NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

SIM CARD

Graduation Project
EE- 400

Student: Shaban Jbarah (990969)

Supervisor: Mr Jamal Abu Hasna

Lefkosa - 2002

ACKNOWLEDGMENT

Initially I would like to thank Mr Jamal Abu Hasna for being my adviser actually I could overcome many difficulties successfully under his guidance ,He always helps me either in my graduation project or during my studying period .

All of my thanks to Mr Ozgur Ozerdem who explained a lot of points for my project regulation .

Finally I would like to thank my family who support me in learning field especially my parents .Without their endless support and love , I would never achieve my current position . I wish them lives happy life .

ABSTRACT

The SIM Card become so important in our life, cause of it can be useful in our life orders , it has many uses which it can make the life more easier .

The main objective of this thesis is to provide analysis and systematisation of the SIM Card ,especially that one which uses for cell phone .

For this Purpose We need a program which can discover the contents of SIM Cards .to full understand how the operation of SIM card accomplish . The underling principle of reconstruction the program to do what we need in the SIM Card through reader and writer devise .

TABLE OF CONTENTS

ACKNOWLEDGMENT i
ABSTRACT ii
INTRODUCTI iii
1. CELLULAR COMMUNICATIONS 1
1.1. Definition 1
1.1.1. Cellular Mobile Communication 1
1.1.2. Global System for Mobile Communication (GSM) 1
1.2. Mobile Communications Principles 1
1.3. Early Mobile Telephone System Architecture 2
1.4.Mobile Telephone System Using the Cellular Concept 3
1.5. Cellular System Architecture 4
1.5.2. Clusters 5
1.5.3. Frequency Reuse 5
1.5.4. Cell Splitting 6
1.5.5. Handoff 7
1.6. North American Analog Cellular Systems 9
1.6.1. The Advanced Mobile Phone Service (AMPS) 9
1.6.2. Narrowband Analog Mobile Phone Service (NAMPS) 10
1.7. Cellular System Components 11
1.7.1. PSTN 11
1.7.2. Mobile Telephone Switching Office (MTSO) 11
1.7.3. The Cell Site 11
1.7.4. Mobile Subscriber Units (MSUs) 12
1.8. Digital Systems 12
1.8.1. Time Division Multiple Access (TDMA) 15
1.8.2. Extended Time Division Multiple Access (E–TDMA) 15
1.8.3. Fixed Wireless Access (FWA) 16
1.8.4. Personal Communications Service (PCS) 16
1.8.5. Code Division Multiple Access (CDMA) 17
2.1 HOW CELL PHONES WORKS 18
2.1. Introduction 18
2.2. The Cell Approach 18
2.3. Cell Phones Codes 20
2.4. From Cell To Cell 21
2.5. Roaming 22
2.6. Cell Phone And CBS 22
2.7. Advance Mobile Phone System (AMPS) 24
2.8. Analog Comes Digital 24
2.9. Cellular Access Technologies 25
2.9.1. Frequency Division Multiple Access (FDMA) 25
2.9.2. Time Division Multiple Access (TDMA) 26
2.9.3. Code Division Multiple Access (CDMA) 27
2.10. The Difference Between Cellular And PCs 28
2.11. Dual Band And Dual Mode 29
2.12. Problems With Cell Phones 30
2.13. Inside A Cell Phone 30
2.14. Cell Phones Tower 34

2.15. What They Can Do 36
2.16. Features 37
2.16.1. Service Plan 37
2.16.2. Mode 38
2.16.3. Battery Type 38
2.16.4. Display 38
2.16.5. Include Function 39
2.16.6. Special Features 39
3. SIM CARD 40
3.1. Introduction 40
3.2. Smart card functions 41
3.3. Smart card standards and platforms 42
3.4. Alternatives to smart cards 43
3.5. Contact, Contactless and combi interfaces SIM Card 43
3.5.1. Contact smart cards 44
3.5.2. Contactless smart cards 44
3.6. Access the information 45
3.6.1. Passwords 45
3.6.2. Authenticating the cardholder 46
3.7. Smart Cards in Wireless Communications 47
3.7.1. General 47
3.7.2. Enhanced Security Benefits 48
3.7.3. Easing Logistical Issues 49
3.7.4. Providing Value-Added Services 50
3.8. Marketing Opportunities 51
3.8.1. Brand Recognition 52
3.8.2. Customer Loyalty Programs 52
3.8.3. Direct Marketing 52
3.8.4. Advertising 53
3.8.5. Trial Subscriptions 53
3.8.6. Incidental Revenues 54
3.9. User Benefits 54
3.9.1. Full Portability of Services 54
3.9.2. International Roaming 54
3.9.3. Intersystem Roaming 55
3.9.4. Multiple Services on a Single Card 55
3.9.5. Separation of Business and Personal Calls 56
3.10. Factors Driving Smart-Card Acceptance 56
3.10.1. Industries and Institutions 56
3.10.2. Consumers Primed to Use Smart Cards 57
4. SIM CARD & GSM SECURITY 58
4.1. Security Of SIM Card 58
4.2. GSM System Security 59
4.2.1. Overview of GSM Security Features 59
4.2.2. Subscriber Identity Authentication 59
4.2.3. User and Signalling Data Confidentiality 61
4.2.3. Subscriber Identity Confidentiality 62
4.3. The French Proposal for the Cipher 63
4.3.1. PDL Description of the Cipher 63
4.3.2 The Shift Function f 64

4.3.3. Software Estimates 64
4.3.4. Evaluating the Shift Function f 65
4.3.5 Performing the Shifts 66
4.3.6. Hardware Estimates 69
4.3.6. Hardware Estimates 70
4.3.8. Shift Function f 71
4.3.9 Speed Estimates 73
CONCLUSION 74
REFERENCES 75

INTRODUCTION

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

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

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

In the chapter two, I present how cell phone works? And I have discussed the cell approach and cell phones codes, and what makes it different from a regular phone?
What do al these confusing terms like PCS, GSM, CDMA and TDMA mean? Also I have described the technology behind call phones.

In the chapter three I present a SIM Card, SIM Card application , advantage and the types either contact smart card or contactless smart cards and the compound one . I have described the architecture of it, security of smart cards ,Authenticating the cardholder, Passwords, access the information .

In Chapter four I research for technology and structure of smartcards ,signaling data of sim card, spectrum efficiency and logical channel which has described logical categories, blocks codes, logical channel formats.

Understanding the security of GSM mobile phone through the SIM card and separately , network security , PDL Description of the Cipher , function of security and algorimths , etc.

1. CELLULAR COMMUNICATIONS

1.1 Definition

1.1.1. Cellular Mobile Communication

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

1.1.2. Global System for Mobile Communication (GSM)

It is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz. It is estimated that many countries outside of Europe will join the GSM partnership.

1.2. Mobile Communications Principles

Each mobile uses a separate, temporary radio channel to talk to the cell site. The cell site talks to many mobiles at once, using one channel per mobile. Channels use a pair of frequencies for communication—one frequency for transmitting from the cell site and one frequency for the cell site to receive calls from the users. Radio energy dissipates over distance, so mobiles must stay near the base station to maintain communications. The basic structure of mobile networks includes telephone systems and radio services. Where mobile radio service operates in a closed network and has no access to the telephone system, mobile telephone service allows interconnection to the telephone network (Figure 1.1).

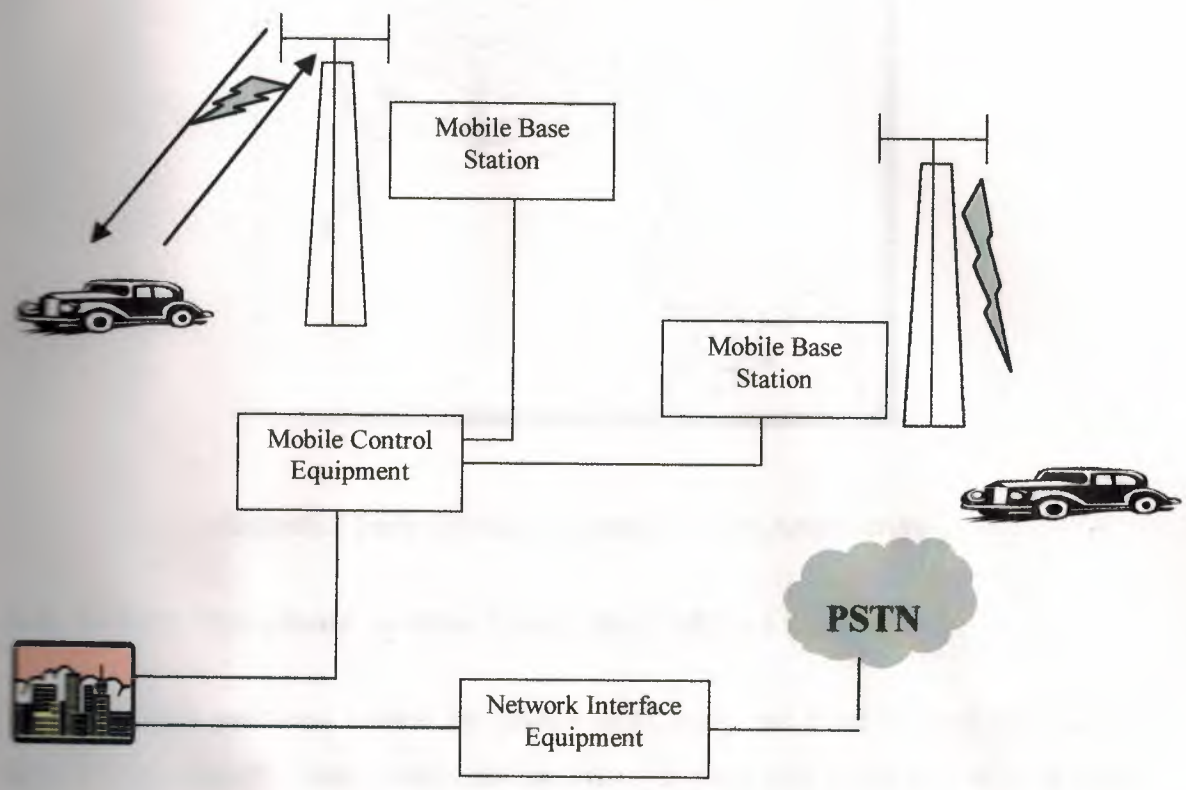


Figure 1.1 Basic Mobile Telephone Service Network

1.3. Early Mobile Telephone System Architecture

Traditional mobile service was structured in a fashion similar to television broadcasting: One very powerful transmitter located at the highest spot in an area would broadcast in a radius of up to 50 kilometers. The cellular concept structured the mobile telephone network in a different way. Instead of using one powerful transmitter, many low-power transmitters were placed throughout a coverage area. For example, by dividing a metropolitan region into one hundred different areas (cells) with low-power transmitters using 12 conversations (channels) each, the system capacity theoretically could be increased from 12 conversations—or voice channels using one powerful transmitter—to 1,200 conversations (channels) using one hundred. low-power transmitters . Figure1.2 shows a metropolitan area configured as a traditional mobile telephone network with one high-power transmitter.

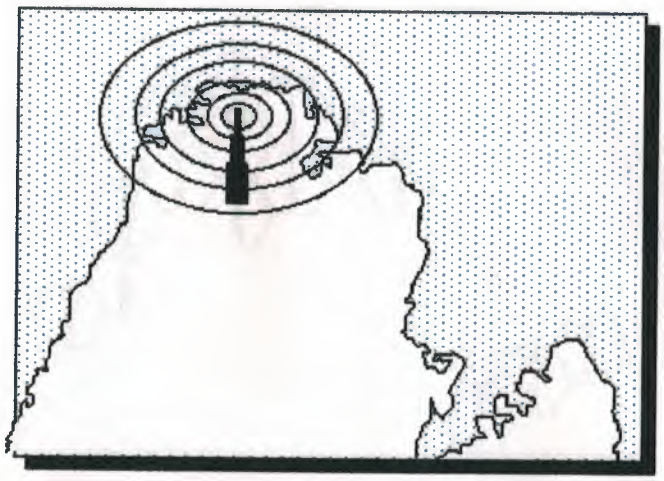


Figure1.2 Early Mobile Telephone System Architecture

1.4. Mobile Telephone System Using the Cellular Concept

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

Engineers discovered that the interference effects were not due to the distance between areas, but to the ratio of the distance between areas to the transmitter power (radius) of the areas. By reducing the radius of an area by 50 percent, service providers could increase the number of potential customers in an area fourfold. Systems based on areas with a one-kilometer radius would have one hundred times more channels than systems with areas 10 kilometers in radius. Speculation led to the conclusion that by reducing the radius of areas to a few hundred meters, millions of calls could be served.

The cellular concept employs variable low-power levels, which allow cells to be sized according to the subscriber density and demand of a given area. As the population grows, cells can be added to accommodate that growth. Frequencies used in one cell cluster can be reused in other cells. Conversations can be handed off from cell to cell to maintain constant phone service as the user moves between cells (Figure 1.3).

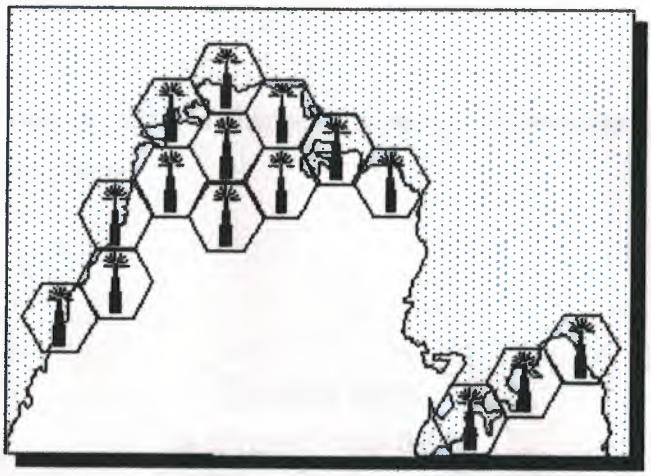


Figure 1.3 Mobile Telephone System Using a Cellular Architecture

1.5. Cellular System Architecture

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

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

1.5.1. 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.

1.5.2. Clusters

A cluster is a group of cells. No channels are reused within a cluster. Figure 1.4 illustrates a seven-cell cluster.

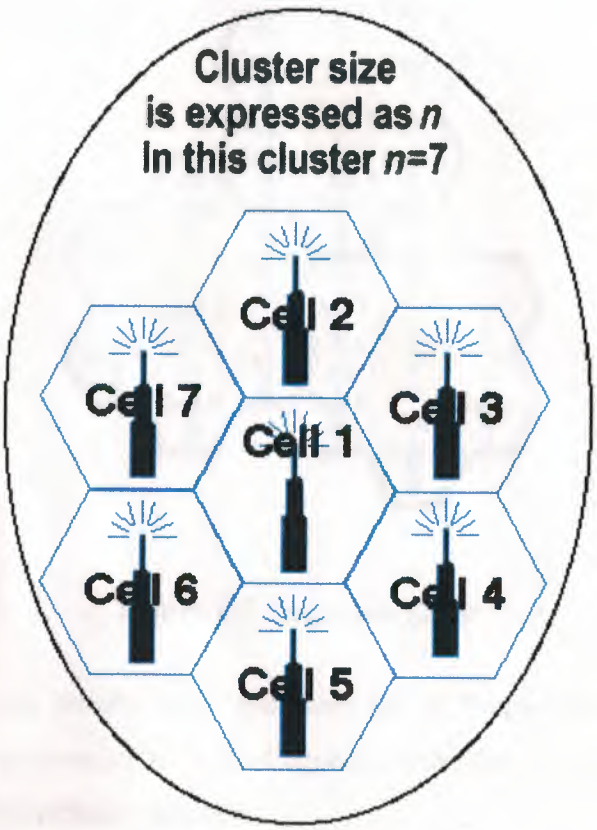


Figure 1.4 A Seven-Cell Cluster

1.5.3. 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 (Figure1.5).

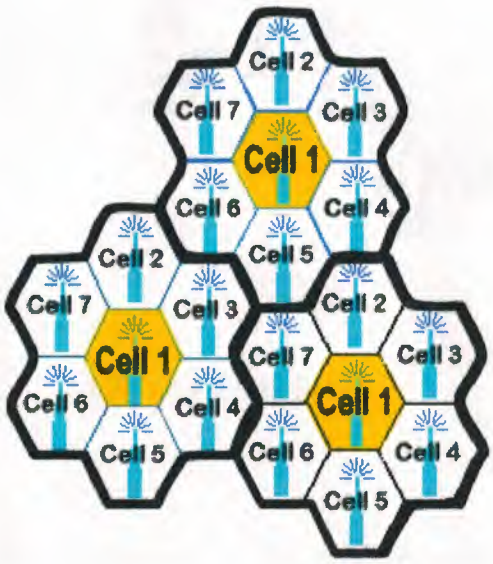


Figure 1.5 Frequency Reuse

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.

1.5.4. Cell Splitting

Unfortunately, economic considerations made the concept of creating full systems with many small areas impractical. To overcome this difficulty, system operators developed the idea of cell splitting. As a service area becomes full of users, this approach is used to split a single area into smaller ones. In this way, urban centers can be split into as many areas as necessary to provide acceptable service levels in heavy-traffic regions, while larger, less expensive cells can be used to cover remote rural regions *(*Figure 1.6*)*.

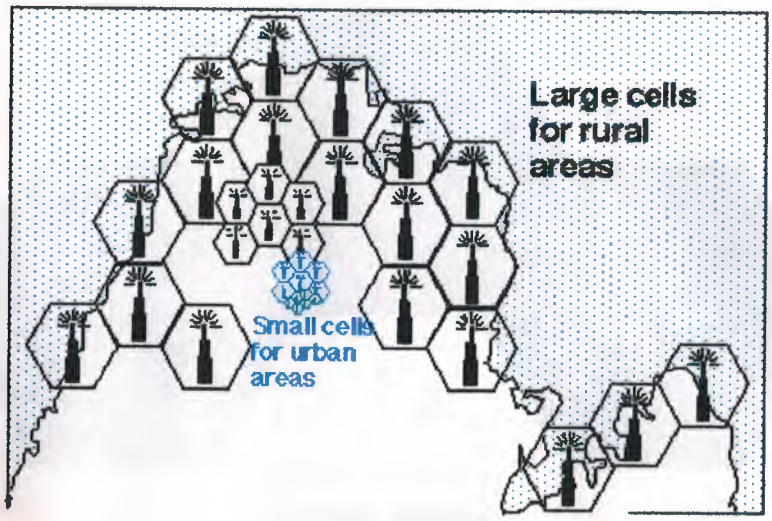


Figure 1.6 Cell Splitting

1.5.5. Handoff

The final obstacle in the development of the cellular network involved the problem created when a mobile subscriber traveled from one cell to another during a call. As adjacent areas do not use the same radio channels, a call must either be dropped or transferred from one radio channel to another when a user crosses the line between adjacent cells. Because dropping the call is unacceptable, the process of handoff was created. Handoff occurs when the network automatically transfers a call from radio channel to radio channel as a mobile crosses adjacent cells as(Figure 1.7*)*.

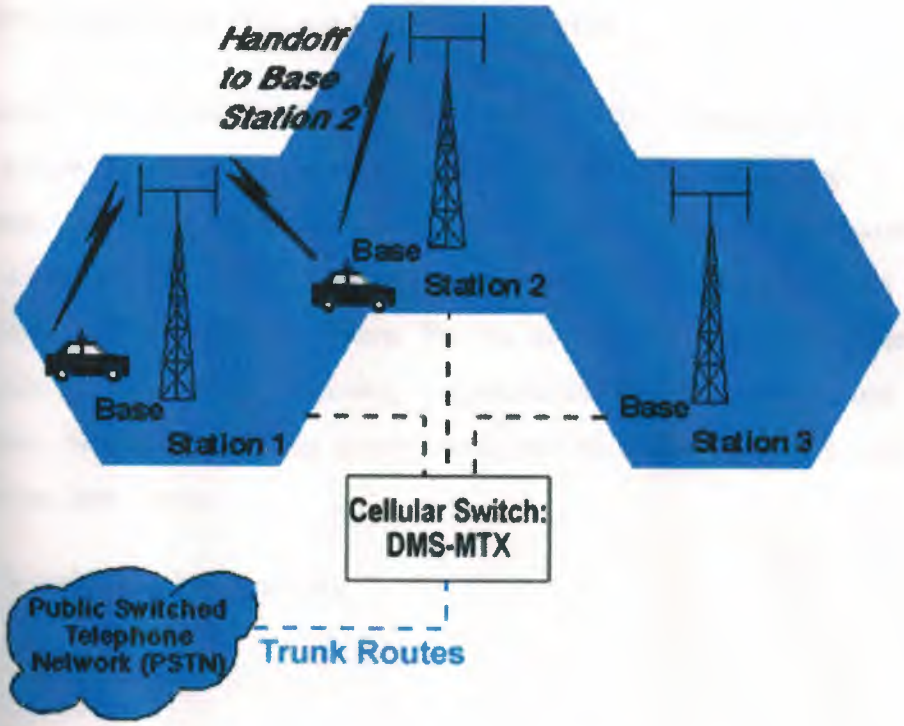


Figure 1.7 Handoff between Adjacent Cells

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.

1.6. 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

1.6.1. The Advanced Mobile Phone Service (AMPS)

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

-low calling capacity

-limited spectrum

-no room for spectrum growth

-poor data communications

-minimal privacy

-inadequate fraud protection

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

1.6.2. Narrowband Analog Mobile Phone Service (NAMPS)

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

1.7. 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)

1.7.1. PSTN

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

1.7.2. 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.

1.7.3. The Cell Site

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

1.7.4. 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.

1.8. Digital Systems

As demand for mobile telephone service has increased, service providers found that basic engineering assumptions borrowed from wireline (landline) networks did not hold true in mobile systems. While the average landline phone call lasts at least 10 minutes, mobile calls usually run 90 seconds. Engineers who expected to assign 50 or more mobile phones to the same radio channel found that by doing so they increased the probability that a user would not get dial tone—this is known as call-blocking probability. As a consequence, the early systems quickly became saturated, and the quality of service decreased rapidly. The critical problem was capacity. The general characteristics of time division multiple access (TDMA), Global System for Mobile Communications (GSM), personal communications service (PCS) 1900, and code division multiple access (CDMA) promise to significantly increase the efficiency of cellular telephone systems to allow a greater number of simultaneous conversations. Figure 1.8 shows the components of a typical digital cellular system.

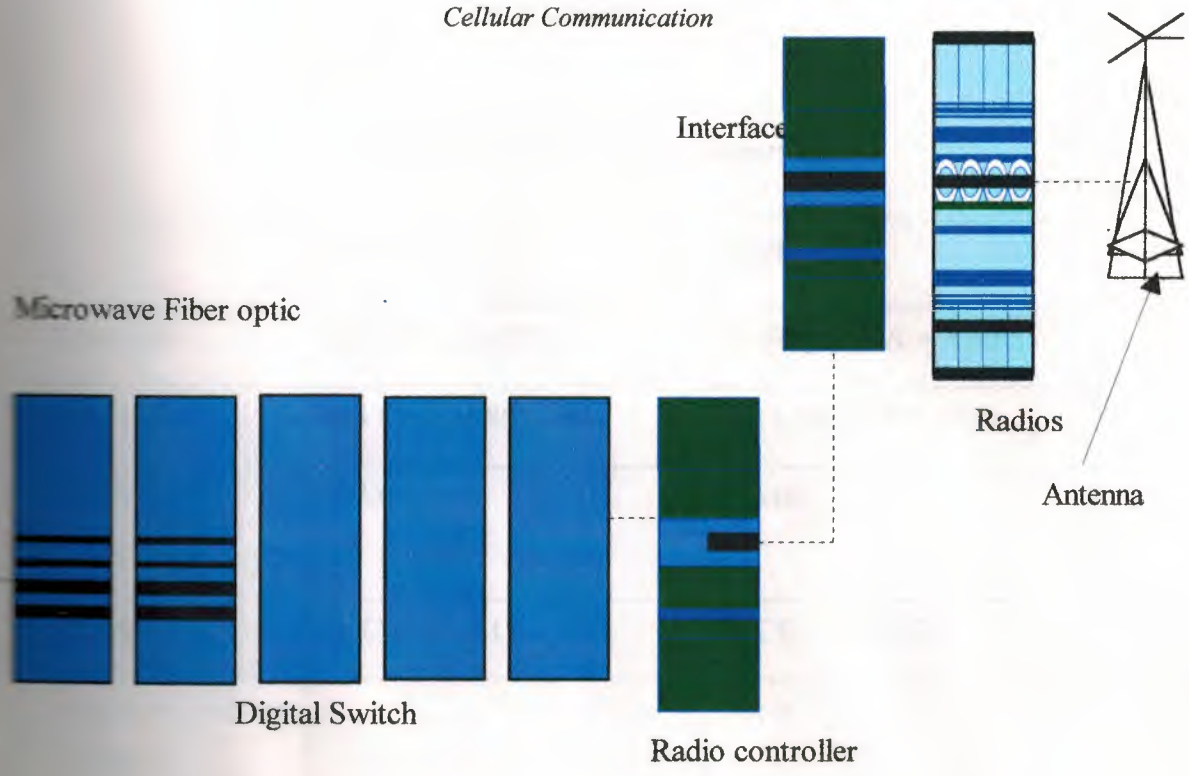


Figure 1.8 Digital Cellular System

The advantages of digital cellular technologies over analog cellular networks include increased capacity and security. Technology options such as TDMA and CDMA offer more channels in the same analog cellular bandwidth and encrypted voice and data. Because of the enormous amount of money that service providers have invested in AMPS hardware and software, providers look for a migration from AMPS to digital analog mobile phone service (DAMPS) by overlaying their existing networks with TDMA architectures(Table 1.1).

Table 1.1 AMPS/DAMPS Comparison

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

1.8.1. Time Division Multiple Access (TDMA)

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

-IS–54 standard specifies traffic on digital voice channels

-initial implementation triples the calling capacity of AMPS systems

-capacity improvements of 6 to 15 times that of AMPS are possible

-many blocks of spectrum in 800 MHz and 1900 MHz are used

-all transmissions are digital

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

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

1.8.2. Extended Time Division Multiple Access (E–TDMA)

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

1.8.3. Fixed Wireless Access (FWA)

FWA is a radio-based local exchange service in which telephone service is provided by common carriers (Figure1.9). It is primarily a rural application—that is, it reduces the cost of conventional wireline. FWA extends telephone service to rural areas by replacing a wireline local loop with radio communications. Other labels for wireless access include fixed loop, fixed radio access, wireless telephony, radio loop, fixed wireless, radio access, and Ionica. FWA systems employ TDMA or CDMA access technologies.

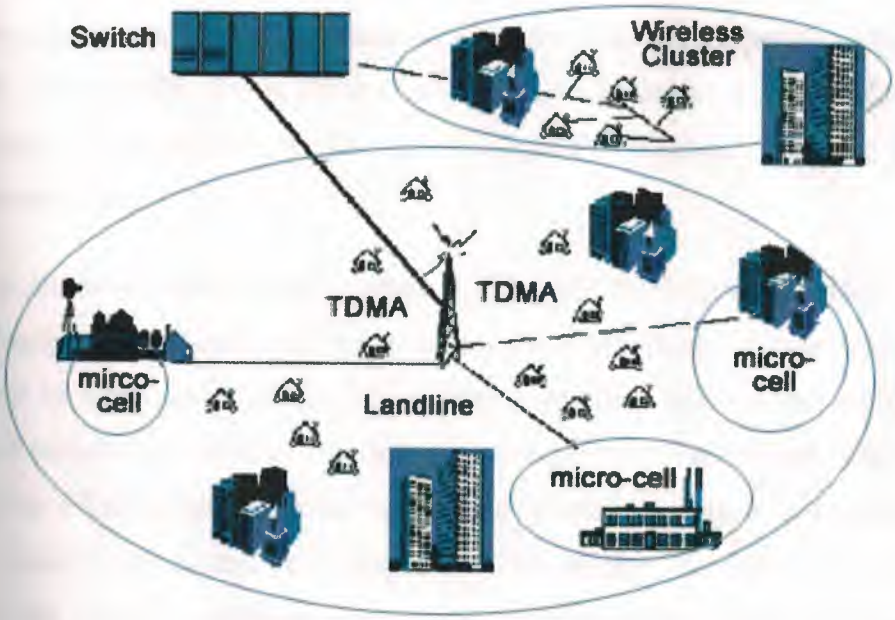


Figure 1.9 Fixed Wireless Access

1.8.4. Personal Communications Service (PCS)

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

a channel number implies one uplink and one downlink frequency (e.g., Channel 512 = 1850.2-MHz uplink paired with 1930.2-MHz downlink).

1.8.5. Code Division Multiple Access (CDMA)

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

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

2. HOW CELL PHONES WORKS

2.1. Introduction

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

Figure 2.1 A digital cell phone from Nokia

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

2.2. The Cell Approach

One of the most interesting things about a cell phone is that it is really a radio an extremely sophisticated radio, but a radio nonetheless. The telephone was invented by Alexander Graham Bell in 1876, and wireless communication can trace its roots to the invention of the radio in 1894 by a young Italian named Guglielmo Marconi. It was only natural that these two great technologies would eventually be combined. In the dark ages before cell phones, people who really needed mobile communications ability installed radiotelephones in their cars. In the radiotelephone system, there was one central antenna tower per city, and perhaps 25 channels available on that tower. This central antenna meant that the phone in your car needed a powerful transmitter big enough to transmit 40 or 50 miles. It also meant that not many people could use radiotelephones there just were not enough channels. The genius of the cellular system is the division of a city into small cells. This allows extensive frequency reuse across a

city, so that millions of people can use cell phones simultaneously. In a typical analog cell phone system in the United States, the cell phone carrier receives about 800 frequencies to use across the city. The carrier chops up the city into cells. Each cell is typically sized at about 10 square miles (26 square kilometers). Cells are normally thought of, as hexagons on a big hexagonal grid. Each cell has a base station that consists of a tower and a small building containing the radio equipment. A single cell in an analog system uses one-seventh of the available duplex voice channels. That is, one cell, plus the six cells around it on the hexagonal grid, are each using one-seventh of the available channels so that each cell has a unique set of frequencies and there are no collisions:

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

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

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

The cellular approach requires a large number of base stations in a city of any size. A typical large city can have hundreds of towers. But because so many people are using

cell phones, costs remain low per user. Each carrier in each city also runs one central office called the Mobile Telephone Switching Office (MTSO). This office handles all of the phone connections to the normal land-based phone system, and controls all of the base stations in the

2.3. Cell Phones Codes

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

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

The system identifier (SID) is an important 1-bit code stored in all base stations and all mobile Stations. In the United States, the Federal Communications Commission issues an SID to an operating company when it issues a license to offer service in a specific area. System is AMPS terminology for cellular operations provided by one company in a specific area. Thus, each base station is part of a system. In many places

,there is one NTSO per system .however, to or more systems with relatively small numbers of subscribers can share a single MTSO. Conversely, large system is likely to operate with two or more MTSOs.

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

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

2.4. From Cell To Cell

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

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

- When you first power up the phone, it listens for an SID (see sidebar) on the control channel. The control channel is a special frequency that the phone and base station use to talk to one another about things like call set-up and channel changing. If the phone cannot find any control channels to listen to, it knows it is out of range, and displays a "no service" message.
- When it receives the SID, the phone compares it to the SID programmed into the phone. If the SIDs matches, the phone knows that the cell it is communicating with is part of its home system.
- Along with the SID, the phone also transmits a registration request, and the MTSO keeps track of your phone's location in a database -- this way, the MTSO knows which cell you are in when it wants to ring your phone.

- The MTSO gets the call, and it tries to find you. It looks in its database to see which cell you are in.
- The MTSO picks a frequency pair that your phone will use in that cell to take the call.
- The MTSO communicates with your phone over the control channel to tell it what frequencies to use, and once your phone and the tower switch on those frequencies, the call is connected. You are talking by two-way radio to a friend!
- As you move toward the edge of your cell, your cell's base station will note that your signal strength is diminishing. Meanwhile, the base station in the cell you are moving toward (which is listening and measuring signal strength on all frequencies, not just its own one-seventh) will be able to see your phone's signal strength increasing. The two base stations coordinate themselves through the MTSO, and at some point, your phone gets a signal on a control channel telling it to change frequencies. This hand off switches your phone to the new cell.

2.5. Roaming

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

2.6. Cell Phone And CBS

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

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

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

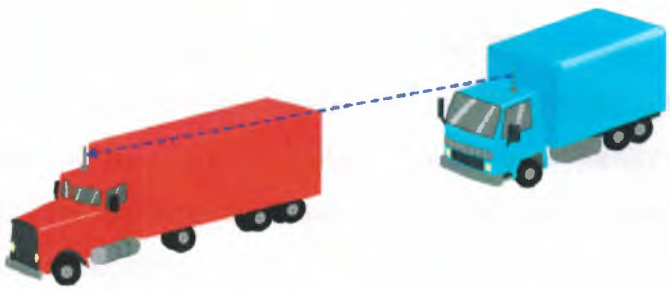


Figure 2.2. In simplex radio, both transmitters use the same frequency. Only one party can talk at a time.

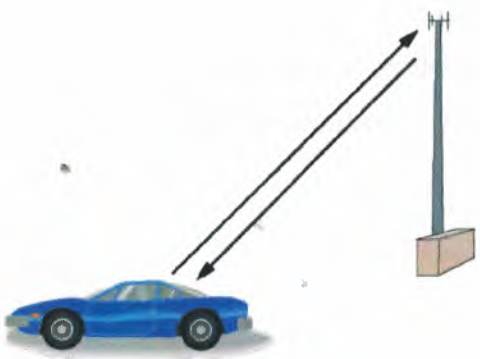


Figure 2.3 In duplex radio, the two transmitters use different frequencies, so both parties can talk at the same time. Cell phones are duplex

2.7. Advance Mobile Phone System (AMPS)

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

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

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

2.8. Analog Comes Digital

Digital cell phones use the same radio technology as analog phones but in a different way. Analog systems do not fully utilize the signal between the phone and the cellular network. Analog signals cannot be compressed and manipulated as easily as a true digital signal. The same reasoning applies to many cable companies that are going to digital so they can fit more channels within a given bandwidth. Digital phones convert your voice into binary information (1s and 0s) and then compress it. This compression allows between three and ten cell phone calls to occupy the space of a *single* analog cell phone voice call. Many digital cellular systems rely on Frequency Shift Keying (FSK)

to send data back and forth over AMPS. FSK uses two frequencies, one for "1"s and the other for "0"s, alternating rapidly between the two to send digital information between the cell tower and the phone. Clever modulation and encoding schemes are required to convert the analog information to digital, compress it and convert it back again while maintaining an acceptable level of voice quality. All this means that digital cell phones have to contain a lot of processing power.

2.9. Cellular Access Technologies

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

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

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

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

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

2.9.1. Frequency Division Multiple Access (FDMA)

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

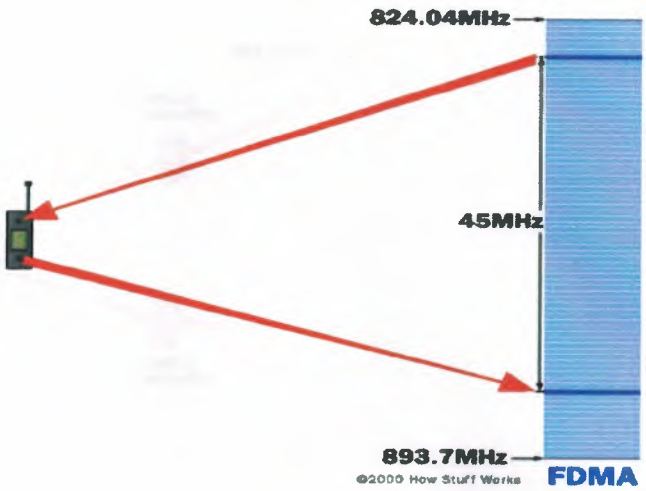


Figure2.4 In FDMA, each phone uses a different frequency.

2.9.2. Time Division Multiple Access (TDMA)

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

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

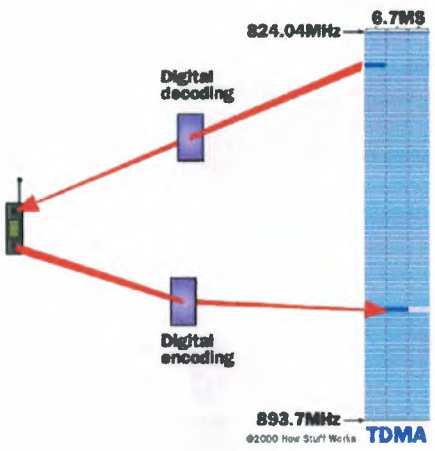


Figure2.5 TDMA splits a frequency into time slots.

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

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

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

2.9.3. Code Division Multiple Access (CDMA)

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

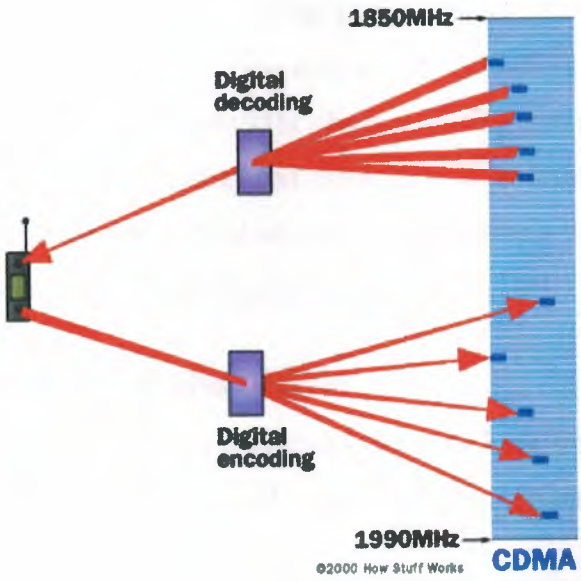


Figure 2.6 In CDMA, each phone's data has a unique code.

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

2.10. The Difference Between Cellular And PCs

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

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

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

2.11. Dual Band And Dual Mode

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

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

Phones that support these options do changing bands or modes automatically. Usually the phone will have a default option set, such as 1900 MHz TDMA, and will try to connect at that frequency with that technology first. If it supports dual bands, it will switch to 800 MHz if it cannot connect at 1900 MHz. And if the phone supports more than one mode, it will try the digital mode(s) first, then switch to analog.

Sometimes you can even find Tri Mode phones. This term can be deceptive. It may mean that the phone supports two digital technologies, such as CDMA and TDMA, as well as analog. But it can also mean that it supports one digital technology in two bands and also offers analog support. A popular version of the TriMode type of phone for people who do a lot of international traveling has GSM service in the 900 MHz band for Europe and Asia, and the 1900 MHz band for the U.S. in addition to the analog service.

2.12. Problems With Cell Phones

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

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

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

2.13. Inside A Cell Phone

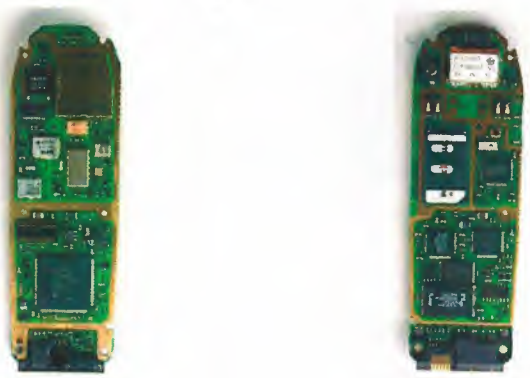
On a "complexity per cubic inch" scale, cell phones are some of the most intricate devices people play with on a daily basis. Modern digital cell phones can process millions of calculations per second in order to compress and decompress the voice stream.

Figure 2.7 The various parts of a cell phone.

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

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

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



a. The front of the circuit board. **b.** The back of the circuit board.

Figure 2.8 The Back and Front of the Circuit Board.

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

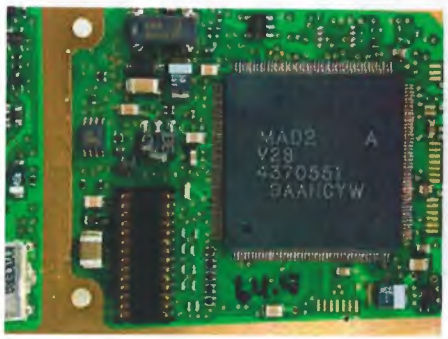


Figure 2.9 The Microprocessor.

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

Figure 2.10 The display and keypad contacts.

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

a. The flash memory card on the circuit board.

b. The flash memory card removed.

Figure 2.11 ROM and Flash Memory

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

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

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

2.14. Cell Phones Tower

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

Figure 2.13 Modern Cell Phone Tower

Figure 2.14 Base Station

Figure 2.15 The Box Houses

As shown in the figure 2.15The box houses the radio transmitters/receivers that let the tower communicate with the phones.

The radios connect with the antennae on the tower through a set of thick cables as shown in the Figure2.16

Figure 2.16 Using cables between radio antenna and tower

2.15. What They Can Do

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

- Call your significant other to let them know that you are on your way home.
- Contact the police or hospital if you have an emergency.

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

2.16. Features

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

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

2.16.1. Service Plan

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

2.16.2. Mode

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

2.16.3. Battery Type

Cell phones use two main battery technologies:

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

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

2.16.4. Display

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

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

2.16.5. Include Function

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

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

2.16.6. Special Features

Some cell phones have special features such as:

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

3. SIM CARD

3.1. Introduction

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. A sim card (subscriber identity module) or smart card is astandard card-sized plastic token within which a microchip has been embedded. This chip is the engine room of the smart card, and indeed is what makes it 'smart'. Smart card chips come in two broad varieties: memory-only chips, with storage space for data, and with a reasonable level of built-in security; and microprocessor chips which, in addition to memory, embody a processor controlled by a card operating system, with the ability to process data onboard, as well as carrying small programs capable of local execution. The main storage area in such cards is normally EEPROM (Electrically Erasable Programmable Read-Only Memory), which - subject to defined security constraints - can have its content updated, and which retains current contents when external power is removed. Newer smart card chips may also have maths co-processors integrated into the microprocessor chip, able to perform quite complex encryption routines relatively quickly.

A smart card is therefore characterised uniquely by its chip, with its ability to store much more data (currently up to about 32,000 bytes) than is held on a magnetic stripe, all within an extremely secure environment. These security features built into smart card chips are amongst the most sophisticated of their type available in the commercial world. Data residing in the chip can be protected against external inspection or alteration, so effectively that the vital secret keys of the cryptographic systems used to protect the integrity and privacy of card-related communications can be held safely against all but the most sophisticated forms of attack. The ingenuity of the cryptographers further supplements the physical security of the chip, ensuring that penetrating one card's security does not compromise an entire card scheme.

It is because of these security and data storage features that smart cards are rapidly being embraced as the consumer token of choice in many areas of the public sector and commercial worlds. The Internet, in particular, is focussing the need for online identification and authentication between parties who cannot otherwise know or trust each other, and smart cards - coupled with effective cardholder verification techniques - are believed to be the most efficient and portable way of enabling the new world of e-trade. is the key requirement to facilitate universal consumer acceptability: the ability of a card function developed by one organisation to be used without difficulty in schemes owned and operated by many organisations. So it is that the current world population of smart cards of some 1.7 billion is set to increase to 4 billion or more cards within the next 3-4 years.

3.2. Smart card functions

Smart cards are being deployed in most sectors of the public and private marketplaces. Single-function cards are being used for payphone telephony, digital mobile telephony (these 'cards' do not in one aspect conform to the basic definition of a smart card, i.e. credit card-sized), the credit and debit functions of financial institutions, retail loyalty schemes, corporate staff systems, subscription TV operations, mass transit ticketing schemes and many more. With the advent of multi-application cards capable of carrying data relating to several functions, more complex schemes are being developed, particularly by cities for their citizens and by central Governments for their residents. In most of these schemes, simple data structures are held and updated within cards, normally comprising personal information about the cardholder and his or her accounting relationship with the card and application issuer, together with transactional data relating to the particular function. Central processing systems often mirror this data, having collected it through a polling mechanism from the terminals that accept the particular cards and enable them to participate in the related transactions.

Most smart card schemes utilise one or more generic functions, this being one of several advantages offered by smart technology. Another advantage of smart cards is that these functions are frequently associated with offline operations, i.e. functions performed without immediate access to the central system. The generic functions of cards include general transaction-based storage, storage of kernel personal data and

account reference information, and - increasingly - the storage of monetary value (electronic purse) able to be loaded and spent repeatedly during the life of the card.

If, by contrast, a completely online scheme (where the user terminal can always make immediate contact with the central processing system) is implemented, the use of smart cards within such a scheme is threatened, because the data storage ability of the card might become redundant if recourse may always be made to the same data held centrally. Such permanently online schemes may be commercially viable within a single organisation, but consumer- and citizen-oriented scheme owners are increasingly recognising the benefits of issuing to the user a powerful, multi-function smart card.

The current proliferation of consumer plastic, giving rise to serious purse and wallet bulge, is focussing card issuers on the challenge of providing multi-application platforms within smart cards, able to carry functions relating not only to the card issuer's business, but also carrying functions issued by third party application providers who may wish to rent space within such cards. This requirement has given rise to the need for suitable platforms able to carry segmented data sets in a discrete way to ensure that one application provider's data cannot be compromised by a third party. Accordingly, a number of multi-application platform products have been developed, not only by the more traditional smart card suppliers but, more unusually, by card scheme operators with an interest in issuing cards and then defraying costs by renting space within them. Such multi-application platforms allow the addition and deletion of application data areas in-flight, without the need for replacing cards. This ability in turn leads to major branding, ownership and control issues, many of which have yet to be addressed and resolved.

3.3. Smart card standards and platforms

The size of the card is determined by the international standard (ISO 7810). The ISO 7816 standard also defines the physical characteristics of the plastic, including the temperature range and flexibility, position of the electrical contacts and how the microchip communicates with the outside world.

3.4. Alternatives to smart cards

Smart card chips are the essential operational components of smart cards, and these also appear in cladding other than credit card-sized plastic tokens. SIMs (Subscriber Identity Modules, initially implemented with simple, single application smart card chips) in a smaller physical format are already incorporated in all GSM handsets, and new developments incorporate smart chips within a variety of other devices such as PDAs and wrist watches.

There are also commercial developments seeking to place e-purse and other similar facilities within software environments in PCs and servers, obviating the need for the deployment of smart cards. It remains to be seen which of these software initiatives will flourish, particularly as it is difficult to ensure their security.

3.5. Contact, Contactless and combi interfaces SIM Card

Traditionally, for use at the retail point of sale or in the banking environment, or as the GSM SIM card in the mobile 'phone, the card has a set of gold- plated electrical contacts embedded in the surface of the plastic on one side. This contact card technology is operated by inserting the card (in the correct orientation) into a slot in a card reader, which has electrical contacts that connect to the contacts on the card face.

For use in a mass transit environment, or wherever the cardholder is in motion at the moment of the transaction, radio frequency technology is used to transmit power from the reader to the card, and data is similarly transmitted over an air-gap of up to 10cms.

This contactless card technology utilises an aerial coil laminated into the card, and allows communication even whilst the card is retained within a wallet or handbag. The same activation method applies to watches, pendants, baggage tags and buttons. No electrical contacts, and therefore "contactless".

Furthermore, in more recent developments, there are now cards with both a contact and a contactless interface (dual-interface or combi-cards). These may incorporate two non-communicating chips - one for each interface - but preferably have a single, dual-interface chip providing the many advantages of a single e-purse, single operating architecture, etc.

Contactless and combi-card architectures have many advantages, but it will be several years before the main and traditional contact card-based schemes start to migrate to these technologies.

3.5.1. Contact smart cards

Contact smart cards must be inserted into a smart card reader.
They have a small gold plate about ½" in diameter on the front, instead of the a magnetic strip on the back like a credit card. When the card is inserted into a smart card reader, it makes contact with electrical connectors that transfer data to and from the chip.(Figure 3.1).

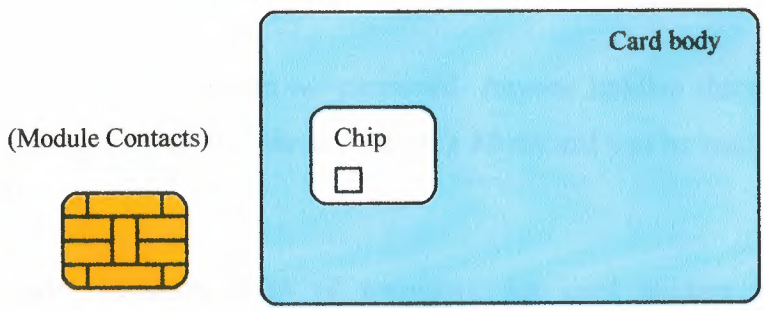


Figure 3.1 contact sim card

3.5.2. Contactless smart cards

Contactless smart cards are passed near an antenna to carry out a transaction. They look just like plastic credit cards, except that they have an electronic microchip and an antenna embedded inside. These components allow the card to communicate with an antenna / coupler unit without an physical contact. Contactless cards are the ideal solution when transactions must be processed very quickly, as in mass-transit or toll collection activities.(Figure 3.2)

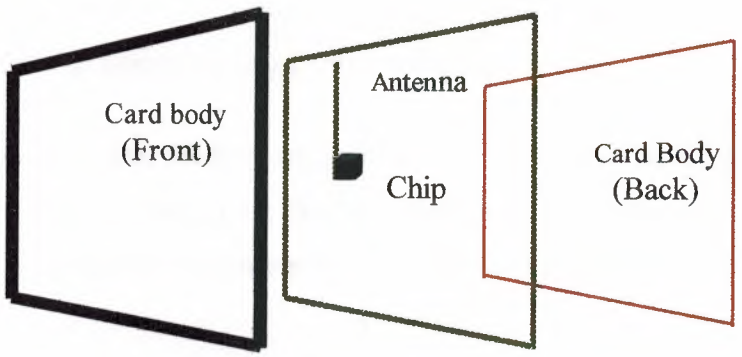


Figure 3.2 Contactless Card

3.6. Access the information

Some smart cards require no password. Anyone holding the card can have access (e.g. the patient's name and blood type on a MediCard can be read without the use of a password).

The most common form of password for card holders is a PIN (Personal Identification Number), a 4 or 5 digit number which is typed in on a key pad. Therefore, if an unauthorized individual tries to use the card, it will lock-up after 3 unsuccessful attempts to present the PIN code. More advanced types of passwords are being developed.

Some smart cards can only be accessed by the party who issued it (e.g., an electronic purse can only be reloaded by the issuing bank).

3.6.1. Passwords

A smart card can restrict the use of information to an authorized person with a password. However, if this information is then transmitted by radio or telephone, additional protection is necessary.

One form of protection is ciphering, which is like translating the information into some unknown foreign language. Some smart cards are capable of ciphering and

deciphering (translating back to an easily understood form) so the stored information can be transmitted without compromising confidentiality.

Smart cards can cipher into billions and billions of foreign languages, and choose a different language at random every time they communicate. This authentication process ensures only genuine cards and computers are used and makes eaves-dropping virtually impossible.

3.6.2. Authenticating the cardholder

Whilst properly designed smart cards cannot in practice be counterfeited, little progress has been made to ensure that it is the accredited cardholder who is using the genuine card. This problem is particularly acute in the e-world, where consumers are transacting business at terminals without operators able to conduct adequate verification routines.

The most common method used for cardholder verification at present is to give the cardholder a PIN (Personal Identification Number) which he or she has to remember: the cardholder has to type in the PIN at each request for signing a message, or perhaps only once per session (e.g. when the card is inserted in the card reader). PINs, however, have several disadvantages, including the risk of being stolen or abused. The only truly effective method of Cardholder Verification is the measurement of a physiological characteristic unique to an individual and incapable of fraudulent replication or abuse. Such biometrics include Iris and Retinal scans, Face or Hand geometry, and of course DNA, but the most likely and most acceptable attribute is the fingerprint. In production systems using fingerprint recognition, the fingerprint sensor is in the terminal, but the fingerprint profile data may be either in the terminal side of the card-to-terminal interface, or preferably held within the card itself (a fingerprint profile takes up only a few hundred bytes of data space). Prototype cards where the fingerprint sensor is on the card surface are now in development and may one day be a commercial proposition. In the meantime, a number of major national schemes around the world are incorporating fingerprint biometrics using optical or proximity readers associated with keyboards, mice and point-of-sale terminals.

3.7. Smart Cards in Wireless Communications

3.7.1. General

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.

3.7.2. 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 (Figure 3.3).

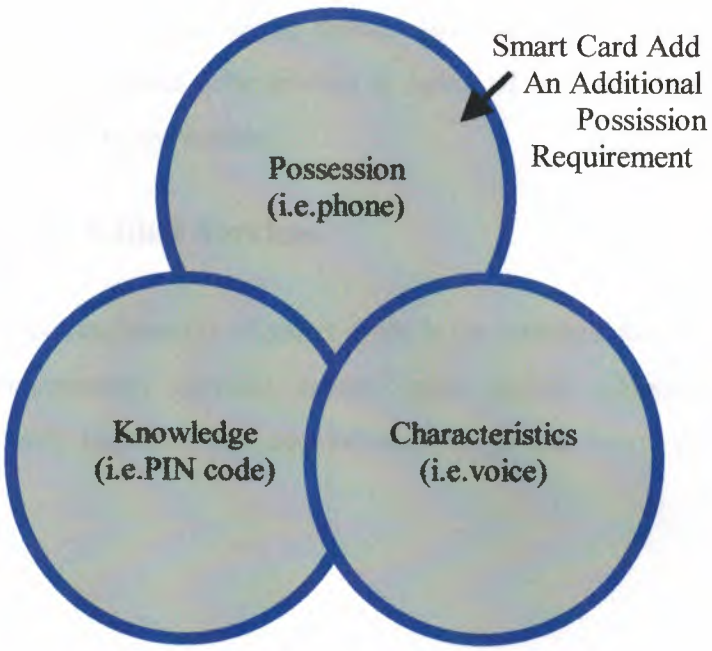


Figure 3.3 Identification Model

3.7.3. 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.

3.7.4. 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 (Figure 3.4).

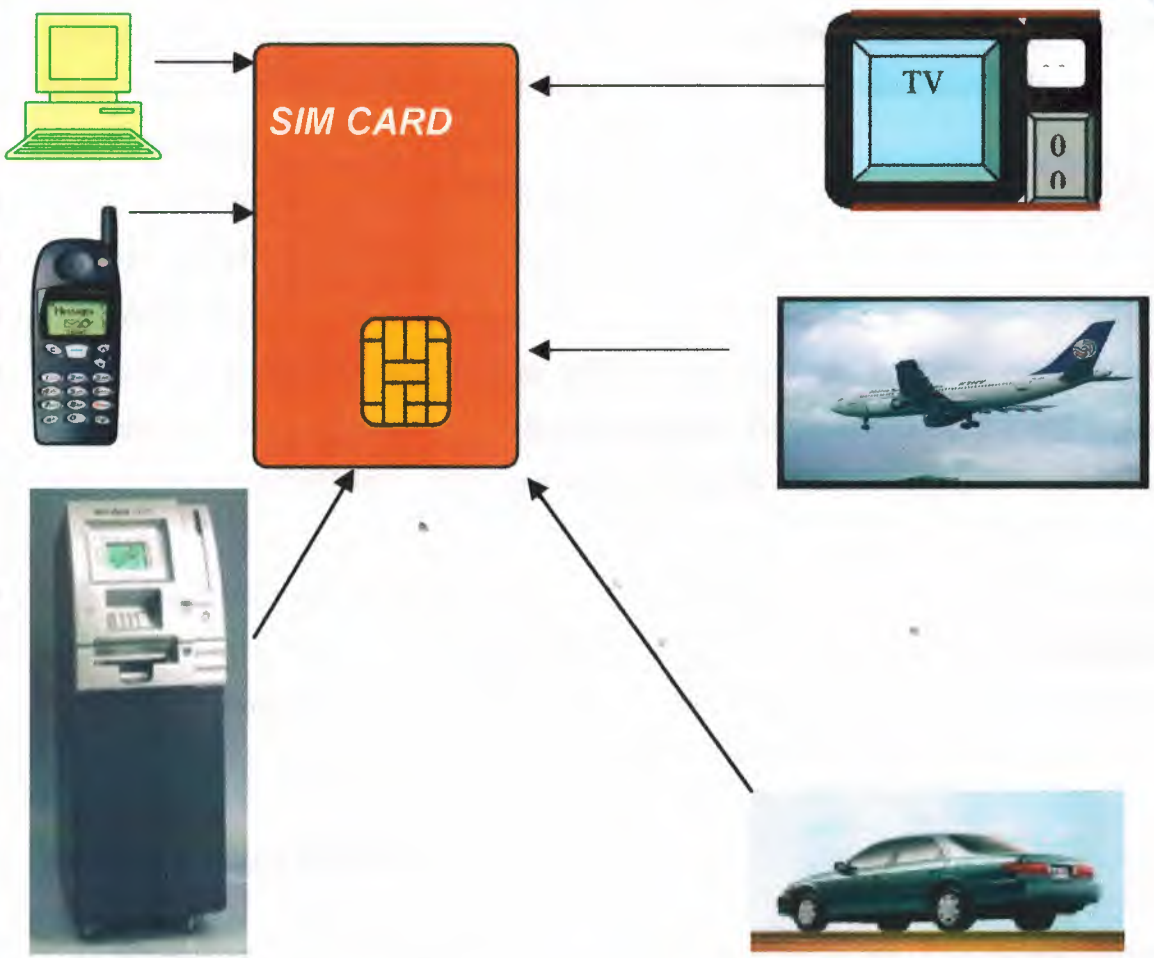


Figure 3.4 Service Bundling with Smart Cards

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.

3.8. Marketing Opportunities

In addition to the value-added services they can provide, smart cards provide many marketing opportunities to network operators.

3.8.1. Brand Recognition

Smart cards provide a means for greater brand exposure and reinforcement. The cards can be considered mini-billboards, providing frequent opportunities for the customer to be exposed to a brand name. Compared to other advertising media, they provide a cost-effective vehicle for achieving a high number of brand exposures to a targeted audience. Network operators with limited brand recognition can co-brand their cards with companies with greater brand equity to strengthen their market positions.

3.8.2. Customer Loyalty Programs

Smart cards can play an extremely valuable role in a carrier's customer retention efforts. The data on a smart card is a digital representation of the customer's habits; i.e., number of calls, services accessed, merchandise purchases, etc. This rich database of customer information makes it possible for network operators to develop highly targeted or one-to-one marketing. Carriers are then able to provide services and offerings particularly suited to their customers, increasing customer loyalty to the carrier.

3.8.3. Direct Marketing

With their convenient form factor, smart cards can be used in direct-mail campaigns to sell wireless subscriptions, both for prospecting and subscription renewal. Using temporary or prepaid smart cards, network operators have a low-cost channel for selling their services. In addition, subscription changes, renewals, and upgrades are easily handled by sending new cards in the mail (Figure3.5).

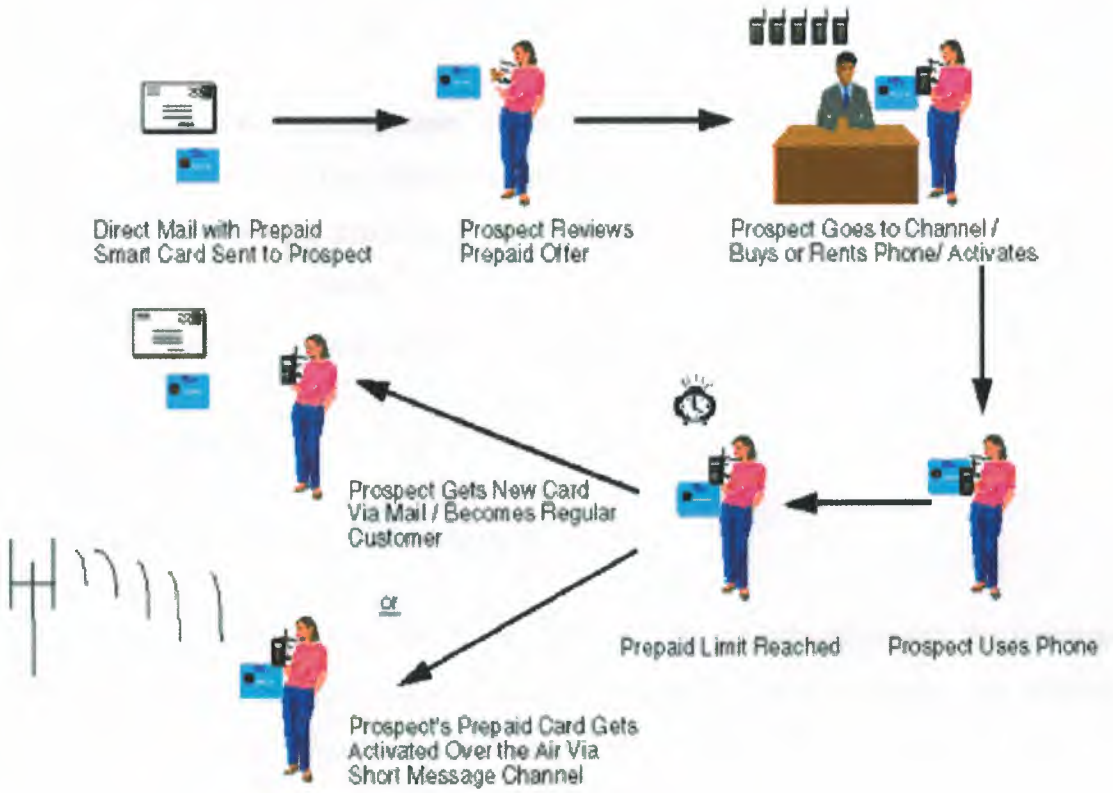


Figure 3.5 A Direct Marketing Scenario

3.8.4. Advertising

Two services, used in conjunction with smart cards, provide network operators with possibilities for highly targeted advertising. Short message service (SMS) and cell broadcast leverage smart cards to send advertising or informational messages that appear on the handset display to wireless users.

3.8.5. Trial Subscriptions

Smart cards are an ideal vehicle for trial subscriptions. Programmed as prepaid cards, they can attract new customers to try wireless services with limited, defined financial risk for both the network operator and the consumer.

3.8.6. Incidental Revenues

Network operators issuing smart cards can generate additional revenue by selling memory space on the card to other companies. For example, available space can be sold to gas stations so that the smart card can also be used as a debit card for gas purchases. The card's surface can also be used for imprinting the participating company's brand, for which the carrier can receive fees for space advertising.

3.9. User Benefits

3.9.1. Full Portability of Services

The smart card effectively breaks the link between the subscriber and the terminal, allowing the use of any properly equipped terminal and helping to realize the wireless promise of any-time, anywhere communications. In fact, subscribers need not be constrained to using voice terminals only. A variety of other mobile communications devices such as personal digital assistants (PDAs) and personal intelligent communicators (PICs) are available that may have voice communications added as an integral part of their capabilities. If these other devices are equipped for smart cards, the potential for communications is increased. Similarly, data communications applications could benefit from the security features inherent in smart cards.

3.9.2. International Roaming

Wireless customers often require the ability to place and receive calls when traveling abroad. For these customers, international roaming enabled by smart cards is quite valuable. For example, Ameritech, AT&T, and GTE have all instituted international roaming programs using GSM phones and smart cards. The program uses co-branded smart cards, which corporate customers bring with them when they travel abroad. Customers are given a telephone number from a GSM carrier, which allows them to be contacted in any of the countries that have international roaming agreements.

3.9.3. Intersystem Roaming

The incompatibility of different communications radio interfaces and authentication protocols (time division multiple access [TDMA], code division multiple access [CDMA], GSM, personal digital cellular [PDC], mobile satellite systems, etc.) requires subscribers to make choices that constrain them to use only one particular type of handset that works with only one radio interface. With a smart card, it becomes possible for subscribers to use one handset for different interfaces and protocols. This feature is already implemented among the three frequencies used by the GSM platform (900, 1800, and 1900 MHz). American National Standards Institute (ANSI) telephone industry price index (T1P1).3 has recommended standards for a user identity module, a smart card that can be used with the major radio access methods. Thus, it becomes conceivable to have current GSM smart cards modified so that they can work with a CDMA handset. For example, North American GSM operators have designed a process to which the SIM holds both the GSM and advanced mobile phone service (AMPS) authentication algorithm and data to provide authentication on both networks in interroaming situations.

3.9.4. Multiple Services on a Single Card

As mentioned earlier, maximum value is realized by the subscriber when multiple applications are stored on a single card (Figure 3.6). A multiapplication smart card could provide access to airline reservation and ticketing systems and information networks, as well as a mobile telephone service. Considering the many cards that the average person carries these days (i.e., numerous credit cards, debit cards, employee ID cards), integrating more applications into a single card (or at least fewer cards) has obvious appeal and benefits. It is important to note that there is clear interest on the part other industries to package their services with mobile telephony. For example, research by Citibank indicates clearly that a substantial percentage of the company's customers would like to be able to conduct its banking on a variety of platforms, including wireless. Such services are already available using a standardized toolbox for smart-card application creation.

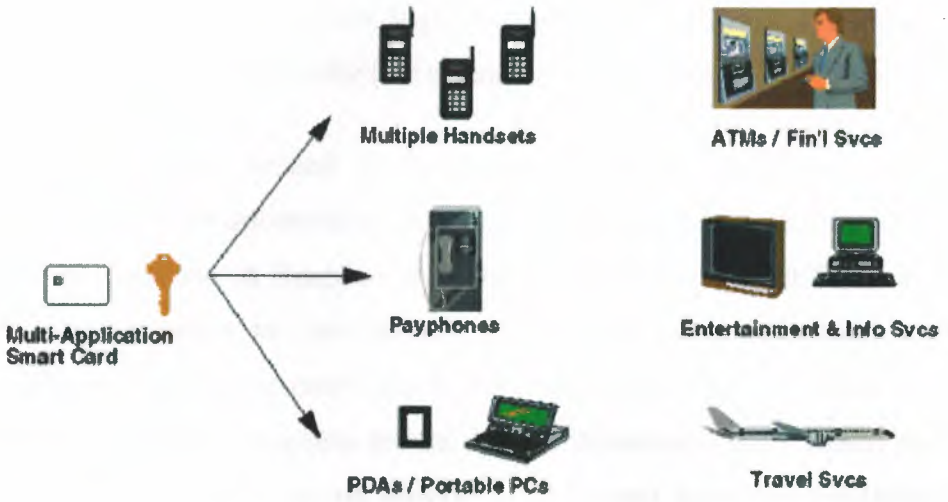


Figure 3.6 Smart Card—A Key to Information Services

3.9.5. Separation of Business and Personal Calls

The smart card allows customers to be billed separately for personal and business calls made on a single phone. For example, Airtel, a Spanish GSM operator, uses a SIM card with two sets of subscription information—one for corporate and the other for personal use. Airtel's dual SIM cards have been well received in the corporate market.

3.10. Factors Driving Smart-Card Acceptance

3.10.1. Industries and Institutions

Certain industries, in particular information technology (IT), government, and financial services, will lead the way to mass-market acceptance of smart cards.

Large IT players are deploying public key infrastructure (PKI) to provide secure logical access to information. PKI is becoming the way to secure messaging and browsing of private information, leading the way to secure electronic commerce. Smart cards are the ideal vehicle to transport the digital certificate associated with the trusted third parties of PKI infrastructures. They provide secure certificate portability and can combine other security applications such as disk file encryption and secure computer log-on. The inclusion of smart-card readers in the equipment listed in the PC99

recommendation has already driven large computer manufacturers to integrate smart-card readers into their product offer (for example, Hewlett Packard and Compaq).

Government agencies around the world are relying on smart-card technology to secure off-line portable information, including identification documents and electronic benefit transfer systems. A Brazilian province has issued its drivers licenses on smart cards to allow the police to view securely stored ticket information immediately. The U.S. government is a major early adopter of smart cards. It has instituted numerous smart card identification programs for its defense department and recently announced that it will further explore the nationwide use of smart cards for electronic benefit transfers as a fraud reduction tool.

In the financial industry, large players such as Barclays and Citibank currently use SIM cards to provide banking information to mobile users via their GSM phones. Electronic purse systems based on VisaCash, Mondex, Proton, and other schemes are deployed around the world and account for tens of millions of cards in Asia, Europe, and Latin America. Major U.S. banks are considering or conducting trials of smart card-based systems. The push by these major financial services firms will serve to accelerate consumer acceptance

3.10.2. Consumers Primed to Use Smart Cards

Research conducted by the Smart Card Forum, an interindustry association dedicated to advancing multiapplication smart cards, has generated the following statistics:

- 45 percent of consumers are favorably disposed to using smart cards
- 25 percent of households would actually obtain these smart cards
- 44 percent of consumers are likely to use identification-type smart cards (telephone cards, gas cards, automated teller machine [ATM] cards, etc.)

4. SIM CARD & GSM SECURITY

4.1. Security Of SIM Card

A)Why do you use a smartcard?

Because it is a secure storage and a secure computation device.

- Physical protection - It is hard to open a smartcard and access data in it. It is not impossible, but is much harder than tampering workstations and PCs.
- Restricted API - A smartcard exports a minimal set of interfaces to avoid exporting flawed interfaces that lead to vulnerabilities.
- Mobility - A user can carry a smartcard, physically separating it from the outside world.

So it is a good place to hide secrets.

B)What do you use a smartcard for?

- Electronic commerce - store money, e.g., M-Card.
- Information Technology - store keys, e.g., authentication, file encryption.

C)What is in smartcard?

Smartcard Directory Structure

how the data are stored in a smartcard.

- Most smartcards have a UNIX like tree-structured file system. (Some do not. Personally, shame on those who don't.)
- File names are two byte long.
- The root of the tree is 3f.00.
- For example, the following is the directory structure of M-Card. There are some files we are interested in ... especially the purse file, i.e., 3f.00/02.00/02.01.
-

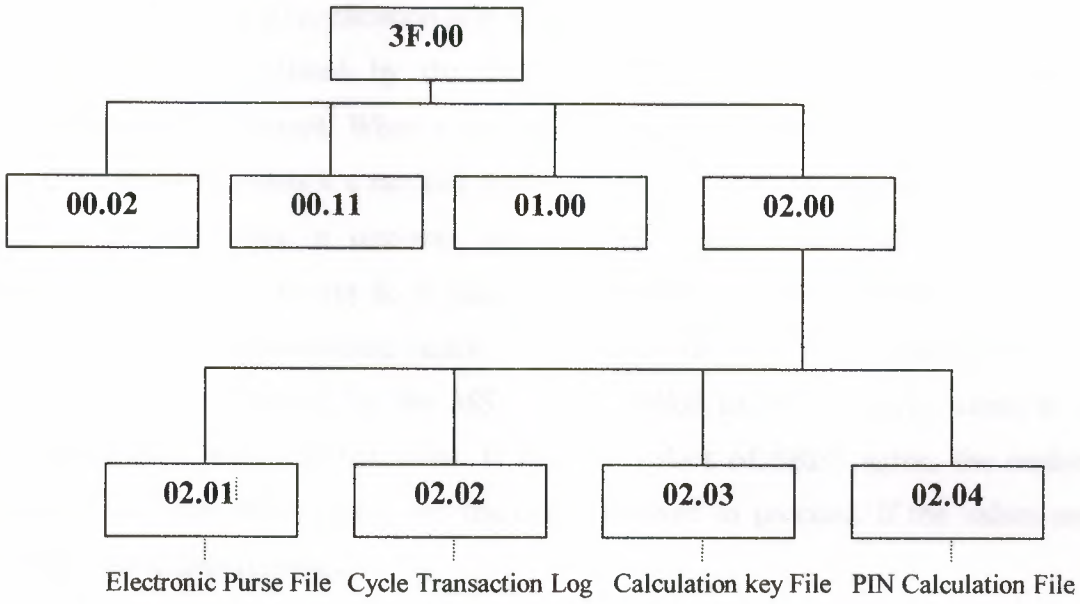


Figure4.1 How the data are stored in asmartcard

4.2. GSM System Security

4.2.1. Overview of GSM Security Features

The object of this part of the report is to provide an overview of the security features in the GSM system. The description is brief, and focuses on the algorithms which are needed and how they are to be used.

Three distinct security services are provided. These are subscriber identity authentication, user and signalling data confidentiality, and subscriber identity confidentiality. Each of these is considered in turn, and the mechanisms used to provide them outlined. Actually the second of the services is a grouping of three GSM features: user data confidentiality on physical connections, connectionless user data confidentiality and signalling information element confidentiality.

The reason for combining them into one service is that they are all provided by one and the same mechanism.

4.2.2. Subscriber Identity Authentication

This subscriber identity authentication service is the heart of the GSM security system. It is used to enable the fixed network to authenticate the identity of mobile subscribers, and to establish and manage the encryption keys needed to provide the

confidentiality services. The service must be supported by all networks and mobiles, although the frequency of application is at the discretion of the network.

Authentication is initiated by the fixed network, and is based upon a simple challenge-response protocol. When a mobile subscriber (MS) attempts to access the system, the network issues it a random challenge RAND. The MS computes a response SRES to RAND using a one-way function A3 under control of a subscriber authentication key K_i. The key K_i is unique to the subscriber,and is shared only by the subscriber and an authentication centre which serves the subscriber's home network. The value SRES computed by the MS is sig-4 nalled to the network, where it is compared with a pre-computed value. If the two values of SRES agree, the mobile subscriber has been uthenticated, and the call is allowed to proceed. If the values are different, then access is denied.

The same mechanism is also used to establish a cipher key K_c for encrypt- ing user and signalling data on the radio path. This procedure is called cipher key setting. The key is computed by the MS using a one-way func- tion A8, again under control of the subscriber authentication key K_i, and is pre-computed for the network by the authentication centre which serves the subscriber's home network. Thus at the end of a successful authentication exchange, both parties possess a fresh cipher key K_c.

The pre-computed triples (RAND, SRES, K_c), held by the fixed networks for a particular subscriber, are passed from the home network's authentication centre to visited networks upon demand. The challenges are used just once.Thus the authentication centre never sends the same triple to two distinct networks, and a network never re-uses a challenge.

In practice the two functions A3 and A8 are combined into a single algo- rithm, called A38 in , which is used to simultaneously compute SRES and K_c from RAND and K_i. In this report this combined algorithm is referred to as the authentication algorithm. The protocol described above makes it quite clear that this algorithm need only be available to an authentication centre and the mobile subscribers which that authentication centre serves. In particular,there is no need for a common GSM authentication algorithm. and different networks may use different algorithms. (The algorithms do, however, need to have the same input and output parameters; in particular, the length of K_c is determined by the GSM cipher algorithm). Never-the-less it is desirable that there is a GSM standard authentication algorithm which may be used

by all networks which do not wish to develop a proprietary algorithm. There is just one candidate for such an algorithm.

4.2.3. User and Signalling Data Confidentiality

As mentioned earlier, this service consists of three elements; user data confidentiality and signalling information on physical connections, connectionless user data confidentiality and signalling information element confidentiality. The first element provides for privacy of all user generated data, both voice and non-voice, transferred over the radio path on traffic channels .

The second element provides for privacy of user data transferred in packet mode over the radio path on a dedicated signalling channel , whilst the third element provides for privacy of certain user related signaling elements transferred over the radio path on dedicated signalling channels .

All of these elements of service are provided using the same layer 1 encryption mechanism, and must be supported and used by all networks and mobiles.

The mechanism is now briefly described. Encryption is achieved by means of a ciphering algorithm A5 which produces a key stream under control of a cipher key K_c. This key stream is then bit-for-bit exclusive-or'd with the data transferred over the radio path between the MS and the base station (BS). Thecipher key is established at the MS as part of the authentication procedure, as described in the last section, and is transferred through the fixed network to the BS after the MS has been identified.

It is essential that the MS and BS synchronise the starting of their cipher algorithms. But this only directly addresses the situation when the network initiates an authentication check. The procedures still need to be specified in detail to cover the situation when the network does not authenticate the MS. When the network intends to issue an authentication challenge, the BS starts deciphering all data immediately after the MS has been identified using the cipher key K_c which the MS will derive upon receipt of the challenge RAND. The MS starts ciphering and deciphering the moment it has computed K_c (and SRES) from RAND, as described in the last section, and before SRES is transmitted. On the BS side,enciphering starts as soon as SRES has been received, deciphered and found to be correct. To cope with possible transmission loss or errors, the authentication request and response message are repeated under the control of timers.

Synchronisation of the ciphering key stream is maintained by using the TDMA frame structure of the radio sub-system. The TDMA frame number is used as a message key for the cipher algorithm AS, and the algorithm produces a synchronised key stream for enciphering and deciphering the data bits in the frame. For each frame, a total of 114 bits are produced for enciphering / deciphering data transferred from the MS to the BS, and an additional 114 bitsare produced for deciphering / enciphering data received at the MS from the BS. A frame lasts for 4.6 ms, so that the cipher has to produce the 228 bits in this time.

The cipher algorithm A5 must be common to all GSM networks, and three algorithms have been proposed as candidates for the GSM standard: a French algorithm, a Swedish algorithm and a UK algorithm. These algorithms are discussed in detail in subsequent parts of this report.

4.2.3. Subscriber Identity Confidentiality

This service allows mobile subscribers to originate calls, update their location,etc, without revealing their International Mobile Subscriber Identity (IMSI)to an eavesdropper on the radio path. It thus prevents location tracing of individual mobile subscribers by listening to the signalling exchanges on the radio path. All mobiles and networks must be capable of supporting the service,but its use is not mandatory.

In order to provide the subscriber identity confidentiality service it is neces-sary to ensure that the IMSI, or any information which allows an eavesdropper to derive the IMSI, it not (normally) transmitted in clear in any signaling message on the radio path. The mechanism used to provide this service is based on the use of a temporary mobile subscriber identity (TMSI), which is securely updated after each successful access to the system. Thus, in rinciple, the IMSI need only be transmitted in clear over the radio path at registration.

The TMSI updating mechanism functions in the following manner. For simplicity, assume the MS has been allocated a TMSI, denoted by $TMSI_o$, and the network knows the association between $TMSI_o$ and the subscriber's IMSI. The MS identifies itself to the network by sending $TMSI_o$. Immediately after authentication (if this takes place), the network generates a new TMSI,denoted $TMSI_n$, and sends this to the MS encrypted under the cipher key K_c as described in the last section. Upon receipt of the message, the MS deciphers and replaces $TMSI_o$ by $TMSI_n$.

4.3. The French Proposal for the Cipher

The cipher proposed by France has always been considered as a hardware rather than a software algorithm. The study of this cipher is based on the description reproduced in Appendix A and described in PDL (program definition language).

4.3.1. PDL Description of the Cipher

Main Algorithm

```
( Load Base Key )
FOR each base key bit from 1 to 64
   Load bit into corresponding LFSR cell
END FOR
( Load Message Key )
FOR each message key bit from 1 to 22
   shift_bits = f()        ( Call to shift function f )
   FOR each register i, from 1 to 3
      Exclusive-or message key bit into lsb
      IF bit i of shift_bits is set
        THEN Shift
      END IF
   END FOR
END FOR
( Produce both enciphering and deciphering streams )
FOR i from 1 to 2
   ( Perform additional shifts )
   FOR j from 1 to 100
      shift_bits = f()
      FOR each register k from 1 to 3
         IF bit k of shift_bits is set
           THEN Shift
         END IF
      END FOR
   END FOR

   ( Output stream of 114 bits )
```

```
FOR J from 1 to 114
   shift_bits = f()
   FOR each register k from 1 to 3
      IF bit k of shift_bits is set
       THEN Shift
      END IF
   END FOR
   Output = Exclusive-or msb of all three registers
 END FOR
END FOR
```

4.3.2 The Shift Function f

```
BEGIN FUNCTION f
  FOR each register i from 1 to 3
    Let middle[i] = the 'middle' bit of register i
  END FOR
  IF less than two of the 'middle bits' are '1'
   THEN bit-complement code
  END IF
  RETURN code
END FUNCTION
```

4.3.3. Software Estimates

In this section the cipher is described in a readable form similar to microprocessor instruction code and an estimate of the speed is made from this. It was suspected that it would not be practical to implement this code in software, so the code was based on a very specialized microprocessor, which may not even exist. If the cipher can not meet the time requirement of 4.6ms on the specialized microprocessor then it will not be able to meet it on a more general one.

This special microprocessor has a word size 5 at least as long as the longest register, i.e., 23 bits, it also has the function PARITY 6 which exclusive-ors all the bits in the accumulator and places the result in the least significant bit while setting all the other bits to zero. Additionally it is assumed that the CARRY can be loaded from the least significant bit of the accumulator. The problem of directing the feedback bit to the appropriate part of the accumulator is ignored.

The external memory, considered to be arranged so that REG contains the registers and MASK contains bit masks for both the extraction of the central bits of each register and for the calculation of the feedback values, with the feedback masks last and in reverse order. The symbol & is used to mean 'address of'.

4.3.4. Evaluating the Shift Function f

The following code extracts the central bits of each register and calculates the corresponding output of the shift function f.

```
Load registers and masks
    LOAD   index register 1 with &REG
    LOAD   index register 2 with &MASK
Extract middle bits of each register
    LOAD   acc with MEM(index 1), POST INC index reg 1
    AND    acc with MEM(index 2), POST INC index reg 2
    PARITY acc
    STORE  acc in M1
    LOAD   acc with MEM(index 1), POST INC index reg 1
    AND    acc with MEM(index 2), POST INC index reg 2
    PARITY acc
    STORE  acc in M2
    LOAD   acc with MEM(index 1), POST INC index reg 1
    AND    acc with MEM(index 2)
    PARITY acc
    STORE  acc in M3
Calculate shift function f
    XOR    acc with M2
    AND    acc with M1
    STORE  acc in I
    LOAD   acc with M2
    AND    acc with M3
    OR     acc with I
    XOR    acc with M1
    STORE  acc in M1
    LOAD   acc with I
```

```
    XOR     acc with M2
    STORE   acc in M2
    LOAD    acc with I
    XOR     acc with M3
    STORE   acc in M3
```

Loading the data itself requires:

2 index register operations k cycles each

Extracting the middle bits of each register requires:

6 index register operations @ k cycles each

3 ALU operations @ m cycles each

3 load / store operations @ n cycles each

The function f requires:

7 ALU operations @ m cycles each

8 load / store operations @ n cycles each

This part of the code requires 8k + 10m + 11n cycles per iteration

4.3.5 Performing the Shifts

The following code clocks the appropriate registers using the results of the shift function. Note that the values of M1, M2 and M3 determine whether or not each register is clocked. Note also that the registers are treated in reverse order since index register 1 'points' to the contents of shift register 3 at this stage.

```
    LOAD    acc with M3
    BRANCH  if zero to A
    LOAD    acc with MEM(index 1)
    AND     MEM(index 2) to acc
    PARITY  acc
    STORE   acc in CARRY
    ROTATE  acc right through CARRY
    STORE   CARRY in 03
    STORE   acc in MEM(index 1)
A:  DEC     index register 1
    DEC     index register 2
    LOAD    acc with M2
    BRANCH  if zero to B
```

```
    LOAD   acc with MEM(index 1)
    AND    MEM(index 2) to acc
    PARITY acc
    STORE  acc in CARRY
    ROTATE acc right through CARRY
    STORE  CARRY in 02
    STORE  acc in MEM(index 1)
B:  DEC    index register 1
    DEC    index register 2
    LOAD   acc with M1
    BRANCH if zero to C
    LOAD   acc with MEM(index 1)
    AND    MEM(index 2) to acc
    PARITY acc
    STORE  acc in CARRY
    ROTATE acc right through CARRY
    STORE  acc in MEM(index 1)
C   LOAD   acc with CARRY
    XOR    acc with 03
    XOR    acc with 02
    OUTPUT acc
```

To estimate the speed it is assumed that 9/4 of the registers are clocked on each iteration, i e., that 3/4 of the operations to shift the registers are performed for each iteration.

Shifting the registers requires:

3 branch operations @ j cycles each

13 index register operations @ k cycles each

6 ALU operations @ m cycles each

8 load / store operations @ n cycles each

The calculation of the output bit requires a further:

2 ALU operations @ m cycles each

1 load / store operation @ n cycles

Therefore, the clocking requires a total of.

$3/4 \times (3j + 13k + 6m + 8n) + 2m + n = 9/4j\ 39/4k + 13/2m + 7n$

cycles per iteration.

The data loading and shift function calculation requires a further $8k + 10m + 11n$ cycles per iteration.

Therefore the total number of cycles required is given by:

$$9/4j + 71/4k + 33/2m + 18n$$

For typical values of $j = k = 5$ and $m = n = 4$ this gives $11.25 + 88.75 + 66 + 72 = 238$ cycles per iteration.

The algorithm must be iterated 450 times to produce 228 bits of output.This corresponds to $\sim\sim$ $450 \times 238 = 107100$ clock cycles to produce 228 bits.On a 1ms microprocessor this would take approximately 107 ms.

The Summary of These estimates show that even on a specialized microprocessor, and ignoring some of the detail, this cipher can not operate at the required speed. It is therefore reasonable to assume that it would not be viable to implement this cipher in software on a more general microprocessor. In light of the unsuitability of this algorithm the memory requirement was not estimated.

4.3.6. Hardware Estimates

The following estimates are based on the two Figures 4.2. and 4.3. Only the hardware necessary for the shift registers and the shift function f is considered, i.e., none of the control, interfacing or test circuitry is studied here.The overall architecture is shown in
Figure 4.1.

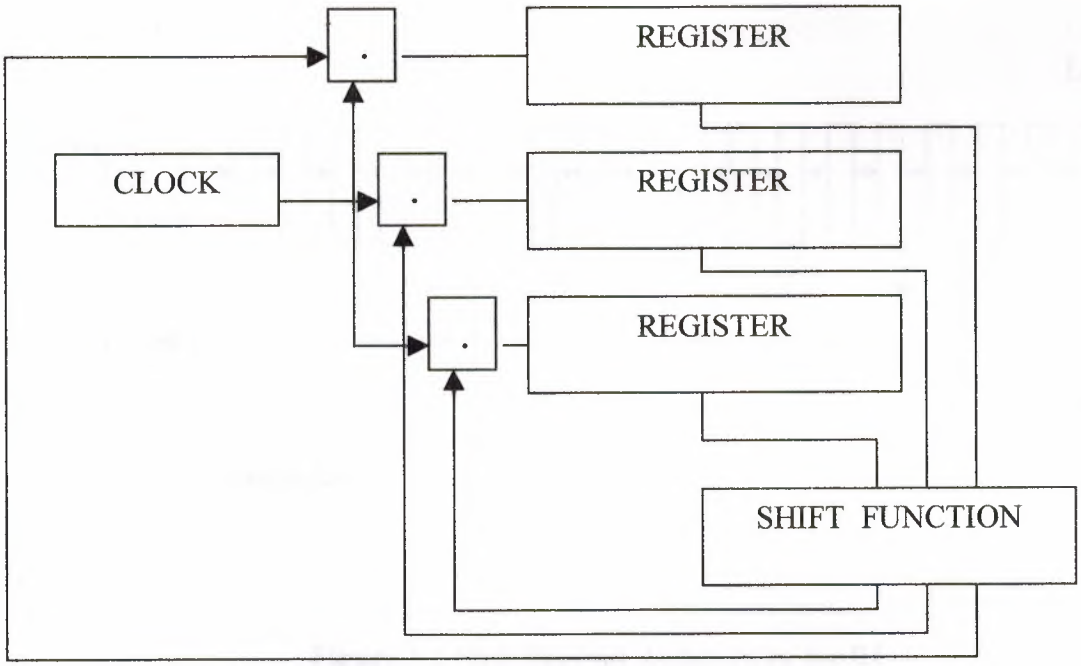


Figure 4.1 Overall Architecture

All the signals shown are single bits. However. the various "Load Control" signals in Figure 4.2 are different signals which control different parts of the loading mechanism.

4.3.7. Shift Registers

Figure 4.2 shows the register R1. The number of exclusive-or gates necessary for each register depends upon the feedback function for that particular register;in total seven such gates are needed for the three registers.

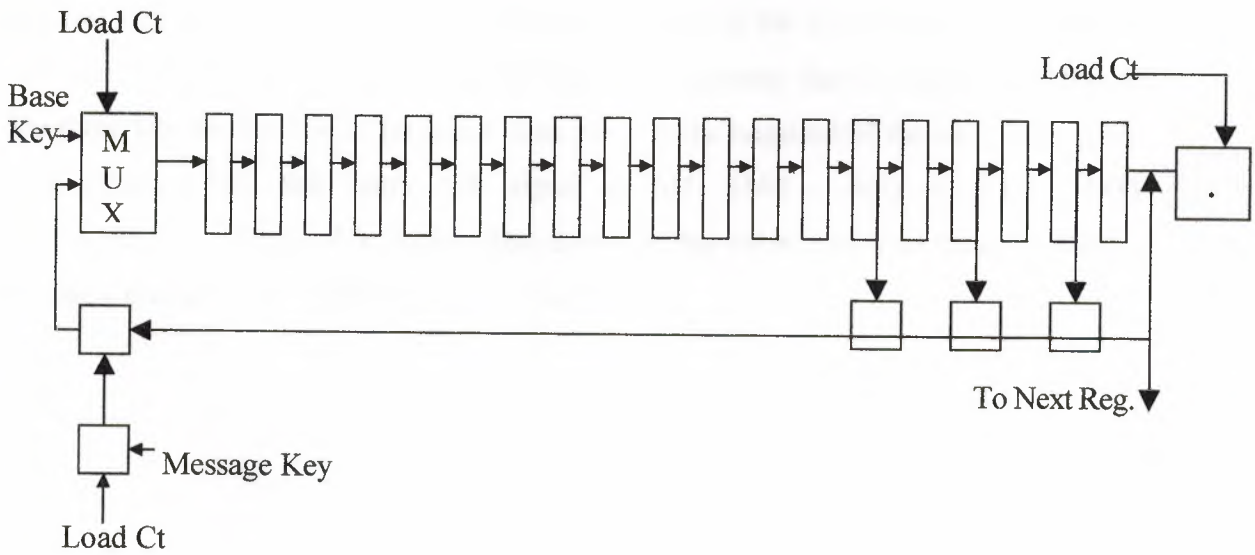


Figure 4.2 Shift Register Architecture for R1

To load the base key, the registers are concatenated together and the key is shifted through, suppressing the output so that the key does not reappear again. To load the message key the key bits are exclusive-or'd into the feedback path. In ordinary operation the feedback path is fed back to the left hand cell without obstruction. In order to implement this a multiplexor is used to chose between the feedback and input, while an and gate is used to suppress the external input to the exclusive-or on the feedback path when it is not required.

The overall components together with their respective transistor counts are:

64 D-types @ 22 transistors each = 1408 transistors

6 2-input AND gates @ 6 transistors each = 36 transistors

10 XOR gates @ 10 transistors each = 100 transistors

3 2-input MUXs @ 12 transistors each = 36 transistors

1580 transistors

An additional two exclusive-or gates are required to combine the output of the three registers, each requiring 10 transistors. This gives a total of 1600 transistors to implement the shift register.

4.3.8. Shift Function f

The shift function is implemented by producing a signal comp which is true if the three bits M1, H2 and M3 need to be inverted. Th;s signal is the exclusiveored with each of the three original bits to effect the inversion. If the three bits are regarded as numbers, then comp is true if and only if their sum is greater than or equal to 2. Thus, if the three bits are fed into a full adder, then comp is the negation of the carry out signal. The equation for this carry out signal is M1 .(M2 - M3) + (M2 . M3) This is shown in Figure 4.3. Rather than inverting this value, and then using exclusive-or gates, exclusive-nor (XNR)gates are used.

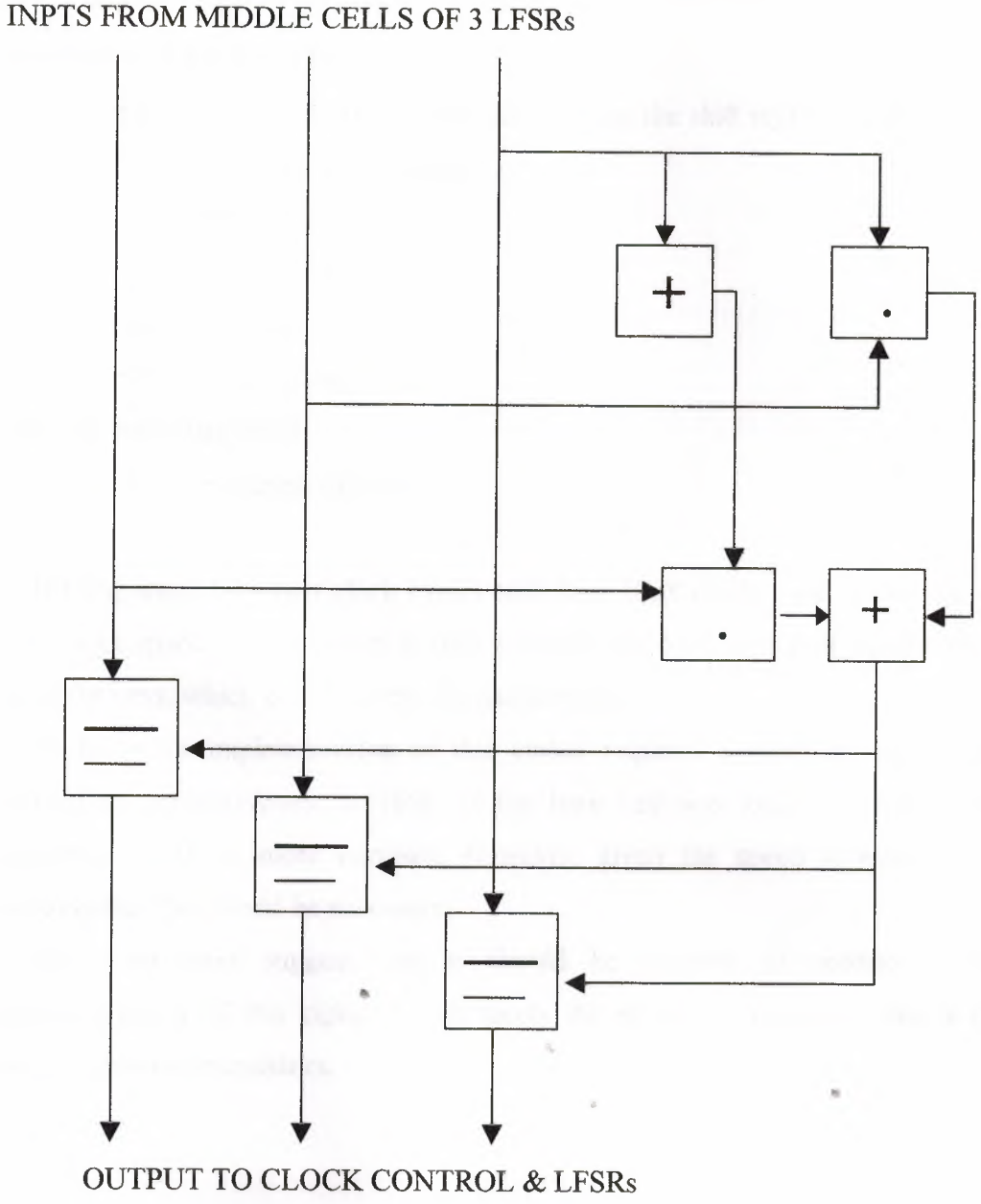


Figure4.3 Shift Function f Architecture

This requires:

2 AND gates @ 6 transistors each = 12 transistors

1 OR gate @ 6 transistors each = 6 transistors

1 XOR gate @ 10 transistors each = 10 transistors

3 XNR gates @ 10 transistors each = 30 transistors

In addition three further And gates are required to combine the output of the shift function with the clock signal. The total number of transistors required is 1600 + 48 + 18 = 1666.

4.3.9 Speed Estimates

In order to produce the two 114-bit key streams the shift registers have to be shifted the following number of times:

64 : to load the base key

22 : to load the message key

100 : intermediate shifts

114 : to produce the encrypt stream

100 : intermediate shifts

114 : to produce decrypt stream

514

If these shifts take two clock cycles each then 1028 clock cycles would be required. At a clock speed of 50ns per cycle then it would take 51.4ms to produce the key streams from the keys, which is well within the requirement.

A hardware implementation of this cipher requires a relatively small number of transistors. approximately in 1666. If the base key was loaded in parallel then the circuitry would be more complex, however, given the speed estimate above it is unlikely that this would be necessary.

These estimates suggest that it should be possible to produce a hardware implementation of this cipher which meets the speed requirement using a relatively small number of transistors.

CONCLUSION

The development of Cellular Communication is the first step towards a true personal communication system that will allow communication anywhere, anytime, and with anyone.

The functional architecture of employing intelligent networking principles, and its ideology, which provides enough standardization to ensure compatibility, but still allows manufacturers and operators freedom, has been widely adopted in the development of future wireless systems.

The SIM Card as an order to GSM network and another applications to give the identity of subscriber to make a high level of security for users.

The future of SIM Card would be more useful especially which can be multiple Card to do many uses(ATM , Cars ,etc.) just with same SIM Card.

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

14. GSM Security http://www.iec.org/online/tutorials/gsm