NEAR EAST UNIVERSITY

FACULTY OF ENGINEERING

Department Of Electrical & Electronic Engineering

MOBILE COMMUNICATION SYSTEMS

Graduation Project
EE- 400

Student : Atif Munir (980849)

Supervisor : Prof. Dr. Fakhreddin Mamedov

Lefkosa - January - 2001

ACKNOWLEDGEMENTS

First of all I want to thank God, who not only gave me light in all the aspects of life but also made me acquainted with His wisdom and knowledge, which I needed most.

Secondly I want to thank Prof. Dr. Fakhreddin Mamedov, for being so persistent and understanding, when ever we seek guidance. His agility in explaining the topics has made me approach the material more rapidly and easily than the material itself. His attitude towards the student is always very inviting, that I seldom stuck to ask a question, and never, remained unanswered.

I would like to thank Ayaz, Mohammad Ali, Hafiz and Khurram. Without their help, this project would have been in utmost jeopardy and would have remained incomplete.

And finally, I would like to thank my beloved parents and family. Their love, prayers, advice and teachings have made me the man I am now, and I guess, their happiness remains the motto of my life, for now and forever.

Atif Munir

ABSTRACT

Mobile Communication Systems is one of the most evolutionary and promising Communication systems of modern Era, having traveled almost 60 years of complex architectural changes, network protocols and system designing implementations, and enhancing more benefits, properties, greater bandwidths, security and internet access to the subscribers than it was once in the 1940's.

The project covers an in-depth look at the evolution of Mobile Communication Systems, as it was and as it is today, Cellular technology, Introduction to the GSM, which is widely regarded as the father of today's mobile technology, and study of some new features as the WAP and I-mode.

Conceptually, the cellular systems are divided into five parts: radios, switching systems, databases, processing centers and external networks. As the FM radio technologies were refined, radio channels got narrower, and bandwidths kept increasing. Swift and reliable switching techniques have changed the concept of mobiles, which was once just restricted for voice channels, but now, video, and audio data compressions, internet access, downloadable items and yet there is more to come in the future, where tiny mobiles will be carried instead of laptops.

Today's cellular digital systems have come from a long travel punctuated by significant advances in radio techniques (for e.g., frequency modulation) and silicon electronics (microprocessors and digital signal processing). FM made the mobile practical, the microprocessor brought the trunking and cellular status to the mobile radio, and the digital signal processor brought digital radio costs down to the consumer level.

TABLE OF CONTENTS

INTRODUCTION

The Convergence of mobile and Internet promise to change the meaning of cellular technology forever. Mobile devices, still used most exclusively for voice, are on the threshold of a wave of new service opportunities for business and for consumers. Mobile phones today include such interactive services as the WAP and SMS. Rudimentary banking services are available on the mobile phones. E-mails from the mobiles have already revolutionized the way we communicate now. But all have been made possible, due to a long evolution in the Mobile Communication Systems, with out that, we would have remained unacquainted with the most unbelievable advantages, services and facilities today's the world have known in its pockets.

This project covers the most part of Basic Mobile Communication Systems, it's concept, and architecture, GSM, how the mobiles work, and a general look at the new technologies related with the mobiles.

Chapter 1, History of Mobile communication Systems, covers the historical background as well as the most basic mobile technologies, namely: First Generation Mobile Technology and the Second-generation mobile technology, which is 1^{s}G and 2G respectively. It also includes the basic steps and idea, which gave way to the modern mobile systems.

In the 2nd chapter, Cellular Technology, basic concept of Cell Approach as well as its architecture and the adaptation of the Digital mobiles are explained. The components of a cell phone and its structure are also examined.

The 3rd chapter, Introduction to GSM, states the History of GSM, it's Architecture, services provided, speech coding and channel coding aspects of GSM.

In 4th chapter, Smart Cards, an over view of SIM cards is detailed: it's logistical issues, security benefits and the services provided by the Smart Cards in today's world.

5th chapter, The Third Generation Technologies, gives a basic idea of WAP, i-mode and Bluetooth, which, all of them have emerged as the modern approach towards standardizing mobiles.

And in 6th Chapter, Modern Radio Interfaces, covers the Radio Frequencies: Spread Spectrum, Code Division Multiple Access (CDMA), Wideband Code Division Multiple Access (WCDMA), Time Division Multiple Access (TDMA), General Packet Radio Service (GPRS) and Enhanced Data For Global Evolution (EDGE). All of them are air interfaces which made possible the: Roaming services, Greater Bandwidths, high speed networks, low interference and background voice (S/N ratio), and other services as power control and cell size. All of these interfaces have their own advantages and disadvantages, which are also, thoroughly covered.

At last, the project ends with a conclusion and references. All the subject of this project has been taken from the same references listed in the end.

1. HISTORY OF MOBILE COMMUNICATION SYSTEMS

1.1. BACKGROUND

Though mobiles and cellular are pretty much synonymous today, they were not always so. Mobile (but not cellular) existed in the late 1940's.Those early systems used a wide-area architecture, one in which a single base site a top a high building managed fewer than a dozen, Radio channels connecting subscribers to the PSTN (Public switched telephone network. The central radio at the base sight transmitted tremendous RF power to the horizon above 100 km. Away, the service was at the best adequate.

The enabling technology for the early forms of mobile radio was FM, which matured during the worldwar2 (pre-war Am technology though fine in the fixed broadcast, and aeronautical applications, defied attempts to get it to the work reliably in the trunk of a car was very sensitive to noise and interference).

In the U.S. the mobile telephone channels offered 1-telephone channels of a FM based mobile phone services in the 40-MHz bands. To improve system (IMTS-MJ and -Mk) followed, occupying 11 and 12 radio channels in the 152-and454MHz band respectively.
As FM radio technologies in practice were defined, radio channels got narrower. The earliest mobile phones needed 120khz of spectrum to transmit 3-Khz voice circuit. The early 1960's had dropped the requirements to 10 and 30khz.

1.1.1. TRUNK IN THE LEAD:

Post war improvements in the FM radio were followed by innovation in trunking-radio techniques that free mobiles from the constraints dedicating a single channel to each user. A frequency agile radio can search for idle channels among a catalogue of frequencies. Rather than wait for it's own assigned channel to be free. Under the most conditions trunking system can support quite a bit more traffic than can a system with as many radio channels available but without trunking aids.

The earliest wide-area mobile phone system uses no trunking techniques at all. Later system employed manual trunking in which subscriber's search for open channels by

switching among the available channels until they found one with no life traffic. Still latest systems flaked any free channels with tones for which mobile phones could search a head of subscribers wish to make a call.

Even with narrow 10-khz channel and the best automatic trunking scheme IMTS service was often abysmal. The largest systems were usually oversubscribed, and blocking (the likely hood of not getting a channel during a short period of time) was typical 20%. Blocking during the busy hours-rush hours was so high as to render some systems useless. Tariffs were as might be expected very high.

1.1.2. OVER WHELMED:

Bad as the service was, waiting list for the privilege of becoming subscriber were worse five times the subscriber system I the total system. Radio channels were simply too few to accommodate the traffic offered. Private dispatch mobile radio (PMR system with 11 or 12 channels can cope with far more traffic than can a mobile radio system offering PSTN inter connection because typical phone connection last 2 3 minutes, as against sec's for connection in a dispatched scenario.

Effort to secure more spectrum for mobile telephone and PMR fell on the defers of federal communication commission, which saw spectrum for broadcast service as more socially responsible. But a political winds began to shift favor of mobile telephone and PMR in 1968 when the commission agreed to hand over T.Vs UHF channels 70-83 (800 MHz band) to land mobile use. At that time mobile phone users in the U.N number only 70,000.

1.2. THE FIRST CELLULAR:

ATNT the bell laboratory proposed the cellular conserve as the advance the mobile system (amps) architecture in 1971 it was an intriguing idea that called for the replacing the single base station high above the center of the city with multiple low-power copies of the fixed infra structure distributed over the coverage area on sides placed closer to the ground. Each cell side was a copy of the trunked radio installation; it's traffic channels being run by a trunking controller over a dedicated controlled channel.

The cellular concept ad a spatial dimension to the simple trunking models. The low profile, low power cell sites were linked through a central switching center and controlled function. It was the old wide area network reemploy on a grand scale.

Reducing each cell's area of the coverage invited frequency reuse. Cell using the same set of the radio channels could avoid mutual interference if they were sufficient distance a part. Interference among the cells is proportional to the transmitter power, system designer have a great leeway in determining the number of the radio channels available to the subscribers. More radio channels can be added to the system simple by decreasing the transmit power per cell, making the cells smaller and filling the vacated coverage area with new cells.

Cellular system started to spring up all over the world in early 1980's. In a crazy quilt of incompatible signals schemes deployed in different frequency bands. Each was a variation on the Amps model that appeared in the western Hemisphere, Australia as parts of Asia Some of the other simple FM systems were NMT-450 and NMT-900. IN Scandinavia, Eastern Europe and parts of Asia; C-NETZ in Germany, Portugal and south Africa; RMTS in Italy; RC-2000 in France; TACS in U.K and elsewhere; and the MCSL1 and JTACS systems in Japan.

1.2.1. FIVE PARTS CONCEPT:

Cellular system may be divided conceptually in to five parts: Radios, switching systems, database, processing centers and external networks. Often, though, multiple parts will be realized in single physical entity- a database combine with a switching system, for e.g.

The mobile connection of the cellar subscriber and fixed telecommunication network is, ofcourse, realized with the radios. The mobile station (MS) is usually hand set these days. It's corresponding base sit radio, and base transceiver station (BTS), works through a base station controller (BSC), which keeps the rest of the fixed network happily in the dark about the radio details of the mobile MS-BTS connection. Together, the BTS and BSC are called Base station.

1.3. FIRST GENERATION MOBILE SYSTEMS (1G)

All First-generation analog cellular system, such as APS, use narrow band FM radio techniques that need only 10-30Khz of a spectrum of each channel. Today, the variety of radio linked technology feeds the controversies in third generation proposals. Since radio link defines the base mobile station a lot is at stake. The arguments that to mass continuing innovation in the fixed part of the mobile networks.

The switching function is a combination of computing platform and transmission facility that out user information and signaling among nodes through out the mobile network. The functional entity is called mobile switching center (MSC). The center, it's attached base station and any inter working function to terrestrial networks or other kinds of network are collectively called a mobile switching center, and in inter working function, BMI. The BMI is said to communicate the mobile station over air interference.

Server types of database are queried by network entities while providing services to mobile subscribers. Location registers manage mobility and are unique to mobile networks. The home location register HLR permanently store subscriber data relative to network intelligence, while the visitor location register (VLR), maintain temporary working copies of active subscriber in the network.

Peripheral computing the platforms enhances the profitability of mobile networks. Authentication center (AC), for instances perform the functions that validate the mobile station identity. Voice announcement systems and message centers are other functions.

1.3.1. CATALOGUE OF EVENTS:

Cellular networks that employ tradition fm for the traffic channels are sometimes referred as First Generation systems. About 15 years past between the time the regulatory way was cleared in the U.S. for the 1st Generation AMPS deployment and their first launch in 1983. Entrenched competitive interests had funded elaborate legal delays cloaked in esoteric technical jargon. Interestingly wireless deployment in the united states have generally fallen out of the Bell monopolies-note MCI 's microwave links and the private radio common carriers. These last were mostly mom and pop organizations supplying al kinds of commercial mobile radio services, like radio paging.

AT&T, which played a key role in developing the AMPS proposal argued that the minimum critical mass of radio channels was needed before the cellular concept could work. But the radio common carrier fought bitterly for the opportunities to be awarded cellular licenses.

After some hesitation Motorola, which inherited a large portion of the mobile radio manufacturing business, took up their cause and AT&T gave up in the 1956 consent decree with the U.S. justice dept.

When the first cellular system at the last went on line in early 80's the FCC tried to foster competition by insisting that two cellular operator share the triple six channels available in each of it" market area. The B operators were the usual wire line (Bell system) operators, and the A operator were any other competent entity, some times a successful radio common carrier. Each operator got half.

1.3.2. AFTER THOUGHT:

In the retrospect, AT&T may have been right. The legacy FM technology, further under cut by this halving of each operator allotment of 30-khz channel operated inefficiently enough to keep cost from falling. Phone prices and Airtime charges were high, but the convenience of wireless tantalized enough new subscribers to courage hope. But the industry had to wait the digital radio innovation of the early 90's before real success and market would come.

1.4. SECOND GENERATION MOBILE PHONES (2G)

Fifteen years ago, mobile telephones were an exotic extravagance. Today as a Cellular phones, they are often give away as freebies in support of marketing schemes and product promotions. Having become a mainstream voice communication medium, they are poised to take over new challenges, transmission (fairly) high-speed video, data and multimedia traffic as well as voice signals to the users on the move.

The technology needed to tackle the challenges is known as Third generation cellular technology.

The principle advantage of Second-generation over it's predecessors are greater capacity and less frequent needs for battery charging. In other word, they accommodate more users in a given piece of spectrum, and they consume new power.

These two improvements have lead to low prices and increased productivity and convenience. Some in the business also claim that digital phones offer better sound quality than analog phones, but that alleged advantage is much debated, and some customers also feel that the opposite is true.

What is not debatable is that the second-generation mobile systems have pretty much the same voice services, as do the first generation systems. As far as the user is concerned, the services differ little among operators, technologies, and equipment manufacturers. That leaves network operators exposed to churn—the tendency of customers to terminate services with one network provider and sign up with another in response to an attractive promotional offering.

The second generation networks retain the inefficient circuit-switched legacy of analog networks. They were, after all, designed to carry voice traffic, which has a little tolerance of delay. Data services are more tolerant to network latencies. They offer incremental income for carriers, and can appear in many forms that encourage a wide variety of uses and terminals. By giving cellular systems a chance to stand out with unusual service providers a chance to stand out with unusual services, the third generation could reduce churn and help service providers sustain the growth rates to which they have become accustomed.

1.5. The First Revolution in Mobile Phones:

When the cellular system began switching from analog to digital transmission in early 1990's, the main goal was to increase capacity. The system therefore needed a different kind of voice coding from that employed in wired networks.

Simple pulse code modulation, as introduced into wired networks, would not, for it increased the bandwidth needed to transmit a voice cal. NO matter twisted wire pairs have bandwidths to spare, rendered unusable for analogue transmission by excessive

noise and distortion. Digital technology vanquished this impairment so that entire bandwidth could carry revenue-producing traffic.

The cellular picture is different. Bandwidth really is limited and must be husbanded. So sophisticated voice coding techniques, implemented in advanced coderdecoders (codecs), compress speech by removing some of it's natural redundancy. This they do by all kinds of assumptions about the voice traffic carried on the radio channel. And they succeeded. Whereas the usual wire line codec converts speech into 64-kb/s bit stream (8000 8-bit samples per sec), the voice coedcs get by with a fifth of that, or even less.

1.5.1. THE BREAK THROUGH:

In fact voice coding and compression may be termed the breakthrough that enabled the Second Generation of cellular radio technologies. Digital radios take some of the redundancy removed by the voice codecs and replace it using some of the codec's own carefully contrived redundancy bits, which their receiver can also use to correct errors. Channel coding extends not just the range of low-powered handsets but battery life, general approaches to be time and code division multiple access (TDMA and CDMA). The TDMA technique serves all second-generation systems except IS-95, which employs CDMA.

1.5.2. CUSTOMER APPEAL:

The digital traffic channel brought the efficiency, quality and privacy that the cellular Networks always needed, but gave subscribers no compelling reason to pay extra for Dual mode.

(AMPS/TDMA) handset. Entire TIA/EID-16 in the mid of 1990's as IS-136, defining a Digital version of the AMPS analog control channel. The digital channel has new logical resources, which brought the networks as a bulk of new features: longer battery cellular networks such as caller ID.

Subscribers finally had some reason to buy a dual-mode phone. Broadcast data, of interest to all mobile phones, and point-to-point data, directed at a specific mobile

phone, are mapped onto a digital control channel in a hierarchical partitioning scheme, on that adaptively accommodates the various messages supporting the new features.

Within a few sec after turn on, a mobile phone synchronizes with the channel's data stream as the phone enters an idle state during which it monitors the channel for message.

Data such as paging messages are partitioned in time according to an intended mobile phone's identity. This phone can then be told to remove power to most of it's circuits and wake up just in time to receive, demodulate, and decode messages in the frames reserved for it. Sleep time conserves battery capacity beyond the TDMA technique itself so that hand set can be even smaller.

While U.S. companies took care to preserve their investments in the AMPS infrastructure and the five million AMPS already in use in 1992, Europeans defined a totally new TDMA radio scheme. The quickly abandoned their early attempts to preserve analog legacy when it made clear just how fragmented that legacy was: the continents three million phones were spread among many incompatible protocols deployed on several frequency bands.

So, For it's second-generation cellular phones, Europe adopted GSM. The new technology, which operates in 900-MHz band, was designed from a clean slate, and appeared in the early 1990's fully formed. It has logical resources a plenty to give subscribers an early taste of advanced services, such as circuit switches data and short message services, that in other technology would not appear until the late 90's.

1.5.3. COMPLETELY DIFFERENT MULTI-ACCESS:

When engineers think about making the most efficient use of the radio frequency spectrum, they tend to mull improving oscillator stability, sharpening filter roll-off, and reducing guard bands. The proposal code division multiple access (CDMA) was particularly bold because it appeared after the IS-54 and GSM standards are well on their path to publication.

In the IS-95 implementation of the CDMA, there is more than one kind of spreading codes. Besides those used to segregate users, there is also a short-sequence pseudorandom code common to all a system's base station.

1.5.4. Tight Uplink Control:

Interference within the CDMA cells is controlled by very tight uplink power control. Closed-loop power control relies on a dedicated control channel over which mobile phones output tower is adjusted in 1-DB increments 800times a second.

An IS-95 channel, which is 1.2288MHz wide, fits in the same 30KHz-channel raster on which AMPS channels are arrayed. In a manner reminiscent f the IS54 protocol, IS-95 allows for CDMA-to-AMPS handoffs, but not the other way round. IS-95 operators can offer the advantages of the comprehensive coverage of AMPS networks, thus relieving the pressure to quickly build out second-generation coverage.

1.5.5. ROAMING THE NETWORKS:

There is ofcourse more to cellular systems than the air interface. Another way to categorize such systems is on the basis of the fixed networks that supported roaming; TIA/EIA and GSM.

TIA/EIA-136 and IS-95 use the TIA/EIA-41 reference model for roaming, while GSM employs a similar model of it own. Their network architectures are certainly similar, but there are four noteworthy differences between the two:

The mobile station in the GSM model is divided into two physical parts, whereas TIA/EIA-41 network see the mobile stations as a single entity in which he subscriber's mobile identification number (MIN) resides in the terminal. GSM separates the subscriber's identity and their personal records—For e.g., quick dialing numbers—from the terminal.

All interfaces in the GSM network model save the Abis interface between the base transceiver station (BTS) and it's controller, are defined in the open standards. Similar standardization is only just now being formulated for the TIA/EIA-41 networks.

The authentication procedures are different. TIA/EIA based authentication relies on the cellular authentication and voice encryption (CAVE) algorithm. GM-based authentication is based on a different scheme, called A3/A8, which resides entirely in the SIM. Operators can have their own implementations of SIM-based authentication. Mobile radio networks use packet switched common channel communication protocols among their databases so those subscribers may roam among network. TIA/EIA-41 allows X.25 and SS7 communication protocols, but most is SS7 based. GSM networks are always SS7 based.

1.5.6. UNMATCHED MESSAGES:

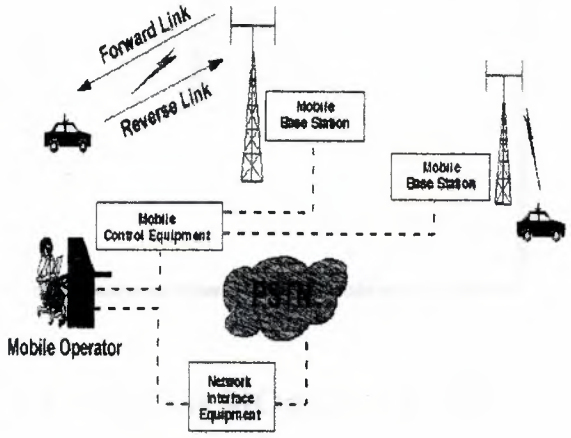
To make subscriber's mobility into account, both mobile radio network types add extra message types to the normal kin moving between the nodes. The applications are called Mobile application Part (MAP) messages.

2. THE CELLULAR TECHNOLOGY

2.1. 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. Alexander Graham Bell invented the telephone, 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!

Figure 2.1 Basic Mobile Telephone Service Network



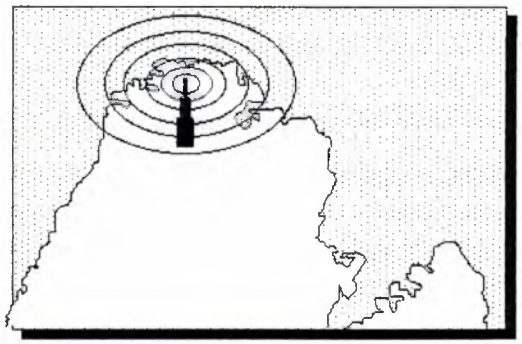
2.2. EARLY MOBILE TELEPHONE SYSTEM ARCHITECTURE

In the dark ages before cell phones, people who really needed mobile communications ability installed radiotelephones in their cars. In the radio telephone 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.

Traditional mobile service was structured in a fashion similar to television broadcasting: One very powerful transmitter located at the highest spot in an area would broadcast in a radius of up to 50 kilometers. The cellular concept structured the mobile telephone

network in a different way. Instead of using one powerful transmitter, many low-power transmitters were placed throughout a coverage area. For example, by dividing a metropolitan region into one hundred different areas (cells) with low-power transmitters using 12 conversations (channels) each, the system capacity theoretically could be increased from 12 conversations—or voice channels using one powerful transmitter—to 1,200 conversations (channels) using one hundred low-power transmitters. *Figure 2* shows a metropolitan area configured as a traditional mobile telephone network with one high-power transmitter.

Figure 2.2 Early Mobile Telephone System Architecture



2.3. CELLULAR MOBILE SYSTEMS

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

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 million 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

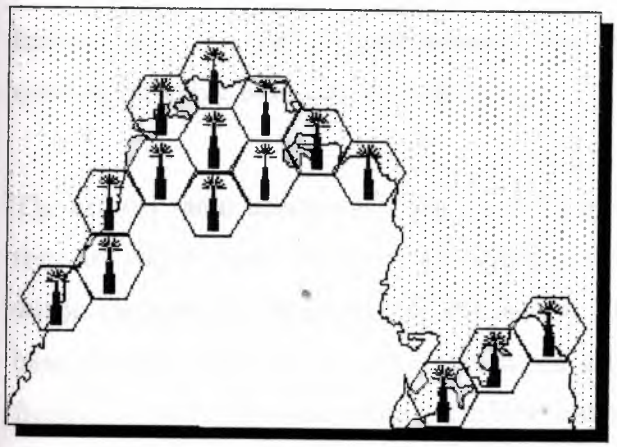
the city into cells. Each cell is typically sized at about 10 square miles (26 square kilometers). Cells are normally thought of as hexagons on a big hexagonal grid

Because cell phones and base stations use low-power transmitters, the same frequencies can be reused in non-adjacent cells. The two purple cells can reuse the same frequencies.

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, is 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.
- Therefore, each cell has 56 or so voice channels available.

Figure 2.3 Mobile Telephone System Using a Cellular Architecture



In other words, in any cell, 56 people can be talking on their cell phones at one time. With digital transmission 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.

2.3.1. POWER TRANSMITTERS:

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.

2.3.2. BASE STATIONS:

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 the entire base stations in the region.

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

2.4. CELLULAR SYSTEM ARCHITECTURE

Increases in demand and the poor quality of existing service led mobile service providers to research ways to improve the quality of service and to support more

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

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

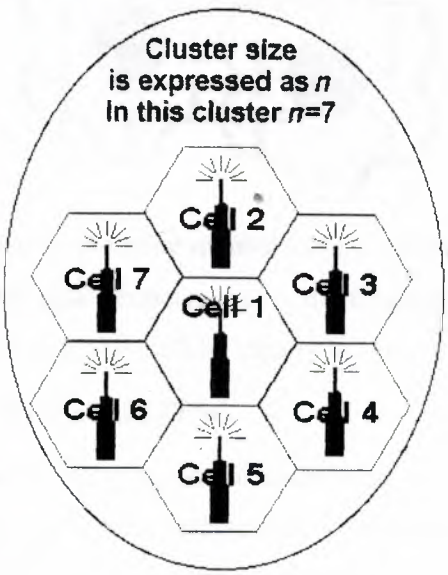
1- CELLS

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

2- CLUSTERS

A cluster is a group of cells. No channels are reused within a cluster. *Figure 4* illustrates a seven-cell cluster.

Figure 2.4 A Seven-Cell Cluster

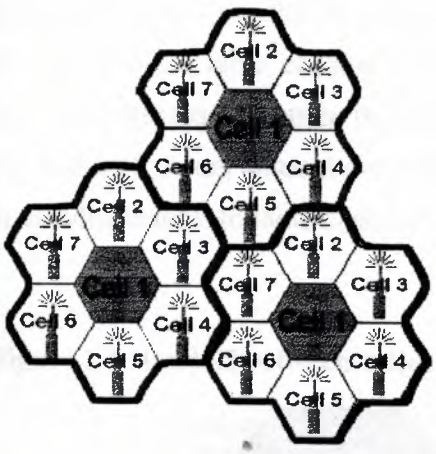


3- FREQUENCY REUSE

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

The concept of frequency reuse is based on assigning to each cell a group of radio channels used within a small geographic area. Cells are assigned a group of channels that is completely different from neighboring cells. The coverage area of cells is called the footprint. This footprint is limited by a boundary so that the same group of channels can be used in different cells that are far enough away from each other so that their frequencies do not interfere (see *Figure 5*).

Figure 2.5 Frequency Reuse



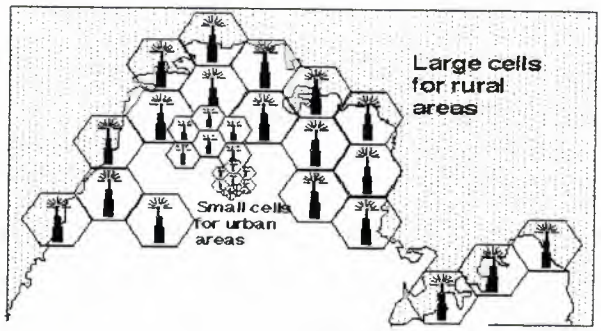
Cells with the same number have the same set of frequencies. Here, because the number of available frequencies is 7, the frequency reuse factor is 1/7. That is, each cell is using 1/7 of available cellular channels.

3- CELL SPLITTING

Unfortunately, economic considerations made the concept of creating full systems with many small areas impractical. To overcome this difficulty, system operators developed the idea of cell splitting. As a service area becomes full of users, this approach is used to split a single area into smaller ones. In this way, urban centers can be split into as many

areas as necessary to provide acceptable service levels in heavy-traffic regions, while larger, less expensive cells can be used to cover remote rural regions (see *Figure 6*).

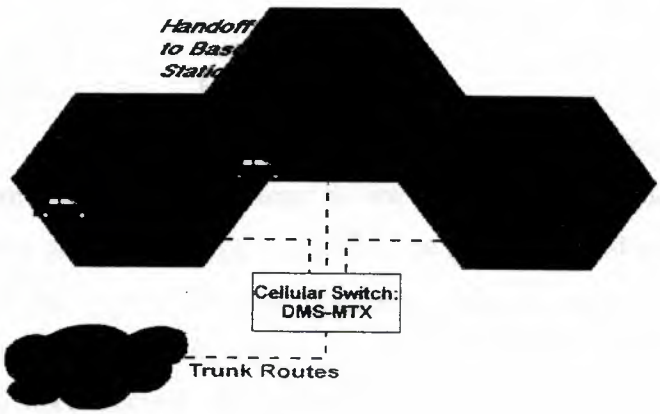
Figure 2.6 Cell Splitting



4- HANDOFF

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

Figure 2.7 Handoff between Adjacent Cells



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

2.5. CELL PHONES 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 vs. 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. 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.

- 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. Cell phones are duplex.

2.6. DIGITAL CELL PHONES

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. It is amazing how much more efficient digital systems can be.

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.

2.7. CELLULAR ACCESS TECHNOLOGIES

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

- **Frequency Division Multiple Access (FDMA)**
- **Time Division Multiple Access (TDMA)**
- **Code Division Multiple Access (CDMA)**

Although these technologies sound very intimidating, you can get a good sense of how they work just by breaking down the title of each one.

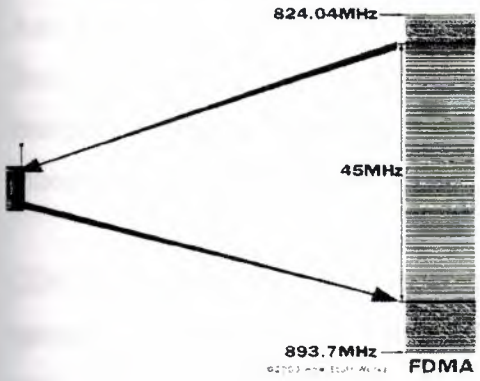
The first word tells you what the access method is and the second word, **division**, lets you know that it splits calls based on that access method.

- 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 access**. This simply means that more than one user (multiple) can use (access) each cell.

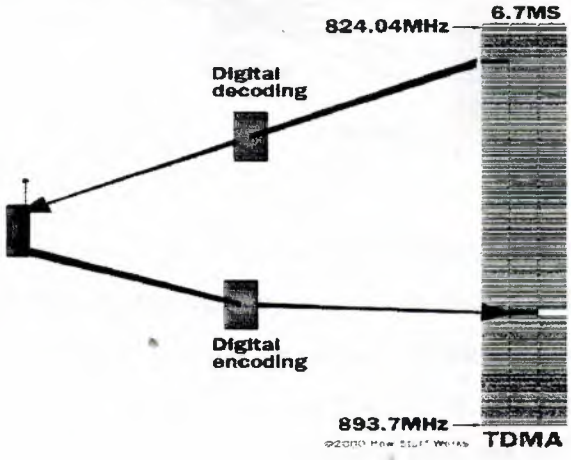
FDMA separates the spectrum into distinct voice channels by splitting it into uniform chunks of bandwidth. To better understand FDMA, think of radio stations. Each station sends its signal at a different frequency within the available band. FDMA is used mainly for analog transmission. While it is certainly capable of carrying digital information, FDMA is not considered to be an efficient method for digital transmission.

Figure 2.8 Use of frequencies in FDMA



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 operate in either the 800 MHz (IS-54) or 1900 MHz (IS-136) frequency bands.

Figure 2.9 Splitting of frequency in TDMA

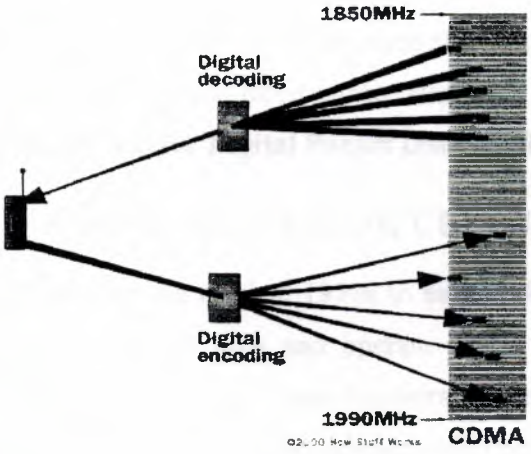


TDMA is also used as the access technology for **Global System for Mobile communications (GSM)**. However, GSM implements TDMA in a somewhat different and incompatible way from IS-136. Think of GSM and IS-136 as two different operating systems that work on the same processor, like Windows and Linux both working on an Intel Pentium III. GSM systems use **encryption** to make phone calls

more secure. GSM operates in the 900 MHz band (890 MHz - 960 MHz) 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.

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. 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 2.10 CDMA



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.

2.8. 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 gigahertz (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.

2.9. NORTH AMERICAN ANALOG CELLULAR SYSTEMS

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

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

- call-processing sequences

2.10. THE ADVANCED MOBILE PHONE SERVICE (AMPS)

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

- low calling capacity
- limited spectrum
- no room for spectrum growth
- poor data communications
- minimal privacy
- inadequate fraud protection

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

2.11. NARROWBAND ANALOG MOBILE PHONE SERVICE (NAMPS)

Since analog cellular was developed, systems have been implemented extensively throughout the world as first-generation cellular technology. In the second generation of analog cellular systems, NAMPS was designed to solve the problem of low calling capacity. NAMPS is now operational in 35 U.S. and overseas markets, and NAMPS was introduced as an interim solution to capacity problems. NAMPS is a U.S. cellular radio system that combines existing voice processing with digital signaling, tripling the capacity of today's AMPS systems. The NAMPS concept uses frequency

division to get 3 channels in the AMPS 30-kHz single channel bandwidth. NAMPS provides 3 users in an AMPS channel by dividing the 30-kHz AMPS bandwidth into 3 10-kHz channels. This increases the possibility of interference because channel bandwidth is reduced.

2.12. CELLULAR SYSTEM COMPONENTS

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

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

1-PUBLIC SWITCHED TELEPHONE NETWORK (PSTN)

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

2-MOBILE TELEPHONE SWITCHING OFFICE (MTSO)

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

3-THE CELL SITE

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

4-MOBILE SUBSCRIBER UNITS (MSUs)

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

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

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

2.12. DUAL BAND VS. 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.

Changing bands or modes is done automatically by phones that support these options. 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

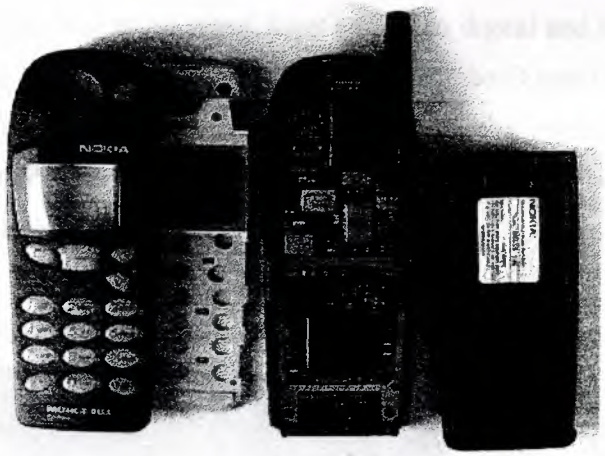
switch to 800 MHz if it cannot connect at 1900 MHz. And if the phone supports more than one mode, it will try the digital mode(s) first, then switch to analog.

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.

2.14. 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.

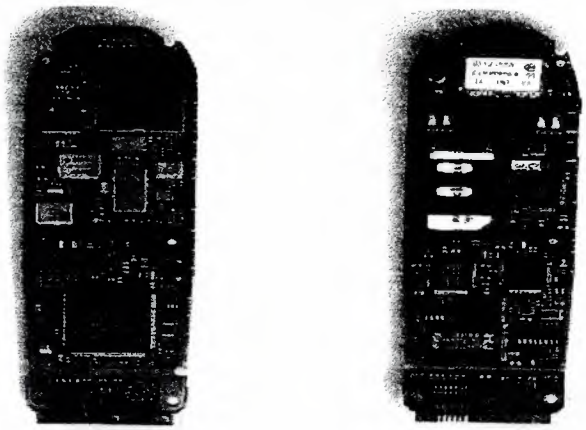
Figure 2.11 An In-depth look at cell phone



- An amazing 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

Figure 2.12 Front and Back of circuit board



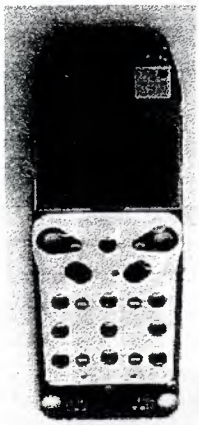
In the photos above, you see several computer chips. Lets talk about what some of the individual chips do. The **Analog-to-Digital** and **Digital-to-Analog** conversion chips translate the outgoing audio signal from analog to digital and the incoming signal from digital back to analog. You can learn more about A-to-D and D-to-A conversion and its importance to digital audio in the **How Stuff Works** article on compact discs. The **Digital Signal Processor (DSP)** is a highly customized processor designed to perform signal manipulation calculations at high speed.

Figure 2.13 The microprocessor

The microprocessor 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 ROM and flash memory chips

provide storage for the phone's operating system and customizable features, such as the phone directory. The RF and power section handles power management and recharging, and also deals with the hundreds of FM channels. Finally, the RF amplifiers handle signals in and out of antenna.

Figure 2.14 The display and keypad contacts.



The display 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**.

Figure 2.15 The flash memory card on the circuit board.

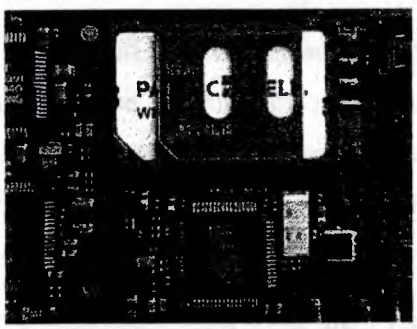
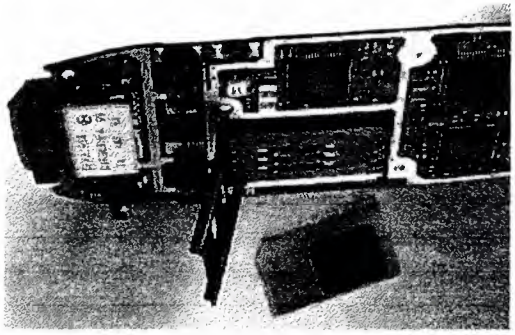
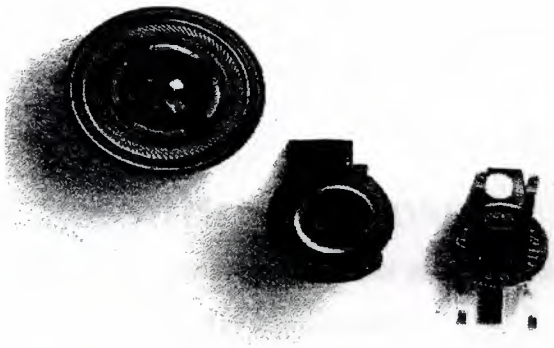


Figure 2.16 The flash memory card removed.



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 2.17 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 you can see in the picture above, 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.

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 phones 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 PADS , MP3 players and GPS receivers (some models).

2.15 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:

- Generally, non-repairable internal **corrosion** of parts results if you get the phone wet or use 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.
- 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.
- **Cracked display screens** can happen when an overstuffed briefcase squeezes the cell phone.
- 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.

3. INTRODUCTION TO GSM

3.1. HISTORY OF GSM

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

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

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

In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase I of the GSM specifications was published in 1990. The original French name was later changed to **Global System for Mobile Communications**, but the original GSM acronym stuck.

Commercial service was started in mid-1991, and by 1993 there were 36 GSM networks in 22 countries. Although standardized in Europe, GSM is not only a European standard. Over 200 GSM networks (including DCS1800 and PCS1900) are operational in 110 countries around the world. In the beginning of 1994, there were 1.3 million subscribers worldwide, which had grown to more than 55 million by October 1997. With North America making a delayed entry into the GSM field with a derivative of GSM called PCS1900, GSM systems exist on every continent.

The developers of GSM chose an unproven (at the time) digital system, as opposed to the then-standard analog cellular systems like AMPS in the United States and TACS in the United Kingdom. The over 8000 pages of GSM recommendations try to allow flexibility and competitive innovation among suppliers, but provide enough standardization to guarantee proper interworking between the components of the system. This is done by providing functional and interface descriptions for each of the functional entities defined in the system.

1-Analogue Cellular Networks

AMPS	Advanced Mobile Phone System. Developed by Bell Labs in the 1970s and first used commercially in the United States in 1983. It operates in the 800 MHz band and is currently the world's largest cellular standard.
C-450	Installed in South Africa during the 1980's. Now known as Motorphone and run by Vodacom.
C-Nezt	Cellular technology found mainly in Germany. It operates at 450 MHz.
N-AMPS	Narrowband Advanced Mobile Phone System. Developed by Motorola as an interim technology between analogue and digital. It has some three times greater capacity than AMPS and operates in the 800 MHz range.
NMT450	Nordic Mobile Telephones/450. Developed specially by Ericsson and Nokia to service the rugged terrain that characterizes the Nordic countries. Operates at 450 MHz.
NMT900	Nordic Mobile Telephones/900. The 900 MHz upgrade to NMT 450 developed by the Nordic countries to accommodate higher capacities and handheld portables.

TACS	Total Access Communications System. Developed by Motorola. and is similar to AMPS. It was first used in the United Kingdom in 1985, although in Japan it is called JTAC. It operates in the 900 MHz frequency range.
NTT	Nippon Telegraph and Telephone. The old Japanese analogue standard. A high-capacity version is called HICAP.

2-Digital Cellular Networks

CDMA	Code Division Multiple Access. Developed by Qualcomm Inc. and is characterized by high capacity and small cell radius. The Telecommunications Industry Association (TIA) in 1993 adopted it. The first CDMA-based networks are now operational.
D-AMPS	Digital AMPS. An upgrade to the analogue AMPS. A AMPS/D-AMPS infrastructure can support use of either analogue AMPS phone or digital D-AMPS phones. This was because the Federal Communications Commission mandated only that digital cellular in the U.S. must act in a dual-mode capacity with analogue. Both operate in the 800 MHz band.
DCS 1800	Digital Cordless Standard. GSM operated in the 1800 MHz range. It is a different version of GSM, and (900 MHz) GSM phones cannot be used on DCS 1800 networks.
GSM	Global System for Mobile Communications. The first European digital standard, developed to establish cellular compatibility throughout Europe. It's success has spread to all parts of the world and over 80 GSM networks are now operational. It operates at 900 MHz.
PCS	Personal Communications Service. The American version of GSM, but GSM phones cannot be used on PCS networks. It operates in the 1,900 MHz range.
PHS	Personal Handy System. A Japanese-centric system that offers high speed data services and superb voice clarity.
TDMA	Time Division Multiple Access. The first U.S. digital standard to be developed. It was adopted by the TIA in 1992. The first TDMA commercial system began in 1993.

3.2. SERVICES PROVIDED BY GSM

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

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

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

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

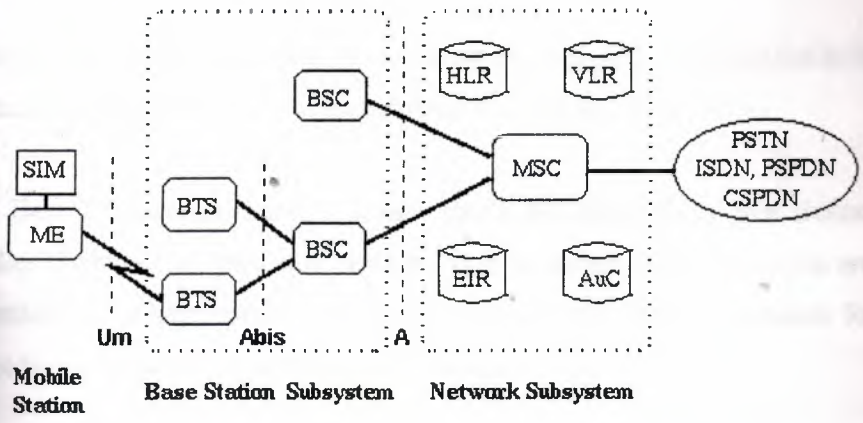
Supplementary services are provided on top of teleservices or bearer services. In the current (Phase I) specifications, they include several forms of call forward (such as call forwarding when the mobile subscriber is unreachable by the network), and call barring

of outgoing or incoming calls, for example when roaming in another country. Many additional supplementary services will be provided in the Phase 2 specifications, such as caller identification, call waiting, multi-party conversations.

3.3. ARCHITECTURE OF THE GSM NETWORK

A GSM network is composed of several functional entities, whose functions and interfaces are specified. Figure 3.1 shows the layout of a generic GSM network. The GSM network can be divided into three broad parts. The Mobile Station is carried by the subscriber. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center (MSC), performs the switching of calls between the mobile users, and between mobile and fixed network users. The MSC also handles the mobility management operations. Not shown is the Operations and Maintenance Center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile services Switching Center across the A interface.

Figure 3.1 General architecture of a GSM network



SIM Subscriber Identity Module
ME Mobile Equipment
BTS Base Transceiver Station
BSC Base Station Controller
HLR Home Location Register
VLR Visitor Location Register
MSC Mobile services Switching Center
EIR Equipment Identity Register
AuC Authentication Center

1-MOBILE STATION

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

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

2-BASE STATION SUBSYSTEM

The Base Station Subsystem is composed of two parts,

1- The Base Transceiver Station (BTS)
2- The Base Station Controller (BSC)

These communicate across the standardized Abis interface, allowing (as in the rest of the system) operation between components made by different suppliers.

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

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

3-MOBILE SWITCHING CENTRE

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

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call routing and roaming capabilities of GSM.

5-HOME LOCATION REGISTER

The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The location of the mobile is typically in the form of the signaling address of the VLR associated with the mobile station. There is logically one HLR per GSM network, although it may be implemented as a distributed database. When we "hand-over" to another cell whilst driving, the HLR is automatically updated, and continues to monitor where exactly it should route our calls should you then move within range of to another Vodacom BS. This sophisticated routing procedure means that out of hundreds of thousands of subscribers, only the correct cellphone will ring when necessary.

6-VISITOR LOCATION REGISTER

The Visitor Location Register (VLR) contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, all manufacturers of switching equipment to date implement the VLR together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR,

thus simplifying the signaling required. Note that the MSC contains no information *about particular mobile stations --- this information is stored in the location registers.* The other two registers are used for authentication and security purposes.

7-EQUIPMENT IDENTITY REGISTER

The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved.

8-AUTHENTICATION CENTER

The Authentication Center (AuC) is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel.

9-SHORT MESSAGE SYSTEM CENTER

Some voicemail systems are linked to a network's SMS Center (SMSC), a special facility that handles Short Messages. The SMSC generates the special SMS message that notifies you that you have mail waiting in your Mailbox.

SMS messages can be received on your SMS-capable cellphone even while you're on a voice call. That's because they are sent on a different radio frequency - the GSM data channel - than voice calls, so that the two never interfere. These sophisticated digital facilities are the reason why GSM is now considered the de facto global cellular standard.

3.4. RADIO LINK ASPECTS

The International Telecommunication Union (ITU), which manages the international allocation of radio spectrum (among many other functions), allocated the bands 890-915 MHz for the uplink (mobile station to base station) and 935-960 MHz for the downlink (base station to mobile station) for mobile networks in Europe. Since this range was already being used in the early 1980s by the analog systems of the day,

the CEPT had the foresight to reserve the top 10 MHz of each band for the GSM network that was still being developed. Eventually, GSM will be allocated the entire 2x25 MHz bandwidth.

3.4.1. MULTIPLE ACCESS AND CHANNEL STRUCTURE

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

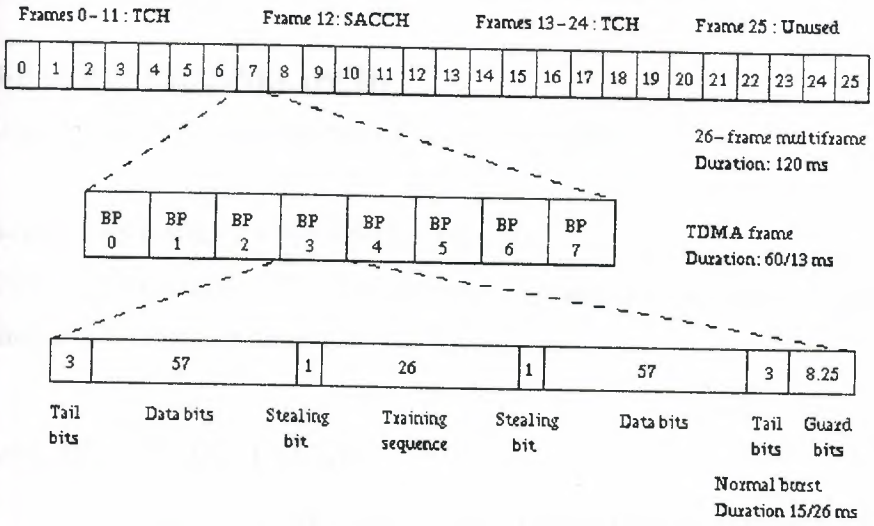
The number and position of their corresponding burst periods define channels. All these definitions are cyclic, and the entire pattern repeats approximately every 3 hours. Channels can be divided into *dedicated channels*, which are allocated to a mobile station, and *common channels*, which are used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

3.4.2. TRAFFIC CHANNELS

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multiframe, or group of 26 TDMA frames. The length of a 26-frame multiframe is 120 ms, which is how the length of a burst period is defined (120 ms divided by 26 frames divided by 8 burst periods per frame). Out of the 26 frames, 24 are used for traffic, 1 is used for the Slow Associated Control Channel (SACCH) and 1 is currently unused (see Figure 2). TCHs for the uplink and downlink are separated in time by 3 burst periods, so that the mobile station does not have to transmit and receive simultaneously, thus simplifying the electronics.

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

Figure 3.2. Organization of bursts, TDMA frames, and multiframes for speech and date



3.4.3. CONTROL CHANNELS

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

1-BROADCAST CONTROL CHANNEL (BCCH)

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

2-FREQUENCY CORRECTION CHANNEL (FCCH) AND SYNCHRONIZATION CHANNEL (SCH)

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

3-RANDOM ACCESS CHANNEL (RACH)

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

4-PAGING CHANNEL (PCH)

Used to alert the mobile station of an incoming call.

5-ACCESS GRANT CHANNEL (AGCH)

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

3.4.4. BURST STRUCTURE

There are four different types of bursts used for transmission in GSM. The normal burst is used to carry data and most singling. It has a total length of 156.25 bits, made up of two 57 bit information bits, a 26 bit training sequence used for equalization, 1 stealing bit for each information block (used for FACCH), 3 tail bits at each end, and an 8.25 bit guard sequence, as shown in Figure 2. The 156.25 bits are transmitted in 0.577 ms, giving a gross bit rate of 270.833 KBPS.

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

3.5. SPEECH CODING IN GSM

GSM is a digital system, so speech, which is inherently analog, has to be digitized. The method employed by ISDN, and by current telephone systems for multiplexing voice lines over high-speed trunks and optical fiber lines, is Pulse Coded Modulation (PCM). The output stream from PCM is 64 KBPS, too high a rate to be feasible over a radio link. The 64 KBPS signal, although simple to implement, contains much redundancy. The GSM group studied several speech coding algorithms on the basis of subjective speech quality and complexity (which is related to cost, processing delay, and power consumption once implemented) before arriving at the choice of a Regular Pulse Excited -- Linear Predictive Coder (RPE--LPC) with a Long Term Predictor loop. Basically, information from previous samples, which does not change very quickly, is used to predict the current sample. The coefficients of the linear combination of the previous samples, plus an encoded form of the residual, the difference between the predicted and actual sample, represent the signal. Speech is divided into 20 millisecond samples, each of which is encoded as 260 bits, giving a total bit rate of 13 KBPS. This is the so-called Full-Rate speech coding. Recently, an Enhanced Full-Rate (EFR) speech-coding algorithm has been implemented by some North American GSM1900 operators. This is said to provide improved speech quality using the existing 13 KBPS bit rate.

3.6. CHANNEL CODING

- The overall data rate for the radio channel is **270kb/s.**
- This is split into B full rate or 16 half rate traffic channels, plus the signaling channels.
- The coding is complex in order to have the maximum chance to detect and correct the errors encountered in a typical propagation path.
- The output of the speech coder is **encrypted**, **coded** and **interleaved** in a sophisticated way to allow **Forward Error Correction** to be applied.

- The data is then sent as bursts **in time slots of 577µs**, each containing **116 encrypted bits**.
- There are 8 or 16 of these time slots per TDMA frame, and the receive and transmit time slots are staggered so that the mobile station is not receiving at the same instant as it is transmitting, thus simplifying the filtering requirements.
- With this scheme, there can be at least one spare slot between transmit and receive, leaving time for the synthesizer to change frequency (whether or not hopping is employed).
- The receiver also monitors adjacent cell for one time slot each frame to determine their signal strength to optimize a possible handover.

3.7. MULTIPATH EQUALIZATION

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

3.8. FREQUENCY HOPPING

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

3.9. DISCONTINUOUS TRANSMISSION

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

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

3.10. DISCONTINUOUS RECEPTION

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

3.11. POWER CONTROL

There are five classes of mobile stations defined, according to their peak transmitter power, rated at 20, 8, 5, 2, and 0.8 watts. To minimize co-channel interference and to conserve power, both the mobiles and the Base Transceiver Stations operate at the lowest power level that will maintain an acceptable signal quality. Power

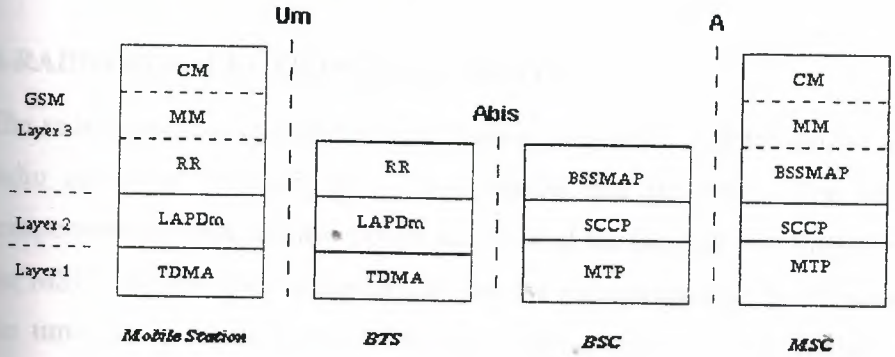
levels can be stepped up or down in steps of 2 dB from the peak power for the class down to a minimum of 13 DBMS (20 milliwatts).

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

3.12. NETWORK ASPECTS

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

Figure 3.3 Singling protocol structure in GSM



The singling protocol in GSM is structured into three general layers, depending on the interface, as shown in Figure 3.3. Layer 1 is the physical layer, which uses the channel structures discussed above over the air interface. Layer 2 is the data link layer. Across the Um interface, the data link layer is a modified version of the LAPD protocol used in ISDN, called LAPDm. Across the A interface, the Message Transfer Part layer 2 of

Singling System Number 7 is used. Layer 3 of the GSM singling protocol is itself divided into 3 sublayers.

1-RADIO RESOURCES MANAGEMENT

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

2-MOBILITY MANAGEMENT

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

3-CONNECTION MANAGEMENT

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

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

4-RADIO RESOURCES MANAGEMENT

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

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

handles the management of radio features such as power control, discontinuous transmission and reception, and timing advance.

5-MOBILITY MANAGEMENT

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

6-COMMUNICATION MANAGEMENT

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

3.13. HANDOVER

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

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

- Channels (time slots) in the same cell
- Cells (Base Transceiver Stations) under the control of the same Base Station Controller (BSC),

- Cells under the control of different BSCs, but belonging to the same Mobile services Switching Center (MSC), and
- Cells under the control of different MSCs.

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

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

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

3.14. CALL ROUTING

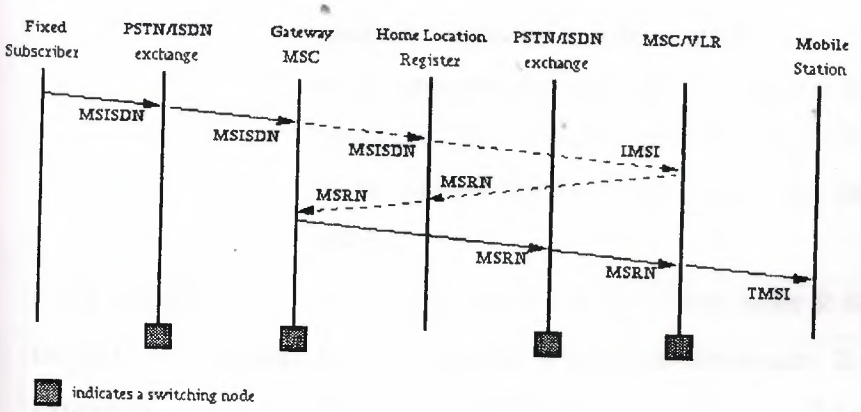
Unlike routing in the fixed network, where a terminal is semi-permanently wired to a central office, a GSM user can roam nationally and even internationally. The directory number dialed to reach a mobile subscriber is called the Mobile Subscriber ISDN (MSISDN), which is defined by the E.164 numbering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

operator. The first few digits of the remaining subscriber number may identify the subscriber's HLR within the home PLMN.

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

The routing information that is returned to the GMSC is the Mobile Station Roaming Number (MSRN), which is also defined by the E.164 numbering plan. MSRNs are related to the geographical numbering plan, and not assigned to subscribers, nor are they visible to subscribers. The most general routing procedure begins with the GMSC querying the called subscriber's HLR for an MSRN. The HLR typically stores only the SS7 address of the subscriber's current VLR, and does not have the MSRN (see the location updating section). The HLR must therefore query the subscriber's current VLR, which will temporarily allocate an MSRN from its pool for the call. This MSRN is returned to the HLR and back to the GMSC, which can then route the call to the new MSC. At the new MSC, the IMSI corresponding to the MSRN is looked up, and the mobile is paged in its current location area (see Figure 3.4).

Figure 3.4 Call routing for a mobile terminating call



3.15. HOW THE MOBILE WORK

Figure 3.5 sectional study of mobile

Component	Purpose
Microphone	Captures your voice for conversion from analogue to digital mode
Speaker	Allows monitoring of remote phone
LCD Display	Shows Call, Phone, Signal & Network Info
Keypad	Allows access to specific remote phones
Battery + Meter	While battery housings on cellphones are standard input deigns, some cellphones also have some "battery processing" intelligence built in. For example, they will check the charge level to start or stop the charge when the phone is connected to a desktop, car or quick charger and even automatically discharge the battery for you when necessary. This is usually linked to the LCD display and to an audible beep to warn you of the battery charge status.
LED Lights	Status Information, usually Green, white & Red.
Digital Signal Processor	The DSP chipset is a critical component. It co-ordinates the voice, SMS and data/fax features of a cellphone. It

	processes speech, handles voice activity detection, as well as discontinuous GSM transmission and reception. Another section amplifies the input signal received from the microphone, while another converts this microphone voice signal from "analogue" to "digital". The digital conversion is necessary because the GSM cellular standard is a completely digital system.
CODEC	This DSP's voice processing is done in tandem with highly sophisticated compression technique mediated by the "CODEC" (compressor/decompressor) portion of the cellphone. T
RF Unit	The CODEC chipset instantly transfers this "compressed" information to the cellphone's Radio Frequency (RF) unit. This RF unit, which is essentially the transmit and receive section of the cellphone, then sends out the voice or data information via the cellphone antenna, over the air and on to the nearest cellular base station - and ultimately to your call destination. The incoming voice also travels much the same route, although it is first uncompressed from it's incoming digital form into an audible analogue form which is then piped out as sound through the cellphone's speaker. This analogue-to-digital and digital-to-analogue voice conversion via the CODEC is done at very high speeds, so that you never really experience any delay between talking and the other person hearing you (and visa versa).
SIM Card Reader	When you switch on your phone with a "live" SIM card inside, the subscriber information on the chip inside the SIM card is read by the SIM card reader and then transmitted digitally to the network via the RF unit. The same route is followed when you hit the Call button (and its variants) on the cellphone: the number you've inputted is instantly and digitally transferred to the network for

	processing.
External Connectors	At the bottom of most cellphones there is an external connector system. You can usually plug in a data/fax adapter, or a battery charger, or a personal hands free device, or a car-kit with external antenna connections. You'll also find many with separate "speaker" and LED lights that are activated when the phone rings and/or when the battery is low. Many phones also have tiny LED lights under the keypad that light up when you press a key and/or when the phone rings.
On-Board Memory	Many cellphones also have a certain amount of on-board memory chip capacity available for storing outgoing telephone numbers, your own telephone number, as well as incoming and outgoing SMS messages. Some allow copying between the (limited) memory on the SIM card and the phone's own internal memory.
Antenna System	Cellphone manufacturers are implementing many weird and wonderful permutations of antenna system designs. While some are stubby, fixed types, the most predominant designs though are those with thin, pull-out steel rods all of whom usually fit snugly into a special antenna shaft. These antenna designs, be they the stubby or pull-out types, all conform to the same circa 900 MHz frequency transmit and receive range required by the GSM specification.

4. SMART CARDS

4.1. SUBSCRIBER'S INFORMATION MODULE (SIM)

Today, the SIM card's basic functionality in wireless communications is subscriber authentication and roaming. Although such features may be achieved via a centralized intelligent network (IN) solution or a smarter handset, there are several key benefits that could not be realized without the use of a SIM card, which is external to a mobile handset. These benefits—enhanced security, improved logistics, and new marketing opportunities—are key factors for effectively differentiating wireless service offerings. will discuss the security benefits, logistical issues, marketing opportunities, and customer benefits associated with smart cards.

4.2. SMART CARD OVERVIEW

The smart card is one of the latest additions to the world of information technology (IT). The size of a credit card, it has an embedded silicon chip that enables it to store data and communicate via a reader with a workstation or network. The chip also contains advanced security features that protect the card's data.

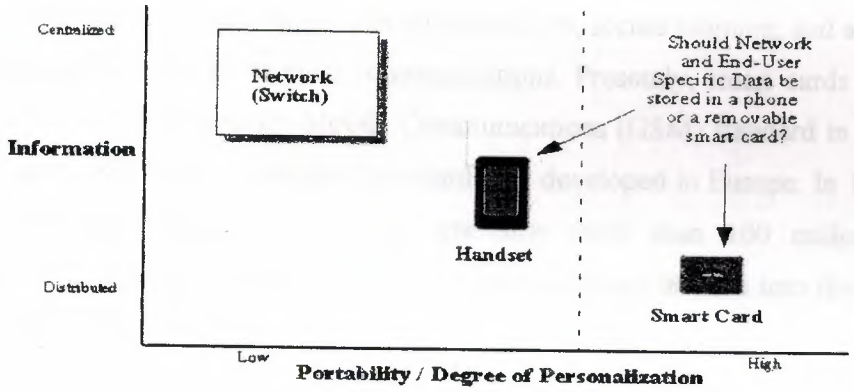
Smart cards come in two varieties: microprocessor and memory. Memory cards simply store data and can be viewed as small floppy disks with optional security. Memory cards depend on the security of a card reader for their processing. A microprocessor card can add, delete, and manipulate information in its memory on the card. It is like a miniature computer with an input and output port, operating system, and hard disk with built-in security features.

Smart cards have two different types of interfaces. Contact smart cards must be inserted into a smart-card reader. The reader makes contact with the card module's electrical connectors that transfer data to and from the chip. *Contactless* smart cards are passed near a reader with an antenna to carry out a transaction. They have an electronic microchip and an antenna embedded inside the card, which allow it to communicate without a physical contact. Contactless cards are an ideal solution when transactions must be processed quickly, as in mass transit or toll collection.

A third category now emerging is a dual interface card. It features a single chip that enables a contact and contactless interface with a high level of security.

Two characteristics make smart cards especially well suited for applications in which security-sensitive or personal data is involved. First, because a smart card contains both the data and the means to process it, information can be processed to and from a network without divulging the card's data. Secondly, because smart cards are portable, users can carry data with them on the smart card rather than entrusting that information on network storage or a backend server where the information could be sold or accessed by unknown persons (see Figure 4.1).

Figure 4.1 Information and Personalization



A smart card can restrict the use of information to an authorized person with a password. However, if this information is to be transmitted by radio frequency or telephone lines, additional protection is necessary. One form of protection is ciphering (scrambling data). Some smart cards are capable of ciphering and deciphering, so the stored information can be transmitted without compromising confidentiality. Smart cards can cipher into billions of foreign languages and choose a different language at random every time they communicate. This process ensures that only authenticated cards and computers are used and makes hacking or eavesdropping virtually impossible. The top five applications for smart cards throughout the world currently are as follows:

- **public telephony**—prepaid phone memory cards using contact technology
- **mobile telephony**—mobile phone terminals featuring subscriber identification and directory services
- **banking**—debit/credit payment cards and electronic purse

- **loyalty**—storage of loyalty points in retail and gas industries
- **pay-TV**—access key to TV broadcast services through a digital set-top box

The benefits of using smart cards depend on the application. In general, applications supported by smart cards benefit consumers where their lifestyles intersect with information access and payment-related processing technologies. These benefits include the ability to manage or control expenditures more effectively, reduce fraud and paperwork, and eliminate the need to complete redundant, time-consuming forms. The smart card also provides the convenience of having one card with the ability to access multiple services, networks, and the Internet.

4.3. SMART CARDS IN WIRELESS COMMUNICATIONS

Smart cards provide secure user authentication, secure roaming, and a platform for value-added services in wireless communications. Presently, smart cards are used mainly in the Global System for Mobile Communications (GSM) standard in the form of a SIM card. GSM is an established standard first developed in Europe. In 1998, the GSM Association announced that there are now more than 100 million GSM subscribers. In the last few years, GSM has made significant inroads into the wireless markets of the Americas.

Initially, the SIM was specified as a part of the GSM standard to secure access to the mobile network and store basic network information. As the years have passed, the role of the SIM card has become increasingly important in the wireless service chain. Today, SIM cards can be used to customize mobile phones regardless of the standard (GSM, personal communications service [PCS], satellite, digital cellular system [DCS], etc.).

Today, the SIM is the major component of the wireless market, paving the way to value-added services. SIM cards now offer new menus, prerecorded numbers for speed dialing, and the ability to send presorted short messages to query a database or secure transactions. The cards also enable greeting messages and company logotypes to be displayed.

Other wireless communications technologies rely on smart cards for their operations. Satellite communications networks (Iridium and Globalstar) are chief examples.

Eventually, new networks will have a common smart object and a universal identification module (UIM), performing functions similar to SIM cards.

4.4. ENHANCED SECURITY BENEFITS

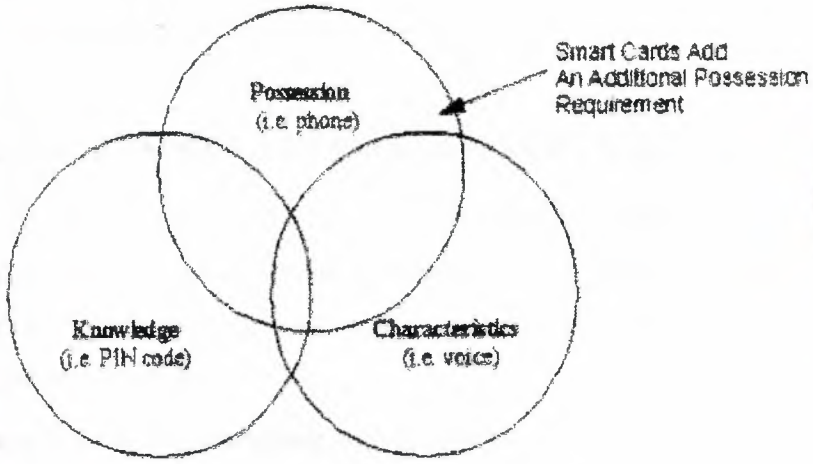
SIM cards have several features that enhance security for wireless communications networks. Smart-card supporters point to the potential of limiting or eliminating fraud as one of their strongest selling points.

SIM cards provide a secure authentication key transport container from the carrier's authentication center to the end-user's terminal. Their superior fraud protection is enabled by hosting the cryptographic authentication algorithm and data on the card's microprocessor chip. SIM cards can be personal identification number (PIN) protected and include additional protection against logical attacks. With added PIN code security, SIM cards offer the same level of security used by banks for securing off-line payments. Because the home network–authentication algorithm also resides in the card, SIM cards make secure roaming possible. They can also include various authentication mechanisms for internetwork roaming of different types.

Complete fraud protection (with the exclusion of subscription fraud) can only be provided in the context of a complete security framework that includes terminal authentication, an authentication center, and authentication key management. Smart cards are an essential piece of this environment, but only the complete architecture can allow fraud reduction and secure roaming.

Finally, it should be noted that biometric smart-card applications such as voice or fingerprint recognition could be added to provide maximum fraud prevention. Smart cards could then combine the three basic security blocks of possession, knowledge, and characteristics (see Figure 4.2).

Figure 4.2. Identification Model



Source : 1994 Advanced Card and Identification Technology Sourcebook

4.5. EASING LOGISTICAL ISSUES

All subscribers may easily personalize and depersonalize their mobile phone by simply inserting or removing their smart cards. The card's functions are automatically enabled by the electronic data interchange (EDI) links already set between carriers and secure personalization centers. No sophisticated programming of the handset is necessary.

By placing subscription information on a SIM card, as opposed to a mobile handset, it becomes easier to create a global market and a distribution network of phones. These noncarrier-specific phones can increase the diversity, number, and competition in the distribution channel, which can ultimately help lower the cost of customer acquisition. Smart cards make it easier for households and companies to increase the number of subscriptions, thereby increasing usage. They also help to create a market for ready-to-use preowned handsets that require no programming before use.

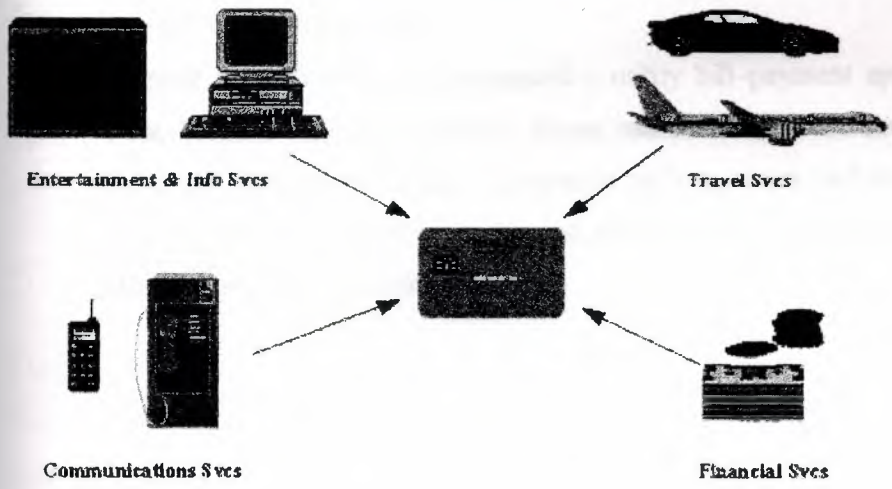
Additionally, managing fraud is also eased by smart cards. In a handset-centric system, if a phone is cloned, the customer must go to a service center to have the handset reprogrammed, or a new phone must be issued to the customer. In a smart card–based

system, the situation can be handled by merely issuing a new card; customers can continue using their current phones. The savings in terms of cost and convenience to both carrier and customer can be substantial.

4.6. PROVIDING VALUE-ADDED SERVICES

One of the most compelling benefits of smart cards is the potential for packaging and bundling various complementary services around basic mobile telephony services. These services can greatly reduce churn and increase usage and brand recognition (see Figure 4.3).

Figure 4.3. Service Bundling with Smart Cards



The SIM card's chip can be programmed to carry multiple applications. The activation of new applications can be downloaded to the card over the air, in real time, thereby reducing the time (and cost) to market.

Providing value-added services such as mobile banking, Web browsing, or travel services creates a high cost of exit for the customer. Long-distance companies have successfully used joint programs with airline companies to ensure the long-term loyalty of their customers. The more services a customer receives, the more difficult it is for the

customer to leave the service provider. Smart cards provide an excellent vehicle for surrounding the core wireless service with these other valuable services, and packaging- and service-bundling opportunities are numerous. Examples of such opportunities are as follows:

- GSM Cellnet and Barclaycard, Europe's largest credit-card issuer, developed a wireless, financial-services smart card. The SIM card activates the user's Cellnet GSM phone and also provides a Barclays services menu. The services available via this alliance include the following:
  - ☐ access to Barclays credit-card information
  - ☐ access to Barclays checking-account information
  - ☐ access to Barclays customer care
- Initially, the Barclaycard services will be provided via live customer service representatives who will answer calls from customers. Future enhancements will enable users to pay household bills, shop, and access financial information services while on the move.
- Swedish bank PostGirot implemented a utility bill–payment application in the Telia Mobitel SIM card. Mobile phone users accessed the service by simple menu navigation and keying information such as origin and destination bank-account numbers, date of payment, and amount, which enables them to pay their utility bills away from home.

5. THIRED GENERATION TECHNOLOGIES

5.1. i-MODE

iMode is a technology used in Japan to add Internet connectivity and web features to their PDC mobile phone system. iMode is a way of providing information to mobile devices. It uses cHTML (Compact HTML) as a markup language, and uses more traditional Internet protocols to deliver it. The content is served using HTTP to a so-called iMode center (under the control of the developers of iMode, NTT DoCoMo). The iMode center performs protocol conversions, which enable the content to be delivered to the phone.

In 1999, NTT DoCoMo, Japan's leading cellular phone operator, launched a service called i-Mode. i-Mode (which stands for information-mode) is a mobile phone service which offers continuous Internet access. i-Mode is similar to WAP (WAP is another technology which has a scope of offering Internet access worldwide).

The reason DoCoMo decided to go with i-Mode instead of waiting for WAP is simple. The Japanese were ready to access the Internet through their mobile phones. They didn't want to have to wait for WAP to provide them with wireless data services they needed.

Consider that last year, NTT DoCoMo had 21 million subscribers and products that were preparing for the coming of W-CDMA (a technology that allows for the high-speed transmission of video and large-volume data). The Japanese - who make up the world's second-largest mobile phone market - were ready to access the Internet through their mobile phones. Thus, DoCoMo created i-Mode, along with a network of partners who offered specially formatted websites to fit into the small screen on the mobile handset.

NTT DoCoMo's decision to forego WAP for i-Mode was a completely practical solution. And with 10 million new subscriptions predicted for the service within the next three years, the decision was obviously the right one.

5.1.1 I-MODE ENABLED PHONE OUTLOOK

An i-Mode enabled cellular phone is similar to in appearance to most cellular phone models. One feature in particular is a four-point command navigation button at

Figure 5.1 Nokia's i-Mode enabled phone

the center of the phone. This allows the user to control the pointer on the display, as well as connect to the i-Mode service by pressing a single button.

There are several companies that manufacture i-Mode cellular phones, including Panasonic, Nokia, Ericsson, and Sony (these models are only available within the Asia Pacific.

5.1.2. UTILIZATION OF SERVICES

The i-Mode service uses an additional packet communication network that is built onto DoCoMo's main network. This packet data transmission technology allows for constant connectivity. Thus, users are not charged for how long they are online, since this time is unlimited. Rather, users are charged only for how much information they retrieve.

5.1.3. MAIN COMPONENTS:

- A cellular phone capable of voice and packet communication and with a browser installed
- A packet network
- An i-mode server
- Information providers

Unfortunately, the i-Mode service is currently available in Japan and Hong Kong only. However, there are plans in the works to bring i-Mode to parts of Europe in the near future. It is unknown at the moment if i-Mode will make it to the United States.

5.1.4. CONNECTION TO A WIRELESS NETWORK:

Typically, networks utilize two types of computers - servers and clients. Servers are the computers that hold information. Clients are the computers that we view the information from.

The way the Internet works is that servers hold our web pages. We then view these web pages from our PCs (the clients). In the case of the i-Mode Internet, an Internet server contains the i-Mode web pages. But now, instead of viewing the pages from a PC, we are using a cellular i-Mode phone. These phones are now the clients.

There are two other factors involved in connecting a to a wireless network. In order to connect a cellular network to a server, a gateway must exist. Also, the web site must be in an i-Mode format.

5.1.5. GATEWAY

A gateway translates wireless requests from a mobile phone to the server. It also sends information from a gateway back to the mobile phone. NTT DoCoMo provides a gateway to their users; however, this is only available to those in Japan.

There are other gateways on the market that allow users outside of Japan to build new mobile Internet services based on cHTML. One of the new gateways to hit the market is the m-WorldGate. This is the world's first commercially available cHTML gateway. m-WorldGate was developed by Logica.

5.1.6. I-MODE ENABLED SITE:

Web pages today are often written in HTML (Hypertext Markup Language), which is too complex for mobile phones because of their slower connection speeds. An i-Mode enabled web sites utilizes pages that are written in cHTML (Compact Hypertext Markup Language), which is a subset of HTML designed for devices with slower connection speeds.

Today, the i-Mode service boasts 500+ i-Mode-enabled websites linked to a portal page, as well as 12,000+ "unofficial" web pages created by private individuals. CHTML.

cHTML is extremely similar to HTML - in fact, it is HTML. The only difference is that some of the more resource intensive areas of the code (such as tables and frames) have been taken out. Mobile devices have a slower connectivity speed. Thus, by eliminating some of the more involved portions of the code, cHTML allows i-Mode web pages to download more quickly to mobile devices.

5.1.7. I-MODE ENABLED WEB SITES

Most i-Mode phones today utilize a micro-browser. These usually have a title bar with icons at the top of an LCD screen. These icons then allow users to access various services such as weather forecasts, transportation schedules, data searches, and news updates. Below this title bar is a text screen that displays text messages and data.

One micro-browser in particular is Compact NetFront, developed by the Japanese Company Access. Compact NetFront is used as the micro-HTML browser for about 75% of all i-mode devices.

Figure 4.2 Compact NetFront Micro-browser

The criteria for creating an i-Mode application or an i-Mode web page are essentially the same as creating web apps and web pages with HTML. You must develop in the cHTML language and then load the page to an Internet web server utilizing FTP or some other transfer method.

Currently, the cHTML language does not support scripting language (this being a major obstacle for developers). However, NTT DoCoMo and Sun Microsystems have announced an alliance recently. There are plans to incorporate Java, Jini, and Java Card technologies into i-Mode cellular phones.

5.2. WAP

The Wireless Application Protocol (WAP) is a hot topic that has been widely hyped in the mobile industry and outside of it. WAP is simply a protocol- a standardized way that a mobile phone talks to a server installed in the mobile phone network. It is amazing how in just six months, it has become imperative for all Information Technology companies in Nordic countries and beyond to have a WAP division. Many advertising agencies and "dot.coms" have announced WAP services.

WAP is hot for several reasons:

- It provides a standardized way of linking the Internet to mobile phones, thereby linking two of the hottest industries anywhere.
- Its founder members include the major wireless vendors of Nokia, Ericsson and Motorola, plus a newcomer Phone.com.
- By April 2000, the WAP Forum had over 350 member companies.
- Mobile information services, a key application for WAP, have not been as successful as many network operators expected. WAP is seen as a way to rectify this situation.

5.2.1. DETRACTORS AND CONTROVERSIES:

- It is very difficult to configure WAP phones for new WAP services, with 20 or so different parameters needing to be entered to gain access to a WAP service.
- Compared with the installed base of Short Message Service (SMS) compliant phones, the relative number of handsets supporting WAP is tiny.
- WAP is a protocol that runs on top of an underlying bearer. None of the existing GSM bearers for WAP- the Short Message Service (SMS), Unstructured Supplementary Services Data (USSD) and Circuit Switched Data (CSD) are optimized for WAP.

- The WAP standard is incomplete, with key elements such as Push (proactive sending of information to mobile devices) and wireless telephony (updating address reports and the like) included in the WAP 1.2, standardized in late 1999 and first expected to be implemented in the Spring of 2000.
- There are many WAP Gateway vendors out there competing against each other with largely the same standardized product. This has led to consolidation such as the pending acquisition of APiON by Phone.com.
- Other protocols such as SIM Application Toolkit and Mobile Station Application Execution Environment (MexE) are respectively already widely supported or designed to supercede WAP.
- WAP services are expected to be expensive to use since the tendency is to be on-line for a long Circuit Switched Data (CSD) call as features such as interactivity and selection of more information are used by the end user. Without specific tariff initiatives, there are likely to be some surprised WAP users when they see their mobile phone bill for the first time after starting using WAP.

5.2.2. HISTORY OF WAP

Motorola, Nokia, Ericsson and the US software company Phone.com (formerly Unwired Planet) were the initial partners that teamed up over two years ago in mid 1997 to develop and deploy the Wireless Application Protocol (WAP). WAP is an attempt to define the standard for how content from the Internet is filtered for mobile communications. Content is now readily available on the Internet and WAP was designed as the (rather than one) way of making it easily available on mobile terminals.

The WAP Forum was formed after a US network operator Omnipoint issued a tender for the supply of mobile information services in early 1997. It received several responses from different suppliers using proprietary techniques for delivering the information such as Smart Messaging from Nokia and HDML from Phone.com (then called Unwired Planet). Omnipoint informed the tender responders that it would not accept a proprietary approach and recommended that that various vendors get together to explore defining a common standard. After all, there was not a great deal of difference between the different approaches, which could be combined and extended to form a powerful standard. These events were the initial stimulus behind the

development of the Wireless Application Protocol, with Ericsson and Motorola joining Nokia and Unwired Planet as the founder members of the WAP Forum.

5.3 BLUETOOTH WIRELESS TECHNOLOGY

Bluetooth wireless technology is a specification designed to enable wireless communication between small, mobile devices. The inspiration behind this technology was the concept to eliminate the need for proprietary cables, which are currently required to enable device connectivity. For instance, in order to transfer images from a digital camera to a laptop PC, a cable is needed in order to connect the camera to the laptop. Each camera manufacturer and model has a different cable requirement. In fact every hand held device manufactured which allows connectivity with a PC has a different cable configuration. Imagine a scenario in which both the laptop PC and the digital camera use Bluetooth wireless technology. In this case there is no need for cables to transfer data between devices. Expanding that idea to include all hand held mobile electronic devices is, in a nutshell, the Bluetooth wireless technology vision.

In addition to eliminating the need for cables and dongles to connect devices, Bluetooth enables devices to form small, ad hoc wireless networks called piconets. These wireless connections are established using a radio transceiver embedded within each Bluetooth device. The radio operates in the 2.4 GHz Industrial, Scientific, and Medical (ISM) band which is globally available. The Bluetooth Radio is designed to operate in a noisy radio environment and to provide a fast, robust, and secure connection between devices. A full duplex data exchange rate of up to 1 Mb/s may be achieved in which a Time-Division Duplex (TDD) scheme is used. Stability is ensured by implementing a frequency-hopping scheme, which enables Bluetooth Radio modules to avoid interference from other signals after transmitting or receiving a data packet. Security within Bluetooth connections is implemented at the hardware layer, with the option of using one of three security levels.

5.3.1. THE BLUETOOTH FAMILY TREE

While Bluetooth wireless technology has many features unique to its own specification, it has borrowed heavily from several existing wireless standards, including Motorola's Piano, IrDA, IEEE 802.11, and Digital Enhanced Cordless Telecommunications (DECT). Motorola's Piano was developed with the concept of

forming ad hoc "Personal Area Networks." This concept was adopted by the Bluetooth SIG to expand the capabilities of the original Bluetooth concept beyond simple cable replacement. The voice data transmission capabilities of Bluetooth are derived from the DECT specification. The object exchange capabilities (the ability to share business card, contact information, messages, etc.) are derived from the IrDA specifications. Bluetooth also inherits the use of the 2.4GHz ISM band, Frequency Hopping Spread Spectrum (FHSS), authentication, privacy, power management, and LAN capabilities provided by the IEEE 802.11 specification.

5.3.2. BLUETOOTH WIRELESS SOLUTION COMPONENTS

There are four major components in any Bluetooth wireless technology system: a radio unit, a baseband unit, a software stack, and application software. The radio unit is the actual radio transceiver, which enables the wireless link between Bluetooth devices. The baseband unit is hardware, consisting of flash memory and a CPU, which interfaces with the radio unit and the host device electronics at the hardware level. The baseband hardware provides all required functionality to establish and maintain a Bluetooth wireless connection between devices. The software stack is essentially driver software or firmware which enables the application level software to interface with the baseband unit. The application software implements the user interface and overall functionality of the Bluetooth device.

1-BLUETOOTH RADIO

The Bluetooth wireless interface is enabled via a radio transceiver, which operates within the 2.4 GHz ISM band. The Bluetooth Radio specification complies with United States FCC as well as international regulations on power output within the ISM band. Bluetooth Radio supports spectrum spreading which allows operation at power levels up to 100mW worldwide. Spectrum spreading is accomplished by frequency hopping in 79 hops displaced by 1 MHz, starting at 2.402 GHz and stopping at 2.480 GHz. The maximum frequency hopping rate is 1600 hops/s. Due to regulations in France, and Spain the number of hops is reduced which limits the allowed frequency spectrum of operation within those countries. These special case situations are handled by an internal software switch, which limits the number of frequency hops used by the radio unit. The

nominal link range between Bluetooth wireless devices is 10 centimeters to 10 meters, but may be extended to more than 100 meters by increasing transmit power or by taking advantage of the supported Bluetooth Baseband network topology.

2-BLUETOOTH BASEBAND

A more proper term for this section would be 'Link Control Unit'. Within the Bluetooth Specification, the Link Controller (LC) is the actual hardware unit which enables the physical RF link between Bluetooth devices and implements baseband protocols and Link Manager (LM) routines. The LM routines enable setup and control of links between devices; and provide the host terminal interface which allows the host device to use a Bluetooth wireless connection.

5.3.3. CONNECTION ESTABLISHMENT

All Bluetooth devices are in standby mode by default. In standby mode, unconnected devices periodically listen for messages. This procedure is called scanning. Scanning is divided into two types, page scan and inquiry scan. Page scan is defined as the connection substate in which a device listens for its own device access code (DAC) for duration of the scan window (11.25 ms) and is used to set up an actual connection between devices. Inquiry scan is very similar to page scan except that in this substate the receiving device scans for the inquiry access code (IAC). Inquiry scan is used to discover which units are in range and what their device addresses and clocks are. Following a successful scanning procedure one of four possible connection states is possible which include: active, hold, sniff, and park. If the scanning procedure was unsuccessful or one or both of the devices do not desire a connection no connection is made.

5.3.4. PAGE SCAN PAGE RESPONSE

During the page scan procedure a device assumes either the role of the master or of the slave. The device that is the slave unit wakes up every 11.25ms (scan window) to listen for its DAC. The scanning done by the slave unit is done on one frequency hop sequence, which is determined by the hardware within the unit. The potential master unit scans using a page train. The page train is a way for the unit to cover all 32 possible

frequency hops and to locate the slave unit, which is listening on only one of those hops. Every 1.28 seconds a different frequency hop is scanned by the master unit. It should be noted that the page train scheme actually involves two page trains. Train A covers half the number of possible frequency hops while Train B covers the other half. Train A is used by default but if no devices are found during an exhaustive search of those frequency hops Train B will be scanned.

During the page substate, the master repeatedly transmits the slave's DAC in an attempt to form a connection between the devices. This transmission occurs during each of the page hops with the page train. If at any point a response is received from the slave unit, the master unit enters the master response substate.

For the purposes of a quick explanation, the master response substate and the slave response substates will be discussed under the umbrella term page response. Page response is the substate in which vital information is exchanged between the master and slave units, which allow a lasting connection to be formed.

3.1.2. INQUIRY SCAN AND INQUIRY RESPONSE

Inquiry procedures involve the same mechanics of the page procedures. The only difference is the information exchanged between the devices. While in the inquiry substates, the master unit is looking for potential slaves and does not have the required DAC needed to establish a connection. The inquiry procedure enables the master device to get the required DAC from potential slave units. Within the inquiry procedures, the only information exchange is the slave unit responding with its address information. Following a successful inquiry scan, the master unit will enter the page scan procedures in order to establish a connection.

5.3.6. CONNECTION MODES

The first of the four possible connection modes is active mode. In active mode, the Bluetooth device actively participates on the channel. Traffic within the channel is scheduled based on the needs of each active device within the piconet. The master also supports regular transmissions to keep all the slaves synchronized to the channel. When

a Bluetooth device participates actively on a channel, it is assigned an Active Member Address (AM_ADDR) which is a 3-bit field. Being only 3 bits, there may be only 7 active slaves within a piconet at any one time. The all zero address is reserved which allows for only 7 addresses to be assigned to active member devices.

The next possible connection mode is hold mode. Hold mode is one of the three reduced power modes available to a Bluetooth device. Hold mode enables a device to keep its AM_ADDR and to support synchronous packets but not to support asynchronous packets. This mode enables the unit to free time in order to accomplish other tasks involving page or inquiry scans.

The next reduced power mode is sniff mode, which basically reduces the duty cycle of the slave's listening activity. This mode enables the unit to support synchronous and asynchronous packets and keep its AM_ADDR. This mode is primarily used to reduce the amount of power used by a device or to allow a device to time share in participation between two piconets.

The last possible mode is park mode, which allows a unit to not actively participate in the channel but to remain synchronized to the channel and to listen for broadcast messages. In park mode a slave device gives up its AM_ADDR and is assigned an 8 bit Parked Member Address (PM_ADDR). Being 8 bits, there may be up to 255 parked slaves if the PM_ADDR alone is used to identify the device (the all zero address has a special meaning). However, if the Bluetooth Device Address (BD_ADDR) is used an unlimited number of slaves may be parked in a given piconet.

5.3.7. LINK AND PACKET TYPES

Bluetooth Baseband provides two types of physical links: Synchronous Connection-Oriented (SCO) and Asynchronous Connectionless (ACL). SCO and ACL links may be used on the same channel or physical RF links. SCO links may be used for both audio and data transmissions. Slave devices may transmit SCO data packets without being polled because SCO links have reserved time slots for transmission. ACL links may be used for data transmission only and slaves must be polled before they can

transmit data. ACL links also support both symmetric and asymmetric traffic and are used to transmit broadcast messages from the master unit.

Any Bluetooth device may support one ACL channel, three simultaneous SCO channels, or a simultaneous ACL and SCO channel. Traffic within the piconet is controlled by the master unit, which allots bandwidth to each slave based on its application needs and available bandwidth. Each link between a master and slave may be of a different type than other links in a piconet. Furthermore, the link type between a master and slave may change arbitrarily during a session if the needs of the slave's application change.

5.3.8. BLUETOOTH WIRELESS NETWORK TOPOLOGY

The Bluetooth wireless system supports point-to-point and point-to-multi-point connections. An ad hoc Bluetooth scatternet may be established by linking several piconets together. A piconet is defined as a group of devices consisting of at least one master and one slave unit which all share the same frequency hopping sequence. A scatternet is a collection of interlinked piconets with each piconet maintaining its unique frequency hopping sequence. A Bluetooth device may link two piconets by being a slave in two different piconets. Additionally it may be a slave in one piconet while being a master in another piconet. Currently, a device may not participate in more than two piconets at the same time. The current specification also limits the number of piconets within a scatternet to 10 piconets. Within a scatternet of 10 fully loaded piconets, a full-duplex data rate of more than 6 Mb/s is possible.

5.3.9. BLUETOOTH WIRELESS VOICE TRANSMISSION

Voice channels within Bluetooth wireless technology use the Continuous Variable Slope Delta Modulation (CVSD) voice-coding scheme. The CVSD scheme was chosen for its robustness in handling dropped or damaged voice samples. Voice channels are SCO links and transmit at a data rate of 64kb/s.

5.3.10. ERROR CORRECTION

There are three error correction schemes defined for Bluetooth baseband controllers: 1/3 rate Forward Error Correction code (FEC), 2/3 rate FEC code, and Automatic repeat request (ARQ). The purpose of applying the FEC scheme is to reduce the number of retransmissions; however, this creates overhead that reduces throughput in a reasonably error-free environment. To allow flexibility in implementation, there is no requirement within the Bluetooth packet specifications to apply FEC to payload data. Packet headers are always protected by a 1/3 rate FEC because this field contains link information, which needs to survive bit errors. An unnumbered ARQ scheme is applied when data is transmitted in one time slot and is directly acknowledged by the recipient in the next time slot. For these data transmissions to be acknowledged, both the header error check and the cyclic redundancy check (CRC) must pass.

5.3.10. BLUETOOTH SECURITY

The Bluetooth specification defines three security modes: non-secure, service-level security, and link level security. In the non-secure mode, the device does not initiate any kind of security procedure. In the service-level security mode, more flexibility in application access policies is allowed. Service-level security mode is especially useful when running several applications in parallel with differing security requirements. In the link level security mode, the device sets up security procedures before the link set-up is completed. Link level securities provides applications with knowledge of "who" is at the other end of the link and provide authentication, authorization, and encryption services.

Authentication is a key component in any Bluetooth system, which allows the user to develop a domain of trust between Bluetooth devices. Authentication services allow two devices to decide if a connection will be formed based on available identification at the hardware level. Once a connection has been established, additional security may be applied to the data transmission using encryption. Encryption procedures are applied to an existing connection between devices while authentication procedures dictate whether or not a connection will ever be formed.

The built-in Bluetooth security mechanisms are secure enough for most applications. However, in the event that the built in mechanisms are not sufficient, stronger encryption schemes may build into Bluetooth products at the software application level.

6. MODERN RADIO INTERFACES

6.1. SPREAD-SPECTRUM COMMUNICATION

The lack of security in cordless telephones (the kind we might have in our home--not mobile cellular phones) is legendary. Perhaps we have even picked up a neighbor's conversation on our cordless phone and wondered whether our neighbor could eavesdrop on us. The idea of using such phones instead of the beepers that physicians and other hospital personnel use so routinely seems attractive. But it quickly loses its appeal when we would realize that, with so many cordless phones in a small area, others would be all too likely to listen in our your conversations.

That's where SpectraLink Corp comes in. It builds the Pocket Communications System (PCS) for facilities whose personnel need to stay in touch with one another, even though they are constantly on the go throughout a limited area. With PCS, a facility can enhance its private branch exchange (PBX) or Centrex system in a way that allows users to access all system features from pocket-sized cordless phones powered by rechargeable batteries. The technology that makes PCS possible is spread-spectrum communication. Thanks to spread spectrum, large numbers of PCS users can operate their cordless phones simultaneously with uncompromised security and without interfering with one another.

Spread spectrum is indeed a marvelous technology. Cloaked in secrecy for many years because of its origins in high-security military systems, it is finding new celebrity as the rising star of wireless communications.

SpectraLink's cordless phones do not require FCC licensing for two reasons: The transmitters use low power and the system operates in a 902- to 928-MHz band. The FCC designates this band for unlicensed, low-power industrial, scientific, and medical (ISM) use. Transmissions in the ISM bands use spread-spectrum techniques, and, as a consequence, multiple signals can be present in the same frequency band at the same time without interfering with each other. Moreover, the system offers greater immunity to noise than do cordless phones that use Narrowband technology.

Industry observers, even in the nontechnical press, have widely touted spread spectrum's signal/noise and data-security advantages. In fact, the enthusiasm of nontechnical journalists is running so high that it may be positioning the technique for a fall. Those who have embraced spread spectrum without becoming familiar with its exquisite complexity and arcane nuances should remember the old adage about claims that sound "too good to be true": Even if much of the hype surrounding spread spectrum isn't downright false, it is misleading.

6.1.1. ADVANTAGES AND DISADVANTAGES

1- Spread spectrum inherently provides high data security.

2- Spread spectrum can provide excellent noise immunity. But blindly applying the technology fails to guarantee S/N ratios better than those of Narrowband communication systems; incorrectly applied, spread spectrum can even cause inferior noise performance.

3- Compared with Narrowband communications, spread spectrum promises vastly more efficient spectrum use. But phasing spread spectrum into the existing cellular network poses gargantuan problems.

4- Spread spectrum is difficult to understand. That factor is one of the most potent militating against the technology's rapid takeover of wireless voice and data communication. Deciding whether Narrowband or spread-spectrum communication is best for an application requires a host of complex trade-offs. These trade-offs involve such factors as the nature of the information--for example, is it voice or data? In data communication, the delays introduced by error-correcting protocols are usually not serious. However, similar delays become unacceptable in two-way voice communication--even when the voice is encoded in digital form.

5- The nature of the interfering signals is another factor that affects spread-spectrum's suitability and determines whether an application should use direct sequence or frequency hopping (spread spectrum's two main forms). Although spread-spectrum communications might seem to be immune to Narrowband interference, such interference can be devastating. A frequency-hopping system that hops to a frequency occupied by a Narrowband signal can lose all data until its next hop. But if the hops occur often enough and are of short-enough duration, the loss of information may be acceptable.

6- Spread spectrum owes its surge in popularity not only to its unique attributes but also to modern semiconductor technology. Even five years ago, implementing a spread-spectrum receiver for a consumer application was not economically feasible. But higher levels of integration have driven down the size and cost of the hardware to the point where handheld spread-spectrum cellular phones are both technically and economically practical.

7- Of the two basic spread-spectrum technologies--frequency hopping and direct sequence--frequency hopping is the easier to understand. In frequency hopping, the information is modulated onto a carrier derived from a frequency synthesizer. A pseudorandom sequence (PRS) determines the synthesizer's output frequency.

6.1.2. SIMPLE & ELEGANT

The direct-sequence approach is at once simpler, more elegant, and harder to understand than frequency hopping. Even though the system is simpler and more elegant, it isn't necessarily better or worse. Like frequency hopping, direct sequence uses a PRS. Unlike frequency hopping, it does not use frequency synthesizers. In contrast with frequency hopping, direct-sequence combines the (binary) data with a pseudorandom binary signal in an exclusive-OR gate ahead of the modulator. The highest frequency present in the PRS (the so-called chipping rate) is at least as high as the highest frequency in the data and is usually considerably higher.

The result of combining the data with the PRS is that the bandwidth of the signal that modulates the carrier is much greater than it otherwise would be; the modulated carrier covers a much greater range of frequencies; and less energy is present at any frequency than would be present without use of the PRS. The total energy contained in the modulated carrier is unaffected by combining the data with the PRS, however.

To recover the original signal, the down-converted receiver output passes through a correlator. The same PRS that was X-ORed with the original data also feeds into this correlator. Other direct-sequence signals are uncorrelated with this PRS, making it possible to recover the original data. Indeed, just as with frequency hopping, multiple direct-sequence signals can occupy the same frequency band simultaneously without interfering with each other. Moreover, the system rejects noise because the correlator

behaves, in a sense, like a sharply tuned filter that rejects noise uncorrelated with the PRS. Neither Narrowband nor truly random noise correlates with a PRS.

Although the use of frequency synthesizers might make frequency-hopping systems more expensive than direct-sequence systems, general agreement on this point is lacking. Furthermore, frequency-hopping transmitters emit signals that, at any instant, cover only a narrow frequency range. As a result, frequency-hopping systems might be able to use lower transmitter power to achieve S/N ratios equivalent to those of direct-sequence systems. If frequency hopping can provide S/N ratios equivalent to or better than those of direct sequence, frequency hopping could become the technology of choice in battery-powered applications. If you try to determine what direction the technology actually will take, however, the answer you get depends on whom you ask.

6.2. CODE DIVISION MULTIPLE ACCESS(CDMA)

CDMA is a "spread spectrum" technology, which means that it spreads the information contained in a particular signal of interest over a much greater bandwidth than the original signal.

When implemented in a cellular telephone system, CDMA technology offers numerous benefits to the cellular operators and their subscribers. The following is an overview of the benefits of CDMA.

6.2.1. ADVANTAGES

1. Capacity increases of 8 to 10 times that of an AMPS analog system
2. Improved call quality, with better and more consistent sound as compared to AMPS system
3. Simplified system planning through the use of the same frequency in every sector of every cell
4. Enhanced privacy
5. Improved coverage characteristics, allowing for the possibility of fewer cell sites
6. Increased talk time for portables
7. Bandwidth on demand

6.3. WIDE BAND CODE DIVISION MULTIPLE ACCESS (WCDMA)

A technology for Wideband digital radio communications of Internet, multimedia, video and other capacity-demanding applications. WCDMA, developed by Ericsson and other from CDMA, has been selected for the third generation of mobile telephone systems in Europe, Japan and the United States.

Voice, images, data, and video are first converted to a narrowband digital radio signal. The signal is assigned a marker (spreading code) to distinguish it from the signal of other users. WCDMA uses variable rate techniques in digital processing and it can achieve multi-rate transmissions.

WCDMA has been adopted as a standard by the ITU under the name IMT-2000 direct spread.

6.3.1. THE WIDEBAND 'RADIO PIPE' FOR 3G

WCDMA (Wideband Code Division Multiple Access) is the radio access technology selected by ETSI (European Telecommunications Standards Institute) in January 1998 for Wideband radio access to support third-generation multimedia services. Optimized to allow very high-speed multimedia services such as voice, Internet access and videoconferencing, the technology will provide access speeds at up to 2Mbit/s in the local area and 384kbit/s wide area access with full mobility. These higher data rates require a wide radio frequency band, which is why WCDMA with 5MHz carrier has been selected; compared with 200kHz carrier for narrowband GSM.

6.3.2. EASY INTEGRATION INTO EXISTING INFRASTRUCTURE

WCDMA can be added to the existing GSM core network. This will be particularly beneficial when large portions of new spectrum are made available, for example in the new paired 2GHz bands in Europe and Asia. It will also minimize the investment required for WCDMA rollout – it will, for example, be possible for existing GSM sites and equipment to be

reused to a large extent.

6.3.3. A SINGLE STANDARD FOR ALL

An agreement on a globally harmonized third-generation CDMA radio standard that addresses the needs of all current wireless communities was reached by the Operators' Harmonization Group in May 1999. There will be three modes in the harmonized 3G CDMA standard; a direct-sequence mode for WCDMA, a multi-carrier mode for cdma2000 (an evolution of narrowband CDMA), and a time division duplex (TDD) CDMA mode.

6.4. TIME DIVISION MULTIPLE ACCESS (TDMA)

Time division multiple access (TDMA) is digital transmission technology that allows a number of users to access a single radio frequency (RF) channel without interference by allocating unique time slots to each user within each channel. The TDMA digital transmission scheme multiplexes three signals over a single channel. The current TDMA standard for cellular divides a single channel into six time slots, with each signal using two slots, providing a 3 to 1 gain in capacity over advanced mobile-phone service (AMPS). Each caller is assigned a specific time slot for transmission.

6.4.1. OVERVIEW

The wireless industry began to explore converting the existing analog network to digital as a means of improving capacity back in the late 1980s. In 1989, the Cellular Telecommunications Industry Association (CTIA) chose TDMA over Motorola's frequency division multiple access (FDMA) (today known as Narrowband analog mobile-phone service [NAMPS]) Narrowband standard as the technology of choice for existing 800 MHz cellular markets and for emerging 1.9-GHz markets. With the growing technology competition applied by Qualcomm in favor of code division multiple access (CDMA) and the realities of the European global system for mobile communications (GSM) standard, the CTIA decided to let carriers make their own technology selection.

The two major (competing) systems that split the RF are TDMA and CDMA. CDMA is a spread-spectrum technology that allows multiple frequencies to be used simultaneously. CDMA codes every digital packet it sends with a unique key. A CDMA

receiver responds only to that key and can pick out and demodulate the associated signal.

Because of its adoption by the European standard GSM, the Japanese Digital Cellular (JDC), and North American Digital Cellular (NADC), TDMA and its variants are currently the technology of choice throughout the world. However, over the last few years, a debate has convulsed the wireless community over the respective merits of TDMA and CDMA.

The TDMA system is designed for use in a range of environments and situations, from hand portable use in a downtown office to a mobile user traveling at high speed on the freeway. The system also supports a variety of services for the end user, such as voice, data, fax, short message services, and broadcast messages. TDMA offers a flexible air interface, providing high performance with respect to capacity, coverage, and unlimited support of mobility and capability to handle different types of user needs.

6.4.2. THE DIGITAL ADVANTAGE OF TDMA

All multiple access techniques depend on the adoption of digital technology. Digital technology is now the standard for the public telephone system where all analog calls are converted to digital form for transmission over the backbone.

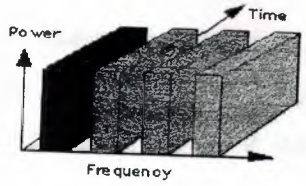
Digital has a number of advantages over analog transmission:

- It economizes on bandwidth.
- It allows easy integration with personal communication systems (PCS) devices.
- It maintains superior quality of voice transmission over long distances.
- It is difficult to decode.
- It can use lower average transmitter power.
- It enables smaller and less expensive individual receivers and transmitters.
- It offers voice privacy.

6.4.3. Frequency Division Multiple Access (FDMA)

TDMA is basically analog's FDMA with a time-sharing component built into the system. FDMA allocates a single channel to one user at a time (see *Figure 1*). If the transmission path deteriorates, the controller switches the system to another channel. Although technically simple to implement, FDMA is wasteful of bandwidth: the channel is assigned to a single conversation whether or not somebody is speaking. Moreover, it cannot handle alternate forms of data, only voice transmissions.

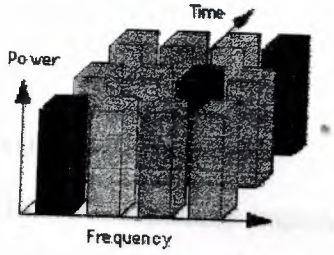
Figure 6.1 FDMA



6.4.4. HOW TDMA WORKS

TDMA relies upon the fact that the audio signal has been digitized; that is, divided into a number of milliseconds-long packets. It allocates a single frequency channel for a short time and then moves to another channel. The digital samples from a single transmitter occupy different time slots in several bands at the same time as shown in Figure 6.2.

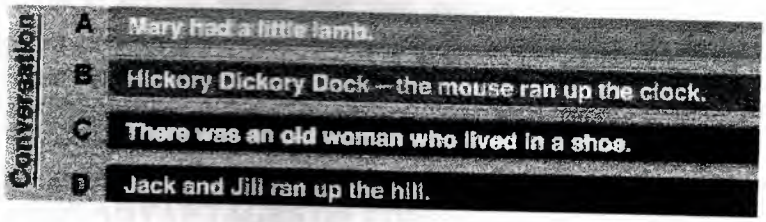
Figure 6.2. TDMA



The access technique used in TDMA has three users sharing a 30–kHz carrier frequency. TDMA is also the access technique used in the European digital standard, GSM, and the Japanese digital standard, personal digital cellular (PDC). The reason for choosing TDMA for all these standards was that it enables some vital features for system operation in an advanced cellular or PCS environment. Today, TDMA is an available, well-proven technique in commercial operation in many systems.

To illustrate the process, consider the following situation. *Figure 3* shows four different, simultaneous conversations occurring.

Figure 6.3. Four Conversations—Four Channels



A single channel can carry all four conversations if each conversation is divided into relatively short fragments, is assigned a time slot, and is transmitted in synchronized timed bursts as in *Figure 4*. After the conversation in time-slot four is transmitted, the process is repeated.

Figure 6.4. Four Conversations—One Channel

Effectively, the IS–54 and IS–136 implementations of TDMA immediately tripled the capacity of cellular frequencies by dividing a 30–kHz channel into three time slots, enabling three different users to occupy it at the same time. Currently, systems are in place that allow six times capacity. In the future, with the utilization of hierarchical cells, intelligent antennas, and adaptive channel allocation, the capacity should approach 40 times analog capacity.

6.4.5. ADVANCED TDMA

TDMA substantially improved upon the efficiency of analog cellular. However, like FDMA, it had the weakness that it wasted bandwidth: the time slot was allocated to a specific conversation whether or not anyone was speaking at that moment. Hughes' enhanced version of TDMA extended time division multiple access (ETDMA) attempts to correct this problem. Instead of waiting to determine whether a subscriber is transmitting, ETDMA assigns subscribers dynamically. ETDMA sends data through those pauses which normal speech contains. When subscribers have something to

transmit, they put one bit in the buffer queue. The system scans the buffer, notices that the user has something to transmit, and allocates bandwidth accordingly. If a subscriber has nothing to transmit, the queue simply goes to the next subscriber. So, instead of being arbitrarily assigned, time is allocated according to need. If partners in a phone conversation do not speak over one another, this technique can almost double the spectral efficiency of TDMA, making it almost 10 times as efficient as analog transmission.

6.4.5. THE ADVANTAGES OF TDMA

In addition to increasing the efficiency of transmission, TDMA offers a number of other advantages over standard cellular technologies. First and foremost, it can be easily adapted to the transmission of data as well as voice communication. TDMA offers the ability to carry data rates of 64 KBPS to 120 MBPS (expandable in multiples of 64 KBPS). This enables operators to offer personal communication-like services including fax, voiceband data, and short message services (SMSs) as well as bandwidth-intensive applications such as multimedia and videoconferencing.

Unlike spread-spectrum techniques which can suffer from interference among the users all of whom are on the same frequency band and transmitting at the same time, TDMA's technology, which separates users in time, ensures that they will not experience interference from other simultaneous transmissions.

TDMA also provides the user with extended battery life and talk time since the mobile is only transmitting a portion of the time (from 1/3 to 1/10) of the time during conversations.

TDMA installations offer substantial savings in base-station equipment, space, and maintenance, an important factor as cell sizes grow ever smaller.
TDMA is the most cost-effective technology for upgrading a current analog system to digital.

TDMA is the only technology that offers an efficient utilization of hierarchical cell structures (HCSs) offering pico, micro, and macrocells. HCSs allow coverage for the

system to be tailored to support specific traffic and service needs. By using this approach, system capacities of more than 40-times AMPS can be achieved in a cost-efficient way.

Because of its inherent compatibility with FDMA analog systems, TDMA allows service compatibility with the use of dual-mode handsets.

Dual band 800/1900 MHz offers the following competitive advantages:

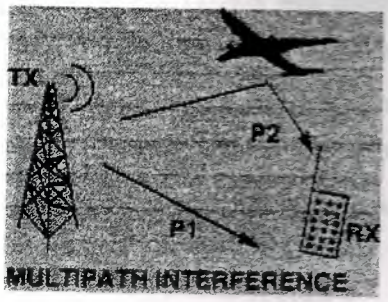
- Identical applications and services are provided to subscribers operating in both bands.
- Carriers can use the same switch for 800– and 1900–MHz services.
- Seamless interworking between 800– and 1900–MHz networks through dual-band/dual-mode phones.
- Using dual-mode, dual-band phones, subscribers on a TDMA 1,900 channel can hand off both to/from a TDMA channel on 800 MHz as well as to/from an analog AMPS channel

6.4.6. THE DISADVANTAGES OF TDMA

One of the disadvantages of TDMA is that each user has a predefined time slot. However, users roaming from one cell to another are not allotted a time slot. Thus, if all the time slots in the next cell are already occupied, a call might well be disconnected. Likewise, if all the time slots in the cell in which a user happens to be in are already occupied, a user will not receive a dial tone.

Another problem with TDMA is that it is subjected to multipath distortion. A signal coming from a tower to a handset might come from any one of several directions. It might have bounced off several different buildings before arriving (see *Figure 5*) which can cause interference.

Figure 6.5. Multipath Interference



One way of getting around this interference is to put a time limit on the system. The system will be designed to receive, treat, and process a signal within a certain time limit. After the time limit has expired, the system ignores signals. The sensitivity of the system depends on how far it processes the multipath frequencies. Even at thousandths of seconds, these multipath signals cause problems.

All cellular architectures, whether microcell- or macrocell-based, have a unique set of propagation problems. Macrocells are particularly affected by multipath signal loss—a phenomenon usually occurring at the cell fringes where reflection and refraction may weaken or cancel a signal.

6.5. TDMA VERSUS CDMA

Since the introduction of CDMA in 1989, the wireless world has been occupied by a debate over the relative merits of TDMA and CDMA—a debate whose fervor makes it reminiscent, at times, of a religious debate.

The proponents of CDMA have claimed bandwidth efficiency of up to 13 times that of TDMA and between 20 to 40 times that of analog transmission. Moreover, they note that its spread-spectrum technology is both more secure and offers higher transmission quality than TDMA because of its increased resistance to multipath distortion.

The defenders of TDMA, on the other hand, point out that to date there has been no successful major trial of CDMA technology that support the capacity claims. Moreover, they point out that the theoretical improvements in bandwidth efficiency claimed for

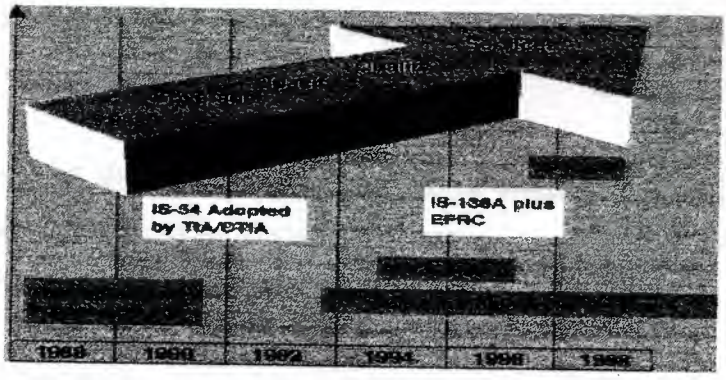
CDMA are now being approached by enhancements to TDMA technology. The evolution of TDMA will allow capacity increases of 20 to 40 fold over analog in the near future. This combined with the vastly more expensive technology needed for CDMA ($300,000 per base station compared with $80,000 for TDMA) calls into question what real savings CDMA technology can offer. So far, IS–136 TDMA is the proven leader as the most economical digital migration path for an existing AMPS network.

We still lack the final word in this debate. However, it seems clear that for the near future at least, TDMA will remain the dominant technology in the wireless market.

6.6. THE IS–136 DIGITAL-CONTROL CHANNEL (DCCH)

The original TDMA standard was IS–54, introduced in 1988–89 by the Telecommunications Industry Association (TIA)/CTIA (see *Figure 6*). It inaugurated a feature set including authentication, calling-number ID, a message-waiting indicator (MWI), and voice privacy.

Figure 6.6. TDMA Standards Evolution



IS–54B was superseded in 1994 with the introduction IS–136 followed closely by revisions A and B.

IS–136 was backward compatible to IS–54B and included a DCCH and advanced features.

IS–136A upbanded IS–136 for seamless cellular service between the 800–MHz and 1,900–MHz frequency bands. In addition, it introduced over-the-air activation and programming services.

IS–136B includes a new range of services including broadcast SMS, packet data, etc.

6.7. GENERAL PACKET RADIO SERVICE (GPRS)

The global GPRS (General Packet Radio Service) market is now beginning to take off. The introduction of GPRS is one of the key steps in the evolution of today's GSM networks to 3G, and GSM operators around the world are upgrading their networks, with a view to launching commercial GPRS services in 2000.

Data traffic is increasing enormously, and is expected to grow 40-50 per cent this year. This growth in demand for Internet access and services has paralleled the explosion in demand for mobile communications. Users want access to the Internet while they are away from their offices and homes, and GPRS can deliver this mobile Internet functionality.

With the capability to charge per data bit sent and received, customers will be able to pay only for usage. GPRS will offer a tenfold increase in data throughput rates, from 9.6kbit/s to 115kbit/s. Using a packet data service, subscribers are always connected and always on line so services will be easy and quick to access.

GPRS will allow innovative services to be created, enabling new and previously inaccessible market segments to be addressed, increasing customer loyalty and reducing churn. Machine-to-machine and person-to-machine communications will become possible.

The next stepping stone towards 3G will be the implementation of EDGE, offering data services and applications at speeds up to 384kbit/s essentially using existing infrastructure. Ericsson has been involved in the standardization of GPRS and EDGE from the beginning, and has a leading position in the burgeoning GPRS market with its complete solution, which can be easily and quickly integrated into existing GSM networks.

6.8. ENHANCED DATA FOR GLOBAL EVOLUTION (EDGE)

One step in Ericsson's strategy to evolve GSM is the implementation of EDGE (Enhanced Data rates for Global Evolution). This will allow GSM operators to use existing GSM radio bands to offer wireless multimedia IP-based services and applications at speeds up to 384kbit/s – or even higher.

EDGE will allow the advantages of GPRS to be fully explored, with fast connection set-up and higher bandwidth than traditional GSM. The combination of GPRS and EDGE will also result in much improved utilization of the radio network.

Introducing EDGE will have little technical impact, since it is fully based on GSM, and will require relatively small changes to network hardware and software. Operators do not have to make any changes to the network structure, or invest in new licenses. For example, EDGE uses the same TDMA (Time Division Multiple Access) frame structure, logic channel and 200kHz carrier bandwidth as today's GSM networks, which allows existing cell plans to remain intact. This makes the technology particularly beneficial to existing operators seeking a way to roll out wideband services rapidly and cost-efficiently across large areas of existing networks.

With EDGE, operators can offer more wireless data applications for both consumer and business users, including wireless multimedia, e-mail, web infotainment and videoconferencing.

As soon as the standard is finalized, next-generation base stations from Ericsson will be prepared to implement EDGE with a software update. EDGE is planned to be commercially available in 2001.

CONCLUSION

The Modern world of mobile communications is observing a flood of change in the system as the third generation technology is on its way out. When the 3G technology arrives, our cell phones will morph into an all purpose communicator, watch color video, download CD-quality music from net, check e-mails, even online auctions, and concerts, browse the web, use positioning services and make old fashioned phone calls as well.

The big idea behind the latest in mobile communications is to give same services on the mobiles as we receive it on the desktop computers today.

But to make all that happen, 3G networks will need to run a lot faster than today's inefficient GSM digital cell phone systems. GSM sets up a dedicate channel for every call—wasting a lot of valuable transmission capacity. And sending and receiving data on a single channel can be painfully slow, as any WAP user knows.

The 3G networks will be very flexible. They'll send signals from many mobiles over a single channel, moving voice, text, switching—the same which is used for the internat.

Right now GSM is being upgraded to GPRS (General Packet Radio Service). GPRS gangs together GSM channels to move data packets fast. GPRS mobiles handle data up to 100kbps.An enhanced version of GPRS, called EDGE will push speeds up to 380kbps. Bt GPRS and EDGE will be left standing by 3Gdevices. Each will have the access to a 5Mhz channel against GSM's 25 kHz.

Several Engineering problems must have to be overcome before 3G becomes a reality: like maintaining an always-on-internet connection while we are on the move, and keeping it live as we move from one base station to another, and the other is the packet header called the 'Envelope'.

But still, having access to 2Mbps mobile phones, makes a lot more difference than we could possibly imagine, and yet there are more ideas and theories on the move, as Ericsson is going to enhance 3G to 8MBPS, anticipating the arrival of 4G.

REFERENCES

[1] Prof. Dr. Fakhreddin Mamedov, "Mobile Communication Systems", *Telecommunications*.

[2] Mark Schrope," Technology special", *New Scientist*, vol-2261, October 2000.

[3] Leander Kahney," The third generation gap ", *Scientific American*, October 2000

[4] Steve Wallage & Rae Hegarty, " The Future Of Mobile ", *Business Week*, December 4, 2000.

[5] Malcolm W. Oliphant, " The mobile phones meet the internet", *IEEE Spectrum*, August 1999.

[6] Malcolm W. Oliphant, "Radio interfaces makes the difference in 3G cellular technology ", *IEEE Spectrum*, October 2000.

[7] "Mobile Communication systems ", "http://www.Epanorama.net ", retrieved December 2000.

[8] "Everything about Wireless ", " http://www.anywhereyougo.com ", Retrieved December 2000.

[9] " Radio Frequencies ", "http://www.ucwa.com", retrieved on December 2000.

[10] "3G Partnership project ", " http://www.3gpp.org "

[11] "All About mobiles ", "http://www. Mobileinfo.Com", retrieved on January 2001.

[12] "Basics knowledge about bluetooth ". http://www.bluetooth.com..retreived on January 2001.

[13] " 3G Is Here ", " http://www.pcworld.com ", retrieved January 2001.

[14] " 3G TDMA Systems ", " http://www.uwcc.org ", retrieved December 2000.

[15] "W-CDMA Information "," http://www.ericsson.com ", retrieved December 2000.

[16] " Introduction to GSM "," http://www.gsm.com", retrieved January 2001.

[17] "Cellular Technology "," http://www.mobileoffice.com", retrieved December 2000.