizing sequence contains 30 bits, while on the two-voice channels, each transmission begins with an alternating sequence of 101 bits. The voice channels also insert a 37-bit alternating sequence before each repetition of a BCH code word. The other synchronization pattern common to all four channels is an 11-bit Barker sequence, labeled "word sync" in Figures 4. 8, 4.10, 4.11, and 4.12. When a receiver detects the Barker sequence; it learns that the synchronization transmission has ended and that control information, in the form of protected code words, is about to arrive.

4.4.3.1 Forward Control Channel

In Figure 4.8, the notation *word A* and *word B* indicates that the channel carries two multiplexed message streams. Word carries messages for mobiles with even phone numbers (MIN), and word B carries messages for mobiles with odd phone numbers. Transmissions occur continuously on the FOCC in frames containing 463 bits (46.3 ms duration). Each frame carries one 28-bit code word to terminals with even telephone

numbers and one code word to terminals with odd phone numbers. Figure 4.8 indicates that the arriving information rate for each terminal is 28 bits per 46.3 ms, or 604.75 b/s.

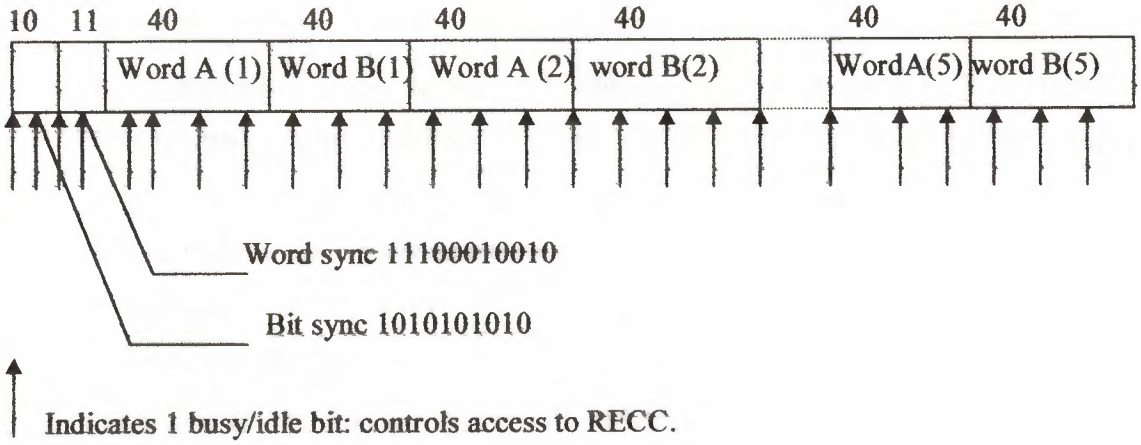


Figure 4.8 Forward Control Channel (FOCC).

Word A(1), word A(2), word A(3), word A(4), and word A(S) are

Identical with 28 information bits coded in (40,28;5) BCH format.

Word B has the same format as word A.

Word A bit rate = $(\frac{28}{463}) \times 10$ kb/s =604.75 b/s.

Total bit rate, word A and word B = 1,209.5 b/s.

4.4.3.2 Reverse Control Channel Access Protocol

Expanding Figure 4.8 to show all ten code words would reveal 42 vertical arrows. Each arrow corresponds to busy/idle bit that controls the random access of mobiles to an RECC. The control mechanism is necessary because many terminals use the same RECC. The random access protocol coordinates transmissions from dispersed terminals with the aim of preventing multiple simultaneous transmissions from different terminals. When two or more terminals transmit at the same time on an RECC, their mutual interference usually prevents the base station from detecting any of them. The random access protocol for the RECC uses the FOCC that shares the same two-way

physical channel with the RECC. Before transmitting information on the RECC, a terminal examines the state' of the busy/idle bits on the corresponding FOCC. These bits are in the idle (1) state when the base station is not in the process of receiving information on the RECC.

Observing the idle state, a cellular terminal with information to transmit initiates a burst in the format shown in Figure 4.10. It continues to observe the $FOCC_1$ expecting the busy/idle bits to change to busy (0) within a certain time window. If the transition from idle to busy occurs too soon (in less than 5.6 ms), the mobile station turns off its transmitter to avoid interference with another mobile station that caused the transition. If the mobile station observes no idle-to-busy transition within 10.4 ms, the mobile station turns off its transmitter, assuming that the base station failed to detect the beginning of the burst. If a terminal initially observes

Busy bits in the FOCC, or if it fails in an attempt to transmit an RECC Message, it pauses for a random time interval between 0 and 200 ms and begins the process again. It continues in this wav and counts the number of times it observes busy bits (NBUSY) or the number of failed attempts to "seize" the RFCC (NSZTR). When one of these numbers exceeds a limit (MAXBUSY or MAXSZTR), the terminal abandons its task. The quantities MAXBUSY and MAXSZTR are system variables broadcast by the FOCC.

After transmitting a message on the RECC, a terminal waits for a response from the system. If the expected response does not arrive within 5 seconds, the terminal returns to the initialization mode. Figure 4.9 is a flowchart of the RECC access protocol.

4.4.3.2 Reverse Control Channel

On the RECC, terminals transmit network control information to the system in bursts that convey between one and five code words, depending on the control message. Each code word appears on the physical channel.

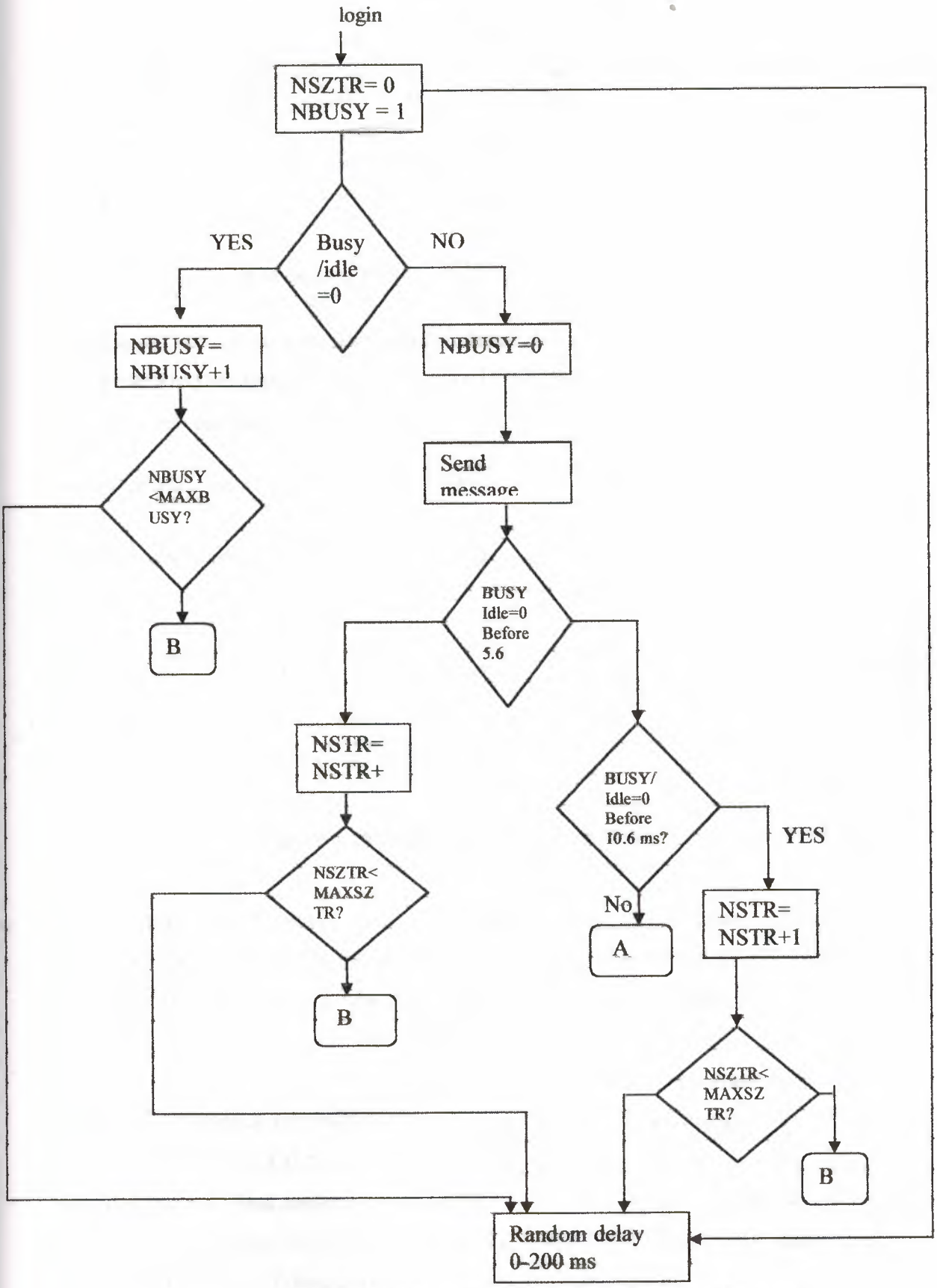
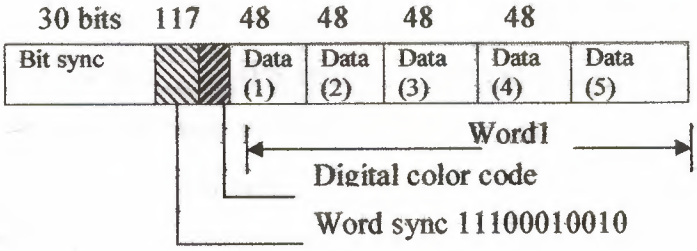


Figure 4.9 Reverse Control Channel Access Protoco



Bit sync provided by dotting sequence 1010101010... 10

Data (1). Data (2), Data (3), Data (4), and Data (5) are identical with 36 information bits coded in (48,36; 5) BCH format.

From one word per frame $5 \times 48 + 30 + 11 + 7bits = 288bits$

To five words per frame $5 \times (5 \times 48) + 30 + 11 + 7bits = 1{,}248bits$

$$withonewor\,d, rate = \frac{36}{288} \times 10kb/s = 1{,}250b/s$$

$$withfivewo\,rds, rate = \frac{5 \times 36}{1{,}248} \times 10kb/s = 1{,}442b/s$$

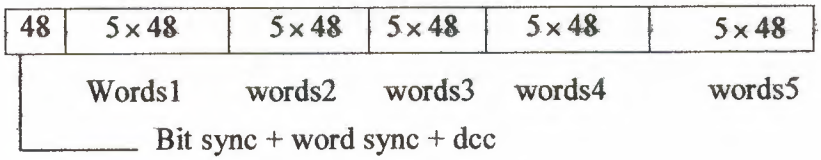


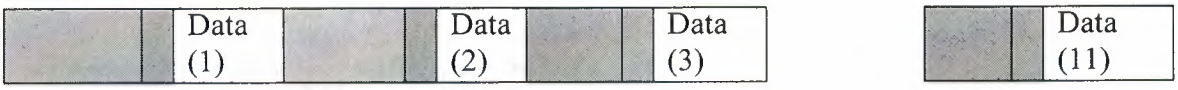
Figure 4.10 Reverse Control Channel (RECC)

As a sequence of 240 bits (a 48-bit BCH sequence repeated five times). Each message begins with a sequence of 41 synchronization bits, 30 alternating bits for bit synchronism and the fl-bit Barker sequence for frame synchronism. This is followed by a 7-bit *digital color code*. The digital color code plays the same role that the SAT plays in voice channels. Each base station has its own digital color code, broadcast in the FOCC information stream. A terminal echoes this code when it sends a message on the RECC. It is possible for an RECC burst to reach more than one base station tuned to the same physical charnel. Base stations ignore RFCC signals containing the wrong digital color code. There are four digital color codes in AMPS. The 7-bit RECC transmission corresponds to a (7,2; 4) block code with minimum distance dmin= 4

4.4.3.3 Forward and Reverse Voice Channels

To convey system control information between a base station and a terminal when a call is in progress, AMPS relies on In-band signaling over the forward and reverse voice channels. It interrupts user Information and sends a control burst in the format of Figure 4.11(base to terminal)

Or Figure3 .12 (terminal to base). Network control transmissions on a voice detecting this alternating pattern, the base station silence its transmission of the Received signal to the MTSO. Similarly, the terminal blanks the audio signal Relayed to the loudspeaker in the handset. The base or terminal then waits to detect The H-bit Barker -code, which indicates that the control information is about to before each repetition of a 40-bit or 48-bit BCH code word, there is a 37-bit Alternating sequence followed by the H-bit Barker code. This enables the base Station or the terminal to recover from a complete loss of signal, due to a deep Fade, during the transmission of a control message over the voice channel. As discussed earlier, each coded message is repeated 11 times on the barker code a High likelihood that the message will be received at the terminal. The FVC carries Handoff messages those are essential to preventing call dropping as a subscriber Crosses cell boundaries. Handoff messages are transmitted when the signal at the Serving base station is weak and therefore requires extra error protection.



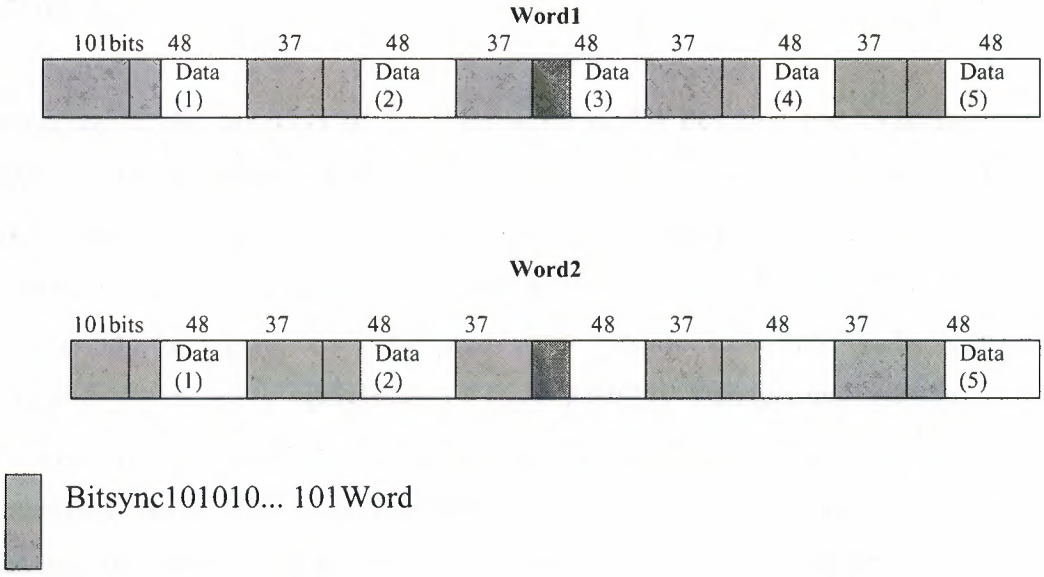
Bit sync 10101010…101

Word sync 11 bits 11100010010

Data (1), Data (2), Data (3),…….. Data (11), are identical with 28 information bits coded in (40,28; 5) BCH format.

$$Bitrate = \frac{28}{1{,}032} \times 10kb/s = 271b/s$$

Figure 4.11 Forward Voice Channel (FVC).



Word sync 11 bits 1110000**010**

Sync 11 bits 1110001001Data (1). Data (2), Data (3), Data (4), and Data (5) are identical with 36 information bits coded in (48.36; 5) BCH format.

One word per frame: $101+11+48+4\times(37+11+48)=544bits$,

, Or two words per frame: $544+5\times(37+11+48)=1{,}024bits$

$$withoneword, rate=\frac{36}{544}\times 10kb/s=662b/s$$

$$withoneword, rate=\frac{2\times 36}{1.024}\times 10kb/s=703b/s$$

Figure 4.12 Reverse Voice Channel (PVC).

FVC transmissions consist of a single code word containing 28 information bits. Transmissions on the RVC contain either one or two code words, each 36 information bits long. The effective information rate on the FVC is only 271 b/s on a channel with a binary transmission rate of 10 kb/s. On the RVC, the effective rate is either 662 b/s or 703 b/s.

4.5 Messages

In aggregate, the contents of Sections 4.3 and 4.4 describe the techniques used by AMPS to transmit network control code words between terminals and base stations. Each code word is part (or all) of a message that influences the operation of a cellular system. This section begins by examining the structure of AMPS messages. It then decibels the S) operations associated with specific messages. Table 2.3 lists six categories (of network operations. of these mobility management, authentication call management, and radio resources management, play a role in every phone call, stimulating An exchange of messages between the terminal and base station. Each message moving from a base station to a terminal consists of a sequence of 28-bit words transmitted on a forward channel (FOCC or FVC). Messages transmitted by terminals are sequence of 36-bit words transmitted on a reverse control channel (RECC or RVC). Table 4.3 is a list of AMPS messages, with an indication of the logical channel that carries each one and the categories of network control operations related to the message. A high proportion of the messages in the AMPS repertory travel from base stations to mobile stations. This reflects the hierarchical nature of AMPS. The MTSO takes major responsibility for the quality and efficiency of AMPS communications. In Table 4.3, the majority of messages are *mobile station control orders.* These are commands from the MTSO to specific terminals. Each command is relayed through a base station and transmitted to a specific terminal by an FOCC (when a terminal is idle or in the process of setting up a call), or a PVC (when a call is in progress). In contrast to the mobile station control orders, the first four messages (each marked with an asterisk) in Table 4.3 are broadcast control messages that provide the same information to all active terminals in a cell.

TABLE 4.3 Amps Message

Message	network operation
Forward control channel message	
SYSTEM PARAMTER*	call management radio resource management
GOLBAL ACTION *	radio resource management
REGISITRATION IDENT *	mobility management
CONTROL-FILTER	radio resource management
PAGE	call management
INTIAL VOICE CHANNEL	radio resource management
REDER	call management
INTERCEPT	call management
SEND CALLED-ADDRESS	call management
DIRECTED RETRY	radio resource management
RELEASE	call management
CONFIRM REGISTRATION	mobility management
Forward voice channel messages	
ALERT	call management
STOP ALERT	call management
MAINTENCE	operation and administration And maintains
RELEASE	call management
SEND CALLED-ADDRESS	call management
HANDOFF	radio resource management
CHANE POWER LEVEL	radio resource management

MESSAGES	NETWORK OPERATIONS
Reverse control channel messages	
ORIGINATION	call management, uthentication
PAGE RESPONSE	call management, uthenticatıon
REGISTRATION	mobility management
Reverse voice channel messages	
CALLED-STATION ADDRESS	Call management
ORDER CONFIRMATION	

* Indicates a broadcast message. All other messages are mobile station control orders directed at a specific terminal.

4.5.1 Message Structure

Before addressing the system actions stimulated by specific messages, we give a few examples of the structure of the AMPS sages. A striking property of the AMPS system is the lack of uniformity in the formats of different messages. All messages have a common structure. Within a given system, all code words have the same length. Each message contains a field of fixed length that identifies the message and other fields that transmit variable parameters. In AMPS, code words contain either 28 or 36 bits and each message has its own way of specifying the message type and conveying variable parameters. As examples, we examine the structures of two messages transmitted on a forward control channel, and the terminal operations stimulated by the messages. Table4.4 displays a handoff message and Table 4.5 displays a change power level message, which has an entirely different structure. The only fields common to the two messages are the reamble, in bit positions 1 and 2, and the present-channel SAT

indication, in bit positions 5 and 6. On receiving either a HANDOFF message or a CHANGE POWER LEVEL message on the FVC, the terminal verifies that the SAT indication in the message corresponds to the SAT (5,970 Hz, 6,000 Hz, or 6,030 Hz) of the cell occupied by the terminal. If the SAT indication does not correspond to the SAT of the present base station, the terminal ignores the message. This occurs when the terminal detects a message from a distant base station communicating with another terminal using the same physical channel. The terminal learns that the message in Table 4.4 is a handoff command by recognizing a valid SAT identifier in bit positions 3 and 4. If these 2 bits are 11, the terminal has to analyze the message further to determine the control action it conveys. The remainder of the HANDOFF message carries three variable parameters: the channel number of the new channel, the power level of the new channel, and the SAT of the present channel. After receiving the HANDOFF message, the mobile station turns off it's transmit

Table 4.4 Contents Of A 28-Bit HANDOFF Message Carried On The FVC

Bit position	Information
1-2	10 preamble indicates start of message
3-4	SAT of the new channel (00,01,10)
5-6	SAT of present channel (00,01,or 10)
7-14	Not used
15-17	Power level of new physical channel (VMAC)
18-28	New physical channel number

And tunes its transmitter and receiver to the center frequencies corresponding to the new channel number. It then generates the SAT tone corresponding to the new SAT indication in bit positions 3 and 4 of the Handoff message. Finally, it turns on its transmitter to emit a signal at the power level specified in the *handoff* message.

In Table 4.5, the bits 11 in positions 3 and 4 are not a valid SAT identification. This tells the mobile station that the control message does not command a handoff. To determine the nature of the command, the terminal examines bit positions 24-28. In this case, 01011 indicate that the action is change power level. This causes the terminal to examine bit positions21-23 to determine the new power level. It then adjusts its transmitter power accordingly.

Tables 4.4 and 4.5 are examples of commands transmitted to terminals on a forward voice channel (FVC). Because this is a (one-to-one) dedicated control channel (Table 4.2), there is no need to identify the terminal that is the target of the command. By contrast, the terminals in a cell that do not have a call in progress receive messages transmitted on a forward control channel (FOCC). These messages must, therefore, identify the terminal that has to take the action specified. To do so, they contain, at the beginning of a message, the 34-bit mobile station identifier (NIIN). Therefore, with only 28 bits per code word, mobile station control orders on an FOCC occupy multiple code words.

4.5.2 Message Content

The first four messages in Table 4.3 are broadcast messages that contain information for all of the terminals in a cell. They are referred to as *overhead messages* in AMPS. The FOCC periodically transmits a sequence of

Table 4.5 Contents of A 28-Bit Change Power Level Message Carried On The FVC

Bit position	information
1-2	10 permeable indicates start of message
3-4	11 indicates that this is not handoff message
5-6	SAT of presence channel
7-20	Not used
21-23	New power level (VMAC)
24-28	01011 indicates power control massage

Overhead messages in an *overhead Massage train.* The information in these messages pertains to a single cell and prepares a terminal for communications with the AMPS infrastructure. The first message in an overhead message train is a *SY5TE PRAMETERR* message consisting of two 28-bit words. This message contains the first 14 bits of the 15-bit system identifier (SID). (THE final bit is determined by the system numbering convention described in Section 4.3.1. If the message arrives on an A-channel, the least

significant bit is 1; otherwise it is 0.) The terminal compares the received SID with the SID of its home system (stored in the terminal's memory) in order to determine whether it is tuned to its home system or roaming in another system. If the system identifier does not correspond to the home system of the terminal, the terminal activates an indicator on the terminal's visual display. This indicates to the subscriber that he cannot be certain of access to the local system. If he can use the system, it is possible that service charges will be higher than in the home system. The *SYSTEM PARAMETER* message also indicates the number of forward control channels that carry paging information in the current cell and the number of reverse control channels available to terminals for sending call setup and registration message AMPS specifies that each FOCC broadcast a *SYSTEM PARAMETER message* at least every 1.1 seconds and at most two times per second. In addition to a *SYSTEM PARAMETER* message, an overhead message train can carry one or more ~*DBRL Parameter* messages. These messages contain parameters of the RECC access protocol (Section 4.4.3). Two of these parameters are MAXBUSY and MAXSZTR, which control the maximum number of attempts to transmit an RECC message. Figure 4.9 indicates that if the RECC is busy after MAXBUSY examinations of the busy/idle bits in the FOCC, the terminal abandons its attempt to send the message. It also abandons the attempt if, after MAXSZTR transmissions of a message, the terminal fails to observe the expected response from the base station. Global action messages contain two pairs of values for MAXBUSY and MAXSZTR. MAXBUSY-PGR and MAXSZTR-PGR control the transmission of page response messages and MAXBUSY-OTHER and MAXSZTR-OTHER control the transmission of all other messages. The third broadcast message that may appear in an overhead message train is a *REGIS TRRTIDII IDENT* message. This message contains a 20-bit number (REGID) that controls the frequency with which terminals transmit *REGIS TRRTIUIY* messages to the system. An AMP specifies continuous transmission on each FOCC. The transmitter always radiates energy. The system uses *CONTROL FILLER* messages to fill Gaps between necessary control messages. *CONTROL* FILLER messages contain a3-bit number, CMAC (control mobile attenuation), that specifies the transmit power level for messages transmitted by terminals on an RECC.

Except for the first four messages (those with an asterisk) in Table 4.3, each FOCC message is a mobile station control order directed to a specific terminal. Each control order contains the address of the terminal (34-bit mobile identification number) to which the message is directed. Many of the message names clearly indicate the purpose

of the message. A *PAGE* message informs the terminal of an incoming call. An *INTIAL VOICE CHANNEL* message directs the terminal to tune to a traffic channel in order to begin a new call. The message contains the voice channel number (CHAN) and the transmit power level (VMAC) on the voice channel. A *REDRDER* message causes the terminal to emit an audible signal to the subscriber. This takes the form of a fast busy signal that indicates that the system is unable, usually because of congestion, to meet the person's call setup request. Similarly, an *INTERCEPT* message causes the terminal to produce a different audible signal to indicate that the subscriber has issued a request (number sequence) that the system cannot interpret. A SEND CALL ADDRESS message causes the terminal to transmit the telephone number that the subscriber is trying to reach.

Directed retry is a radio resources management procedure. A *DIRECTED RETRY* message commands a terminal to try- to gain access to the system through another base station. An AMPS system issues *DIRECTED RETRY* messages when there is an uneven demand for service in a cluster of cells. Before setting up a call, each terminal tunes to the control channel with the strongest received signal. This is likely to come from the nearest base station. It may be that communications are also possible through other Se stations. If the original base station is too busy to accommodate a n w call request, it can command a terminal to attempt to gain access to the system through one or more other base stations. The *DIRECTED RETRY*

A massage specifies the FOCC channel numbers at adjacent base stations. The terminal, if possible, tunes to one of these channels and attempts gain to gain access to the system.

A *RELERSE* message received on the FOCC causes the terminal to abandon its current operation and return to monitoring the FOCC. A CONFIRM REGISTRATION message acknowledges receipt of a *REGISTRAION* message on an RECC.

Turning to transmissions on an FVC, the first five messages in Table 4.3 play a role in call management operations. An *RLERT* message causes the mobile station to generate an audible tone (beep) to inform the user of an arriving call. While alerting the user, the terminal transmits an SAT tone and a 10 kHz supervisory tone on the forward traffic Channel When the subscriber answers the call by pressing a button on the terminal, the terminal turns off the supervisory tone and the base station reacts by sending a STDP ALERT message that commands the terminal

Stop beeping. AMPS terminals contain a 65-second timer that controls the duration of the alerting process. If a call is not answered after 65 seconds AMPS abandons the attempt to reach the mobile subscriber. When happens, the terminal releases the voice channel and returns to an FOCC. This mechanism limits the amount of time that a voice channel is occupied by an unsuccessful call setup attempt.

A MAINTENANCE message allows the system to check the operation of a terminal. The terminal responds to this message in the same way it responds to an ALERT message, except that it does not emit an audible beep. When the MTSO learns that the party communicating with a mobile subscriber has ended a call, it commands the base station to send a RELEASE message to the terminal. This causes the terminal to leave the voice channel and tune once again to an FOCC. The SEND CALLED-ADDRESS message on the FVC stimulates the terminal to transmit a stored telephone number to the system. The other two FVC messages, HANDOFF and CHANGE POWER LEVEL, play an important role in radio resources management as discussed in Section 4.5.1.

The upstream control messages on the RECC play a vital role in call management and mobility management. In response to the mobile sub-scriber pressing the SEND button on the terminal, the terminal sends an ORGINATION message to set up a call. This message contains the called party number and three identifiers of the mobile terminal (see Section 4.2.2): the telephone number (MIN), the electronic serial number (ESN), and the station class mark (SCM). The mobile station transmits a PAGE RESPONSE message on the RECC when it detects its MIN in a PRGE message on the FOCC. Like the ORGINATION message, the PAGE RESPONSE message contains the MIN, ESN, and SCM of the mobile terminal. AMPS uses REGISTRATIOIN messages to keep track of the locations of terminals before a call is set up When a terminal is in the service area of its home system, REGISTRARION messages can reduce the number of PAGE messages necessary to deliver calls to cellular phones. In the absence of registration, every cell in the home system sends a PAGE message in an attempt to set up a call to a mobile terminal. In a large system, with hundreds of base stations and hundreds of thousands of subscribers, the volume of PAGE messages can overwhelm the capacity of the system to transmit them. When terminals register their locations, the system can restrict the transmission of PAGE messages to cells in the vicinity of the cell that received the most recent REGISTRATIOIN message, and greatly reduce the volume of PAGE messages.

Registration is essential to deliver calk to terminals that are roaming of their home service areas. On receiving a REGISTRATION message from a roaming terminal, a system informs the terminal's home system of the terminal's present location. Home systems and visited systems.

The two messages that the terminal can send on the RVC during conversations are both responses to messages received on the FVC. This Reflects the hierarchical nature of AMPS, with control operations concern Traded in the MTSO. A CRLLED-STATION RDDRE5S message contains a telephone number entered into the terminal's memory by the user. This Message is a response to a SEND CALLED-RDDRESS message received from the Base station. An ORDER CONFIRMATION message acknowledges the receipt of a Message sent to the terminal such as a power control command.

4.6 Amps Protocol Summary

Figure 4.13 summarizes the AMPS transmission technologies presented in Sections 3 .3, 4.4, and 4.5. All information leaves a terminal or base station in the form of a frequency modulated carrier confined to a bandwidth of 30 kHz. The transmitted signal can convey analog user supervisory audio tone (SAT) at 5,970 Hz, 6,000 Hz, or 6,030 Hz. Traffic information, network control messages, and signaling tones, including a channels can also carry, as an on-hook indication, a 10 kHz supervisory tone (ST). Each network control message is a sequence of from one to five code words. The message is carried on one of four types of logical channels. Each

Logical channel has its own code-word length, channel-coding techniques, and added synchronization codes. The modulation technique for all four logical channel types is frequency shift keying with a deviation of +or- 8kHz from the carrier.

4.7 Tasks Performed by AMPS Terminals

Thus far Chapter 3 has described the capability of AMPS to move network control messages between base stations and mobile stations. We now examine how AMPS uses these messages to establish and maintain telephone calls. To do so, we first look inside a Terminal and observe that at any instant we can identify a "task" being performed by the terminal. The AMPS specification defines a large number of tasks. Each can be

viewed as one state of a finite-state machine. The terminal moves from one task to another in response to a specific stimulus such as the completion of a task, a message received from the base station, an action on the part of the subscriber, or a measurement performed by the AMPS terminal itself.

As indicated in Figure 4.14, there are four modes of operation: Initialization, idle, access, and conversation. Each mode consists of a sequence (of tasks. When a successful communication takes place, the terminal cycles through the four modes, following the heavy lines in Figure 4.14.

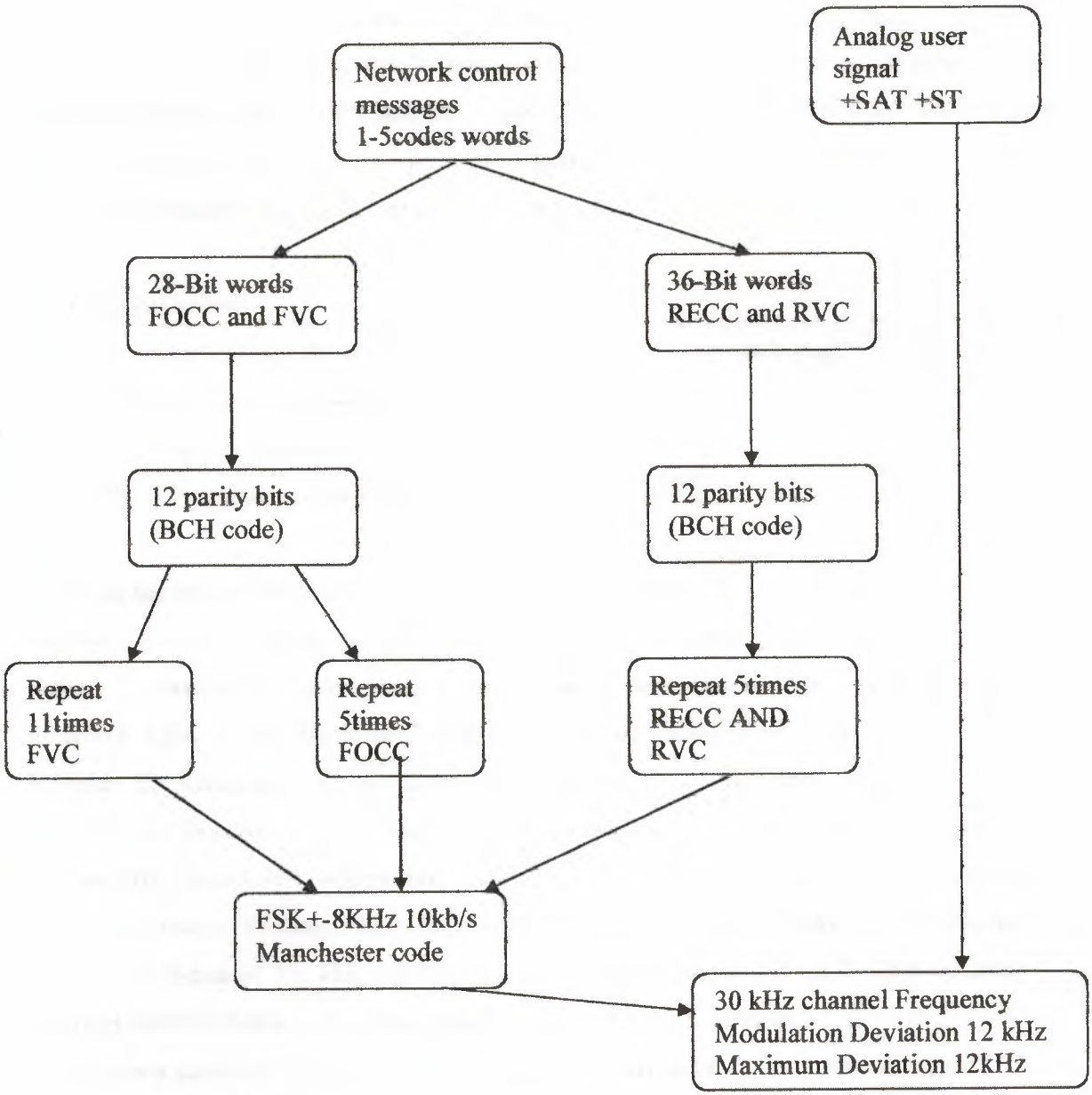


Figure 4.13 Summary of AMPS Transmission Protocols

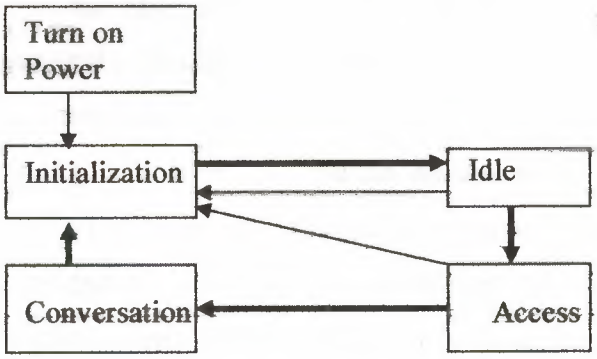


Figure 4.14 Cellular Terminal Operating Modes

However, at any point during the normal sequence of operations it is possible the Terminal to lose contact with the base station. If this occurs, or if the terminal cannot complete a specific task successfully (such access to the RECC), the terminal returns to the initialization mode, as indicated by the light lines in Figure 4.14. If this happens while the terminal is in the access mode, a call attempt or a registration attempt fails. If it happens prematurely during a conversation, the system drops a call in progress.

4.7.1 Initialization

Several conditions place the terminal in the initialization mode, including:

1. The user turns the power on
2. A Conversation ends, or
3. The terminal loses contact with the current base station

To begin the initialization process, the terminal scans either 21-control channels (channel numbers 331-33) in the A-band or 21 channels in the A-band). Each terminal begins with a Preference for either the A-band or the B-band (Figure 4.2). In general, the preferred band is the frequency band used by the subscriber's operating company however the subscriber can use the terminal keypad to override this Preference and program the terminal to set either A or B as the preferred band. Each base station continuously broadcasts information in the FOCC format on one of the 21 control channels. In most Systems; the control channels operate with omnidirectional antennas and a reuse factor of 21. This implies that the distance between two cells with the same physical control channels is approximately eight times the cell radius.

The receiver scans the 21 channels in the preferred band and locks on to the strongest one. If no channel in the preferred band is strong enough for accurate reception, the

terminal can scan the other band in search of an adequate control channel. The user can program the terminal to per-form this search. If the telephone is programmed to remain in the preferred band, the terminal continues to scan the preferred band, in hopes of eventually arriving at a location with an adequately strong control channel. If the terminal cannot find a usable control channel, it turns on a visible "no service" display. With cellular telephony becoming a mature service, companies generally provide coverage throughout their service areas, so that a large majority of initialization procedures result in the terminal tuning to an FOCC broadcast by the nearest base station With its receiver tuned to an FOCC, the terminal performs an "update overhead information" task in order to extract important information from the overhead message train broadcast on the FOCC. As described in Section 4.5.2, overhead messages contain the 15-bit identifier of the local cellular system and information about active paging channels in the cell occupied by the terminal. On interpreting these broadcast messages, the terminal decides whether or not to turn on a visible roaming indication. It then tunes to the strongest paging channel operating in the current cell. In all but the busiest cells, there is only one channel transmitting FOCC information, and the paging channel is identical to the original FOCC monitored by the terminal. On completing the initialization tasks, the terminal enters the idle mode. Typically the terminal is in the initialization mode for 5 to 10 seconds.

4.7.2 Idle

Selected on the basis of information obtained during initialization. The paging channel transmits, in the FQCC format, system status information. The terminal records this information and uses it to perform mobility management and call setup procedures. Some of the broadcast messages contain registration parameters that determine how often the terminal transmits a message to indicate its location to the system. Other broadcast messages monitored by the system indicate the Physical channels used as RFCCs in the current cell. In addition to this global information, the paging channel also broadcasts messages directed at specific terminals. These are the eight FOCC messages in Table 4.3 that are not marked with asterisks.

There are several conditions that move the terminal from the idle mode to the access mode.

The most important of these are

A call initiated when the terminal user presses the SFND button,

- An incoming call request detected when the terminal recognizes its MIN in a page message, and
- A registration event stimulated by the value of the parameter REGID received in a *REGESTRATION IDENT* message a terminal can remain in the idle mode indefinitely. It moves to the access mode in response to one of the events listed previously. It returns to the initialization mode when it fails to receive accurate information on the current FOCC. Usually; a weak signal on the FOCC is due to the fact that the terminal has entered a new cell the terminal responds to the weak signal by returning to the initialization mode, which begins with a search for a strong FOCC signal.

4.7.3 Access

In the access mode, the terminal attempts to transmit a message in the RECC format (Figure 4.10) to a base station. To do so it uses a physical channel selected according to information received in the idle mode. This information indicates a set of physical channels available in the present cell for RECC transmissions. The terminal scans the FOCC transmissions on these channels and tunes to the strongest one. It then monitors the global information transmitted by the FOCC on this physical channel in order to extract two access attempt parameters (MAXBUSY and MAXSZTR) that control the access protocol (Figure 4.9). These parameters control the maximum number of times the terminal can attempt to send a message on the RECC.

Upon entering the access mode, a terminal follows the procedure specified in Figure 4.9. When it enters state An in Figure 4.9, indicating that the transmission has apparently succeeded, the terminal waits for a response to the message. In a call setup situation (origination or page response), this system response takes the form of an *INTIAL VOICE CHANNEL* message, which orders the terminal Transmission. On receipt of this message, the terminal tunes to the designated physical channel and enters the conversation mode. If the terminal has entered the access mode to register its location, it waits for a CONFIRM REGISRTAION message and eventually returns to the initialization mode. Figure 4.9 indicates that the access protocol can direct the terminal to return to the initialization mode (state B) if the number of access attempts exceeds one of the limits specified by the system. This occurs when the RECC is

congested or the signals transmitted by the terminal encounter too much attenuation or interference to be accurately received at the base station.

When it enters the access mode, the terminal sets a timer with duration of 12 seconds for an origination and 6 seconds for any other task if this timer expires, the terminal returns to the initialization mode, regard-less of the current status of the access protocol

4.7.4 Conversation

With a mobile station in the conversation mode, the system serves its ultimate purpose- to connect a mobile station to any other telephone in the worldwide Public Switched Telephone Network. The technical name for the conversation mode is *mobile station control on THE voice channel,* and, in fact, various control operations have to take place before a conversation can begin. On entering the conversation mode, the terminal first indicates to the system that it has properly complied with the order to tune to a traffic channel. The SAT transmitted by the terminal (see Section 4.3.3) provides this confirmation. The terminal enters the conversation mode in response to an INTIAL VOICE CHANNEL message. Like the HAND*OFF* message (Table 4.4), this message contains an SAT color code indicator that specifies the SAT (5,970 Hz, 6,000 Hz, or 6,030Hz) of the assigned base station. The base station transmits the specified SAT in the forward direction and listens for the SAT on the corresponding reverse channel. The mobile station confirms that it has properly selected a voice channel by transmitting the SAT received from the base station. The tuning procedure is complete when the base station detects the correct SAT transmission from the mobile station.

4.7.5 Phone Call Examples

If the call originates at the terminal, the base station confirms to the MTSO that the Turing procedure has succeeded and the MTSO completes the call through the public network. Figure 4.15 displays the sequence of messages and control operations that set up and release a call originating at a mobile station.

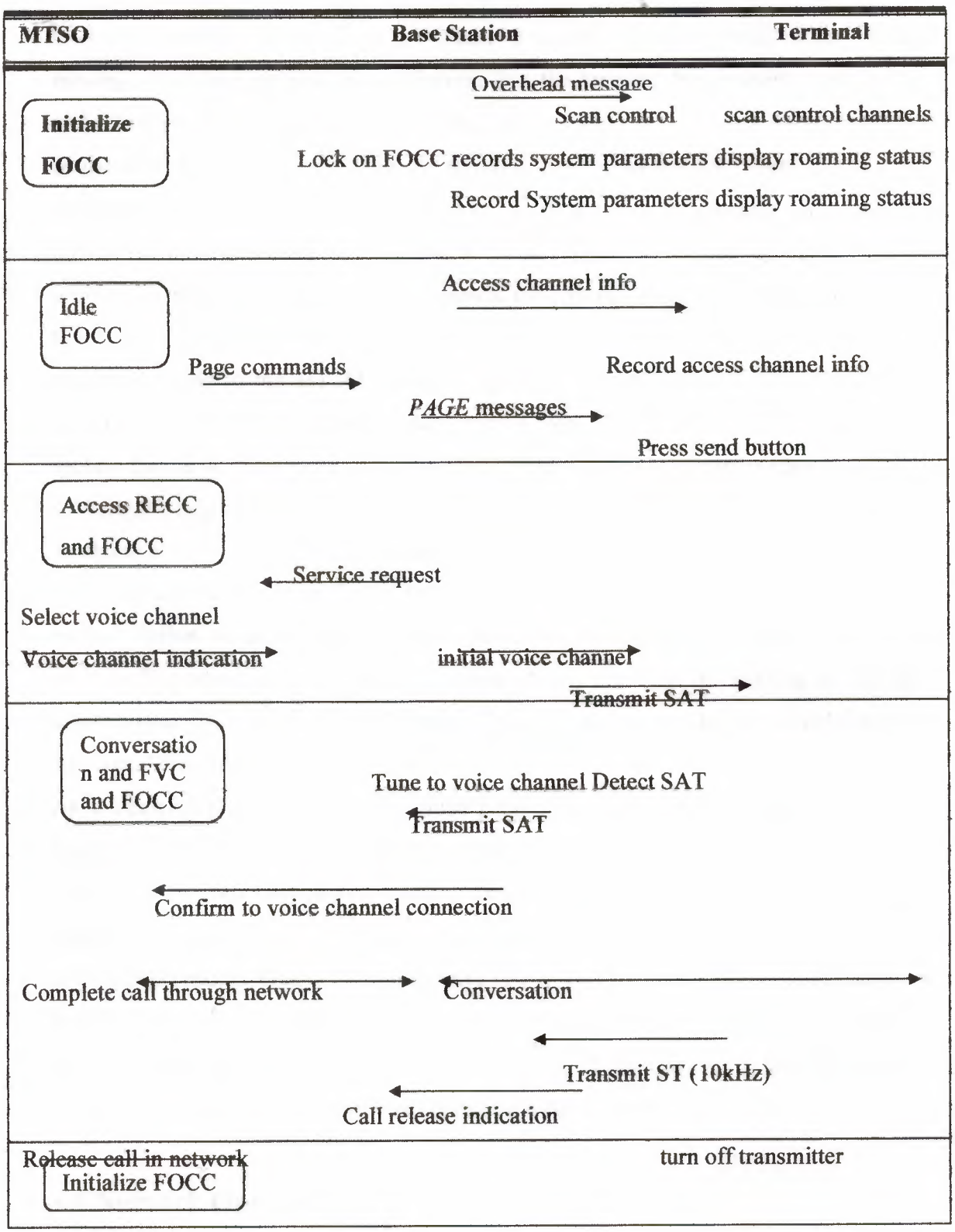


Figure 4.15 Network Control Sequence For A Call Originating At A Terminal. The Call Ends When The User Presses The End Button

If the call originates in the public network, the terminal enters the conversation mode after it transmits a *Page response* message and receives an *initial voice channel message.* The base station, on confirming that the terminal has properly tuned to the correct voice channel, sends an *ALERT* message

In the FVC format *this* stimulates the terminal to emit *an* audible (beep) that prompts the user to respond to an incoming call. Until User responds by pressing one of the keys on the terminal, the stops transmit a 10 kHz supervisory tone indicating that the terminal is oh hook. When the user responds, the terminal stops transmitting the 10 kHz tones, an event that tells the base station that the call can begin. The base station signals this information to the MTSO, which then completes a voice path to the person who placed the call. The base station also sends a *stop ALERT* message to command the mobile station to turn off the audible -tone. This sequence of events is shown in Figure 4.16, which begins with the terminal in the idle mode. Initialization procedures conform to those shown in Figure 4.15.During the call, the base station can send a *order confirmation* message (see Table 4.5) on the forward voice channel to command the mobile station to adjust its transmitter power to one of the eight levels defined by AMPS. The terminal acknowledges receipt of this message by sending an *ORDER confirmation* message in the RVC format. The base station can also command a handoff and signal the end of the conversation.

As in a conventional telephone call, either party can conclude the call. If the remote user hangs up first, the base station sends, in the FVC format, a *RELERSE* message to the terminal. The terminal acknowledges this message by transmitting the 10 *kHz* supervisory tones for 1.8 seconds. It then *turns* off its transmitter and returns to the initialization mode. This sequence appears *in* Figure 4.16. *If* the mobile user hangs up first, by pressing the END button, the terminal signals this event to the base station by sending the 10 kHz tone for 1.8 seconds. As indicated in Figure 4.15, the terminal then turns off its transmitter and returns to the initialization mode.

4.8 Network Operations

The earlier sections of Chapter 3 present the techniques available for per-forming the six categories of operations, listed in Table 2.3. Section 4.3 describes in detail AMPS technologies for user information transport and Section 4.7 provides a comprehensive survey of call management in AMPS. This section summarizes the AMPS procedures

that contribute to the three sets of network management operations that play a critical role in wireless commendation: mobility management, authentication, and radio resources management.

4.8.1 Mobility Management

In the manner described in Section 2.3.2, idle AMPS terminals periodically transmit *registration* messages on a reverse control channel to indicate their locations. The time intervals between REGISTRATION messages are controlled by REGISTRATION IDENT messages broadcast on a forward control channel. By transmitting these messages at frequent intervals, a system causes terminals to register their locations frequently and thus provide accurate Information about their locations. This information allows the system to restrict the number of cells in which it pages terminals that receive phone calls from the network. Each system adjusts the rate of registration to balance the burdens placed on control channels by *REGISTRATION* messages and *PAGE me*ssages. The AMPS system gives network operators considerable flexibility in adopting paging and registration strategies. One sophisticated approach is to monitor messages in order to determine subscriber mobility patterns [Madhavapeddy, Basu, and Roberts, 1995J. The system then refers to these patterns to devise a sequential paging strategy, in which it sends *PRGE* messages first to the cells most likely to be occupied by a terminal. If it receives no response to the initial page messages, the system pages the terminal in the remaining cells. This has the effect of reducing the number of *PAGE* messages relative to simpler approaches. To gain this information, the system has to acquire, store, and analyze information about mobility patterns.

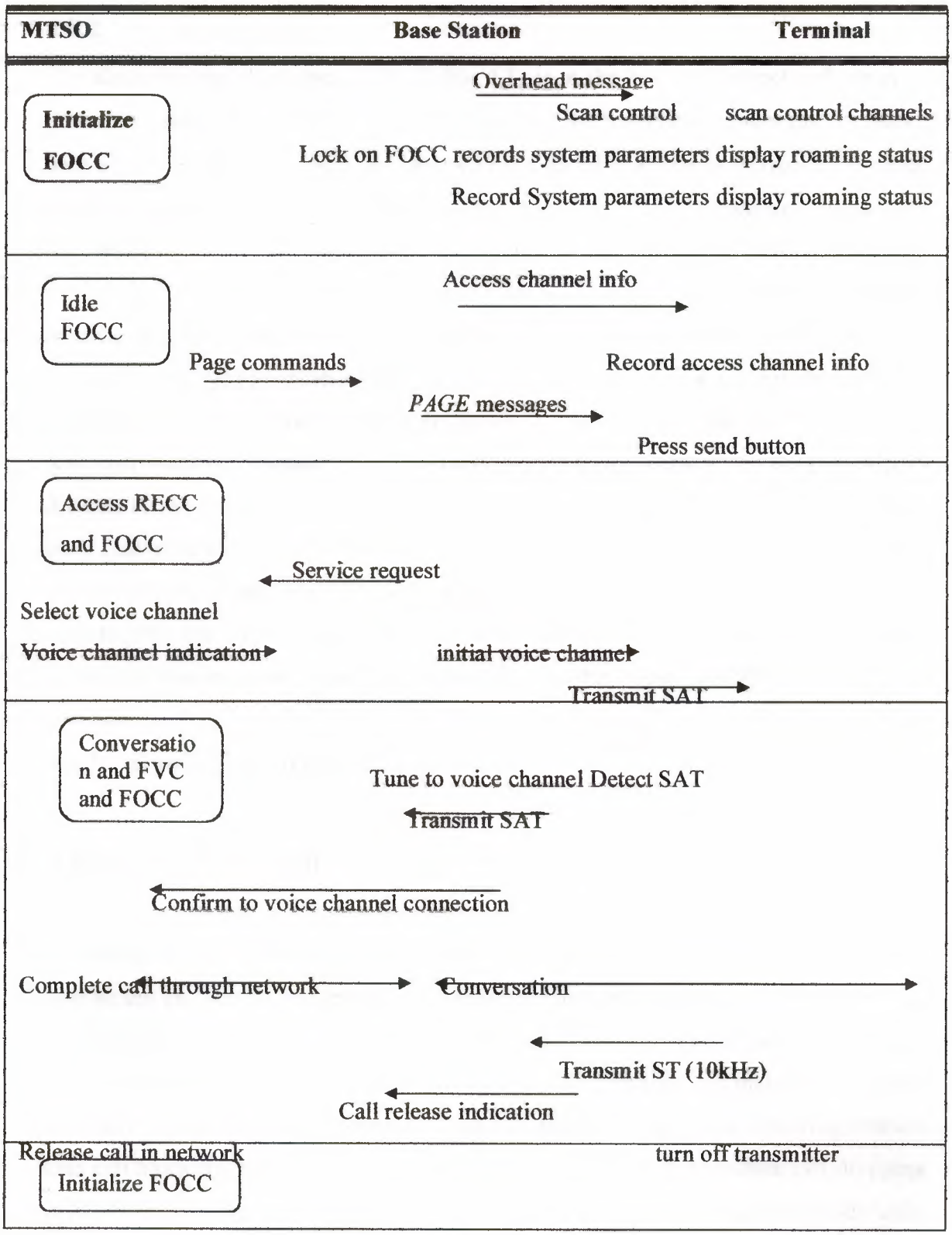


Figure 4.15 Network Control Sequence For A Call Originating At A Terminal. The Call Ends When The User Presses The End Button

4.8.2 Authentication

The electronic serial number (FSN, Table 4.1) is at the heart of the network security procedures built into AMPS. To gain access to AMPS services, a terminal transmits both its mobile identifier (MIN in Table 4.1) and its ESN. As the subscriber's telephone number, the MIN is considered public information. The ESN, installed electronically in the terminal, is considered private information; belonging to the cellular operating company a database in the subscriber's home MTSO records the ESN. &Fore granting a terminal access to the network, the MTSO verifies that the transmitted ESN is the correct one for the subscriber's MIN. In this sense, the ESN is like a computer password or a personal identification number (PIN) used at automatic teller machines. Just as computer security depends on the secrecy of passwords, network security in AMPS depends on the secrecy of the ESN. This turns out to be a major weakness of AMPS and other first-generation cellular systems. &Cause mobiles transmit their ESNs through the air; the MIN/ESN pair is subject to interception and fraudulent use. In response to this vulnerability the systems we study in later chapters all incorporate authentication procedures that are more secure, and more elaborate, than those of AMPS.

4.8.3 Radio Resources Management

4.8.3.1 Call Admission

In AMPS, the call admission policy is part of the MTSO software. The simplest policy is to accept any service request that arrives when there are inactive physical channels in the cell occupied by the terminal requesting service and to deny service when all physical channels are in use procedure minimizes call blocking, but makes the 5' 5-tem relatively vulnerable to call dropping. Since call dropping is far more annoying to users than call blocking, Systems adopt *channel reservation* schemes to reduce call dropping at the expense of higher blocking rates. To do so, the system denies service to new calls when there is a small number of an inactive channel in a cell, and reserves these channels to satisfy handoff requests.

4.8.3.2 Channel Assignment and Power Control

With respect to base station and channel assignment, AMPS generally assigns a new call to an available channel at the nearest base station. However, to balance the load over a group of cells, systems can employ a *directed retry* procedure, by which the nearest base station commands a terminal to attempt to gain service through a nearby base station that is less congested than the nearest one. An AMP has the capability for dynamic power control over transmissions from terminals. It does so by commanding each terminal to transmit at one of eight power levels (see Section 4.3.2) listed in the system specification. The system uses *CONTROL FILLER* messages on the forward control channel to specify the power level (parameter CMAC) for transmissions on a reverse control channel (see Section 4.5.2). The initial power level for transmissions on traffic channels (VMAC) is specified in INTIAL VOICE CHANNEL messages and HANDOFF messages (see Table 4.4). As the terminal changes location within a cell, the system can command it to change its power level by transmitting ACHANGE POWER *LEVEL* message (see Table 4.5) on a forward voice channel.

4.8.3.3 Handoff

Perhaps the most impressive property of a cellular telephone system is its ability to maintain calls as mobile stations move from cell to cell or into different sectors of cells operating with directional antennas. In AMPS, handoff from one base station to another is controlled by the MTSO, which assembles measurements of received signal strength from the current base station and surrounding base stations. Each system has its own proprietary handoff algorithm, which typically consists of a set of signal strength thresholds, referred to as *RSSI (received signal strength indication) levels.* One threshold, typically around 100 dBm, is the level at the current cell that causes the system to initiate a hand off. &Low this level; AMPS may be unable to maintain adequate voice quality. Another, higher, threshold, perhaps 90 dBm, is the signal strength required at the new cell. The difference between these two thresholds introduces hysteresis, which inhibits repeated handoffs as a mobile station moves along the boundary between two cells. The handoff algorithm may also be designed to limit call dropping due to overload by considering the number of active channels in candidate

cells before directing a call in progress to a new cell. In addition to handoff from one cell to another, the base station can also initiate an "intracell" handoff to another channel in the same cell. Typically, this type of handoff takes place in response to the mobile station moving to a new sector, served by a different directional antenna. When the system control software decides to initiate a handoff, the sequence of messages in Figure 4.17 begins. First, the base station transmits, over the current physical channel, a HANDOFF message in the FVC signal format. This message includes the new channel number, an indication of the SAT in the new cell, and the initial transmitter power level (VMAC). The terminal acknowledges this message by transmitting the 10 kHz supervisory tone for 50 ms. It then turns off its transmitter, tunes to the new channel, generates the SAT of the new cell, turns on its power, and resumes voice transmission

4.9 AMPS Status

With respect to both technology and commerce, AMPS is a major success story. However, since the late 1980s, the cellular industry has recognized the need for improvements in several areas including capacity, roaming, security, and support for non-voice services. All of these issues are addressed by new technology described briefly in the previous paragraphs and in detail in Chapters 1 and 2.

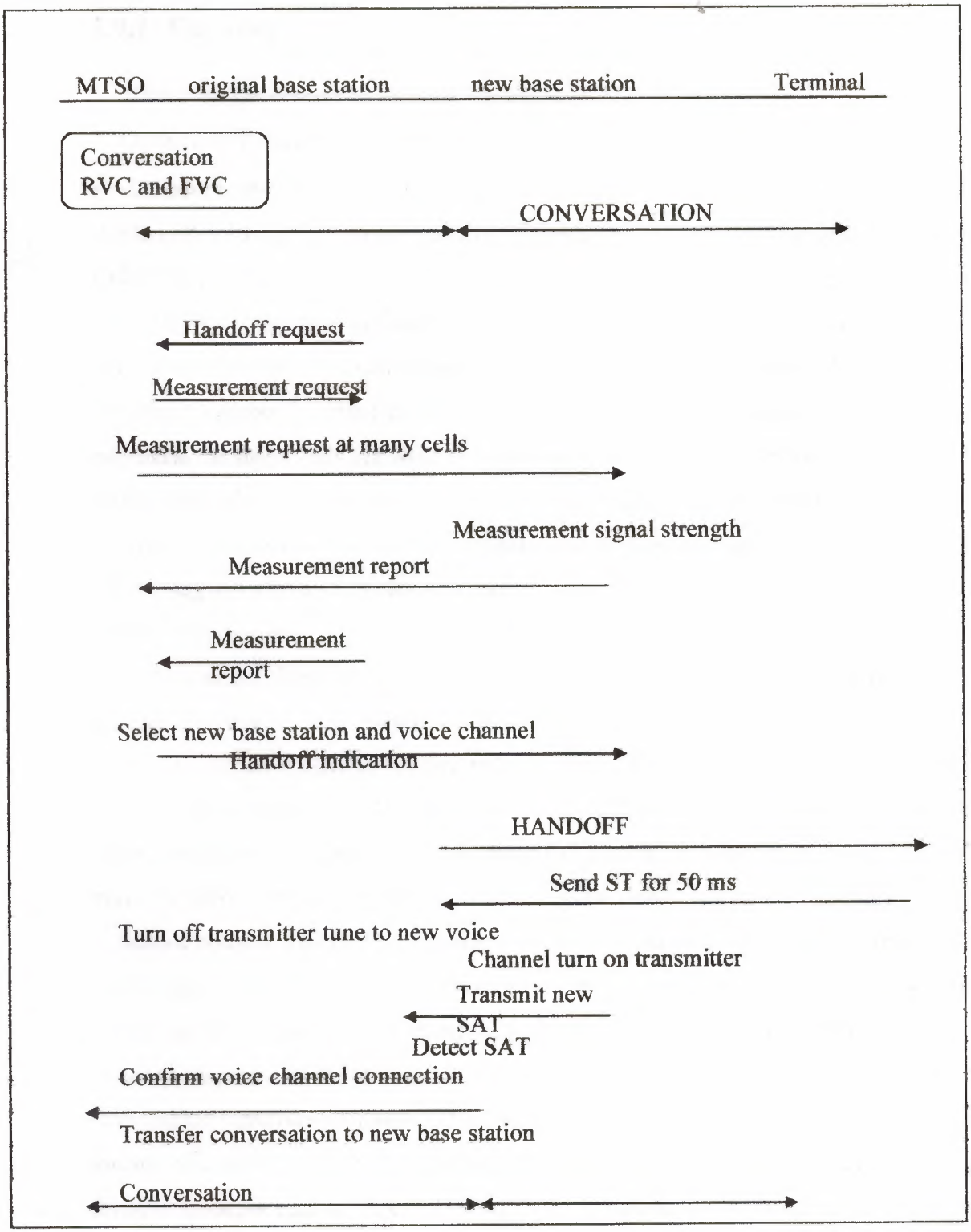


Figure4.17 Network Control Sequence For Handoff

3.9.1 Capacity

There are three ways to increase the capacity of cellular systems:

- Operate with smaller cells, obtain additional spectrum allocations, and
- Introduce new technology to improve spectrum efficiency.

While cell-splitting to increase capacity is fundamental to the cellular idea [MacDonald, 1979], this approach has its limitations. *Using* the original, high-power, high-elevation base stations of cellular systems, the practical lower limit on cell radius is around 1.5 km [Mehrotra, 994]. To achieve smaller dimensions, companies install low-power, low-elevation *micro*cells [Steele, 1992: 24-41] in densely populated areas. In many instances, the microcells are within the service areas of larger, conventional cells. Thus, many terminals in microcells have access to at least two base stations, one serving a low-power microcell and the other operating in a conventional high-power mode. This situation raises a host of challenging radio resources management issues.

Beyond the practical problems of operating with small cells, cell splitting is the most expensive of the three approaches to increasing capacity. With respect to the preferred approach, obtaining new spectrum, the U.S. Federal Communications Commission, in the ^{19}80s, added 10 MHz to the original 40 MHz allocation of radio spectrum to cellular services (see Figure 4.2). The FCC then announced that no additional cellular band-width would be available. However, the FCC also issued new rules [FCC, 1990a] to make the third approach to capacity enhancement, deploying new technology; available to license holders. The FCC encouraged operating companies to adopt new transmission technologies by permitting each operating company to transmit signals in any format, providing the signals do not interfere with the signals of other license holders. The industry response to these rules is embodied in three transmission technologies that have higher spectrum efficiency than AMPS. Two of them transmit speech in digital format, one using time division multiple access [TIA, 1996dJ and the other using code division multiple access (TIAA, 1993b). They are presented in detail in Chapters 5 and 6, respectively The third new technology NAMPS, based on analog speech transmission, closely resembles AMPS and is described briefly in the following paragraphs.

Motorola developed Narrowband AMPS [TIA, 1993a] in response to uncertainties about the relative merits of the two digital standards and Uncertainties about when they

would be available in commercial products. Operating companies use NAMPS technology to provide a short-term solution to capacity problems and then introduce the preferred digital standard after uncertainties are resolved. NAMPS gains its capacity advantage by dividing an original AMPS channel into three narrowband channels; one with a carrier frequency equal to an AMPS carrier (Equations 4.1 and 4.2), and the other two offset by +10 or –10 kHz relative to an AMPS carrier. The modulation technique on a narrowband channel is FM with a maximum deviation of 5 kHz from the carrier.

NAMPS is a dual-mode system, so that all NAMPS terminals are capable of operating with 30 kHz channels as well as 10 kHz channels. In a system not equipped for NAMPS operation, the dual-mode terminal functions a conventional AMPS terminal. NAMPS employs the AMPS control channels for call setup and the call management sequence conforms to Figure 4.14. In the access mode, an *INTIAL VOICE CHANNEL* message on a forward control channel directs a NAMPS terminal to either a wide traffic channel (30 kHz bandwidth) or a narrow traffic channel (10 kHz bandwidth). NAMPS systems are capable of four types of handoff: wide channel to wide channel, wide to narrow, narrow to narrow, and narrow to wide.

In the conversation mode, network control in NAMPS differs significantly from AMPS. Instead of the blank-and-burst operation on forward and reverse voice channels, NAMPS transmits out-of-band control information continuously in both directions over narrow traffic channels. It conveys network control information in logical *associated* control *channels,* which transmit 200 b/s (non-return-to-zero) signals and 100 b/s (Manchester coded) signals in the "sub-audible" (low-frequency) portion of the traffic channel input signal spectrum. Figure 348 shows the contents of an AMPS channel divided into three narrow physical channels. There are four types of network control information:

- Messages similar in format or identical to AMPS messages,
- Synchronization sequences that replace the dotting sequences and Barker codes of AMPS control channels (see Section 4.4.3),
- Digital versions of the AMPS supervisory audio tone (seven possible codes), and a digital replacement for the AMPS supervisory tone.

In addition to transmitting AMPS call management messages and radio resources management messages; NAMPS control channels are capable of

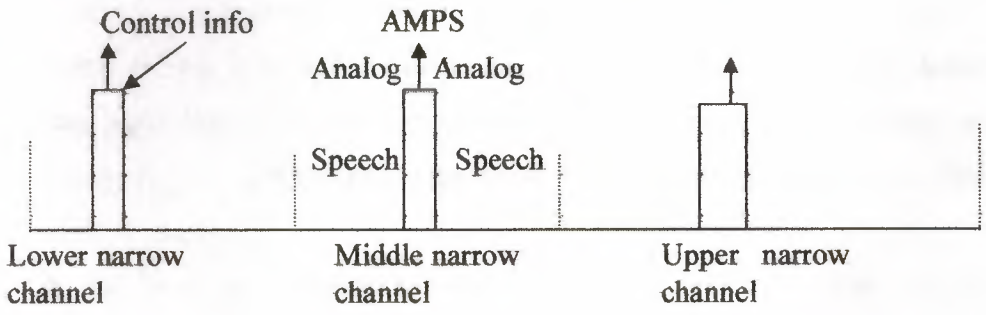


Figure 4.18 Partition Of One AMPS Channel Into Three Narrow Channels, Each Carrying Analog User Signals And Digital Control Signals.

Operating with an extended protocol that brings special features and network services to subscribers, including calling-number identification, voice mail control, and short message services (see Section 2.2.2). The principal purpose of NAMPS is to achieve higher spectrum efficiency than AMPS. In cellular Systems, spectrum efficiency depends on the bandwidth of each signal and also the sensitivity of the signal to interference (see Section 9.3). With its smaller bandwidth, a narrow traffic channel is more vulnerable to interference than a wide traffic channel and would normally require a higher reuse factor (*N* in Section 9.3.2) than AMPS signals have. To control the interference to signals in narrow channels, NAMPS introduces a radio resources management procedure referred to as *mobile reported interference.* To perform this procedure, a terminal measures the received signal strength on a forward narrow traffic channel and the binary error rate of the control signals on the associated control channel. When the measurements go outside of a range specified in a message sent by the base station, the terminal reports these measurements to the base station by means of a message on the reverse associated control channel. Based on this report, the system can initiate a handoff in order to improve signal quality.

4.9.2 Network Security

The AMPS authentication procedures are Weak. They rely on the secrecy of each terminal's electronic serial number (ESN). The terminal transmits this number on a reverse control channel each time it initiates a call, responds to a *page* message, or registers its location. As a consequence, the FSN can be intercepted by radio receivers

tuned to AMPS control channels. People who operate these receivers illegally use the serial numbers to gain unauthorized access to cellular systems. This activity referred to as *cloning,* is highly prevalent and a matter of great concern to the cellular industry. To address this problem, network operators have introduced a variety of measures. A common one is to require each sub-scriber to key in a personal identification number each time she makes a phone call. The terminal transmits this number on a reverse voice channel, making it somewhat harder to intercept than the ESN transmitted on a common control channel.

In addition, the industry has devised robust network security technology based on encryption and secure key distribution. These measures, which are integral parts of the digital systems, these cryptographic authentication techniques were introduced to analog systems. However, they have to be implemented at terminals, as well as at base stations and switching offices. Therefore, they are available only to subscribers with new terminals that incorporate the secure authentication technology. Tens of millions of existing terminals remain vulnerable to cloning.

4.9.3 Non-Voice Service

A growing proportion of the population uses telephone lines to gain access to a wide variety of digital information services such as facsimile, electronic mail, the World Wide Web, and a large collection of specialized services. The data protocols that link fax machines and personal computers to these information services in many situations suffer severe performance degradation in the presence of the interference levels on cellular channels as well as the signal interruptions caused by handoffs and blank and-burst transmission of signaling information. To cope with these problems, advanced cellular systems apply several approaches. One approach is to convey short text messages through special logical channels, as in NAMPS and North American TDMA. Another approach is to introduce a separate packet data network, cellular digital packet data [CDPD Forum, 1995] that transmits its own signals through ANMPS logical channels. A third approach is to incorporate special signal processing methods for signals moving to and from telephone data modems and fax machines.

CONCLUSION

As it had shown the many kind of working system of a cell phone and it have been discussed how it works.

We come up with one of the best sytem it has been recommended to use based on this study which is the AMPS system,

AMPS delivers basics of telephony and supplementary services of which voice mail and call forwarding are the most popular, although it is possiple to transmit digital data over AMPS channel, service quailty is vulnerable to channel impairments and handoffs .

The main desgin goals of AMPS and other first-generation systems were wide area geographical coverage, low probabilities of call blocking and call dropping, high transmission quality, high user mobility, high spectrum efficiency, and early deployment.

REFERENCES

[1] Vineet Sachdev, System Engineer

[2] Trueposition Inc. 1111 West DeKalb Pike Wayne, PA 19087

[3] Asha Mehrotra, "GSM System Engineering"

[4] MOBILE COMMUNICATIONS SERIES, Artech House Publishers.

[5] Brian McIntosh "Telecommunications"
http://telecomindustry.about.com/business/telecomindustry/library/weekly/aa1115999.ht

[6] Dick Tracy "The Applications We Promote...." http://www.comm-nav.com/commnav.htr

[7] GRAYSON WIRELESS, a division of Allen Telecom. "Geometrix Wireless Location Sensor" http://java.grayson.com/geodatasheet.htrr

[8] Louis A. Stilp "Examining the Coming Revolution in Location Services" http://www.trueposition.com

[9] Paul J, Bouchard "AccuCom Wireless Service Inc." http://www.Global-Images.com

[10] Tutorial "How GPS works?" http://www.trimble.com