NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

HOW CELL PHONE WORKS

Graduation Project
EE- 400

Student: Hani Albreem (971248)

Supervisor: Mr. Jamal fathi

Lefkoşa - 2001

ACKNOWLEDGEMENTS

First I would to thank MR. Jamal Fathi to be advisor. Under his guidance, I successfully overcome many difficulties and learn a lot about my project. In each discussion, he explained my questions clearly, and I felt my quick progress from his advises.

Asst. prof Fa'eq Radwan He always help me a lot either in my study. I asked him many question in mathematics and he always answered my questions quickly and in details. Thanks to faculty of engineering for having such a good computational environment.

Finally, I would to thank my family, especially my parents. 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 in the heaven be proud of me.

TABLE OF CONTENTS

ABSTRACT

Mobile unit in the user's vehicle consist of a receiver containing amplifiers. a mixer and demodulator; a transmitter conatining a modulator . carrier oscillators and amplifiers:the necessary control logic : a control unit with microphone. speaker. keypad and switches; antennas and interconnecting cables. The control units perform all of the funcions associated with normal telephone use . the mobile telephone user places and receives the call. in the same manner as with an ordinary telephone.the thing is differnce between the normal teephone and mobile telphone is mobility of the radio link and worldwide switched network of the existing telephone system to provide a communiction link to any other telephone in the world.

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.

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.

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.

CHAPTER ONE

AN OVERVIEW OF CELLULAR SYSTEMS

1.1 Introduction

In this chapter we briefly present the concept of cellular communication and discuss the first- and second-generation cellular systems used in United States and Europe. We outline the problems associated with the second-generation-plus PCS system and provide the vision of a third-generation system.

1.2 Concept Of Cellular Communication

The idea of cellular communication is simple. During the late the bell system proposed to alleviate the problem of spectrum congestion by restructuring the coverage areas of mobile radio systems. The traditional approach to mobile radio involved setting up a high-power transmitter located on the top of the highest point in the coverage area. the mobile telephone needed to have a line of sight to the base station for adequate radio coverage. Line of sight transmissions limited to the distance to horizon (as much as 40 or 50 miles away for a high base station antenna). The result adequate coverage over

A large area. It also implied that the a few available radio channels were locked up over a large area by small number of users. In 1970 the bell system in New York City could support just 12 simultaneous mobile conversations. The 13th caller was blocked. The cellular concept handles the coverage problems differently. It does not use the broadcasting method; it uses a large number of low-power transmitters designed to serve only a small area.thus, insted of an area like New York city being covered by a single transmitter, the city was divided into the smaller coverage areas called |cells. BY reducing the total coverage of area into smaller cells, it with small cells was that not all mobile calls would now be completed within a single cell. To deal with this problem, the idea handoff of was used.

It is enormously expensive to build a system with thousands of cells right from the beginning.however; larage-radius cells can evolve gracefully into small-radius cells over a period of time using cell-splitting. When the traffic reaches a point in a particular cell such that the existing allocation of channels in that cell can no large support a good grade of service, that cell is subdivided into smaller cells with lower transmitter power to fit within the area of the former cell.

Thus the essential elements of a cellular system are:

1- Low-power transmitter and small coverage areas or cells

2- frequency reuse

3- handoff and central control

4- cell splitting to increase call capacity

1.3 First-Generation Cellular System

AS the United states was planning its cellular network in the 1970s. England, Japan, Germany, and Scandinavian countries were also planning their systems. Each system used a different frequency band and different protocols for signaling between mobile units its and base stations. They all used analog FM (with during the 1970s the FCC forced the TV broadcasters off the little-used UHF channels 70-84 and made the frequencies available for two-way radio and the new cellular technology. During that time, the Bell system and Motorola actively pursued support for a 900-MHz cellular system using different designs for channel reuse and protocols.

In the late 1970s, the FCC mandated that a single nationwide standard must be developed before licenses for cellular systems would be awarded. The Electronics Industry Association (EIA) formed a cellular standards committee and standardized the Advanced Mobile Phone System (AMP) protocol for the United States.

In1985 the total access communication system (TACS) was introduced in the United Kingdom. TACS is a close relative of North America's Nordic Mobile telephone (NTT). The cellular approach promised virtually capacity through cell splitting. As the popularity of wireless communications escalated in the 1980, the cellular industry faced practical limitations. For a fixed allocation of spectrum, a large increase in capacity implies corresponding reduction in cell size .For example, the U.S AMPS design allows for cells as small as 1,600 meters (m)(1mile). As the cells get smaller, it becomes increasingly difficult to places base station at the locations that offer necessary radio coverage. Also, reduction cell size demand increased signaling activity as more rapid handoffs occur; in addition, base station as required to handle more access requests and registrations from the mobile stations. The problem becomes particularly difficult in large urban areas where capacity requirements are most pressing. In addition to the capacity bottleneck, the utility of the first generation analog systems was diminished by proliferation in of incompatible standards in Europe. The same mobile Telephone frequencies cannot be used in different European countries. The limitations of first-generation analog systems provided motivations to the second- generation systems. The principal goals of the second-generation systems were: higher capacity and hence lower cost, and, in Europe, a continental system with full international roaming and handoff capabilities. In Europe, these goals are served by new spectrum allocations and by the formulation of a Pan-European cellular Standard GSM.

In North America, where one standard (United States, Canada, and Mexico) existed and covered a region as large as Europe, the push for a new system was not as strong. In the new digital systems. Higher capacity is derived from applications of advanced transmission techniques including efficient speech coding. Error correcting channels codes, and band with-efficient modulation techniques. In Europe. The approach was to open new- frequency bands for a pan-European system and not to have compatibility with existing cellular systems. In the United States, the same frequency bands were shared with new digital systems, and the standards supported dual-mode telephones that could be used in both analog and digital systems.

1.4 Technologies For Second-Generation Cellular Systems

Standards and system designs exist for several new and competing technologies for the second-generation cellular systems. They are:

1. Narrow-band Advanced Mobile Phone Service (N-AMPS)

2. Time-Division Multiple Access (TDMA) (already explained in chapter2 section 2.9.2)

3. Extended Time-Division Multiple Access (E-TDMA)

4. Spread Spectrum (SS)-Code-Division Multiple Access (CDMA) (already explained in chapter2 section 2.9.3)

NOT all systems have seen widespread use, and some may disappear. The following sections provide a brief description and status of these technologies

1.4.1 Narrow-Band Advanced Mobile Phones Service (N-AMPS)

Motorola developed N-AMPS by dividing an analog channel into three parts; thereby tripling the present analog channel capacity Bandwidth per user is decreased from 30 kHz to 10 kHz. Each new channel is capable of handling its own calls. N-AMPS acts primarily as a bridge to digital communications that allows cellular systems to increase capacity at a low cost.

A smaller bandwidth per user in N-AMPS results in a slight degradation in speech quality that is compensated for with the addition of an interference avoidance scheme called Mobile Reported Interference (MRI). This capability, along with full call control (e.g., conference call, call waiting, call transfer, handoff, power control) is provided using a (new) continuous 100 bits per second (bps) in- band, sub-audible, signaling control channel. This scheme has the additional benefit of eliminating the audio gaps typical in the AMPS blank and burst-signaling scheme. The associated control channel can also be used for sending alphanumeric characters when not actively managing call control. It has been typically used for features such as displaying calling line identification numbers, as well as features similar to those provided by an alphanumeric pager. This capability has allowed for the combining of cellular and paging applications in a single device. N-AMPS was standardized as EIATIA IS-88, IS-89, and IS-90 in late 1992. In 1993, IS-88 and IS-553 (AMPS) were combined to form a single analog standard called IS-91. N-AMPS has been implemented in both U.S. and international markets.

Although there has been some concern about the ultimate capacity of N- AMPS, many operators have chosen to implement N-AMPS in the identical reuse pattern as the original AMPS design. With trunking efficiencies excluded, this results in three times AMPS capacity. In a typical international market, up to 90% N-AMPS penetration has been achieved using a four-cell reuse pattern with very small (500 m) cell radii. It has been claimed by those operators that audio quality is at least as good as the AMPS systems they replaced. In addition, they report that overall dropped call performance is considerably less than AMPS due to the signaling enhancements made to the N-AMPS air interface.

1.4.2 Extened Time-Divsion Multiple Access (E-TDMA)

General Motors' (GM's) effort to enter the cellular market uses E-TDMA. E-DMA uses half rate voice coding at 4.5 KB that requires only one IS-54 time slot and thus allows six calls per frequency. Digital Speech Interpolation (DSI) permits deleting silence on calls. It thus reduces activity by 55-65% and allows more calls to be handled by the same number of time slots. E-TDMA is claimed to increase capacity by 12 times that of AMPS and 4 times that of IS-54. GM plans to include E-TDMA mobile phones in a future automobile model. E-TDLA supporters must solve many technical problems. Voice quality being the most important one. Furthermore. None of the cellular carriers seem to be interested in deploying it. E-TDMA does not appear to be a serious contender in the digital technology.

1.5 Cordless Phones And Telepoint Systems

Closely related to cellular and often confused with the mobility aspects of cellular and PCS are cordless phones and Telepoint systems. Cordless phones are e the low-power, low-range phones that enable an individual to move around a house or apartment and still place and receive phone calls. First-generation cordless telephones are stand-alone consumer products they do not require any interoperability specifications at all. Each cordless telephone comes with its own base station and needs to be compatible only with that base station. The billing, security, and privacy are achieved (to a limited degree) by preventing the phone from operating with any other base station. Because of the popularity of cordless phones and the inability of some telephone companies to maintain public telephones in large cities, a hybrid approach was conceived, called "Telepoint" In the Telepoint system, the user owns a small low-power phone (similar in size and functionality to a cordless phone). The Telepoint phone works within 100 m of a public base station. The phone typically cannot receive calls and can place calls only when in range of the base station. The user would walk or drive within range of the base station and place the call. Roaming is not supported; the user must remain within range of the base station or the call is dropped. This concept, based on a limited frequency allocation, was implemented as the Cordless Telephone-1 (CT- 1) 900-MHz analog system. It was implemented or proposed in 13 European and Scandinavian countries. Different incantations of the design can serve residential (wireless local loop) or public pay phone markets. CT-1 was intended to serve the residential market. An enhanced version; CT -1+, is similar to CT- 1, but has added Telepoint capabilities. CT-1 uses FDMA, in which a single channel per radio carrier frequency is employed. CT-1 carries multiple narrowband carriers within a frequency band. Duplex operation, i.e., the simultaneous transmission and reception of voice signals, is implemented using separate frequencies.

Once the concept of a small low-power phone was introduced, designs were evolved to Support wireless PBXs, cellular phones, PCS, and neighborhood wire- less local loops. Often the system designs for second-generation cordless phones and Telepoint systems and the designs for digital cellular systems overlap.

The culmination of research in digital technologies resulted in CT- 2, CT- 3/ DCT-900 and DECT standards for cordless telephones/Telepoint in Europe. These systems are being offered for a variety of uses-cellular, PCS, cordless phones, Telepoint, and wireless PBXs.

Cordless phones in the United States have either used FM in the 46/49-MHz band or SS in the 902-928-MHz band. Telepoint systems have not seen widespread use in the United States.

1.6 Second-Generation Cellular Systems

First-generation cellular systems were designed to satisfy the needs of business customers and some residential customers. With the increased demand of cellular telephones in Europe, several manufacturers began to look for new technologies that could overcome the problems of poor signals and battery performance. Poor signals resulted in poor performance for the user and a high frequency of false handoffs for the system operator. Better battery performance was needed to reduce size and cost of self contained handheld units (handsets). Research efforts were directed toward wireless technologies to provide high-quality, interference- free speech and decent battery performance. The size of handset and better battery performance led to low-power designs and performance targets possible only with fully digital technologies. Digital cellular systems based on the GSM (TDMA) standard have emerged in Europe, while systems based on IS-54 (TDMA) and IS-95 (CDMA) are being developed in the United States. Table 2.2 provides a summary of the cellular and cordless systems.

The following sections describe the CT 2, DCT 90OfDECT/CT 3, GSM, IS-54, and IS-9 systems and point out the main differences between them.

1.6.1 CT- 2

The handsets used in offices and homes these systems were developed for residential, business, and Telepoint applications in the United Kingdom. The handsets used in offices and homes were provided with a "value-added" public service from base stations located in railway stations, airports, and shopping centers. Although business and residential use of CT- 2 offered full incoming and outgoing call facilities, Telepoint service was limited to outgoing calls only The United Kingdom chose FDMA for CT -2 to meet the original goal of a simple, single-user, home mobile telephone that avoids interference at call setup and supports multichannel multiplexing or handoffs. FDMA/TDD meets the needs for simple single-user channelization and simple measurement of signal power for a frequency channel from both ends of a radio link.

With the introduction of Telepoint and Wireless Private Branch Exchange (WPBX) applications in the United Kingdom, there was a need for a handset user to roam between different Telepoint operators' base stations and WPBX products. Therefore. The message protocols across the air interface needed to be well defined and common to all users. This resulted in the Common Air Interface (CAI) concept for CT- 2.

CT- 2 uses 4 MHz of spectrum, from 864 to 868 MHz, divided into 40 100- kHz channels. On each channel, the base station and mobile station alternate in the transmission of TDD data packets. The TDD rate, the rate at which base station

And mobile stations switch between "send" and "receive" is set at 500 Hz-1 ms each for send and receive. Power from both the mobile and base stations is restricted to I0 mW, and the mobile station selects the channel with the lowest noise. The mobile station is frequency agile during a call if the bit error rates on the selected channel reach unacceptable levels. Within this burst structure

There is a data rate of 72 kbs. In each burst, 72 bits of data are available for speech, control, signaling, and base/mobile station synchronization purposes. There is an allowance for a guard time between bursts to allow the sender to turn off its transmitter and settle into receiver mode and for the receiver to turn on its transmitter and settle at. Its center frequency. The guard time is nominally 4 bits long. By use of the guard period, both ends of the links are sure that the receiver is able to decode accurately the first- and later-transmitted bits in the burst.

The CT-2 modulation technique is binary frequency shift keying. With a channel spacing of 100 kHz, the bandwidth efficiency of CT-2 is O.72 bps/Hz about half of that of GSM. The speech coder is a standard Adaptive Differential Pulse Code Modulator (ADPCM) operating at 32 kbs.

1.6.2 DCT 9OO/DECTICT 3

The application of wireless technology, particularly for a large business complex with WPBXs that support roaming and handoffs between different cells is demanding. The system should manage the traffic in the cells in real time as the handsets move throughout the complex. This dramatically increases the complexity of the call processing software over that of a standard PBX. The software must also account for the three-dimensional environment of the system with the overlap of radio waves through different floors. Furthermore, the building environment affects the propagation of radio waves with the reflection and absorption of radio energy dependent on the construction materials. Ideally, a large building should be designed with a WPBX in mind; in practice, real buildings will have been designed before the WPBX, and compromises will be needed.

The capacity needs of a large modern office building can be met only with a high frequency reuse achieved by use of Pico-cells with an indoor cell size of less than 50 m. Low-output power enables the handsets to be small and provides a talk time that exceeds the possibilities of other technologies. The most important requirement of the business PBX user is that the voice quality of the call is comparable to that of existing wired extensions.

The DCT 900/DECT/CT- 3 choice of TDMA/TDD was dictated by the needs of multiple mobile telephones accessing multiple base units and connected to a PBX and by the shortage of paired frequency bands in Europe. The solution to this problem required the multiplexing of multiple users at a base unit and sup- port for handoff and was readily implemented in a single-frequency TDMA/TDD. With only one frequency, TDD permitted simple rapid monitoring of power in all channels from both ends of a radio link. Dynamic time slot allocation algorithms for Dynamic Channel Allocation (DCA), with continuous transmission in at least one time slot as a "beacon" from all base units, provided a convenient mechanism for initial base-unit and time-slot selection.

The emerging standard for the large WPBX is DECT. This standard was frozen by ETSI in 1991, and the first system appeared in 1993. DECT standards do not compete directly with CT 2 because they are not oriented on the same market. DECT standards are more dedicated to PBX with large capacity, whereas CT- 2 fulfills the requirements of the PBX with small capacities.

The modulation technique of DECT is Gaussian Minimum Shift Keying. The relative bandwidth of the Gaussian filter is wider (0.5 times of the bit rate) than in GSM. The bandwidth efficiency is 0.67-bps/Hz, which is comparable to that of CT-2. The speech coder of DECT is ADPCM with bit rate of 32 Kbs.

The DECT standard enables the development of systems specially designed to handle high capacity in a stationary environment. DECT cannot compete with cellular technology for use in vehicles, but it will be considerably cheaper in the applications it has been designed for. DECT's TDMA broadband solution may more adequately cover the businessperson's demands, such as high voice quality and data transmission capability

1.6.3 Global System Mobile (GSM)

GSM was driven by the need for a common mobile standard throughout Europe and the desire for digital transmission compatible with data and privacy Spectrum was reallocated near 900 MHz throughout much of Europe and the surrounding region so that completely new technology could be developed by GSM. The GSM effort in the early to mid-1980s considered several system implementations including TDMA, CDMA, and FDMA technologies. A TDMA/FDMA/ FDD technology was chosen with a radio link bit rate of 270 kbs.

The GSM modulation is Gaussian Minimum Shift Keying (GMSK). The bandwidth efficiency of 270-kbs signals operating with 200-kHz carrier spacing Is 1.35 bps/Hz. The GSM's speech coder is r referred to linear predictive coding with regular pulse excitation. The source rate is 13 kbs and transmission rate, including error detecting and correcting codes; is 22.8 kbs.

1.6.4 IS-54

In North America, where a common analog air interface was available and roaming anywhere in Canada, the United States or Mexico was possible; there was no need to replace the existing analog systems. Therefore, the Cellular Telecommunication Industry Association (CTIA) requested the TIA to specify a system that could be retrofitted into the existing AMPS system. The high cost of the cell sites was the major driving force. Thus, the important factor in the IS-54 was to maximize the number of voice channels that can be supported by a cell site within the available cellular spectrum. Several TDMA/FDMA and pure FDMA system proposals were considered before the IS-54 standard was selected. IS-54 fits three TDMA 8-kbs encoded speech channels into each 30 kHz AMPS channel.

IS-54 uses a linear modulation technique, Differential Quadrature Phase Shift Keying (DQPSK) to provide a better bandwidth efficiency: The transmission rate is 48.6 kbs with a channel spacing of 30 kHz. This gives bandwidth efficiency of 1.62 bps/Hz, a *20% improvement* over GSM. The main penalty of linear modulation is power efficiency that affects the weight of handsets and time between battery charging The IS-54 speech coder is a type of code book excited linear predictive coding r referred to as Vector Sum Excited Linear Prediction (The source rate is 1.95 kbs and the transmission rate is 13 kbs.

1.6.5 IS-95

Recently a CDMA protocol has been proposed by QUALCOMM and standardized in the United States as IS-95. IS-95 is aimed at the dual-mode operation with the existing analog cellular system. The basic idea behind increased capacity in IS-95 is the use of a wideband channel the proposed channel width is 1.25 MHz in each cell or 42 30-kHz channels where many subscribers can talk together without interfering with each other. Many users with different codes share each channel. IS-95 proposes soft. Handoff to improve voice quality and RAKE receiver to take advantage of multipath fading and to lower signal-to- interference (S/I) ratio. Other factors that affect the channel capacity include use of variable rate vocoder, voice activity factor, a power control in the forward and reverse channel.

1.6.6 Japanese Digital Cellular (JDC)

Japanese Digital Cellular standards are aimed to replace the three incompatible analog cellular systems in Japan. The basic radio channel design defined in the JDC standard is comparable with the North American IS-54 ITDMA,) digital and European GSM system. The JDC systems use three-channel TDMA. Two required Frequency bands have been reserved: 800-MHz band with 130 MHz of duplex separation and 1.5-GHz band with 48 MHz of duplex separation. The 800-MHz band will be used first, whereas the 1.5-GHz band is for future use. The modulation scheme is $\frac{\Pi}{4}$-QPSK with interleaved carrier spacing of 25 kHz. The speech coder uses 11.2-kbs VSELP including channel coding.

1.7 Second-Generation-Plus PCs Systems

Although many people describe PCS as a third-generation system, the U.S. implementation uses modified cellular protocols. The opening of the 2-GHz band by the FCC has generated a flurry of activity to develop new systems. Unfortunately, in the race to deploy systems, most work has been to up band the existing cellular systems to the new 2-GHz band: Whether the protocol is GSM, IS-54, or IS-95, each proponent wants to make minimum changes in its protocol to w-in the PCS race.

It may not be until later in the 1990s before true third-generation systems offering Wireless multimedia access emerges. The initial offering may be tailored to the environment and the need for rapid entry into the marketplace.

A further factor is the need to support wireless residential service (wireless CENTEREX), cordless phones, Telepoint, wireless PBXs, low-mobility (on-street) portable phones, and high-mobility (in-vehicle) mobile phones. Although there is a desire for one protocol to support all needs, cost constraints may result in several solutions. Each one optimized to a particular need. This need and demand for wireless communications in several environments has been shown by the rapid growth of different technologies that are optimized for particular applications and environments. Examples are:

1. Residential mobile telephones and their evolution to digital technology in CT- 2 and to DCT 900/DECT/CT 3 for in-building PBX environments

2. Analog; cellular telephones for widespread mobile service and their digital evolutions to GSM, E-TDMA, IS-54, and CDMA

3. Wireless data networks both for low-rate wide-area coverage and higher- rate wide Local Area networks (WLANs)

Basic needs for PCS include standardized low-power technology to provide voice and moderate-rate data to small, lightweight, economical, pocket-size personal handsets that can be used for tens of hours without attention to batteries and to be able to provide such communications economically over wide areas, including in homes and other buildings, outdoors for pedestrians in neighborhoods and urban areas, and anywhere there are reasonable densities of people.

The CT- 2 and DCT 900/DECT/CT- 3 technologies look attractive for providing low-priced personal communications services with volume penetration. To permit widespread use of these technologies in outside environments where base stations have less attenuation between themselves than between mobile stations and base stations, time synchronization of base station transmissions is r To achieve good performance with TDD. While the DCT 900lDECT/CT-3 technology was appropriate for WPBXs, it needs modification for more widespread PCS applications, for which it also incurs synchronization requirements and additional complexity

The DC51800 is a standard for PCN that has been developed by ETSI. It is a derivative of the GSM 900 MHz cellular standard. In Europe DCS has been allocated frequencies from 1710 to 1785 MHz and 1805 to 1880 Hz to provide a maximum theoretical capacity of 375 radio carriers, each with 8 or 16 (half rate) voice/data channels. In DC51800 there are provisions for national roaming between operators with overlapping

These protocols will use powerful for- Ward error correction and digital speech interpolation techniques to match the quality of service of the fixed network.

Because of the multitude of teleservices offered in different operating scenarios, the teletraffic density generated will depend on the environment, the mix of terminal types, and the terminal density Teletraffic density will vary substantially for high-bit-rate services provided in business areas, whereas basic services such as speech and video telephony will be offered in all other environments.

The third-generation network will concentrate on the service quality, system capacity; and personal and terminal mobility issues. The system capacity will be improved by using smaller cells and the reuse of frequency channels in a geographically ordered fashion. A third-generation network will use different cell structures according to the operational environment. Cell structures will range from conventional macro-cells to indoor pico-cells. In particular, micro-cells with low transmission power will be widely deployed in urban areas, while other cell structures will be used according to the environment to provide ubiquitous coverage. It is expected that the cost of base station equipment for micro-cells will be significantly reduced because of the elimination of costly high-power amplifiers and the economies of scale in micro-cell base station manufacturing. Nevertheless, the system's cost will still play a dominating role in the design of the net- work infrastructure because more micro-cellular base stations will be required to provide adequate radio coverage. Micro-cells with a radius less than 1,000 m will be used extensively to provide coverage in metropolitan areas. Micro-cell base Stations will be mounted on lampposts or on buildings where electric supply is readily available. For high-user-density area such as airport terminals, railway stations, and shopping malls, pico-cells with coverage of tens of meters will be used. To facilitate efficient handoff when the vehicle-based user

Cells at high speed, these calls will be handled by umbrella cells (overlay macro-cells) whose coverage areas will contain several to tens of micro-cells.

The planning of third-generation systems will be mo complicated than the design of present speech-oriented, micro-cell-based mobile systems and will require a more advanced and intelligent network-planning tool.

Coverage. These modifications have enabled the GSM cellular standard to be enhanced to provide a high capacity, quality PCN system that can be optimized for handheld operation. The 1800-112Hz operating band in the DCS results in a small cell structure that is compatible with the PCN concept. The 1800-MHz band is occupied by fixed radio links for which alternative technologies exist, and clearance of the band can be more readily effected than attempting to manage coexistence and transition between the first-and second-generation cellular systems at 800/900 MHz.

The initial implementation of European PCN is based on the provision of a high-quality small cell network (cell radius Less than 1 km in a dense urban environment to 5 km in the rural environment). Radio cover age and system parameters are optimized for low-power handsets, and emphasis is placed on providing a significantly higher statistical call success and quality level for the handheld portable than current cellular networks provide.

The future evolution of DCS1800 may include microcell structure for cover- age and capacity enhancement into buildings such as airport terminals, railway stations, and shopping centers, where. Large numbers of people gather. A further development would then be in "private" cells within offices to provide business communications. Ubiquitous deployment of microcells in a PCN environment will require a very fast handoff processing capability that is not currently avail- able on DCS1800. How successfully the DC51800 technology can be implemented in office environments to replace DCT 9OO/DECT/CT- 3 is in question.

1.8 Vision Of The Third-Generation Systems

First-generation analog and second-generation digital systems are designed to support voice communication with Limited data communication capabilities. Third-generation systems are targeted to offer a wide variety of services Listed in Table 2.3. Most of the services are wireless extensions of Integrated Services Digital Network (ISDN), whereas services such as navigation and location information are mobile specific. Wireless network users will expect a quality of service similar to that provided by the wire line networks such as ISDN. Service providers will require higher-complexity protocols in the physical link layer because of the unpredictable nature of the radio propagation environment and the inherent terminal mobility in a wireless network.

Table 2.3 Proposed Teleservices A Third Generation System

Teleservices	Throughput (kbs)	Target bit error
Telephony	8-32	10^{-3}
Voice mail	32	10^{-3}
Program sound	32	10^{-3}
Video telephony	128	10^{-7}
Video conference	64	10^{-7}
Remote terminal	384-768	10^{-6}
User profile editing	1.2-9.6	10^{-6}
Telefax(group4)	1.2-9.6	10^{-6}
Voiceband data	64	10^{-6}
Database access	2.4-768.0	10^{-6}
Message broadcast	2.4	10^{-6}
Unrestricted digital information	64-1,920	10^{-6}
Navigation	2.4-64.0	10^{-6}
Location	2.4-64.0	10^{-6}

CHAPTER TWO

HOW CELL PHONES WORKS

2.1 Introduction

Millions of people in the United States and around the world use cellular phones. They are such great gadgets with a cell phone; you can talk to anyone on the planet from just about anywhere as shown in the figure 2.1 a digital cell phone from nokia

Figure 2.1 A digital cell phone from Nokia

We will be starting to explain how a cell phone works? What makes it different from a regular phone? What do all those confusing terms like PCS, GSM, CDMA and TDMA mean? In this chapter of, we will discuss the technology behind cell phones.

2.2 The Cell Approach

One of the most interesting things about a cell phone is that it is really a radio an extremely sophisticated radio, but a radio nonetheless. The telephone was invented by Alexander Graham Bell in 1876, and wireless communication can trace its roots to the invention of the radio in 1894 by a young Italian named Guglielmo Marconi. It was only natural that these two great technologies would eventually be combined. In the dark ages before cell phones, people who really needed mobile communications ability installed radiotelephones in their cars. In the radiotelephone system, there was one central antenna tower per city, and perhaps 25 channels available on that tower. This central antenna meant that the phone in your car needed a powerful transmitter big enough to transmit 40 or 50 miles. It also meant that not many people could use radiotelephones there just were not enough channels. The genius of the cellular system is the division of a city into small cells. This allows extensive frequency reuse across a city, so that millions of people can use cell phones simultaneously. In a typical analog cell phone system in the United States, the cell phone carrier receives about 800 frequencies to use across the city. The carrier chops up the city into cells. Each cell is typically sized at about 10 square miles (26 square kilometers). Cells are normally thought of, as hexagons on a big hexagonal grid. Each cell has a base station that consists of a tower and a small building containing the radio equipment. A single cell in an analog system uses one-seventh of the available duplex voice channels. That is, one cell, plus the six cells around it on the hexagonal grid, are each using one-seventh of the available channels so that each cell has a unique set of frequencies and there are no collisions:

- A cell phone carrier typically gets 832 radio frequencies to use in a city.
- Each cell phone uses two frequencies per call a duplex channel so there are typically 395 voice channels per carrier. (The other 42 frequencies are used for control channels.
- Therefore, each cell has 56 or so voice channels available.

In other words, in any cell, 56 people can be talking on their cell phones at one time. With digital transmitter methods, the number of available channels increases. For example, a TDMA-based digital system can carry three times as many calls as an analog system, so each cell would have about 168 channels available. Cell phones have low-power transmitters in them. Many cell phones have two signal strengths: 0.6 watts and 3 watts (for comparison, most CB radios transmit at 4 watts). The base station is also transmitting at low power. Low-power transmitters have two advantages:

- The transmissions of a base station and the phones within its cell do not make it very far outside that cell. Therefore, in the figure above, both of the purple cells can reuse the same 56 frequencies. The same frequencies can be reused extensively across the city.
- The power consumption of the cell phone, which is normally battery-operated, is relatively low. Low power means small batteries, and this is what has made handheld cellular phones possible.

The cellular approach requires a large number of base stations in a city of any size. A typical large city can have hundreds of towers. But because so many people are using cell phones, costs remain low per user. Each carrier in each city also runs one central office called the Mobile Telephone Switching Office (MTSO). This office handles all of the phone connections to the normal land-based phone system, and controls all of the base stations in the

2.3 Cell Phones Codes

An AMP specifies several identification codes for each mobile station. The mobile £identification number (MIN) is a ten-digit telephone number, stored in a 34-bit binary representation. In the United States, this number has the same format as a conventional telephone number. The first three digits comprise the area code associated with the subscriber's home service area. This is followed by a seven-digit telephone number consisting of an exchange number (three digits) and a subscriber number (four digits). The exchange number is assigned to the cellular operating company. When a subscriber changes operating companies, it is necessary to change cellular phone numbers. In contrast to U.S. practice many countries assign special prefixes (corresponding to area code) exclusively to mobile telephone numbers. This practice makes it possible for callers to distinguish calls to mobile telephones from calls to conventional telephones.

Another identification code is a 32-bit electronic serial number (FSN) assigned permanently to each terminal. As a permanent characteristic of a physical unit, the ESN is similar to the engine number of a car. The MIN is analogous to the car's registration number, which, in the United States, changes when the car changes owners, or when the owner moves to a different state. A third identification code is the 4-bit station class mark (SCM), which describes the capabilities of the terminal. Station class marks indicate whether the terminal has access to all 832 AMPS channels or whether it is an old model with only 666 channels. Another property conveyed by the SCM is the maximum radiated power of the terminal. This could be either 600 mW or 4 W. As the AMPS system evolves, the industry specifies new station class marks to identify mobile stations with special properties that influence network

Control operations.

The system identifier (SID) is an important 1-bit code stored in all base stations and all mobile Stations. In the United States, the Federal Communications Commission issues an SID to an operating company when it issues a license to offer service in a specific area. System is AMPS terminology for cellular operations provided by one company in a specific area. Thus, each base station is part of a system. In many places ,there is one NTSO per system .however, to or more systems with relatively small numbers of subscribers can share a single MTSO. Conversely, large system is likely to operate with two or more MTSOs.

Each mobile station stores the identifier of the system that administers its subscription. This is the home system of the terminal. When the mobile its subscription. This is the home system of the terminal. When the mobile station performs an initialization procedure, it compares its own SID with the SID broadcast by the local cell site. Identical SIDs indicate that the mobile station is using its home system .if the SIDs are not identical ,the mobile station is a roamer in another system. in this event, the terminals indicates, on its display, that its in roaming area. This alerts the subscriber to the possibility of incurring special roaming charges

In addition to the SID assigned by regulatory authorities to the each base station, the local operating company assigns two identifiers, the digital color code(DDC) and the supervisory audio tone (SAT) ,which help mobile station distinguish neighboring base station from one another. The SAT assigned to a base station is one of three analog sine waves. Neighboring base stations operating with different SATs. The 2-bit digital color code serves a similar purpose.

2.4 From Cell To Cell

All cell phones have special codes associated with them. These codes are used to identify the phone, the phone's owner and the service provider.

Let's say you have a cell phone, you turned it on, and someone tries to call you. Here is what happens to the call:

- When you first power up the phone, it listens for an SID (see sidebar) on the control channel. The control channel is a special frequency that the phone and base station use to talk to one another about things like call set-up and channel changing. If the phone cannot find any control channels to listen to, it knows it is out of range, and displays a "no service" message.

- When it receives the SID, the phone compares it to the SID programmed into the phone. If the SIDs matches, the phone knows that the cell it is communicating with is part of its home system.
- Along with the SID, the phone also transmits a registration request, and the MTSO keeps track of your phone's location in a database -- this way, the MTSO knows which cell you are in when it wants to ring your phone.
- The MTSO gets the call, and it tries to find you. It looks in its database to see which cell you are in.
- The MTSO picks a frequency pair that your phone will use in that cell to take the call.
- The MTSO communicates with your phone over the control channel to tell it what frequencies to use, and once your phone and the tower switch on those frequencies, the call is connected. You are talking by two-way radio to a friend!
- As you move toward the edge of your cell, your cell's base station will note that your signal strength is diminishing. Meanwhile, the base station in the cell you are moving toward (which is listening and measuring signal strength on all frequencies, not just its own one-seventh) will be able to see your phone's signal strength increasing. The two base stations coordinate themselves through the MTSO, and at some point, your phone gets a signal on a control channel telling it to change frequencies. This hand off switches your phone to the new cell.

2.5 Roaming

if the SID on the control channel does not match the SID programmed into your phone, then the phone knows it is roaming. The MTSO of the cell that you are roaming in contacts the MTSO of your home system, which then checks its database, to confirm that the SID of the phone you are using is valid. Your home system verifies your phone to the local MTSO, which then tracks your phone as you move through its cells. And thing is that all of this happens within seconds.

2.6 Cell Phone And CBS

A good way to understand the sophistication of a cell phone is to compare it to a CB radio or a walkie-talkie.

Simplex and Duplex: Both walkie-talkies and CB radios are simplex devices. That is, two people communicating on a CB radio use the same frequency, so only one person can talk at a time as shown in the figure 2.2. A cell phone is a duplex device. That means that you use one frequency for talking and a second, separate frequency for listening. Both people on the call can talk at once as shown in the figure 2.3. Channels: A walkie-talkie typically has one channel, and a CB radio has 40 channels. A typical cell phone can communicate on 1,664 channels or more.

Range: A walkie-talkie can transmit about one mile using a 0.25-watt transmitter. A CB radio, because it has much higher power, can transmit about five miles using a 5-watt transmitter. Cell phones operate within cells, and they can switch cells as they move around. Cells give cell phones incredible range. Someone using a cell phone can drive hundreds of miles and maintain a conversation the entire time because of the cellular approach.

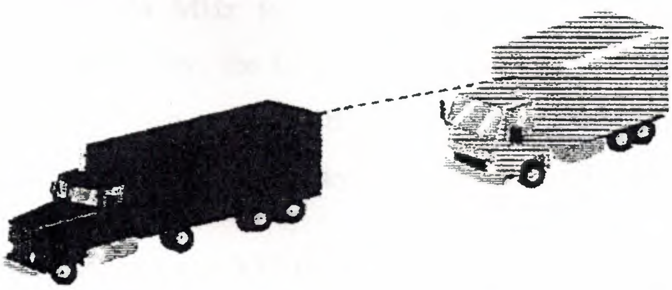


Figure 2.2. In simplex radio, both transmitters use the same frequency. Only one party can talk at a time.

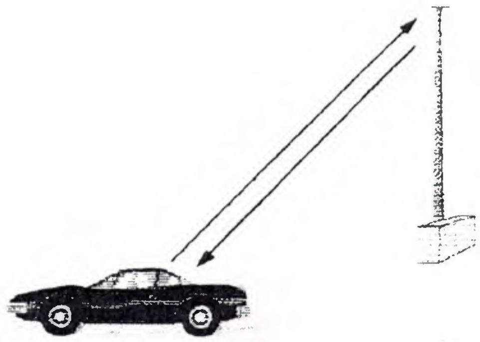


Figure 2.3 In duplex radio, the two transmitters use different frequencies, so both parties can talk at the same time. Cell phones are duplex

2.7 Advance Mobile Phone System (AMPS)

In 1983, the analog cell phone standard called AMPS (Advanced Mobile Phone System) was approved by the FCC and first used in Chicago. AMPS use a range of frequencies between 824 MHz and 894 MHz for analog cell phones. In order to encourage competition and keep prices low, the U. S. government required the presence of two carriers in every market, known as A and B carriers. One of the carriers was normally the local exchange carrier (LEC), a fancy way of saying the local phone company.

Carriers A and B is each assigned 832 frequencies: 790 for voice and another 42 for data. A pair of frequencies (one for transmit and one for receive) is used to create one channel. The frequencies used in analog voice channels are typically 30 kHz wide. The reason that 30 kHz was chosen as the standard size is because it gives you voice quality comparable to a wired telephone.

The transmit and receive frequencies of each voice channel are separated by 45 MHz to keep them from interfering with each other. Each carrier has 395 voice channels, as well as 21 data channels to use for housekeeping activities like registration, paging, etc. A version of AMPS known as Narrowband Advanced Mobile Phone Service (NAMPS) incorporates some digital technology to allow the system to carry about three times as many calls as the original version. Even though it uses digital technology, it is still considered analog. AMPS and NAMPS only operate in the 800 MHz band and do not offer many of the features common in digital cellular service such as e-mail and Web browsing.

2.8 Analog Comes Digital

Digital cell phones use the same radio technology as analog phones but in a different way. Analog systems do not fully utilize the signal between the phone and the cellular network. Analog signals cannot be compressed and manipulated as easily as a true digital signal. The same reasoning applies to many cable companies that are going to digital so they can fit more channels within a given bandwidth. Digital phones convert your voice into binary information (1s and 0s) and then compress it. This compression allows between three and ten cell phone calls to occupy the space of a *single* analog cell phone voice call. Many digital cellular systems rely on Frequency Shift Keying (FSK) to send data back and forth over AMPS. FSK uses two frequencies, one for "1"s and the other for "0"s, alternating rapidly between the two to send digital information between the cell tower and the phone. Clever modulation and encoding schemes are required to convert the analog information to digital, compress it and convert it back again while maintaining an acceptable level of voice quality. All this means that digital cell phones have to contain a lot of processing power.

2.9 Cellular Access Technologies

There is three common technologies used by cell phone networks for transmitting information:

1. Frequency Division Multiple Access (FDMA)
2. Time Division Multiple Access (TDMA)
3. Code Division Multiple Access (CDMA)

The first word tells you what the access method is and the second word, division, lets you know that it splits calls based on that access method.

- FDMA puts each call on a separate frequency.
- TDMA assigns each call a certain portion of time on a designated frequency.
- CDMA gives a unique code to each call and spreads it over the available frequencies.

The last part of each name is multiple accesses. This simply means that more than one user (multiple) can use (access) each cell.

2.9.1 Frequency Division Multiple Access (FDMA)

Separates the spectrum into distinct voice channels by splitting it into uniform chunks of bandwidth. Sends its signal at a different frequency within the available band. FDMA is used mainly for analog transmission as shown in the figure2.4. While it is certainly capable of carrying digital information, FDMA is not considered to be an efficient method for digital transmission.

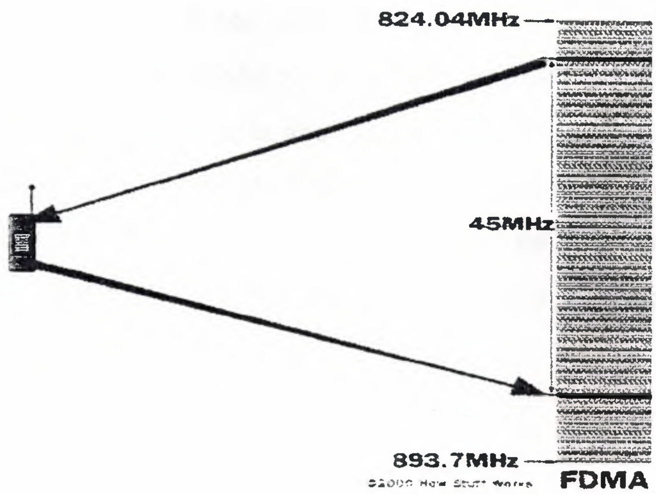


Figure2.4 In FDMA, each phone uses a different frequency.

2.9.2 Time Division Multiple Access (TDMA)

Do the Electronics Industry Alliance and the Telecommunications Industry Association use the access method for Interim Standard 54 (IS-54) and Interim Standard 136 (IS-136). Using TDMA, a narrow band that is 30 kHz wide and 6.7 milliseconds long is split time-wise into three time slots. Narrow band means channels in the traditional sense. Each conversation gets the radio for one-third of the time. This is possible because voice data that has been converted to digital information is compressed so that it takes up significantly less transmission space. Therefore, TDMA has three times the capacity of an analog system using the same number of channels. TDMA systems as shown in the figure 2.5 operate in either the 800 MHz (IS-54) or 1900 MHz (IS-136) frequency bands.

TDMA Is also used as the access technology for Global System for Mobile communications (GSM) However, GSM implements TDMA in a somewhat different and incompatible way from IS-136. Think of GSM and IS-136 as two different operating systems that work on the same processor, like Windows and Linux both working on an Intel Pentium III. GSM systems use encryption to make phone calls more secure. GSM operates in the 900 MHz and 1800 MHz bands in Europe and Asia and in the 1900 MHz (sometimes referred to as 1.9 GHz) band in the United States. It is used in digital cellular and PCS-based systems. GSM is also the basis for Integrated Digital Enhanced Network (IDEN), a popular system introduced by Motorola and used by Nextel.

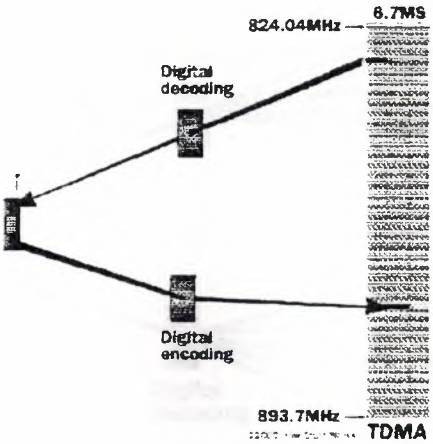


Figure2.5 TDMA splits a frequency into time slots.

GSM is the international standard in Europe, Australia and much of Asia and Africa. In covered areas, cell-phone-users can buy one phone that will work anywhere else the standard is supported. To connect to the specific service providers in these different countries, GSM-users simply switch subscriber identification module (SIM) cards. SIM cards are small removable disks that slip in and out of GSM cell phones.

They store all the connection data and identification numbers you need to access a particular wireless service provider.

Unfortunately, the 1900 MHz GSM phones used in the United States are not compatible with the international system. If you live in the United States and need to have a cell phone access when you're overseas, the easiest thing to do is buy a GSM 900MHz/1800MHz cell phone for traveling.

2.9.3 Code Division Multiple Access (CDMA)

Takes an entirely different approach from TDMA. CDMA, after digitizing data, spreads it out over the entire bandwidth it has available. Multiple calls are overlaid over each other on the channel, with each assigned a unique sequence code as shown in the figure 2.6. CDMA is a form of spread spectrum, which simply means that data is sent in small pieces over a number of the discrete frequencies available for use at any time in the specified range.

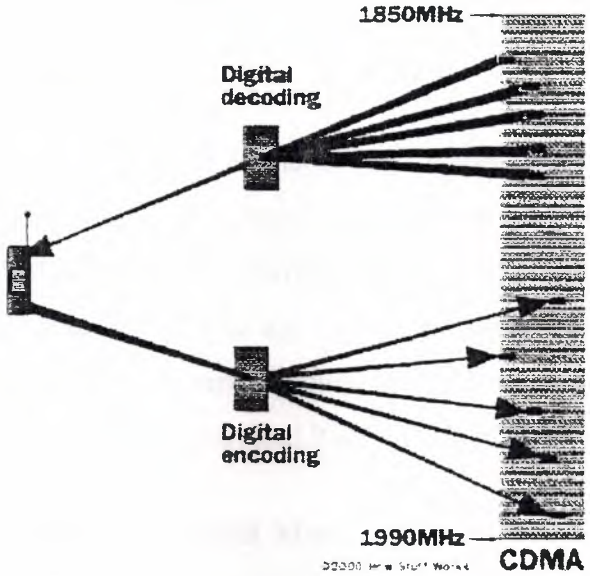


Figure 2.6 In CDMA, each phone's data has a unique code.

All the users transmit in the same wide-band chunk of spectrum. Each user's signal is spread over the entire bandwidth by a unique spreading code. At the receiver, that same unique code is used to recover the signal. Because CDMA systems need to put an accurate time stamp on each piece of a signal, it references the GPS system for this information. Between eight and 10 separate calls can be carried in the same channel space as one analog AMPS call. CDMA technology is the basis for Interim Standard 95 (IS-95) and operates in both the 800 MHz and 1900 MHz frequency bands. Ideally, TDMA and CDMA are transparent to each other. In practice, high power CDMA signals will raise the noise floor for TDMA receivers, and high power TDMA signals can cause overloading and jamming of CDMA receivers.

2.10 The Difference Between Cellular And PCs

Personal Communications Services (PCS) is a wireless phone service very similar to cellular phone service with an emphasis on *personal* service and extended mobility. The term "PCS" is often used in place of digital cellular, but true PCS means that other services like paging, caller ID and e-mail are bundled into the service.

While cellular was originally created for use in cars, PCS was designed from the ground up for greater user mobility. PCS has smaller cells and therefore requires a larger number of antennas to cover a geographic area. PCS phones use frequencies between 1.85 and 1.99 gig hertz (1850 MHz - 1990 MHz).

Technically, cellular systems in the United States operate in the 824-894 megahertz (MHz) frequency bands; PCS operates in the 1850-1990 MHz bands. And while it is based on TDMA, PCS has 200 kHz channel spacing and eight time slots instead of the typical 30 kHz channel spacing and three time slots found in digital cellular. Just like digital cellular, there are several incompatible standards using PCS technology. Two of the most popular are Cellular Digital Packet Data (CDPD) and GSM

2.11 Dual Band And Dual Mode

If you travel a lot, you will probably want to look for phones that offer dual band, dual mode or both. Lets take a look at each of these options.

- Dual Band: A phone that has dual band capability can switch frequencies. This means that it can operate in both the 800 and 1900 MHz bands. For example, a dual band TDMA phone could use TDMA services in either an 800 MHz or a 1900 MHz system.
- Dual Mode: In cell phones, mode refers to the type of transmission technology used. So, a phone that supported AMPS and TDMA could switch back and forth as needed. An important factor to look for is that one of the modes is AMPS. This gives you analog service if you are in an area that doesn't have digital support.
- Dual Band/Dual Mode: The best of both worlds allows you to switch between frequency bands and transmission modes as needed.

Phones that support these options do changing bands or modes automatically. Usually the phone will have a default option set, such as 1900 MHz TDMA, and will try to connect at that frequency with that technology first. If it supports dual bands, it will switch to 800 MHz if it cannot connect at 1900 MHz. And if the phone supports more than one mode, it will try the digital mode(s) first, then switch to analog.
Sometimes you can even find Tri Mode phones. This term can be deceptive. It may mean that the phone supports two digital technologies, such as CDMA and TDMA, as well as analog. But it can also mean that it supports one digital technology in two bands

and also offers analog support. A popular version of the TriMode type of phone for people who do a lot of international traveling has GSM service in the 900 MHz band for Europe and Asia, and the 1900 MHz band for the U.S. in addition to the analog service

2.12 Problems With Cell Phones

a cell phone, like any other consumer electronic device, can break. Here are some of the preventive measures you can take:

1. Generally, non-repairable internal corrosion of parts results if you get the phone wet or uses wet hands to push the buttons. Consider a protective case. If the phone does get wet, be sure it is totally dry before you switch it on to avoid damaging internal parts.
2. You can lessen the chance of dropping a phone or damaging the connectors if you use a belt-clip or a holster. The use of headsets really makes this consideration important.
3. Cracked display screens can happen when an overstuffed briefcase squeezes the cell phone.
4. Extreme heat in a car can damage the battery or the cell phone electronics. Extreme cold may cause a momentary loss of the screen display.

Analog cell phones suffer from a problem known as "cloning." A phone is "cloned" when someone steals its ID numbers and is able to make fraudulent calls on the owner's account. Here is how cloning occurs: When your phone makes a call, it transmits the ESN and MIN to the network at the beginning of the call. The MIN/ESN pair is a unique tag for your phone, and it is how the phone company knows whom to bill for the call. When your phone transmits its MIN/ESN pair, it is possible for nefarious sorts to listen (with a scanner) and capture the pair. With the right equipment, it is fairly easy to modify another phone so that it contains your MIN/ESN pair, which allows the nefarious sort to make calls on your account.

2.13 Inside A Cell Phone

On a "complexity per cubic inch" scale, cell phones are some of the most intricate devices people play with on a daily basis. Modern digital cell phones can process millions of calculations per second in order to compress and decompress the voice stream.

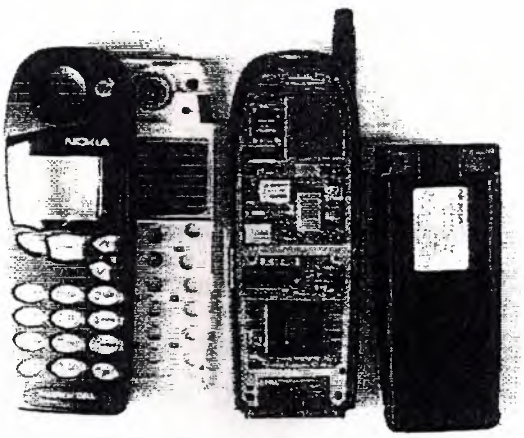
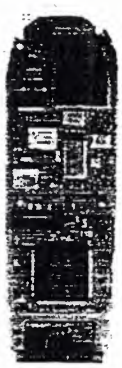


Figure 2.7 The various parts of a cell phone.

If you ever take a cell phone apart as shown in the figure 2.7, you will find that it contains just a few individual parts:

- An circuit board containing the brains of the phone
- An antenna
- A liquid crystal display (LCD)
- A keyboard not unlike the one we saw in a TV remote control
- A microphone
- A speaker
- A battery

The circuit board is the heart of the system. Here is one from a typical Nokia digital phone:



a. The front of the circuit board.

b. The back of the circuit board.

Figure 2.8 The Back and Front of the Circuit Board.

In the figure2.8, there are several computer chips I will talk about what some of the individual chips do. The Analog-to-Digital and Digital-to-Analog conversion chips translate the outgoing audio signal from analog to digital and the incoming signal from digital back to analog. The Digital Signal Processor (DSP) is a highly customized processor designed to perform signal manipulation calculations at high speed.

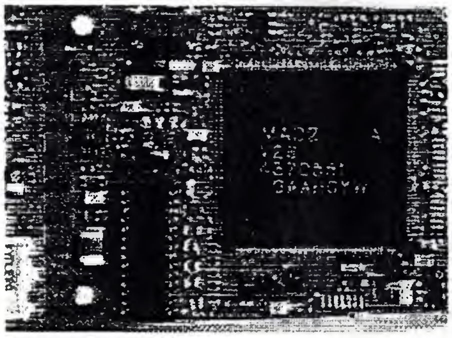


Figure 2.9 The Microprocessor.

The microprocessor as shown in the figure 2.9 handles all of the housekeeping chores for the keyboard and display, deals with command and control signaling with the base station, and also coordinates the rest of the functions on the board. The RF and power section handles power management and recharging, and also deals with the hundreds of FM channels. Finally, the RF (Radio Frequency) amplifiers handle signals in and out of the antenna.

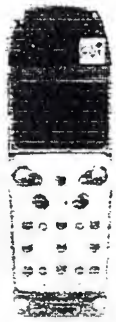
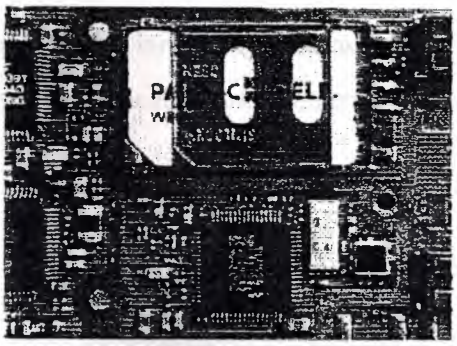
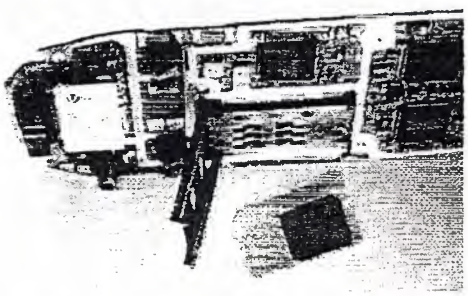


Figure 2.10 The display and keypad contacts.

The display as shown in the figure 2.10 has grown considerably in size as the number of features in cell phones has increased. Most phones currently available offer built-in phone directories, calculators and even games. And many of the phones incorporate some type of PDA, or Web browser.



a. The flash memory card on the circuit board.



b. The flash memory card removed.

Figure 2.11 ROM and Flash Memory

In the figure 2.11 the ROM and flash memory chips provide storage for the phone's operating system and customizable features, such as the phone directory. Some phones store certain information, such as the SID and MIN codes, in internal flash memory while others use external cards that are similar to Smartmedia cards.

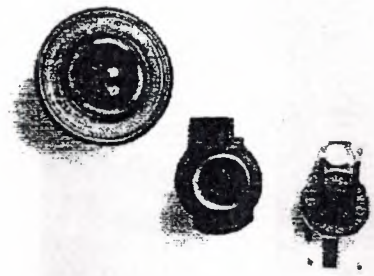


Figure 12.2 The cell phone speaker, microphone and battery backup.

Cell phones have such tiny speakers and microphones that it is incredible how well most of them reproduce sound. As shown in the figure2.12, the speaker is about the size of a dime and the microphone is no larger than the watch battery beside it. Speaking of the watch battery, this is used by the cell-phone's internal clock chip.

2.14 Cell Phones Tower

A cell phone tower as shown in the figure2.13 is typically a steel pole or lattice structure that rises hundreds of feet into the air. This cell phone tower along I-85 near Greenville, S.C. is typical in the U.S.: This is a modern tower with three different cell phone providers riding on the same structure. In the figure 2.14 if you look at the base of the tower, you can see that each provider has its own equipment, and you can also see how little equipment is involved today (older towers often have small buildings at the base):

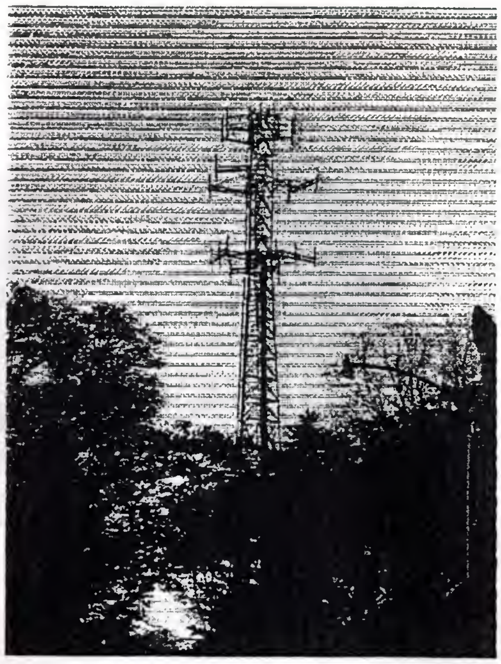


Figure 2.13 Modern Cell Phone Tower

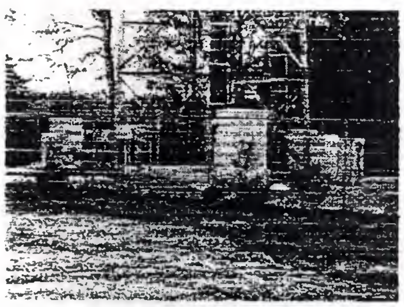


Figure 2.14 Base Station

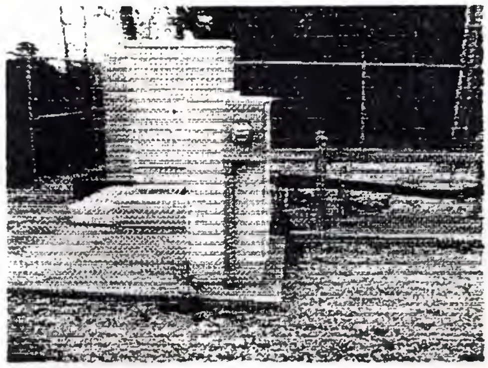


Figure 2.15 The Box Houses

As shown in the figure 2.15The box houses the radio transmitters/receivers that let the tower communicate with the phones. The radios connect with the antennae on the tower through a set of thick cables as shown in the figure2.16

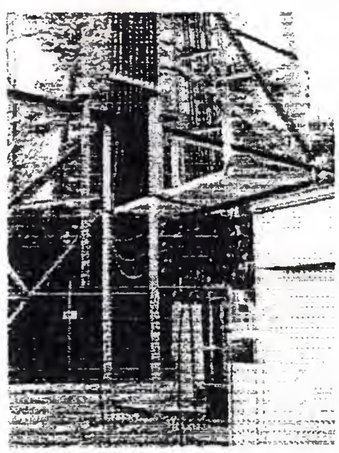


Figure 2.16 Using cables between radio antenna and tower

2.15 What They Can Do

Cell phones provide a way of staying in touch and having instant communication at your fingertips. With a cell phone, you can:

- Call your significant other to let them know that you are on your way home.
- Contact the police or hospital if you have an emergency.
- Let the boss know that you are stuck in traffic and will be late for that big meeting.
- Provide a way for others to contact you if you are always on the go.
- Call home or work to check your messages while on the road.
- Store contact information (names and phone numbers).
- Make task or to-do lists (some models).
- Keep track and remind you of appointments (date book, calendar).
- Use the built-in calculator for simple math.
- Send or receive e-mail (some models).
- Get information (news, entertainment, stock quotes) from the Internet. (Some models).
- Play simple games (some models).
- Integrate other devices such as PDAs, MP3 players and GPS receivers (some models).

2.16 Features

Here is a list of features that should be considered when looking for a cell phone:

- Service plan
- Mode
- Battery type
- Display
- Included functions
- Special Features
- Size

- Price

2.16.1 Service Plan

Before you set your sights on a particular make or model of cell phone, you should decide on the service plan that interests you. Otherwise, you could find that the phone you want is not supported by the plan you need. We will go in depth about this subject in a dedicated article on "How Cell Phone Service Plans Work."

2.16.2 Mode

Are you looking for analog or digital? Do you prefer PCS or cellular? TDMA or CDMA? If you have read the How They Work section, then you know what each of these terms mean. Look for dual mode/dual band phones if you travel a lot.

2.16.3 Battery Type

Cell phones use two main battery technologies:

- NiMH (Nickel Metal Hydride) - high capacity battery that provides extra power for extended use
- Li-ion (Lithium Ion) - has a lot of power in a lightweight package but usually costs more than NiMH batteries

Note both the talk time and standby time when comparing phones. Also, check to see how long the battery takes to recharge and whether a rapid charger is available. Most cell phone batteries are removable, but some of the smaller models have a built-in battery instead.

2.16.4 Display

All cell phones have LCD displays, but the specific features of the display can vary:

- Size - A large multi-line display is typically more expensive but necessary if you plan to use the phone for wireless Internet.
- Colors vs. monochrome - Most cell phones have monochrome displays (16 grays), but a few are beginning to appear that have color. Cell phones with color screens need more memory and tend to be more expensive.
- Reflective or backlit - Almost all cell phones have backlit screens, which are good for low light conditions.

2.16.5 Include Function

Most premium phones offer all of these features while more economical phones may only have a few:

- Phone Directory
- Clock
- Calculator
- Games
- Personalized/custom sounds
- Appointment Reminder/Calendar
- Incoming number storage
- Automatic redial
- Last number recall
- Mute/hold button
- One touch dialing/speed dialing
- Vibrate mode
- Lock/Alarm
- Call forwarding

- Multiparty calls
- E-mail/text messaging
- Minibrowser

2.16.6 Special Features

Some cell phones have special features such as:

- Wireless Internet
- Hands-free Headset/speakerphone
- External volume/ringer control
- Rapid charger/built-in charger
- Car adapter
- Modem function
- PC synchronization
- PDA
- MP3 player
- GPS receiver

CHAPTER 3

ANALOG CELLULAR COMMUNICATIONS AMPS SYSTEM

3.1 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.

3.2 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.

3.3.1 Networks Elements

The system architecture displayed with the amps terminology in the figure 3.1 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)

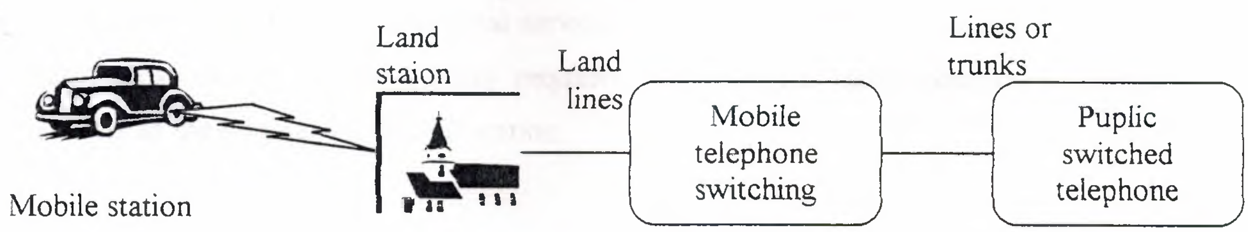


Figure 3.1 AMPS Architecture and Terminology

3.3 Radio Transmission

3.3.1 Frequency Bands And Physical Channels

AMPS operate in the frequency bands shown in the figures 3.2. The original allocation in the United States covered a bandwidth of 40MHz (figure 3.2a). The bandwidth was later extended to 50 MHz (figure3.2b). 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

$$F(c)= 825,000 +30 C \text{ kHz} \quad (3.1)$$

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.

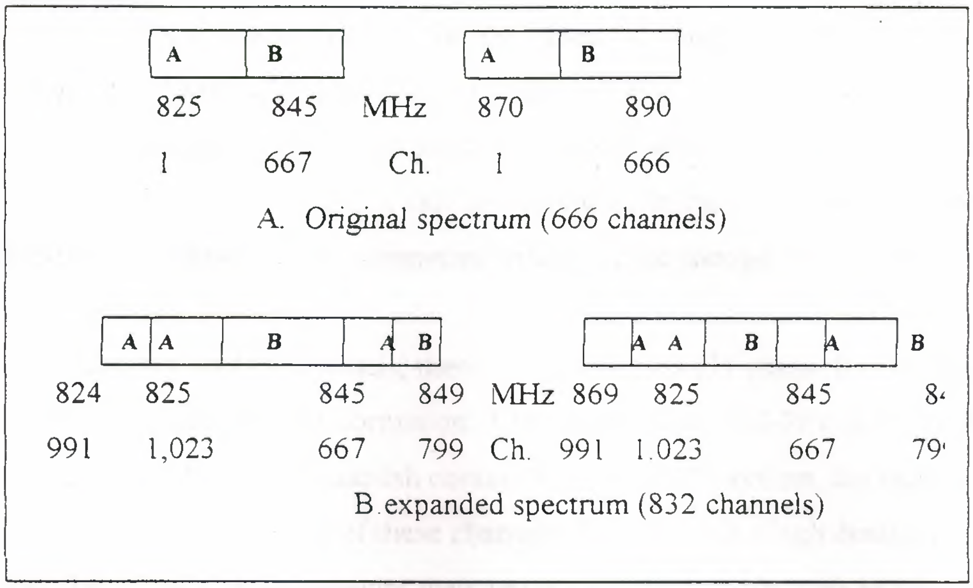


Figure 3.2 AMPS Spectrum And Channel Numbers

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 equation3.1. 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

$$F(C) = 825{,}000 + 30(C-1, o23);\ KHz;\ 991<C<1{,}o23 \qquad (3.2)$$

Figure 3.2 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.

3.3.2 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.

3.3.3 Analog Signal Processing

In Figure 3.3 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.

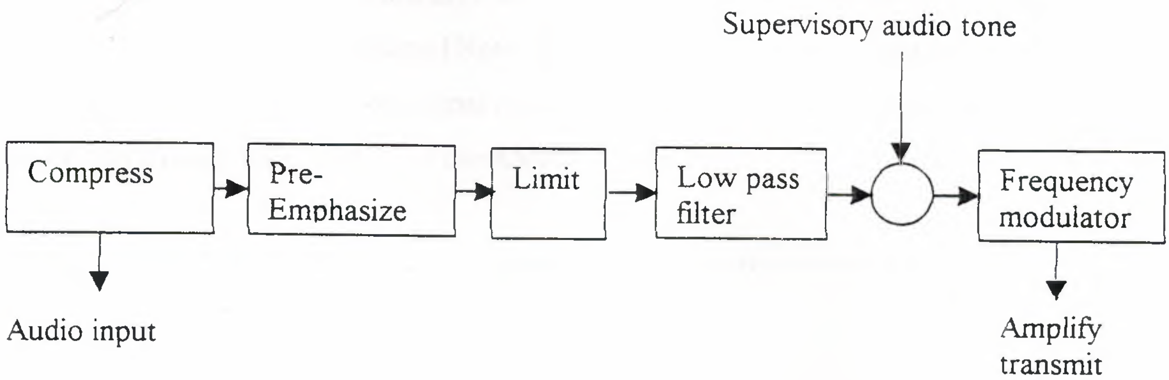


Figure3.3 Analog Signal Processing

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 3.4and 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 3.5. 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.

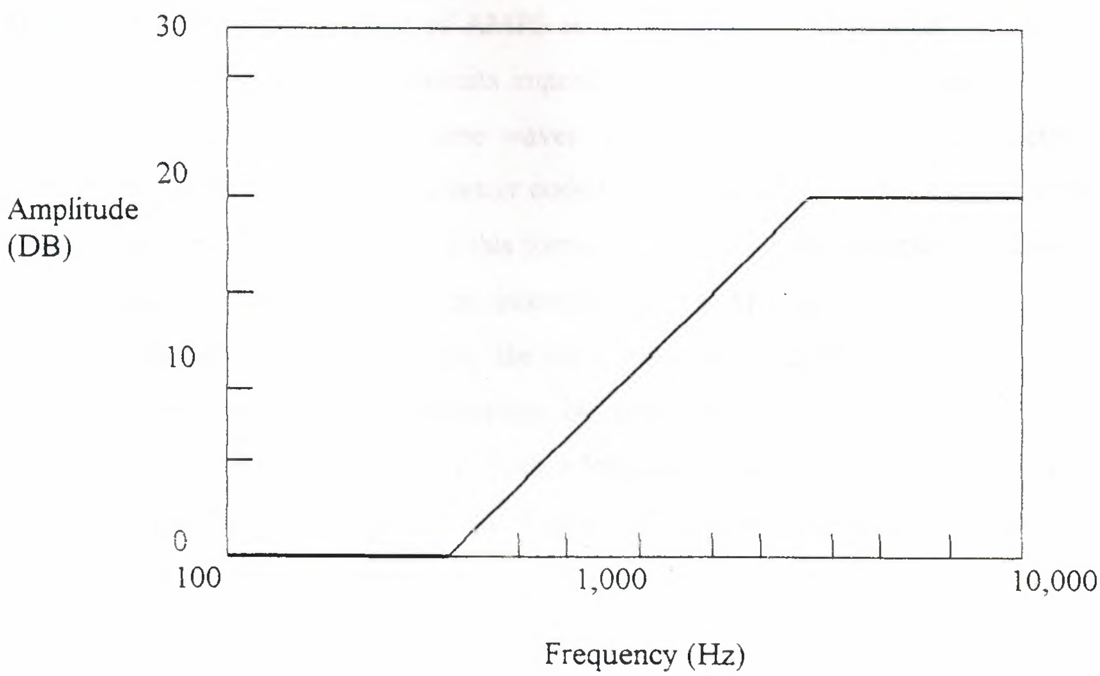


Figure 3.4 Pre-Emphasis Filters.

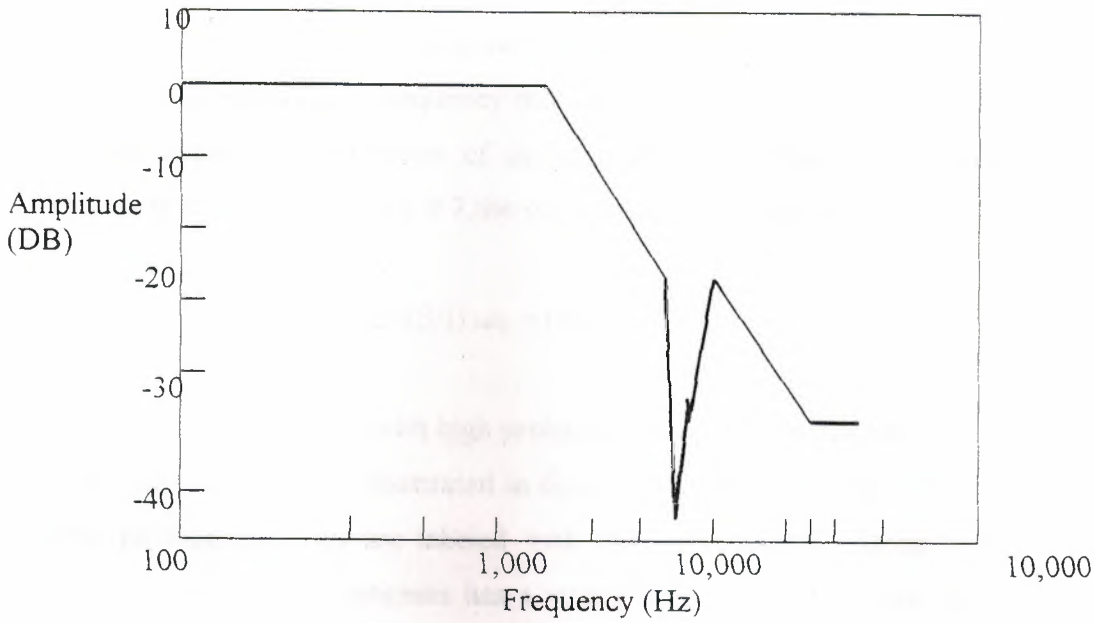


Figure 3.5 Lowpass Filter With A Notch At 6 KHz.

3.3.4 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 3.6a, while Figure 3.6b shows the pattern corresponding to1010101Q1010 digital signal.

3.3.5 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

$$(S/I)>(S/I)_{req} = 18dB. \quad (3.3)$$

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,

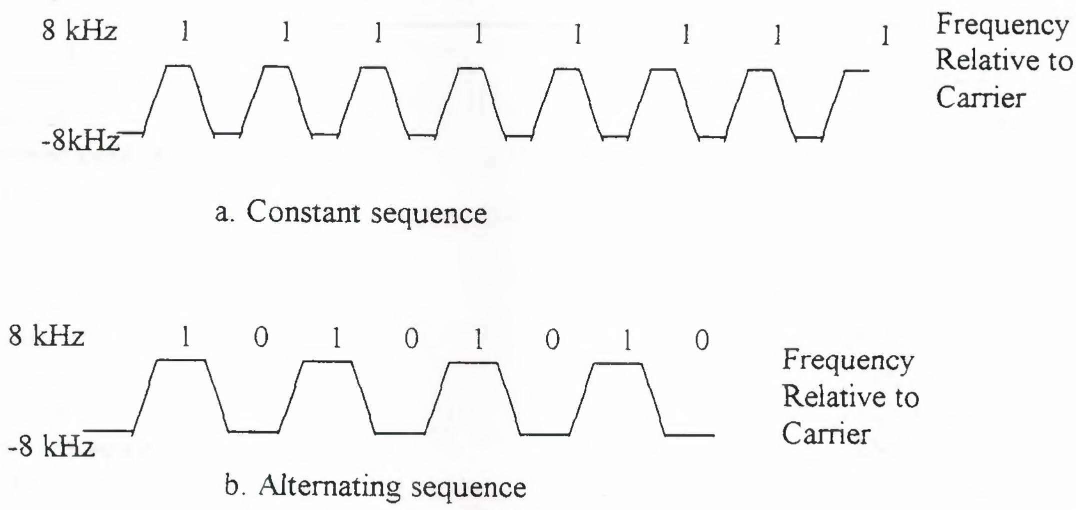


Figure 3.6 Manchester Coded Frequency Shift Keying

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,

$$E = \frac{395}{7 * 25} = 2.26 \qquad \text{Conversations/cell/N/Hz.} \qquad (3.4)$$

3.4 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 3.2 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 3.2 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 3.2 refers to the pair of channels that carry user information in an analog format (see Section 3.3.3) as traffic *channels*. In addition to the traffic channels, there are four formats for signaling information, as indicated in Table 3.2. 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 3.3 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.

3.4.1 Logical Channel Categories

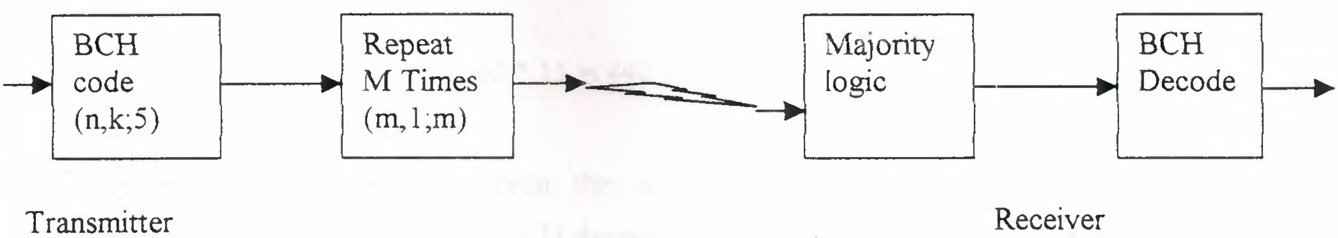
Table 3.2 indicates the topologies of the logical channels. A forward control channel (FOCC) carries the same information from one base station to all of the terminals in a particular cell that have their power turned on and do not have a call in progress. Similarly, a reverses control channel (RECC) 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.

3.4.2 Block Codes

All of the logical channels protect the control information with a concatenated pair of block codes, as indicated in Figure 3.7. 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 3.7 Channel Coding In AMPS.

Figure 3.7 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.

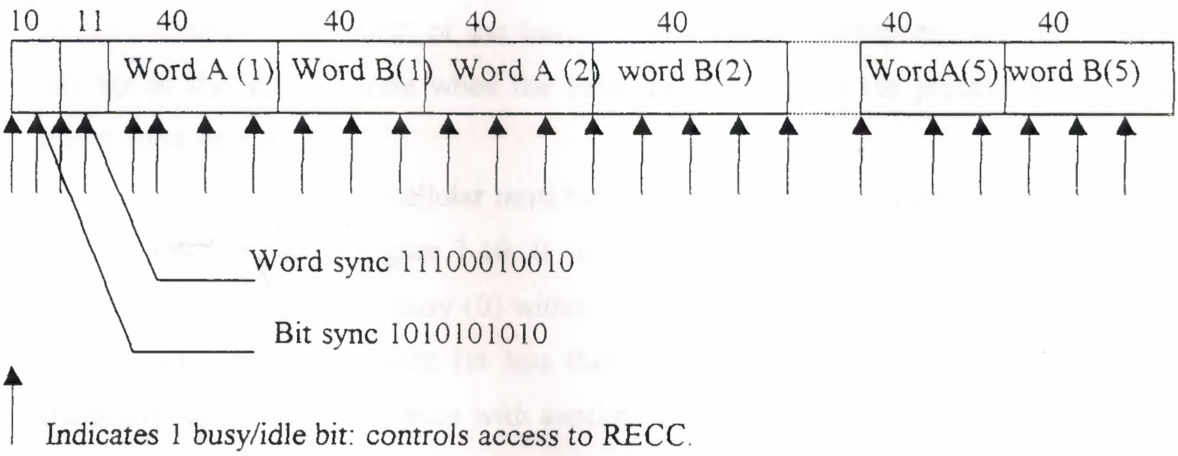
One approach is to perform majority logic decoding of the inner code [alternative (a) above] and single-bit error correction of the BCH code [alternative (0)]. With this approach, the inner code decoder examines the detected versions of a bit that was transmitted five times (11 times in the case of the 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.

3.4.3 Logical Channel Formats

Figures 3.8, 3.10, 3.11, and 3.12 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 3.6b 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 3. 8, 3.10, 3.11, and 3.12. 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.

3.4.3.1 Forward Control Channel

In Figure 3.8, 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 3.8 indicates that the arriving information rate for each terminal is 28 bits per 46.3 ms, or 604.75 b/s.



Indicates 1 busy/idle bit: controls access to RECC.

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.

Figure 3.8 Forward Control Channel (FOCC).

3.4.3.2 Reverse Control Channel Access Protocol

Expanding Figure 3.8 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 3.10. 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 3.9 is a flowchart of the RECC access protocol.

3.4.3.2 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

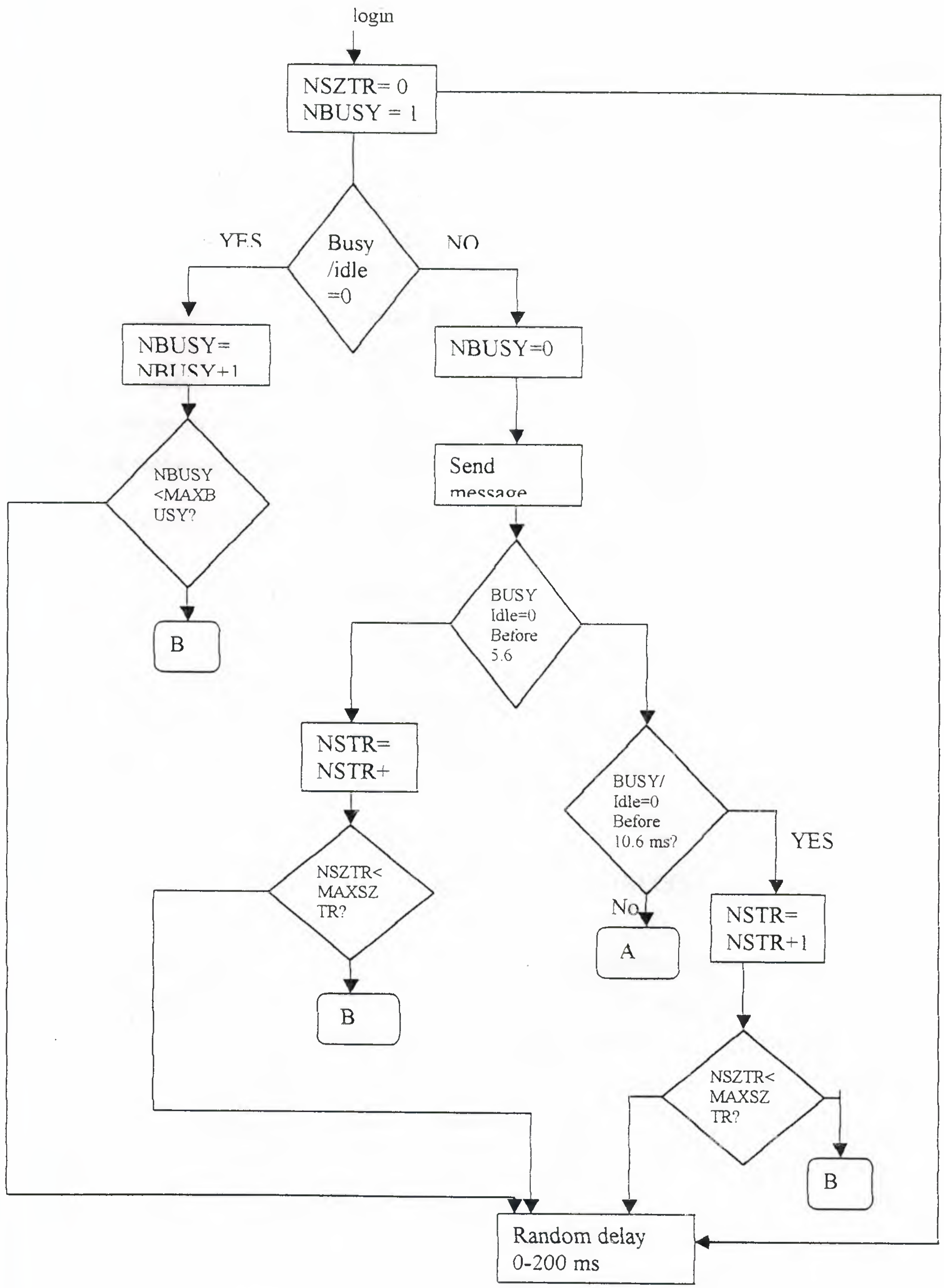
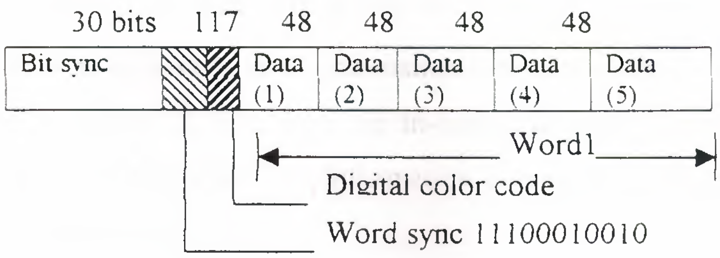


Figure 3.9 Reverse Control Channel Access Protocol



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 $5 \times 48 + 30 + 11 + 7 bits = 288 bits$

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

$$with one word, rate = \frac{36}{288} \times 10 kb/s = 1{,}250 b/s$$

$$with five words, rate = \frac{5 \times 36}{1{,}248} \times 10 kb/s = 1{,}442 b/s$$

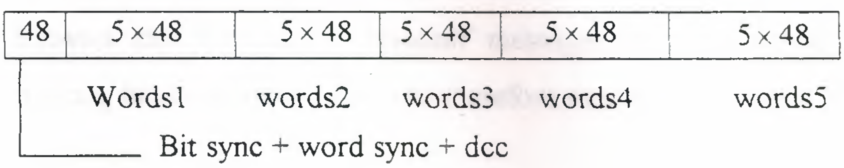


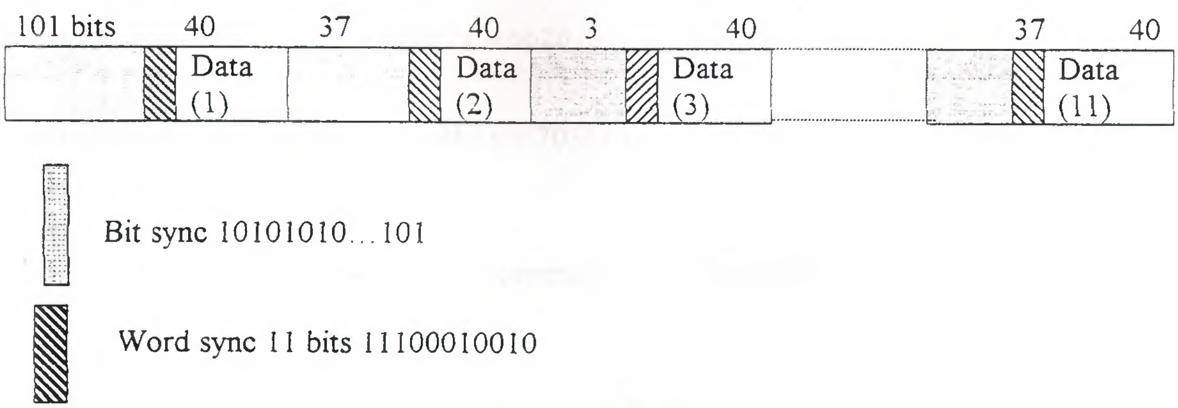
Figure 3.10 Reverse Control Channel (RECC)

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.

3.4.3.3 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 3.11(base to terminal)

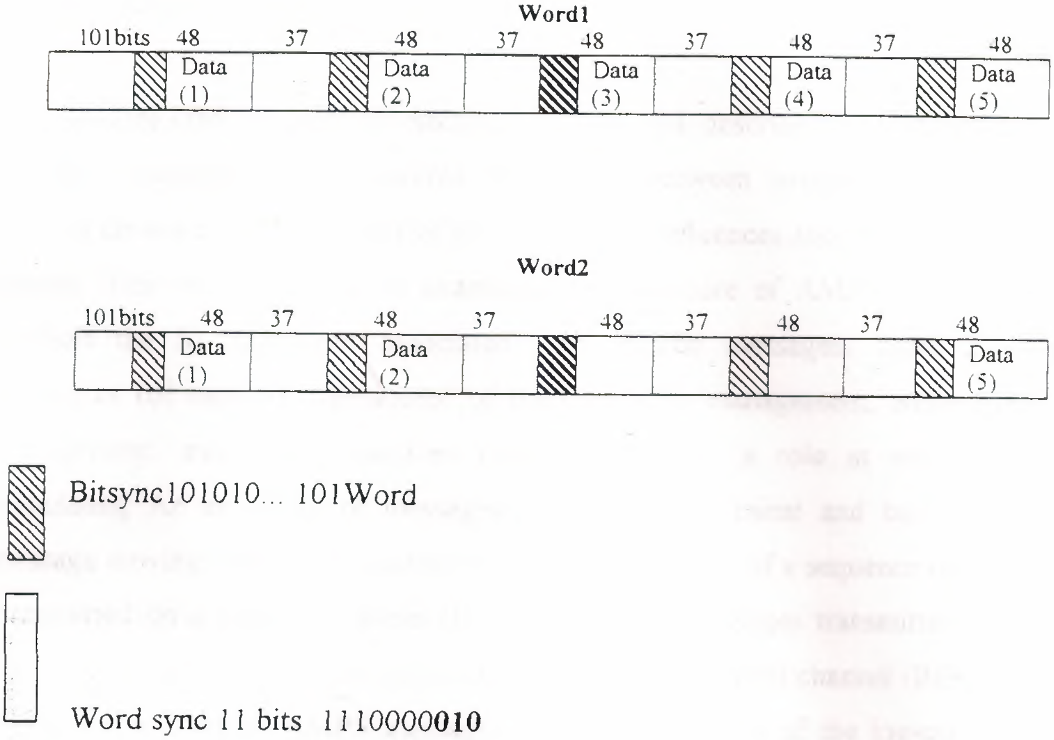
Or Figure3 .12 (terminal to base). Network control transmissions on a voice detecting this alternating pattern, the base station silence its transmission of the Received signal to the MTSO. Similarly, the terminal blanks the audio signal Relayed to the loudspeaker in the handset. The base or terminal 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.



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 3.11 Forward Voice Channel (FVC).



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

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

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

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

Figure 3.12 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.

3.5 Messages

In aggregate, the contents of Sections 3.3 and 3.4 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 3.3 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 3.3, 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 3.3 are broadcast control messages that provide the same information to all active terminals in a cell.

TABLE 3.3 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, uthentication
REGISTRATION	mobility management
Reverse voice channel messages	
CALLED-STATION ADDRESS	Call management
ORDER CONFIRMATION	Call management

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

3.5.1 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. Table3.4 displays a handoff message and Table 3.5 displays a change power level message, which has an entirely different structure. The only fields common to the two messages are the preamble, 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 3.4 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 3.4 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 3.5, 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 3.4 and 3.5 are examples of commands transmitted to terminals on a forward voice channel (FVC). Because this is a (one-to-one) dedicated control channel (Table 3.2), 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.

3.5.2 Message Content

The first four messages in Table 3.3 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 3.5 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 3.3.1. 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 3.4.3). Two of these parameters are MAXBUSY and MAXSZTR, which control the maximum number of attempts to transmit an RECC message. Figure 3.9 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 3.3, 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 3.3 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 3.5.1.

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 3.2.2): 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.

3.6 Amps Protocol Summary

Figure 3.13 summarizes the AMPS transmission technologies presented in Sections 3 .3, 3.4, and 3.5. 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.

3.7 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 3.14, 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 3.14.

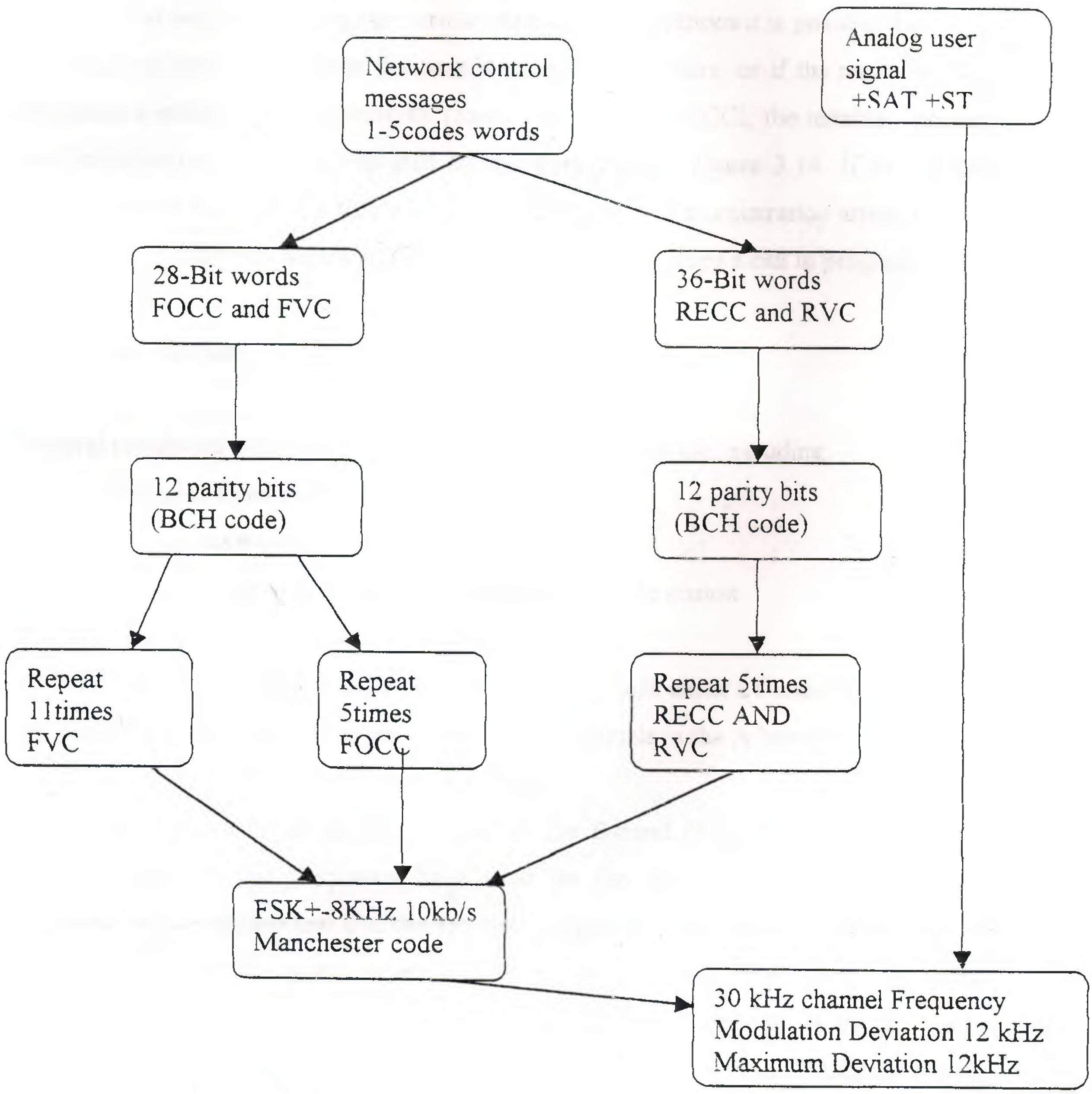


Figure 3.13 Summary Of AMPS Transmission Protocols

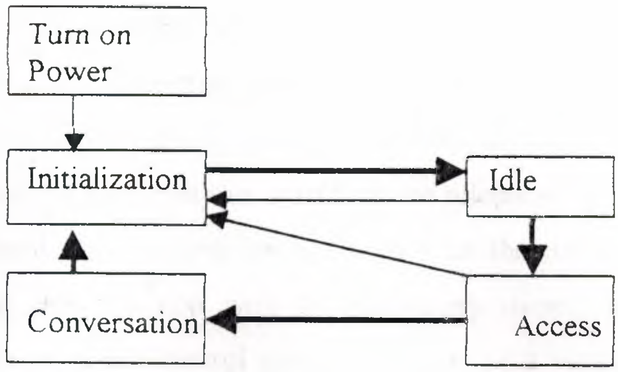


Figure 3.14 Cellular Terminal Operating Modes

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 3.14. 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.

3.7.1 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 3.2). 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 3.5.2, 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.

3.7.2 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 3.3 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.

3.7.3 Access

In the access mode, the terminal attempts to transmit a message in the RECC format (Figure 3.10) 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 3.9). 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 3.9. When it enters state An in Figure 3.9, 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 3.9 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

3.7.4 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 3.3.3) provides this confirmation. The terminal enters the conversation mode in response to an INTIAL VOICE CHANNEL message. Like the HAND*OFF* message (Table 3.4), 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.

3.7.5 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 3.15 displays the sequence of messages and control operations that set up and release a call originating at a mobile station.

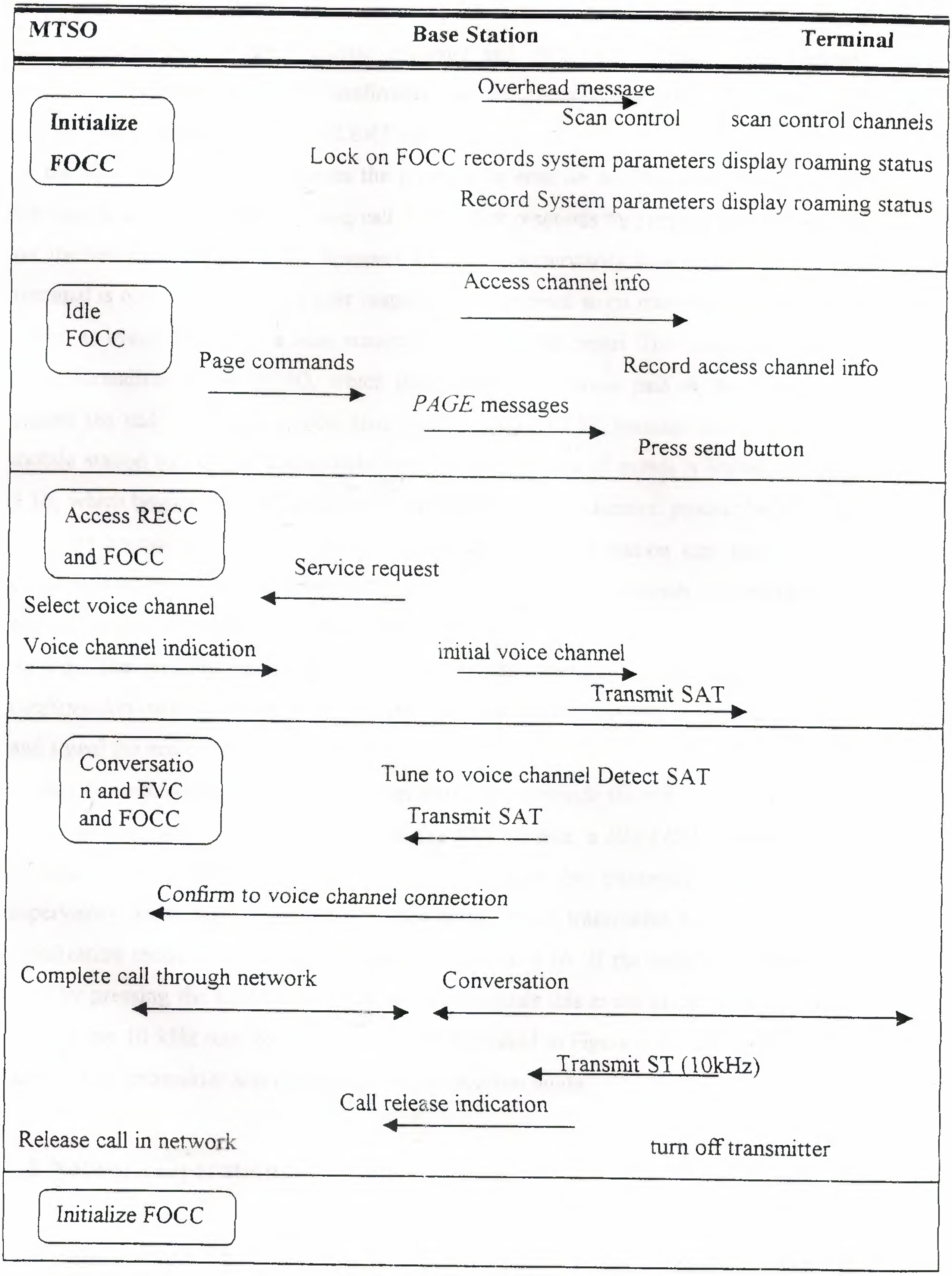


Figure 3.15 Network Control Sequence For A Call Originating At A Terminal. The Call Ends When The User Presses The End Button

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 3.16, which begins with the terminal in the idle mode. Initialization procedures conform to those shown in Figure 3.15.During the call, the base station can send a *order confirmation* message (see Table 3.5) 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 3.16. *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 3.15, the terminal then turns off its transmitter and returns to the initialization mode.

3.8 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 3.3 describes in detail AMPS technologies for user information transport and Section 3.7 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.

3.8.1 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* messages. 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.

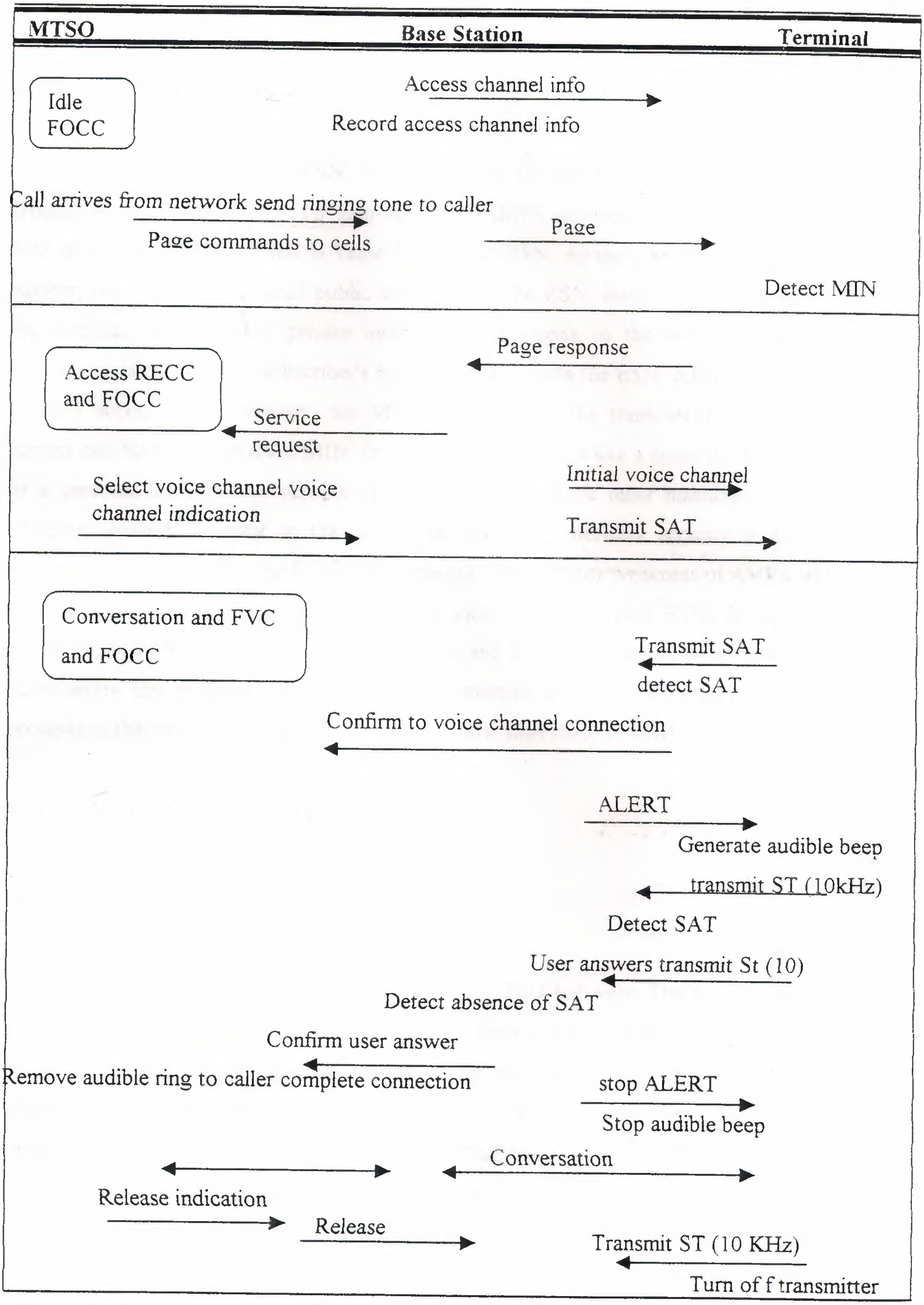


Figure 3.15 Network Control Sequence For A Call Originating At A Terminal. Call Ends When The User Presses The End Button

3.8.2 Authentication

The electronic serial number (FSN, Table 3.1) 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 3.1) 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.

3.8.3 Radio Resources Management

3.8.3.1 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.

3.8.3.2 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 3.3.2) 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 3.5.2). The initial power level for transmissions on traffic channels (VMAC) is specified in INTIAL VOICE CHANNEL messages and HANDOFF messages (see Table 3.4). 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 3.5) on a forward voice channel.

3.8.3.3 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 3.17 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

3.9 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.

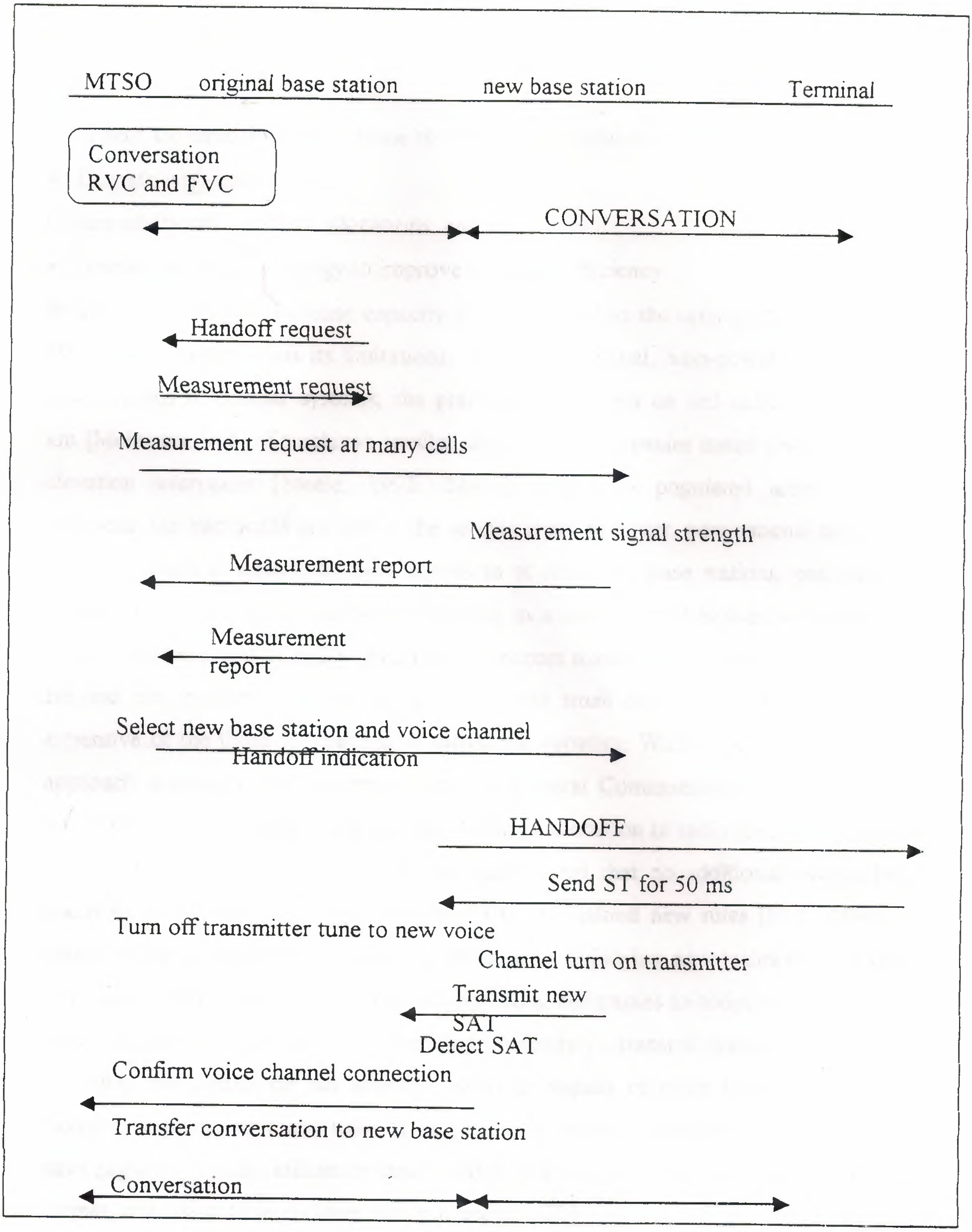


Figure3.17 Network Control Sequence For Handoff

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 1980s, added 10 MHz to the original 40 MHz allocation of radio spectrum to cellular services (see Figure 3.2). 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 3.1 and 3.2), 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 3.14. 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 3.4.3),

- 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

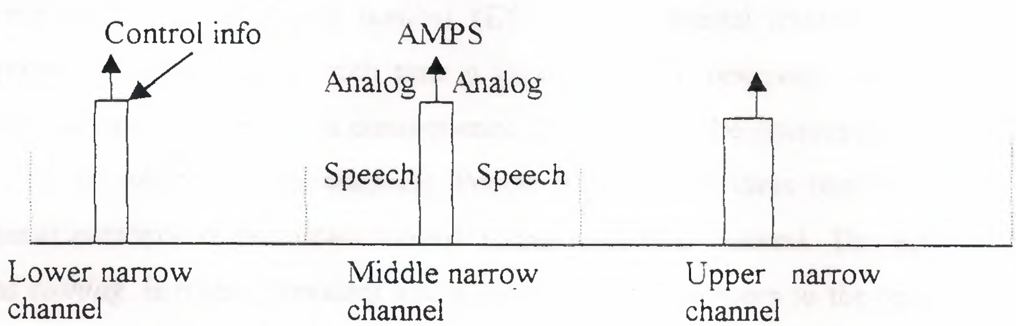


Figure 3.18 Partition Of One AMPS Channel Into Three Narrow Channels, Each Carrying Analog User Signals And Digital Control Signals.

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.

3.9.2 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.

3.9.3 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, and inside of cell phone and tower cell.

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.

REFERENCE

[1]. Bellcore Technical Advisories, "Generic Framework Criteria for Universal Digital Personal Communications Systems (PCS)," FA-TSY-001013, Issue 1 (March 1990), and FA-NWT-001013, Issue 2 (December 1990); "Generic Criteria for Version 0.1 Wireless Access Communications Systems (WACS)," TA-NTWT-001313, Issue 1 (July 1992).

[2]. Cheung et al., "Network Planning for Third-Generation Mobile Radio Systems," *IEEE Communications Magazine* 32, no. 11 (November 1994): 54-69.

[3]. Chia, "Beyond the Second-Generation Mobile Radio Systems, "British *Telecom Engineering* 10 (January 1992): 326-335.

[4]. Cox, D. C., "Personal Communications-A Viewpoint,"IEEE *Comnunication Magazine* (November 1990): 8-20.

[5]. European Telecommunications Standards Institution (ETSI i, "Recommendations for G5M9OO/DC51800" (ETSI, Cedex, France).

[6]. Gardiner. J. D. "Second Generation Cordless Telephony in U.K: Telepoint Services and the Common Air Interface," *IEE Electronics and Communications Engineering Journal* (April 1992).

[7]. Gilhousen, K. S., et al., "On the Capacity of a Cellular CDMA system."IEEE *transaction on Velzicular technology* VT-40, no. 2 (May 1991): 303-12.

[8]. Goodman, D. J., "Trends in Cellular and Cordless Communications;'IEEE *Communications Magazine* (June 1991): 31-40.

[9]. Grillo and Macnamee, "European Perspective on Third Generation Personal Communication Systems," Proceedings of the IEEE VTC Conference. Orlando, Florida. May 1990.

[10]. Mehrotra, A. *Cellular Radio Analog & Digital Systems,* Boston-London: Artech House. 1994.

[11]. Owen and C. Pudney, "DECT'-Integrated services for cordless communications," Proceedings of the Fifth International Conference on Mobile Radio and Personal Communications. Institution of Electrical Engineers, Warwick. United Kingdom. December 1989.

[12]. Tuttle bee, *Cordless Teleconinunication in Europe,* London-Heidelberg-NEW York: Springer-Verlag, 1990.

[13]. Viterbi. A. J., and Roberto Padovani, ``Implications of Mobile Cellular CDZ'IA."IEEE *communication magazine (*December 1992): 30 no.
12 3841.