THE FLORIDA STATE UNIVERSITY

COLLEGE ENGINEERING

TDMA AND CDMA IN MOBILE COMMUNICATIONS.

By

ARUN A BHATJI.

A Thesis submitted to the
Department of Electrical and Computer Engineering
in partial fulfillment of the
requirements for the degree of
Master of Science.

Degree Awarded:
Spring Semester, 2004.

The members of the Committee approve the Thesis of Arun A. Bhatji defended on April 13, 2004.

Bruce Harvey
Professor Directing Thesis

Krishna Arora.
Committee Member

Simon Foo.
Committee Member

Approved:

Reginald J. Perry, Chair, Electrical and Computer Engineering.

The Office of Graduate Studies has verified and approved the above named committee members.

Dedicated to my Parents.

ACKNOWLEDGEMENTS

I would like to express my gratitude to my major professor, Dr. Bruce Harvey for his guidance, advice and constant support throughout my thesis work. I would like to thank him for being my advisor here at Florida State University. I would like to thank Dr. Krishna Arora for her guidance and valuable suggestions. I also wish to thank Dr. Simon Foo for his advice and support. I would like to thank my mother, sister and relatives for their constant encouragement. I would like to convey my utmost gratitude towards my mentor Naresh Shenoy for all his guidance and help in every walk of life. I wish to thank the administrative staff of the Electrical and Computer Engineering Department for their kind support. Finally, I would like to thank my friends here at Florida State University.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ACRONYMS

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project-2
AAA	Authentication, Authorization and Accounting
AC	Authentication Center
AMPS	Advanced Mobile Phone System
ANSI	American National Standards Institute
ARQ	Acknowledge ReQuest
ASN.1	Abstract Syntax Notation number 1
AuC	Authentication Center
BCCH	Broadcast Control Channel
BER	Bite Error Rate
BPSK	Binary Phase Shift Keying
BSC	Base Station Controller
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CELP	Code-Excited Linear Prediction
CM	Connection Management
CRRM	Common Radio Resource Manager
CS	Circuit Switched
DCS	Digital Communication System
DS-CDMA	Direct Sequence Code Division Multiple Access
EDGE	Enhanced Data rate for GSM Evolution
EIR	Equipment Identity Register
ESN	Electronic Serial Number
FBCCH	Forward Broadcast Common Channel
F-CAPICH	Forward Common Auxiliary Pilot Channel
FCCCH	Forward Common Control Channel
FCS	Frame Check Sequence
F-DAPICH	Forward Dedicated Pilot Channel
FDD	Frequency Division Duplexing
FDMA	Frequency Division Multiple Access
FM	Frequency Modulation
F-QPCH	Forward Quick Paging Channel
GGSN	Gateway GPRS Support Node
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSP	Global Positioning System
HDLC	High level Data Link Control
HF	High Frequency

HLR	Home Location Register
HND_ACC	Handover Acknowledge
HND_CMD	Handover Command
HSCSD	High Speed Circuit Switched Data
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IS-95	Interim System-95.
ITU	International Telecommunication Union
JD-CDMA	Joint Detection Multiple Access
LAPD	Link Access Protocol for D-channel
LAPDm	Link Access Protocol for D-channel modified
LLC	Logical Link Control
LPM	Local Protocol Mapping
LTP	Long Term Prediction
LU	Location Update
MAC	Medium Access Control
MGW	Media Gateway
MIN	Mobile Identification Number
MM	Mobility Management
MOC	Mobile Originating Call
MS	Mobile Station
MTC	Mobile Terminating Call
MTP	Message Transfer Part
NADC	North American Digital Cellular
NMT	Nordic Mobile Telephone
NSS	Network Switching Subsystem
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnection
PCM	Pulse Code Modulation
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communication System
PDA	Personal Data Assistant
PDC	Personal Digital Cellular
PDU	Protocol Data Unit
PGW	Packet-switched Gateway
PS	Packet Switched
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RAN	Radio Access Network
RAN GW	Radio Access Network Gateway
RAND	Random Number
RANDSSD	Special Random Number

R-DCCH	Reverse Dedicated Control Channel
RNAS	RAN Access Server
RNC	Radio Network Controller
RPE	Regular Pulse Excited
RR	Receive Ready
S/I	Signal/Interference
SABM	Set Asynchronous Balance Mode
SCP	Service Control Point
SDU	Service Data Unit
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SMC	Short Message Center
SMS	Short Message Service
SNR	Signal-to-Noise Ratio
SRES	Signed Response
SS7	Signaling System number 7
SSD	Shared Secret Data
SWIA	Stop and Wait with Immediate Acknowledge
TACS	Total Access Communication System
TCAP	Transaction Capabilities Application Part
TDMA	Time Division Multiple Access
UA	Unnumbered Acknowledge
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
UTRAN	UMTS Radio Access Network
VLR	Visitor Location Register
VLSI	Very Large Scale Integration systems
VoIP	Voice Over Internet Protocol
WAP	Wireless Application Protocol
WCDMA	Wideband CDMA
WLAN	Wireless Local Access Network
WLL	Wireless Local Loop

ABSTRACT

This thesis is intended to cover two of the most basic, important and highly applied multiple access communication techniques in modern age. It will provide an in-depth literature on the history, evolution, present and future of FDMA (Frequency Division Multiple Access), TDMA (Time Division Multiple Access) and CDMA (Code Division Multiple Access). Along with the basics of TDMA and CDMA, this research will also explain the systems implementing these techniques and an active attempt is made to elaborate their fundamentals, operation, parameters, protocols and other relevant details.

CHAPTER 1

INTRODUCTION

1.1 Multiple Access Procedures

The radio channel is a communication medium shared by many users in one geographic region. Mobile stations compete with one another for the frequency resource to transmit their information streams. Without any other measures to control simultaneous access of several users, collisions can occur (a multiple access problem)[22]. Since collisions are very undesirable for a connection-oriented communication like mobile telephony, the individual subscribers/mobile stations must be assigned dedicated channels on demand. In order to divide the available physical resources of a mobile system, i.e. the frequency bands, into voice channels, special multiple access procedures are used, which are presented in Figures 1, 2, 3 and 4.

1.1.1 Frequency Division Multiple Access (FDMA):

Frequency Division Multiple Access (FDMA) is one of the most common analog multiple access procedures. The frequency band is divided into channels of equal bandwidth such that each conversation is carried out on different frequency See Figure 1. Guard bands are used between adjacent signal spectra to minimize crosstalk between channels.

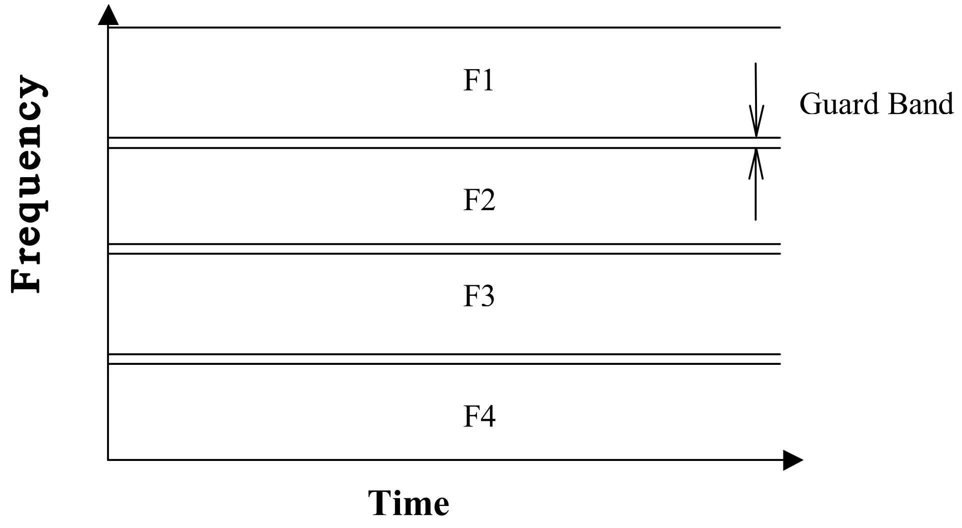

Figure 1- Frequency Division Multiple Access [24].

1.1.1.1 Advantages of Frequency Division Multiple Access

The main advantages of FDMA can be summarized as follows,

- Reducing the information bit rate and using efficient digital codes can obtain capacity increases.
- As FDMA systems use low bit rates (large symbol time) compared to average delay spread, they reduce the cost, and there is low Inter Symbol Interference (ISI).
- There is hardly any equalization required.
- Technological advances required for implementation are simple. A system can be configured so that improvements in terms of speech coder bit-rate reduction could be readily incorporated.
- Since the transmission is continuous, less number of bits are needed for synchronization and framing.

1.1.1.2 Disadvantages of Frequency Division Multiple Access

The main disadvantages found with FDMA were,

- It does not differ significantly from analog systems; capacity improvement depends on reducing signal-to-interference ratio, or signal-to-noise ratio (SNR).
- The maximum bit rate per channel is fixed and small.
- The guard bands result in wastage of capacity.
- Hardware involves narrow band filters, which cannot be realized in VLSI and thus increase cost.

1.1.2 Time Division Multiple Access (TDMA)

Time Division Multiple Access (TDMA) is a more complex technique, for it needs a highly accurate synchronization between transmitter and receiver [14]. The TDMA technique is used in digital mobile radio systems. The individual mobile stations are cyclically assigned a frequency for exclusive use only for the duration of a time slot as shown in Figure 2.

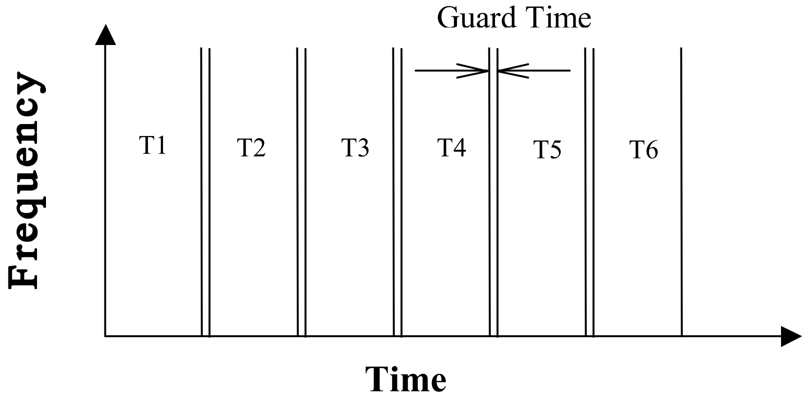

Figure 2- Time Division Multiple Access.

Furthermore in most cases the whole system bandwidth for a time slot is not assigned to one station, but the system frequency is subdivided into sub bands, and TDMA is used for multiple accesses to each sub band. The sub bands are known as carrier frequencies, and the mobile system using the technique are designated as multiple carrier systems. The pan-European digital system GSM (Global System for Mobile communication) employs such a combination of

FDMA and TDMA; it is a multicarrier TDMA system. A frequency range of 25 MHz holds 124 single channels (carrier frequencies) of 200 kHz bandwidth each; with each of these frequency channels containing again 8 TDMA conversation channels.

Thus the sequence of time slots and frequency assigned to a mobile station represents the physical channels of a TDMA system. In each time slot, the mobile station transmits a data burst. The period assigned to a time slot for a mobile station thus also determines the number of TDMA channels on a carrier frequency. The time slots of one period are combined into a so-called TDMA frame. Figure 3 shows five channels in a TDMA system with a period of three time slots and four carrier frequencies.

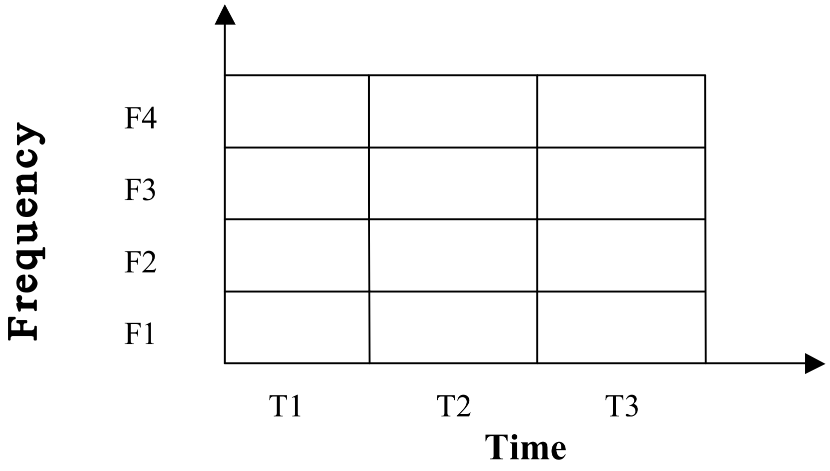

Figure 3: Combined FDMA/TDMA

The TDMA signal transmitted on a carrier frequency in general requires more bandwidth than a FDMA signal, because of multiple time use, the gross data rate has to be correspondingly higher.

1.1.2.1 Advantages of Time Division Multiple Access.

The Advantages of TDMA are summarized below.

- Permits flexible bit rates (i.e., multiple time slots can be assigned to a user, e.g., if each time slot translates to 32Kbps, then a 64Kbps user gets assigned 2 slots per frame).
- Can support bursts or variable bit rate traffic. Number of slots assigned to a user can be changed frame by frame (e.g., 2 slots in frame 1, 3 slots in frame 2, 1 slot in frame 3, 0 slots in frame 4, etc.)
- No guard bands required for wideband system.
- No narrowband filters required for wideband system.

1.1.2.2 Disadvantages of Time Division Multiple Access.

The Disadvantages of TDMA are,

- The high bit rates of wideband systems require complex equalization.
- Because of burst mode of operation, a large number of overhead bits for synchronization and framing are required.
- Guard time is required in each slot to accommodate time inaccuracies because of clock instability.
- Electronics operating at high bit rates increase power consumption.
- Complex signal processing is required for synchronize within a short slot time.

1.1.3 Code Division Multiple Access (CDMA)

Code Division Multiple Access system is very different from time and frequency division multiplexing. In this system, a particular user has access to the entire bandwidth for the entire time duration as shown in Figure 4 [22]. The basic principle of CDMA is that different codes are used to distinguish between the different users. Typically used forms of modulation are Direct Sequence spread spectrum (DS-CDMA), frequency hopping or Joint Detection CDMA (JD-CDMA). Here a signal is generated that spreads out over a wide bandwidth. A code known as a spreading code is used to perform this action. By using a group of codes, which are orthogonal to each other, it is possible to pick out a signal with a given code in the presence of many other signals with different orthogonal codes [24]. In fact many different baseband "signals" with different spreading codes can be modulated onto the same carrier to enable many different users to be supported. By using different orthogonal codes interference between the signals is minimal. Conversely when signals are received from several mobile stations, the base station is able to isolate each one as they have different orthogonal spreading codes.

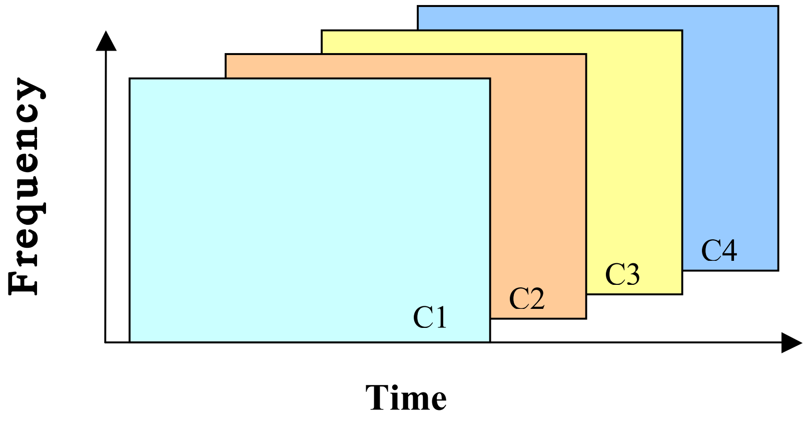

Figure 4: Code Division Multiple Access

1.1.3.1 Advantages of Code Division Multiple Access

The following are the advantages of CDMA

- CDMA has a soft capacity. The more the number of codes, more the number of users. However as more codes are used the S/I ratio will drop and the BER (Bit Error Rate) will go up for all users.
- CDMA requires tight power control as it suffers for far-near effect. In other words, a user close to the base station transmitting with the same power as a user farther away will drown the latter's signal. All signals must have more or less equal power at the receiver.
- Rake receivers can be used to improve signal reception. Time delayed versions (a chip or more delayed) of the signal (multipath signals) can be collected and used to make bit level decisions.
- Soft handoffs can be used. Mobiles can switch base stations without switching carriers. Two base stations receive the mobile signal and the mobile is receiving from two base stations.
- Burst transmission - reduces interference.

1.1.3.2 Disadvantages of Code Division Multiple Access

The following are the disadvantages of Code Division Multiple Access.

- The code length has to be carefully selected. A large code length can induce delay or even cause interference.
- Time synchronization is necessary.
- Soft handoff increases use of radio resources and hence can reduce capacity.
- As the sum of the power received at and transmitted from a base station has to constant, a tight power control is needed. This can result in more handoffs.

CHAPTER 2

EVOLUTION OF TDMA AND CDMA

2.1 First Generation

The first generation of mobile telephony systems began with the analog FM, and FDD (Frequency Division Duplex) systems, AMPS (Advanced Mobile Phone System) and TACS (Total Access Communication System). These systems are still in use in many places where there is not much subscriber base like rural and inaccessible areas. Evolution of technology demanded better speech quality, higher capacity and encryption of user information. Handsets needed to cheaper, lighter and simpler. Demand for better services like international roaming, data and supplementary services were the main cause for providers to find a better system, which would also make complete usage of the frequency band, and will require least modifications to be made to the existing fixed public networks [14].

2.2 Second Generation

The 90's saw the rise of various second-generation systems like GSM900, DCS1800 (Digital Communication System), PCS1900 (Personal Communication Systems 1900), NADC (North American Digital Cellular), PDC (Personal Digital Cellular) and IS-95 CDMA. Although these systems did satisfy all the earlier mentioned needs, the need for high-speed data prompted further enhancements. This new generation was termed as 2.5G [14]. This generation also saw the growth of packet switching in the form of GPRS (General Packet Radio Service) for GSM.

2.2.1 Evolution of GSM.

The following systems evolved from GSM for TDMA/FDMA techniques.

2.2.1.1 HSCSD- High Speed Circuit Switched Data. (28.8 Kbps)

High Speed Circuit Switched Data (HSCSD) is an enhancement of data services for all current GSM networks. Subscribers can access data services, which include data files, email, Internet and other file transfers three times faster. Upgrades for rates up to 43.2 kbps are in progress [31]. HSCSD is available to 90 million subscribers across 25 countries around the world and with International Roaming agreements between all HSCSD Operators access has become even simpler. To access HSCSD special handsets, which support the feature have to be used or a special Personal Computer Memory Card International Association (PCMCIA) portable computer card, with a built in GSM phone can be used in the computers. The user can connect to a local ISP, or directly to one's office, using the cellular device rather than a fixed line.

2.2.1.2 GPRS- General Packet Radio Service. (171.2 Kbps)

The General Packet Radio Service (GPRS) is a non-voice value added service that allows information to be sent and received across a mobile telephone network. Theoretically maximum speeds of up to 171.2 kilobits per second (kbps) can be achieved with GPRS provided all eight timeslots are used at the same time. This is about three times as fast as the data transmission speeds possible over today's fixed telecommunications networks and ten times as fast as current Circuit Switched Data services on GSM networks [32]. No dial-up modems are required in GPRS enabled equipments.

2.2.1.3 EDGE- Enhanced Data rates for GSM Evolution. (384Kbps)

EDGE is another high-speed data standard, which can provide a data rate up to 384 Kbps provided all the eight time slots are used. The idea behind EDGE was to provide high data rates by changing the modulation used. Unlike HSCSD and GPRS, which use GMSK (Gaussian Minimum-Shift Keying), EDGE uses 8-PSK (8-Phase Shift Keying)[33]. Although very small software changes have to be made on the network part to accommodate this change, the handsets have to upgrade to use the EGDE network functionality.

2.2.2 Evolution of CDMA.

The evolution of 2.5G for the CDMA technique gave rise to the following technique.

CdmaOne- IS-95B. (115Kbps).

IS-95A was initially launched in 1996 by Hutchison (HK), which could provide circuit switched service data services at 14.4 Kbps. IS-95A was then upgraded to provide higher data rates up to 64 Kbps in addition to voice services and hence was considered an enhancement and was categorized as 2.5G.

The entire evolution can be summarized in Figure 5.

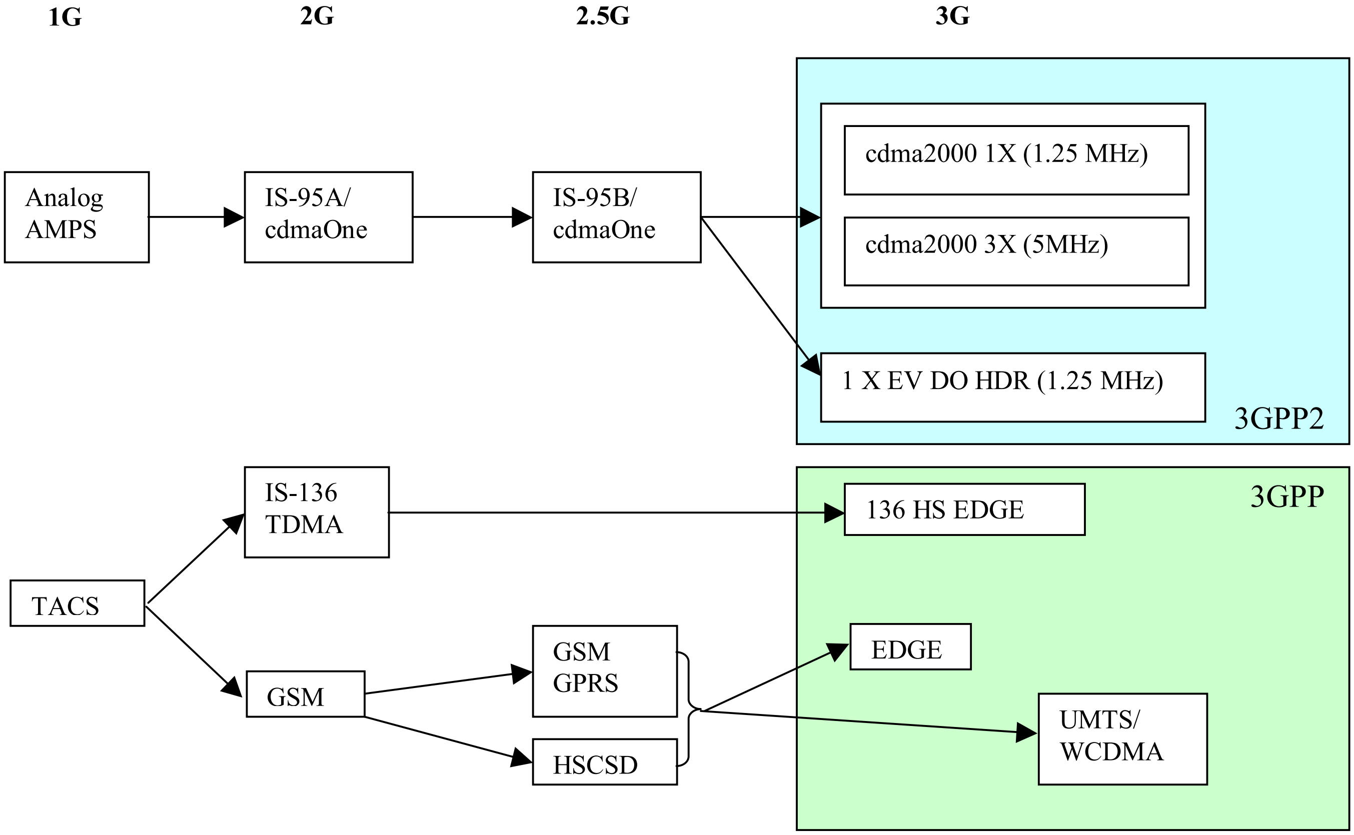

Figure 5- Evolution of TDMA and CDMA

CHAPTER 3

DIFFERENCES BETWEEN GSM AND IS-95

3.1 Specifications

So far enough discussion has been carried out on the basics of multiple access, their advantages and disadvantages. Next the evolution of techniques or systems that worked on these basics was considered. Now Let us now consider the differences two prominent systems (GSM and IS-95) that are currently used and are constantly evolving further. First their basic specifications are tabulated and crucial points are further elaborated.

The Uplink and Downlink frequencies that are allocated for GSM and IS-95 are 890-915 MHz, 824-849 MHz and 935-960 MHz, 869-894 MHz respectively [14]. The frequency at which data is transferred from the mobile station to the base station is called Uplink frequency and the frequency at which the base station communicates with the mobile station is termed as Downlink frequency.

In GSM each carrier in 200 KHz and in IS-95 a carrier is 1.25 MHz. So in a 25 MHz band, 124 channels can be accommodated in GSM and 20 in IS-95 respectively.

The modulation technique used in GSM and IS-95 is different. GSM uses GMSK (Gaussian Minimum Shift Keying) and IS-95 uses QPSK (Quadrature Phase Shift Keying) for spreading modulation and BPSK (Binary Phase Shift Keying) for data modulation. Better spectral efficiency is the reason why separate modulation is used for data and spreading. With BPSK, two signals can be transmitted on a single traffic channel and in QPSK four signals can be transmitted.

Speech coding is carried out to compress the voice. Special coders model the tone and noise generated. The speech of the user is divided in 20 ms blocks and is passed through a coder, which converts 8 bit speech sample to 13 Kbps. So 260 bits are generated every second [14]. The type of speech coding used in GSM is RPE (Regular Pulse Excited) and LTP (Long Term Prediction). The speech coding in IS-95 is CELP (Code-Excited Linear Prediction). The CELP decoder uses a codebook to generate inputs to a synthesis filter. IS-95 implements a rate 1 encoder at 8.55 kbps and supports rates of 4 (1/2), 2 (1/4) and 0.8 (1/8) kbps [7].

Even though GSM and IS-95 work on separate techniques, their basic hierarchical structure is the same, more or less. It is quiet imperative that these basics have to be cleared to prevent further ambiguity. An attempt is made to explain the basics in detail.

The basic building blocks of a cellular network are the cell-sites also called BTS (Base Transceiver Station) or called just Base Stations. Each base station can be broken down into optional three sectors each covering an area of 120 degrees to provide maximum coverage.

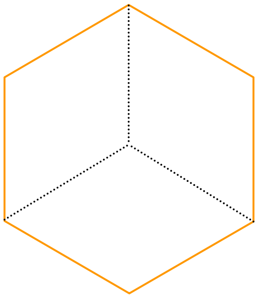

Figure 6: The hexagonal pattern of a BTS with three sectors.

Next in the hierarchy is the Base Station Controller (BSC). These are a collection of a number of base stations. Depending on the density of users and the topology, each BSC can control anywhere from 5-20 BTSs. Base stations are considered as just dummy terminals whereas the BSC can be considered as smart stations. Finally the upper most and the most crucial element is the MSC (Mobile Switching Center). Each MSC covers about 5-15 BSCs. Each service provider has atleast one MSC and incase if multiple MSCs, there is a GMSC, which serves the MSCs. The MSC houses the HLR (Home Location Register), VLR (Visitor Location Register), the AuC and the EIR (Equipment Identity Register). The HLR has all the relevant details of a particular subscriber like the service plan, the supplementary services details, the details about the handset, the latest coverage areas visited and billing details. The VLR primarily deals with roaming and exchanges details of users latching on from foreign networks and also holds latest details of its own users roaming in other networks. The VLR also assists in handovers.

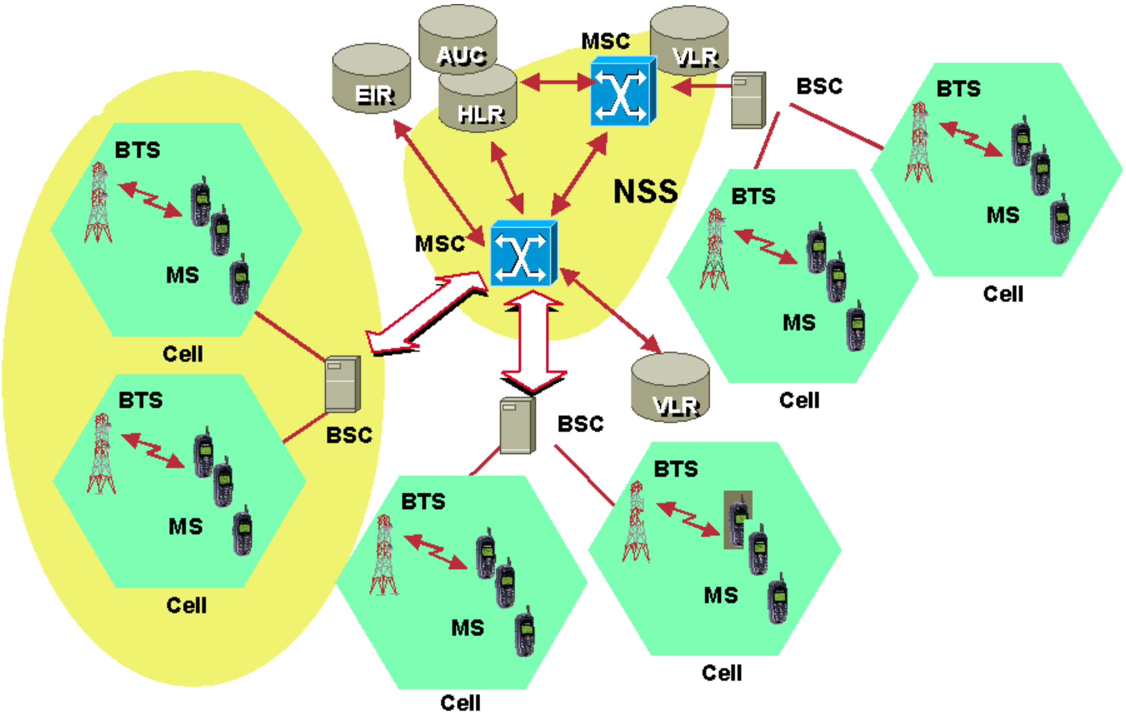

Figure 7: Cellular Hierarchy.

Table 1: Specifications of GSM and IS-95 [25].

	GSM	**IS-95**
Uplink Frequency (MHz)	890-915	824-849
Downlink Frequency (MHz)	935-960	869-894
Multiple Accessing Technique	FDMA/TDMA	CDMA
Duplex Mode	FDD	FDD
Carrier Spacing (KHz)	200.00	1250.00
Modulation	GMSK	QPSK/BPSK
Channels/Frequency Band	124	20
Speech Coding	RPE-LTP	CELP
Speech rate (Kbps)	22.8/11.4	14.4
Data Rate (Kbps)	9.6/4.8/2.4	9.6/4.8/2.4
Traffic Channels/Carrier	8	55

3.2 The Seven Layers of the OSI Reference Model:

Both GSM and IS-95 implement the 7-layer OSI (Open System Interconnection) Reference Model. The major advantage of the OSI Reference Model lies in the fact that the various layers are independent of each other. This means that Layer N shares a common protocol with its peer layer N and with the layer immediately above and below it but not with any other layers. The OSI Reference Model defines only the interface between layers and not the way certain layer is implemented. Therefore, it is, irrelevant to a large degree how the physical signal transmission is achieved.

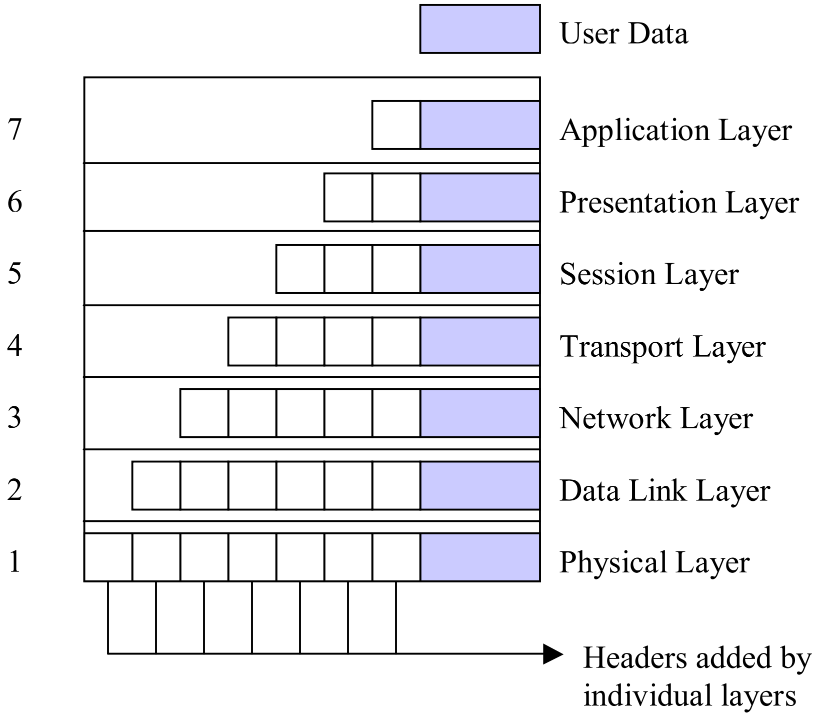

Figure 8: OSI Reference Model

3.2.1 OSI Reference Model used in GSM.

Let us consider the reference model for GSM and the basic functions of individual layers and the protocols involved [8], [10], [11], [13].

3.2.1.1 Layer 1: Physical Layer

The Physical Layer is responsible for the actual transmission of the data and the provision of the necessary facilities. Layer 1 does not know data types or data formats and is not to distinguish between control data and user data. That characteristic, in particular, distinguishes Layer 1 from the other layers. The data packets received from Layer 2 are transmitted without additional verification. Each data packet consists of either a single bit or a number of bits.

With regard to the air-interface of a GSM system, the GMSK (Gaussian Minimum Shift Keying) modulation, the HF (High Frequency) equipment in the MS (Mobile Station) and the BTS (Base Transceiver Station) are part of Layer 1. Over the terrestrial interfaces, the PCM (Pulse Code Modulation), including signal levels and propagation delays, is part of Layer 1.

Naturally, the implementation of the Physical layer depends greatly on the type of interface and might change frequently. For example, between the BTS and the BSC (Base Station Controller), Layer 1 might be implemented as microwave transmission on the first section, as optical fiber on a second section, and as plain cable on the third section.

3.2.1.2 Layer 2: Data Link Layer

The Data Link Layer is responsible for the packaging of the data to be transmitted. The data are combined into packets or frames and then handed to the Physical Layer for synchronous or asynchronous transmission. When information is transmitted or stopped using codes as a reference instead of time, the mode is termed as asynchronous transmission. The devices do not need to be synchronized to a clock. In synchronous transmission, the information is sent in blocks rather than individual characters and the transmission and reception is synchronized to a reference clock [35]. A widespread method for such framing is the high-level data link control (HDLC) protocol, which provides a general structure for data frames and forms, which is the basic for the SS7 (Signaling System number 7) protocol as well as for the LAPD (Link Access Protocol for D-channel) protocol.

SS7 was formed as a basis for signaling traffic between all interfaces in the NSS (Network Switching Subsystems) and the A-interface (interface between the BSC and MSC). There are various protocols, which form the SS7 network. But the one currently relevant in the study is MTP-2 (Message Transfer Part-2).

MTP-2 is a signaling link, which provides reliable transfer of signaling messages between two directly connected signaling points. In case of errors, the MTP-2 requests retransmission of the message [13].

LAPD provides signaling on the Abis-interface (interface between BTS and BSC). It partitions a message into the address field, a control field, a checksum field and a flag at both ends of the message.

The main purpose of all the tasks of Layer 2 is that error detection and correction. Data frames are formed by introducing start/stop marks and by calculation of checksums (Frame Check Sequence, or FCS), which can be checked for consistency by Layer 2 at the receiving side. When the receiver detects an error, it tries to correct the error or requests retransmission.

The Data Link Layer plays a vital role in protocol testing, because all data packets from Layer 3 have to be carried in Layer 2 frame. Note that Layer 2 information is relevant only between two adjacent network nodes and that the Layer 2 protocol might change from interface to interface. For example, the Layer 2 protocol in GSM changes as the data pass on their way from the MS first at the BTS where LAPDm (Link Access Protocol for D-channel modified) converts to LAPD and then again the BSC where LAPD converts to MTP-2/SS7.

On the GSM interface, the LAPDm together with channel coding and burst formatting forms Layer 2. On the Abis-interface, it is LAPD, and the remaining interfaces use the MTP 2 of the SS7 protocol.

3.2.1.3 Layer 3: Network Layer

The network layer prescribes the path a message has to take and who the recipient of the message is. All the information needed to route a data packet is the responsibility of the Layer 3. The RR (Receive Ready) protocol between the MS, the BTS, the BSC and the MSC belongs to Layer 3, as well as all the address information needed to route a call in SS7 system. In GSM it performs the functions of establishing, maintaining, and releasing connections between the network entities and also does the functions of routing and addressing.

3.2.1.4 Layer 4: Transport Layer

Transport layer guarantees the proper end-to-end ordering of message packets, before they are handed to the higher layers. The task of the Transport Layer in the OSI Reference Model is similar to that of the Data Link Layer and the Network Layer. The difference between Layers 2 and 3 on one side and Layer 4 on the other lies in the end-to-end application of Layer 4.

3.2.1.5 Layer 5: Session Layer

The session layer was assigned for global synchronization purposes. It is used for communication process between the communicating entities. In GSM it is used between the MSC and MS to distinguish between a Mobile Terminating Call (MTC), a location update (LU), and a Mobile Originating Call (MOC). Layer 5 is the dialog part of the component sublayer of the Transaction Capabilities Application Part (TCAP). Two TCAP users can coordinate the type of a process, by means of the dialog part of a message and so, for example distinguish between an LU and the activation of a supplementary service.

3.2.1.6 Layer 6: Presentation Layer

Presentation layer is basically a means of data definition and preparation before the data is passed to the Application Layer. The Presentation layer is able to distinguish different data types and to perform data compression and decompression. A typical example for a Layer 6 implementation is ASN.1 (Abstract Syntax Notation number 1), as defined by ITU in Recommendations X.208 and X.209. The ASN.1 is a standardized means to describe operations of interfaces and their parameters. An important part of ASN.1 is the definition of how to assign parameter identifiers, depending on their category and the type of application [Glossary in 13].

3.2.1.7 Layer 7: Application Layer

The Application Layer is the interface of a specific application to the transmission medium or, in other words, to the layer 1 through 6. Note that Layer 7 does not actually contain the application but provides an interface between the application and the communication process. Just as much the implementation of Layer 1 depends on the physical transmission medium, so also the implementation of Layer 7 depends on the specific user.

3.2.2 OSI Reference Model for IS-95

The IS-95 follows more or less the similar structure, but has some additional blocks performing specific functions. Let us consider the model for CDMA (IS-95) in detail [7], [10], [12], [15].

3.2.2.1 The Physical Layer

The physical layer is responsible for the modulation and coding of the data to be transmitted on the radio channel. It also helps in the initialization process like acquiring a paging channel, achieving time synchronization and with the RAKE Receivers reduces the access clashes when multiple users attempt control of a common traffic channel.

RAKE Receivers are used to negate the effects of multipath. The pseudorandom codes, which are orthogonal to each other, are modulated onto a transmitter. These signals are then cross-correlated to the receiver with time-shifted versions of the same pseudorandom codes. The outputs of each delay line after cross-correlation are added in a diversity combiner. This clearly negates multipath and improves the operation of the system.

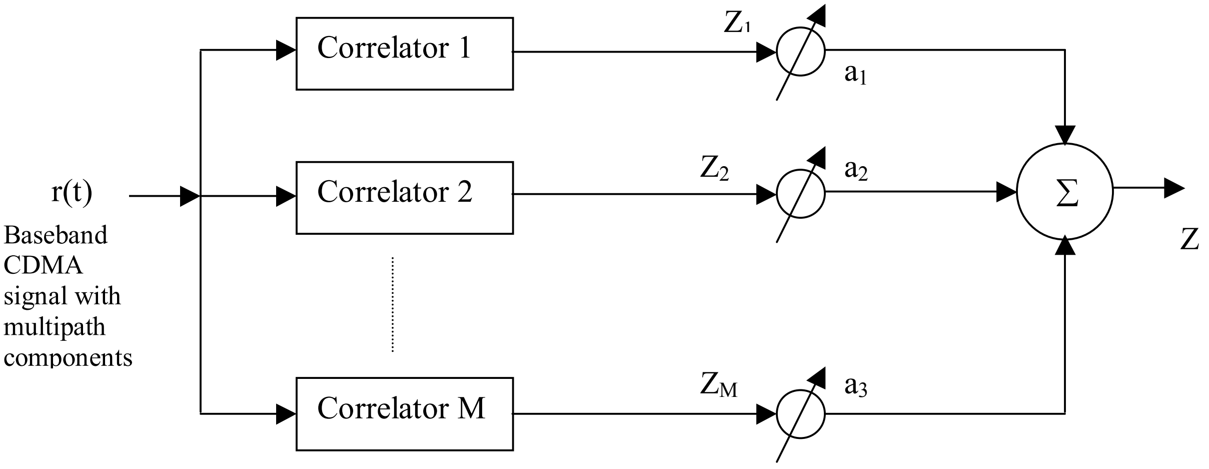

Figure 9- RAKE Receiver Correlator [7].

The RAKE receiver uses multiple correlators to separately detect the M strongest multipath components. The outputs of the M correlators Z_1, Z_2…$Z_{M.}$ Based on the SNR (Signal to Noise Ratio) or power of the correlator output, the respective weights are determined. Lower the SNR or powers, lower the weight. The composite signal is given by

$$Z = \sum_{k=1}^{M} a_k . Z_k$$

Since the codes are orthogonal to each other, the cross correlation with the same data signal will provide the right signal. Whereas, if the code is different, the result would be noise. This makes spreading a very good technique to avoid interference as well. But the only hurdle is that, the signals in uplink have to be time synchronized.

3.2.2.2 The Data Link Layer

Analogous to the network layer, the data link layer is divided into two sublayers: medium-access control (MAC) and logical-link control (LLC) sublayers.

The LLC sub layer is responsible for achieving reliable transmission of data over a single link (from one Mobile Station (MS) to another MS) within the subnet, with the necessary flow control, error control and retransmission. In order to carry out the functions of flow control in a network the protocol used is Stop-and-Wait with Immediate Acknowledgement (SWIA). The protocol requires that the receiver issue an acknowledgement as soon as possible after successful reception of a packet. In case of packet switched networks, error control, retransmission and dynamic routing are often not supported by the network, which leaves the LLC and network layers practically empty. These functions are carried out in the MS.

The MAC layer is responsible for channel access. Due to the multiple access schemes, various MS may be competing for access to the same radio channel.

3.2.2.3 Network Layer

The network layer is often divided into three sublayers: 3a, 3b and 3c. The 3c sublayer, also called the Internet sublayer, contains the functions associated with the interconnection of different subnet. Sublayer 3c may be compared to the local protocol mapping (LPM), as it is called when interfacing the subnet protocol with the user-access protocol. The 3b sublayer, or subnet enhancement sublayer, is designed to harmonize subnets, which offer different services. Also, this sublayer handles end-to-end control within the subnet, including flow and congestion control. The 3a sublayer, or subnet access sub layer, transmits and receives data and control information. It also handles the necessary relaying of data within the subnet, when the end nodes are not directly connected to each other.

3.2.2.4 Upper Layers

All the remaining higher layers are present in the mobile device itself and form the crucial part of the network. Along with the voice and data services, vital functions like authentication and handover are carried out in these layers, so they are covered in detail in the following sections.

3.3 Authentication

With the enormous growth in cellular users, the crucial problems that the providers have to solve are not just system capacity and quality, but also problems of authentication and ciphering. Authentication is different in both GSM and IS-95.

3.3.1 Authentication method in GSM

In the case of a mobile phone working on GSM system, the MS houses a SIM (Subscriber Identity Module), card. The SIM determines the directory number and the calls billed to a subscriber. Physically, it consists of a chip, which the user must insert into the GSM handset before it can be used. The SIM communicates directly with the VLR (Visitor Location Register) and indirectly with the HLR (Home Location Register). The other features that are provided along with authentication are Ciphering and IMEI (International Mobile Equipment Identity) check. Authentication involves two functional entities, the SIM card in the mobile, and the Authentication Center (AuC). Each subscriber is given a secret key (Ki 128 bits), one copy of which is stored in the SIM card and the other in the AuC. During authentication, the AuC generates a 128 bit random number (RAND) that it sends to the mobile. Both the mobile and the AuC then use the random number, in conjunction with the subscriber's secret key and a ciphering algorithm called A3, to generate a signed response (SRES 32 bits) that is sent back to the AuC. If the number sent by the mobile is the same as the one calculated by the AuC, the subscriber is authenticated [14]. This entire process of authentication has to be completed within 500 ms.

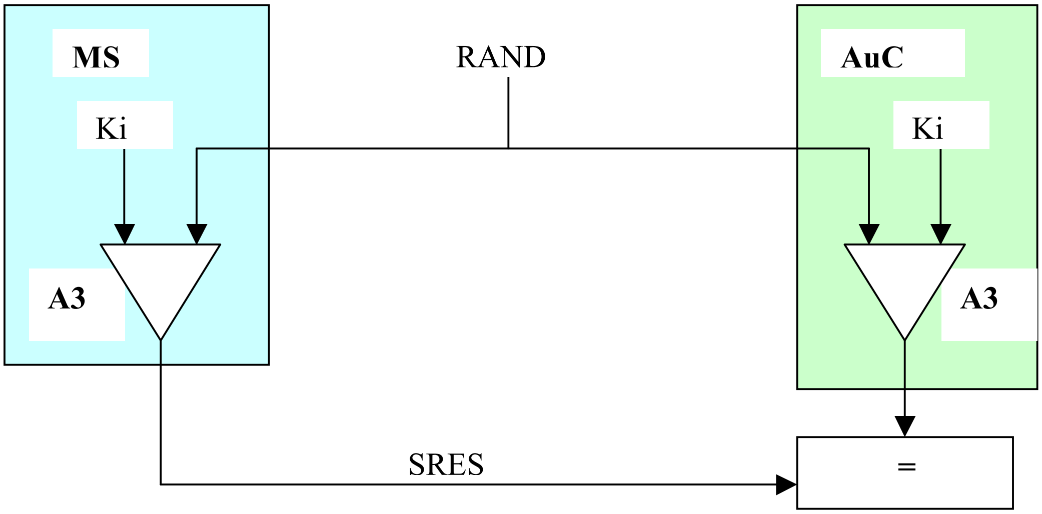

Figure 10- Authentication in GSM [14].

The same initial random number and subscriber key are also used to compute the ciphering key using an algorithm called A8. This ciphering key, together with the TDMA frame number, use the A5 algorithm to create a 114 bit sequence that is XORed with the 114 bits of a burst. This is not that crucial as the burst signal is already coded, ciphered and interleaved in a TDMA manner, but it provides added privacy. As mentioned earlier, a unique International Mobile Equipment Identity (IMEI) number identifies each GSM terminal. A list of IMEIs in the network is stored in the Equipment Identity Register (EIR). The status returned in response to an IMEI query to the EIR is one of the following:

- White-listed: The terminal is allowed to connect to the network.
- Grey-listed: The terminal is under observation from the network for possible problems.
- Black-listed: The terminal has either been reported stolen, or is not type approved (the correct type of terminal for a GSM network). The terminal is not allowed to connect to the network [14].

3.3.2 Authentication in IS-95.

In case of IS-95, there is a dedicated handset that is assigned to a particular number as it does not have a SIM, which the subscriber can insert in any handset and operate at, will. Each handset is identified by an ESN (Electronic Serial Number). But the authentication is more or less similar to that in GSM in which an AC (Authentication Center) of the mobile's home system and the mobile station share a secret data called the A-key.

The network transmits a special random number (RANDSSD), which is used along with the A-key by the MS and the AC to generate a Shared Secret Data (SSD). The RAND is a 32-bit random number issued by the base station in the system overhead data in two 16-bit segments: RAND_A and RAND_B. The mobile stores and uses the most recent version of RAND in the authentication process. The last RAND received by the mobile station is confirmed from the mobile with an 8-bit number RANDC, a part of RAND, since the current system RAND and the one used by the mobile station could differ when the base station receives mobile station results.

The 10-digit directory telephone number is used to form the 34-bit Mobile Identification Number (MIN). The first 3 digits map into the first 10 most significant bits, the second 3 digits map into the next 10 bits, while the last 4 digits map into the remaining 14 bits. SSD is a 128-bit pattern generated using the RANDSSD, the mobile A-key and the ESN and is stored in the semi-permanent memory of the mobile and is known by the base station. SSD is a combination of two 64-bit subsets: SSD_A, which is used to support the authentication procedure, and SSD_B is used to support voice privacy and message confidentiality.

Since the A-key is permanently stored in the handset, there is no need to use a different A-key from the other VLR when the subscriber is roaming. The SSD updates are carried out only in the MS and its associated home system's HLR/AC, not in the serving system [7], [10].

3.4 Handover/Handoff

In any cellular network, the radio links are not permanently allocated to a user for the duration of a call. Handover or handoff is a process of switching an on going call from the coverage of one cell to another.

3.4.1 Handover Procedure in GSM

Depending on the network load and mobility of the user, GSM can perform four different types of handovers [34].

- Handover from one channel (time slots) to another, or from one sector of the cell to another in the same cell also called Intracell Handover.

- Handover from one BTS (Base Transceiver Stations) to another, when both are under the control of the same Base Station Controller (BSC). This is called Intercell handover.
- Handover between BTSs, which, are from different BSCs, but belonging to the same Mobile, services Switching Center (MSC). This is called Inter BSC handover, and
- Handover between two BTSs that are under the control of different MSCs. This type of handover is called Inter MSC.

First we need to consider what are the conditions and situations under which the handover has to be initiated [13]. The MS and the BTS check the quality as well as the strength of received signal during both uplink and downlink. The MS continuously checks the received signal strength of its BTS as well as its surrounding BTSs, which is in the range of –110dBm and –48dBm. Whenever the received signal from any surrounding BTS is greater for a particular interval of time, handover is initiated. Also if a MS moves out of its permissible limits of a cell, handover is initiated [14].

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

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

3.4.1.1 Intracell Handover

Intracell handover can be initiated due to timeslot interference or lack of free time-slots. There are various parameters that are considered in making the decision.

- RXQUAL_UL (Quality of Received signal on the Uplink) and RXQUAL_DL (Quality of Received signal on the Downlink).

- L_RXQUAL_UL_H and L_RXQUAL_DL_H (Rxqual Threshold for Handover).
- RXLEV_UL_IH and RXLEV_DL_IH (Rxlev Thresholds for Interference Handover) (Range: -80dBm to –40dBm).

Uplink Interference Handover:

When the Receiver signal quality at the uplink is greater than the lower level threshold for handover intracell handover is carried out. This may occur due to timeslot interference or congestion in a particular carrier [14].

RXQUAL_UL > L_RXQUAL_UL_H and

RXLEV_UL > RXLEV_UL_IH, where RXLEV_UL is the received signal level at uplink as reported by the BTS (Base Transceiver Station).

Then, Intracell handover is done.

Similarly;

Downlink Interference Handover:

When the same conditions occur in the downlink, Intracell handover must be initiated. RXQUAL_DL (Receiver Signal Quality at downlink), L_RXQUAL_DL_H (Lower level threshold of Receive Signal Quality for handover), RXLEV_DL (Receiver signal level at the downlink) and RXLEV_DL_IH (Receiver signal level threshold for interference handover in downlink)

RXQUAL_DL > L_RXQUAL_DL_H and

RXLEV_DL > RXLEV_DL_IH

Then, Intracell handover is initiated.

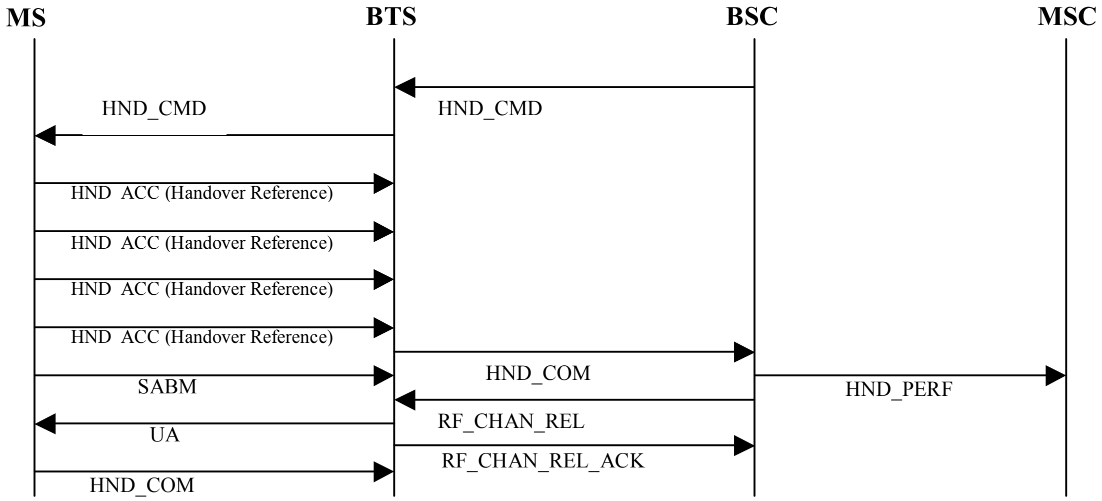
MS
BTS
BSC
MSC
HND_CMD
HND_CMD
HND ACC (Handover Reference)
HND ACC (Handover Reference)
HND ACC (Handover Reference)
HND ACC (Handover Reference)
HND_COM
SABM
HND_PERF
RF_CHAN_REL
UA
RF_CHAN_REL_ACK
HND_COM

Figure 11- Intracell Handover

Intracell Handover Sequence:

- After evaluating the signal quality and level, when the BSC decides to perform an intracell handover, it sends the handover command (HND_CMD) to the BTS, which is passed onto the MS.
- This command contains details like on which time slot and on what frequency is the new channel. It also indicates through the "handover reference" as to what will the MS shall identify itself on that new channel.
- The MS responds by sending the HND_ACC, which acknowledges the handover command and also the handover reference.
- Crucial connections on the Air-interface are established by exchange of messages like SABM (Set Asynchronous Balance Mode) and UA (Unnumbered Acknowledge) frame.
- On completion of the handover, the MS informs the BTS by sending the HND_COM, which is passed on to the BSC over the Abis-interface and to the MSC in the form of the HND_PERF command. This is the only time that the MSC is involved in the intracell-handover.
- After all the procedures are complete, the old channel is relinquished and control is handed over to the new channel by exchange of messages between the BSC and the BTS (RF_CHAN_REL and RF_CHAN_ACK).

3.4.1.2 Intercell handover

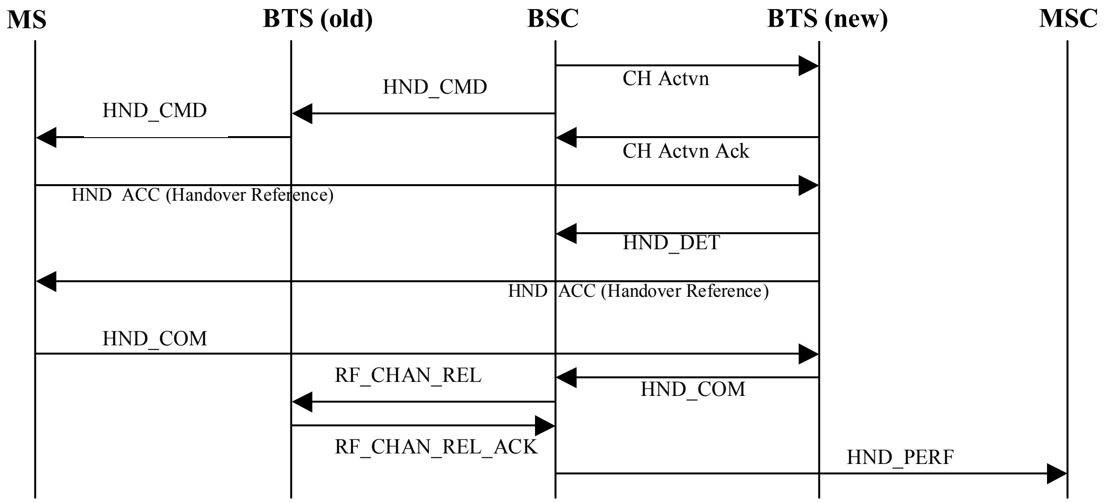

Figure 12- Intercell handover

The BSC regularly checks the quality of the signal on uplink and downlink. The signal can deteriorate either because the user has been receiving better coverage from another base station for some duration of time or due to increase in interference or multipath because of mobility. The BSC can try to initiate a handover within the same base station, but if there are no free channels available, the BSC has to initiate an Intercell handover. Once the BSC decides upon the handover, the following signaling takes place.

- Channel Actvn: BSC sends this message to the target BTS that contains the handover reference number, power setup, ciphering info and timing advance details.
- Channel Actvn Ack: The BTS allocates a channel and waits for reception and then sends this acknowledgement.
- Handover Command: The mobile is now commanded to tune to the new channel by this message, which contains channel description and reference number.
- Handover Access: On receiving the previous message, mobile sends this access message to the new BTS, which is a short burst containing the reference number.
- Handover Detection: This message is sent to the BSC to inform that the mobile has tuned to the channel. BSC on receiving this message switches the circuits.
- Handover Complete: The mobile on synchronizing with the new channel sends this message to the BSC.
- CH Release: The BSC then sends this message to the old BTS to release the radio channel, which is acknowledged by the BTS.

3.4.1.3 Inter BSC handover

In this kind of handover the MSC is completely involved. The previously discussed reasons could also compel the BSC to initiate a handover from one base station, which is in the coverage of one BSC to another base station under the coverage of a different BSC. This may generally occur near borders of cities where the two BSCs share coverage.

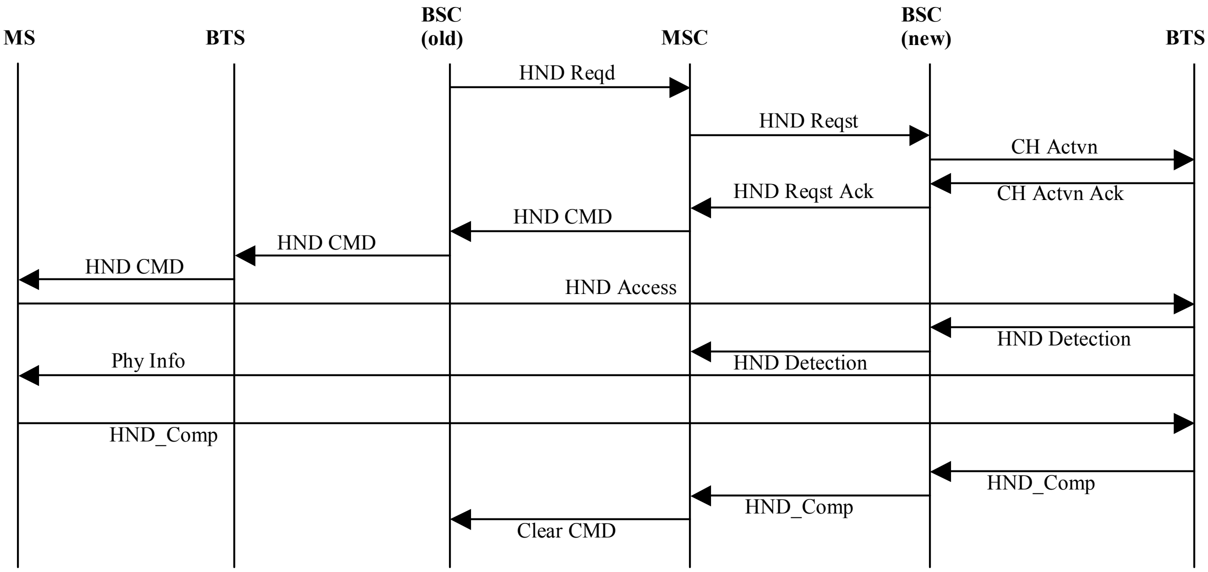

Figure 13- Inter BSC Handover

Upon such a situation the BSC sends a handover request message to the MSC, which contains the handover reference and target cell identity. The MSC then sends a handover request message to the target BSC to activate a channel in that cell. The BSC on activating the channel sends an acknowledgement to the MSC. On receiving the acknowledgement the MSC sends the handover command to the MS through the BSC, which contains the reference number and details of target channel. The mobile tunes to the channel and sends small bursts of handover access. The BSC then on getting an indication of these bursts sends a handover detection message to the MSC. The MSC then does the group switching. The MS in proper synchronization with the new BTS sends the handover complete message, which is forwarded to the MSC. The MSC on receiving this message sends the clear command to the old BSC to release all resources.

3.4.1.4 Inter MSC Handover

In this case, the basic messaging remains the same, more or less. Considering a MS moving from the coverage of a base station, which is governed by MSC A, to that of a base station in MSC B. This can occur at the junction of two states and can be closely related to roaming. The only difference would be that in case of roaming, the other cell site could be governed by a MSC of a different service provider. The BSC A determines that a handover into another BSC is necessary and sends a request to MSC A. On receiving the details of the probable candidates for handover, from the handover request message, the MSC A, sends a handover prepare message to MSC B. The handover request message is passed onto a BSC in MSC B and it receives an acknowledgement when BSC B has any available resources. A traffic channel is used to establish connection between MSC A and MSC B. This part is unique from all other handovers discussed so far, as the former MSC still has control over the channel. The MSC A then sends a handover command to the MS through BSC A. After the resources are received, the acknowledge is passed on from the BTS in MSC B all the way to MSC A. Finally the handover complete message is passed from MSC B to MSC A and this permits BSC A and BTS A to relinquish all radio resources. After the handover MSC B controls all the sub-level handovers that need to be carried out and MSC A is only kept updated, but does not participate in them.

The same process is carried out if the MS travels back to MSC A. But in case the MS moves to another MSC, say MSC C, then the same process is carried out but finally all the resources of MSC B are relinquished and MSC C and MSC A share a communicating traffic channel.

3.4.2 Handoff/Handover in IS-95

The basics of a handover procedure in IS-95 are different than handovers in GSM. There are some differences even in the situations that result in handover to be initiated [7], [27]. In IS-95, the BTS can initiate a handover when the load on the network is not evenly distributed. In GSM the MSC is involved only during inter BSC or inter MSC handovers. Confirmation of handover is the only role that the MSC performs in handovers within BTSs and between BTSs. But in case of IS-95 system, the MSC has major involvement and plays a very crucial role. The other difference in the two systems is that in IS-95, either the MS or the Base Station can initiate the handover, whereas in case of GSM, the BSC has the sole control over the decision-making. The handovers initiated by the MS are called *mobile-assisted handoffs* and those controlled by the network are called *network-controlled handoff*.

As compared to handoffs in GSM, where after the handoff is complete, the old BTS completely relinquishes the channel and the new BTS is in total control, in CDMA the old and new BTS both continue to have contact with the MS and unless and until one of the signal fades and the MS requests it to drop the channel. The advantage of soft handoff is the ongoing call has a redundancy available as it receives transmissions from two different BTS, so this reduces call drops, but this also doubles the system usage and might reduce the system capacity. The MS adjusts its transmitted power so that it is over a threshold level. In case the BTS commands the MS to increase its power but the MS has already reached its limit, then either side can request a handoff.

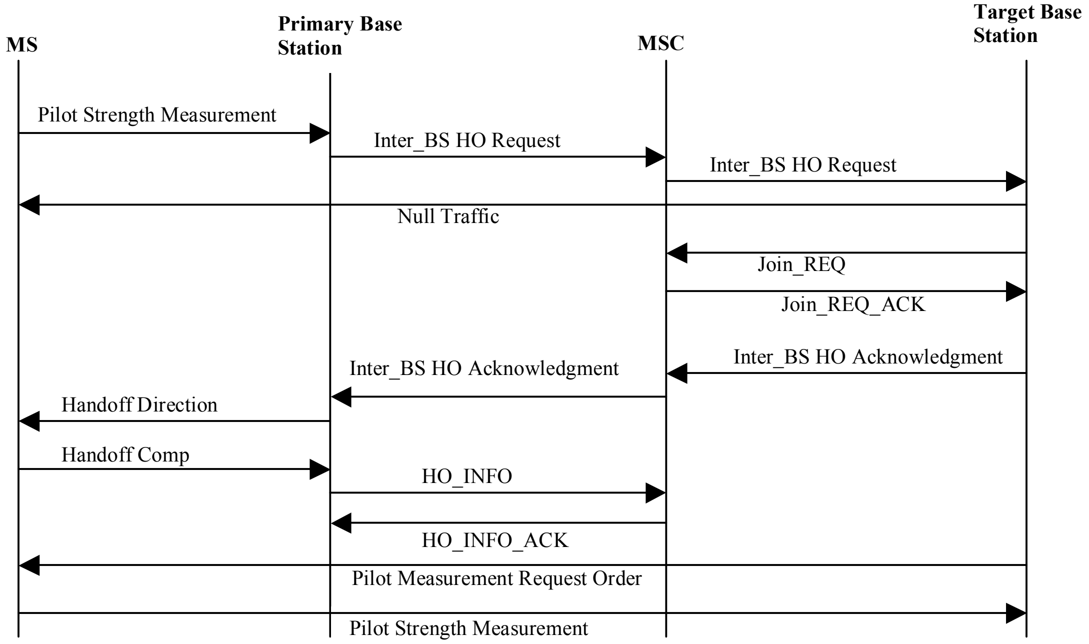

Figure 14- Mobile Assisted Soft-Handoff in IS-95.

The following is a scenario of a mobile station assisted soft-handoff.

1. The mobile station determines that another base station has sufficient pilot signal to be a target for handoff.
2. The mobile station sends a Pilot Strength Measurement message to the serving base station.
3. The serving base station sends an inter-BS Handoff Request message to the MSC.
4. The MSC accepts the handoff request and sends an inter-BS Handoff Request message to the target base station.
5. The target base station establishes communication with the mobile station by sending it a Null Traffic message.
6. The target base station sends a Join Request message to the MSC.
7. The MSC conferences the connections from the two base stations so the handoff can be processed without a break in the connection and sends a Join Acknowledge message to the target base station.

8. The target base station sends an inter-BS Handoff Acknowledgement message to the MSC.
9. The MSC sends an inter-BS Handoff Acknowledgement message to the serving base station.
10. The serving base station sends a Handoff Direction message to the mobile station.
11. The mobile station sends a Handoff Complete message to the serving base station.
12. The serving base station sends a Handoff Information message to the MSC.
13. The MSC confirms the message with a Handoff Information Acknowledgement message.
14. The target base station sends a Pilot Measurement Request Order message to the mobile station.
15. The mobile station sends a Pilot Strength Measurement message to the target base station.

Finally the mobile station receives signals from both the base stations involved in soft handover. If the signal strength of any of the two base stations falls below a predetermined threshold, it will be dropped off from the soft handoff and the control will be taken over by the other base station. It is possible that the signal strength of the new base station itself may fall below the threshold. In both cases the control is transferred to the more powerful base station. The following steps describe this process and it is similar to either of the base stations.

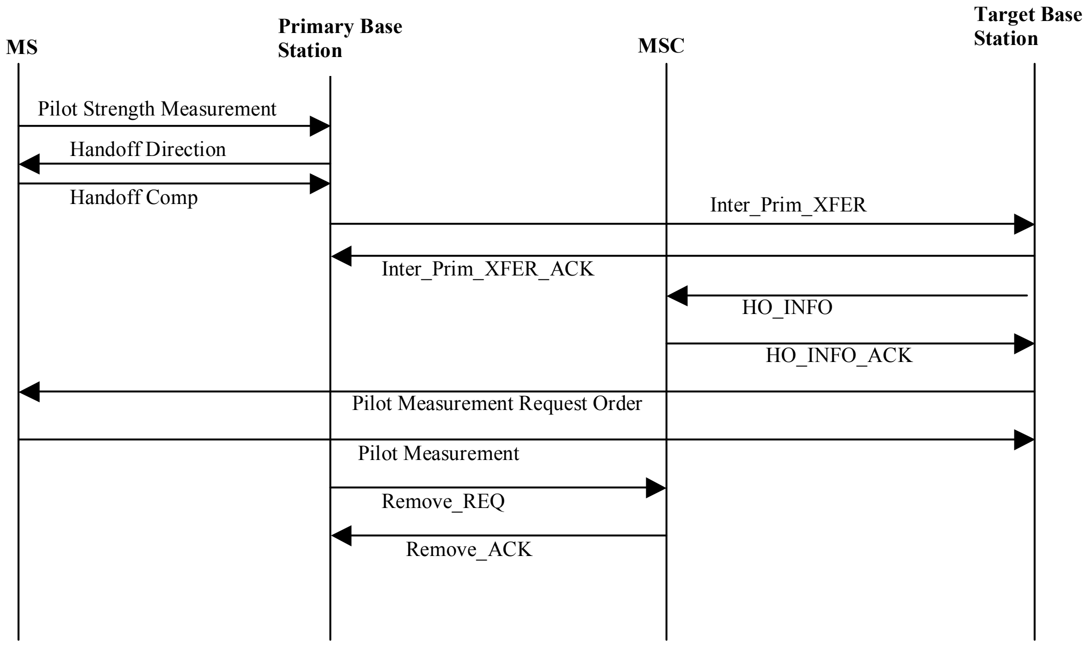

Figure 15- Soft Handoff with Primary Base Station relinquishing control.

1. The mobile station determines that the serving base station has insufficient pilot signal to continue to be a base station in the soft handoff.
2. The mobile station sends a Pilot Signal message to the serving base station. The message requests that the base station drop off from the handoff.
3. The serving base station sends a Handoff Direction message to the mobile station that indicates which base station is to be dropped from the soft handoff.
4. The mobile station sends a Handoff Complete message to the serving base station.
5. The serving base station sends an Interface Primary Transfer message to the target base station with relevant call record information.
6. The target base station confirms the message with an Interface Primary Transfer Acknowledgement message.
7. The target base station then sends a Handoff Information message to the MSC.
8. The MSC sends a Handoff Information Acknowledge message to the target base station.
9. The target base station sends a Pilot Measurement Request Order message to the mobile station.
10. The mobile station sends a Pilot Strength Measurement message to the target base station.
11. The old serving base station sends a Remove Request message to the MSC that requests that the base station be dropped from the connection.
12. The MSC confirms the message by sending a Remove Acknowledgement message to the old serving base station.

In network-controlled handoff, the network checks the RSS (Received Signal Strength) of the base stations regularly. Depending on the RSS of various base stations the network decides for a handoff. The network even creates a temporary connection between the two base stations to save time and also to prevent unwanted use of network resources [36]. This kind of handoff was used in earlier first generation systems like TACS (Total Access Communication System), NMT (Nordic Mobile Telephone) and AMPS (Advanced Mobile Phone System). Network assisted handoffs are longer in use not only as they were not suitable for locations with high density of users but also because they produced a noticeable click in the conversation.

3.5 Network Comparisons and Service Selection:

The factors that can determine which service provider a user would like to select are considered in detail. These factors depend on which kind of a service the user is interested in. The user might be interested in either speech services only, or data services only or might want speech and data services.

While considering only speech services, the user does not need to look into many details. Checking the network coverage and quality of service are the main pointers. The network coverage is crucial as it is not necessary that if the user does receive good signal on the MS, he would have good connectivity. It could be that the network is not optimized and the BTS might have less capacity and might experience frequent call drops or failures of call maturing. If the network coverage is not good due to several reasons like dense vegetation or high-rise buildings, the user might not get good reception. This may result in cases where the user does not receive calls and the network might find the user unreachable or the call might mature but the user could experience mute or cracking of speech. The other situation that can arise is due to improper coverage by the home network, the MS might go into roaming mode very often causing the user to pay extra if roaming is an additional feature in the subscription. Continuing on the network issues, in certain areas where there is not much technological penetration, analog systems (like AMPS) are still in use. The analog systems which work on the 800 MHz band, provided better coverage as concrete walls were transparent to their signals, but the new 1.2 GHz bands find the walls to be opaque and hence the user might not get good coverage in close environments like malls and elevators.

Similarly for a user wishing to avail for only data services, proper coverage is one of the most crucial aspects that have to be focused on. As data files are large files, changes in network coverage can vary download speed. Also if there are problems with mobility and the handovers are improper, and calls drop, then speech calls can be reinitiated but data calls will result in restart of transmission, which would not be expected. On the same lines, if the user expects seamless coverage, then proper tie ups have to be organized between various services like WLAN, WLL, DSL and even IS-95 or GSM.

CHAPTER 4

Future of GSM and IS-95 in Mobile Communications

After providing millions of customers with mobile access, the next primary need that needs to be satisfied is mobility along with higher data rate transmission. There are several systems what are candidates for 3G [16]. They can be grouped based on their basic technology as wideband CDMA, advanced TDMA, hybrid CDMA/TDMA, and Orthogonal Frequency Division Multiplexing (OFDM).

The prime candidate for the future of Mobile Telecommunications is 3G formed of UMTS (WCDMA) and cdma2000. Both of these techniques have WCDMA air interface, so WCDMA has been explained separately.

Wideband CDMA: The nominal bandwidth of all 3G WCDMA proposals is chosen to be 5 MHz because;

- It is enough to provide data rates of 144 and 384 Kbps (which are the 3G target), and even 2 Mbps in good conditions;
- Bandwidth is always scarce, and the smallest possible allocation should be used, especially if the system must use frequency bands already occupied by existing 2G systems;
- This bandwidth can resolve more multipaths than narrower bandwidths, thus improving performance.

The enhancement towards 3G resulted in the formation of two separate organizations, 3GPP and 3GPP2. The main difference between 3GPP and 3GPP2 is that, 3GPP has a new radio access network UTRAN (UMTS Radio Access Network), which is solely created for UMTS and the core network is same as GSM. 3GPP2 supports cdma2000 and has IS-95 as its core network so as to provide backward compatibility to existing CDMA systems. The following two sections consider 3GPP and 3GPP2 in detail.

4.1 3GPP (Third Generation Partnership Project).

3GPP develops specifications for a 3G system based on the UTRA (Universal Terrestrial Radio Access) radio interface and on the enhanced GSM core network [28] [29]. The main objective was to provide GSM with higher bit-rate, providing different quality of service classes for packet data and also provide simultaneous usage of both circuit and packet switched services. 3GPP is planned to provide backward compatibility with GSM and GPRS (General Packet Radio System) [16]. With the expectations of packet-switched services to change more towards IP (Internet Protocol) communications, 3G have to evolve to meet the challenges. Furthermore, it is anticipated that media consumption via mobile networks will become a significant contributor to the traffic of the networks. The new usage patterns of mobile communications lead to an always-on society, where most, if not all, are continuously online to access their favorite media at all times without any delay. 3GPP incorporates two modes, frequency division duplex (FDD) and time division duplex (TDD).

In the FDD mode the uplink and downlink use separate frequency bands. A bandwidth of 5 MHz is divided into 10 ms radio frames and each frame is further divided into 15 time slots. The chip rate of UTRAN is 3.84 Mcps. Each user has a unique sequence of chips called the spreading code, which modulates the data signal. The ratio of the chip rate and the data rate is called the spreading factor. The spreading factor used in UTRAN can vary from 4 to 512.

In the TDD the uplink and the downlink use the same frequency carrier. The 15 time slots in a frame can be dynamically allocated between uplink and downlink directions, thus the channel capacity of these links can be different.

GPRS being packet switched service; it is viable to have both technologies interact separately on the radio interface. This enables the service provider to incorporate both the systems in a common network without much change in hardware. So 3G UTRAN uses dual-system protocol stack. So the main protocols like RLC/MAC in GSM are not the same used in GPRS. Whereas core network protocols like MM (Mobility Management) and CM (Connection Management) are similar and can be reused. This entire dual-system protocol stack is implemented in the mobile unit.

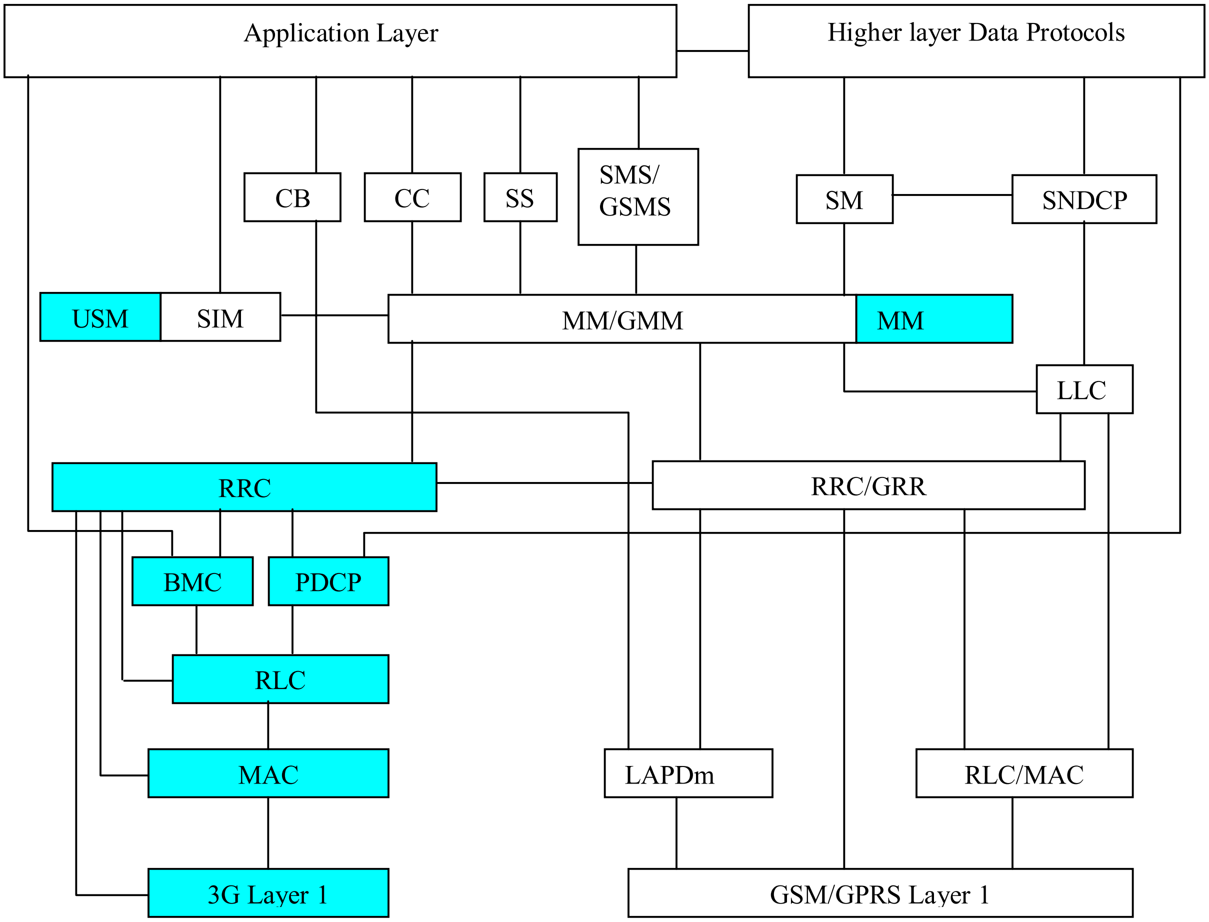

Figure 16- Dual system Protocol Stack [16]

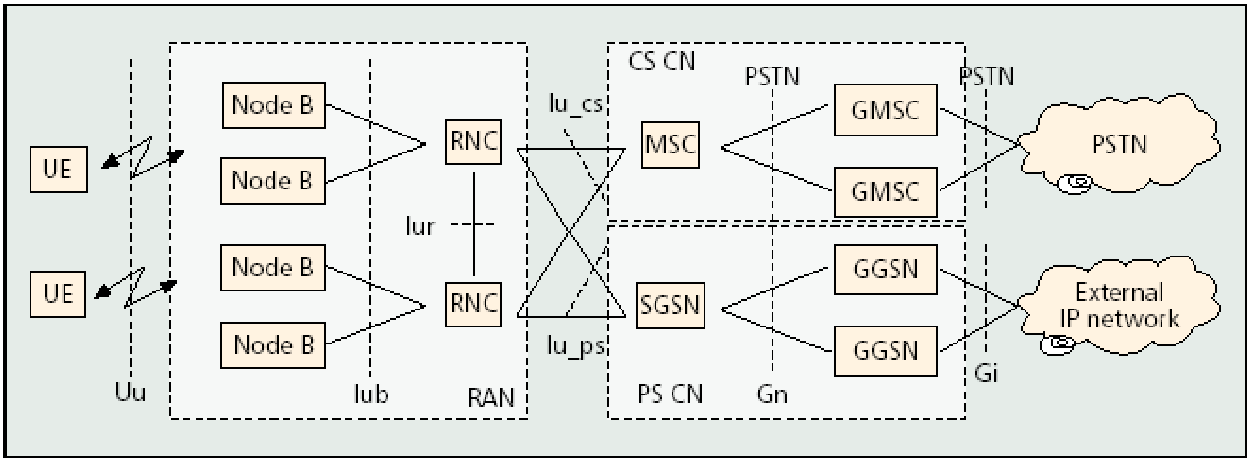

Figure 17: Simplified 3GPP Logical Architecture [20]

Also the logical architecture is designed so as to separate the CS (Circuit Switched) system from the PS (Packet Switched) system along with providing interconnection between them through the RAN (Radio Access Network). The RAN is comprised of several node B's which have one-to-many mapping, which means each node B can be connected to only one RNC (Radio Network Controller), while one RNC can manage various node Bs. Also to maintain communication during soft handover, when the UE (User Equipment) moves from the coverage of a node B of one RNC to the node B of a different RNC, vertical connection between RNCs is needed. The RAN for both CS (Circuit Switched) and PS (Packet Switched) systems are interconnected through interfaces. The core network on the other hand is separate for both systems and intercommunications are carried out only through the interfaces between RAN and CN. The CN for CS network is almost a replica of the GSM network. In case of PS CN, functionality is divided into two network elements: SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node). The former takes care of most of the session management, mobility management, and AAA (Authentication, Authorization, Accounting) functionality of the PS CN. The latter is merely a gateway between external IP (like the internet) and cellular system and has important functionality like QoS (Quality of Service) mapping between the networks, mobility anchoring, packet filtering, and so on.

These individual blocks also can be streamlined for better performance [20].

RAN: The RAN is divided into smaller pieces and the node Bs is upgraded with radio interface related processing, like power control, and radio frame scheduling. The non-radio-interface-specific user plane handling functions along with provisioning of interfaces between CS and PS Core Networks are housed in the RAN GW (Radio Access Network Gateway) block. With the upgrade of the Bs to B+, the performance of the RAN GW is reduced to just acting as a routing point and to separate the RAN and the CS and PS CN. The other new block called the Common Radio Resource Manager (CRRM) handles the radio resource management functionality. Along with this, the hierarchy is dissolved and transparency between the B+ nodes and the RNAS (RAN Access Server) or RAN GW is developed. The RAN Access Server handles all the remaining RNC functionality. Also to assist soft handovers between node B+s, horizontal connection between node B+s is also provided.

CN: The idea to separate the user and control plane functionality was inculcated in the CS and PS CNs with the introduction of the servers and the MGW (Media Gateway) and PGW (Packet-switched media Gateway) for CS and PS systems respectively. The servers handle control plane functionality and the gateways take care of the user plane processing by terminating the respective protocols.

The streamlined logical architecture can be summarized in the following figure and can be stated as the evolved 3G architecture.

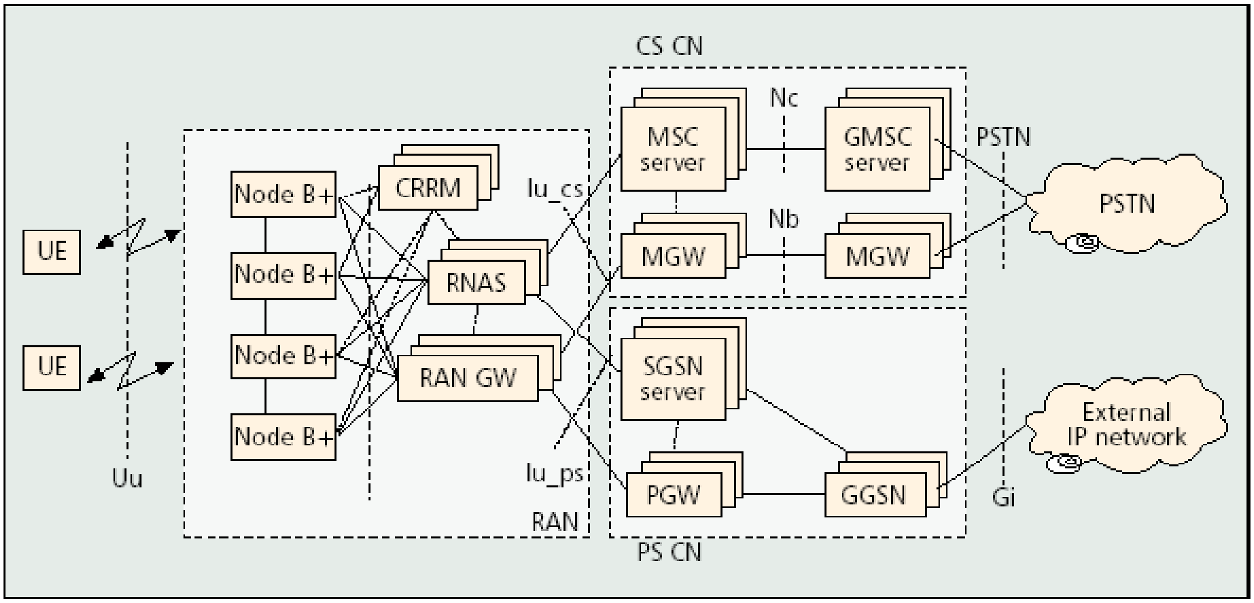

Figure 18- Streamlined and evolved 3G Logical Architecture.

4.2 3GPP2 (Three Generation Partnership Project 2)

3GPP2 has specified a system that is backward compatible with IS-95 systems. Unlike UTRAN, cdma2000 can provide a variable chip rate (in multiples of 1.2288 Mcps). In the initial stages a maximum of a multiple of three will be provided (3.6864 Mcps). Even on the radio end, the uplink and downlink can provide variable configurations. In the downlink, the two options are either multicarrier or direct spread configuration. Multicarrier configuration will include 3 separate 1.25 MHz narrow band carriers are bundled together. In the direct spread, a single wideband carrier of 3.75 MHz is accommodated [16]. But in the uplink, as cdma2000 uses unsynchronized reverse link, it is difficult to have multiple carriers as it will be difficult to introduce mutual orthogonal codes. So the initial stages will use a single 1.25MHz carrier in both the links, so as to have backward compatibility with IS-95.

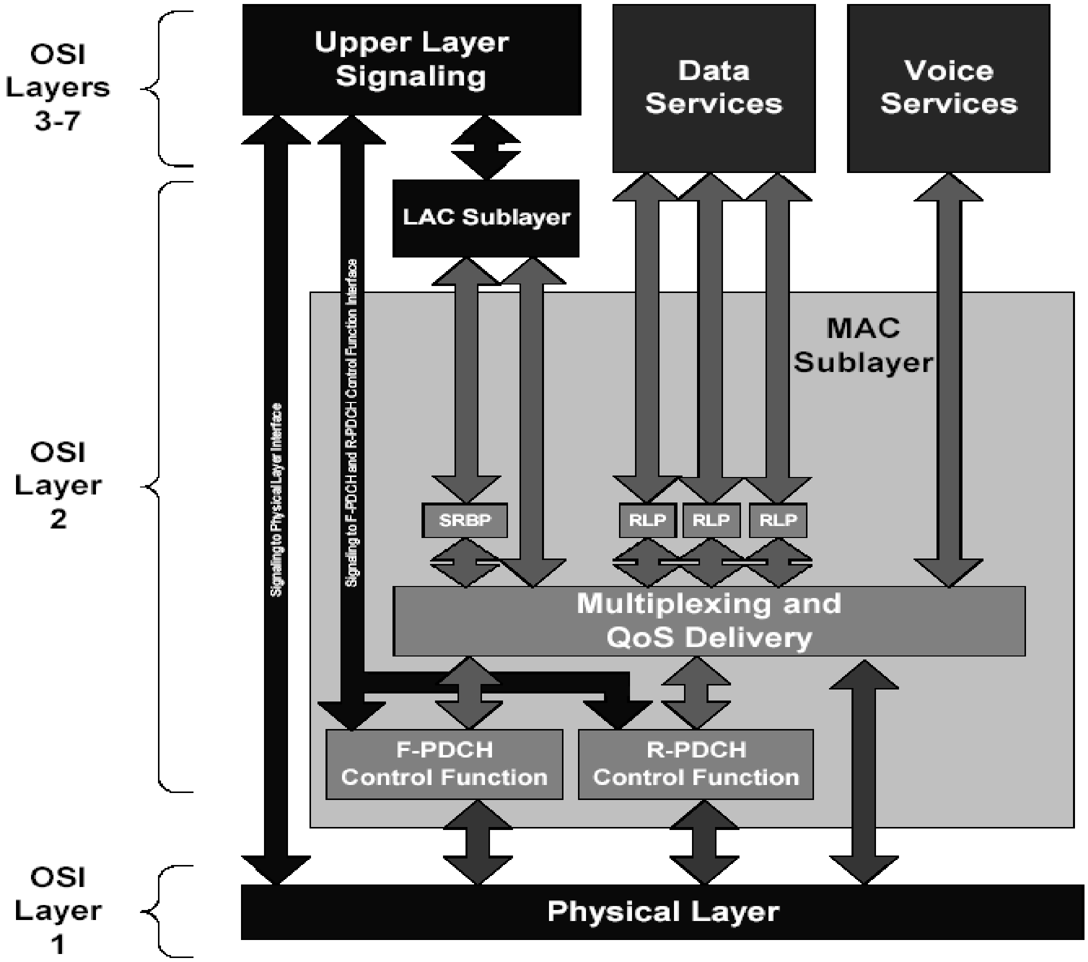

Figure 19- OSI Reference Model for cdma2000 [30].

This is the basic block diagram of the OSI reference model for cdma2000 in 3GPP2. The functions carried out by some of the blocks to are explained to some extent [30].

4.2.1 Physical Layer

There are separate physical channels for forward link and reverse link. These links are further divided into dedicated and common channels [30]. The channels are mainly pilot, synchronization, dedicated control, supplementary, auxiliary and access channels.

Forward Pilot Channel:

- Carries out channel gain and phase estimation.
- Detects multipath rays to assist the RAKE receivers.
- Assists in Handoff.

Forward Sync Channel:

- Assists the mobile devices to acquire the initial time synchronization.

Forward Paging Channel:

- In cdma2000 each base station can have multiple paging channels for sending control information and paging messages at a data rate of 9.6 or 4.8 kbps, which is similar to IS-95.
- It carries overhead messages, pages, acknowledgements, channel assignments, status requests and SSD (Shared Secret Data) updates.

Forward Common Control Channel (F-CCCH)

- Helps communication between layer 3 and MAC messages.

Forward Common Auxiliary Pilot Channel (F-CAPICH)

- This can be used with antenna beam forming applications to generate spot beams. Spot beams enhance the network coverage in a particular geographical location.

Forward Broadcast Common Channel (F-BCCH)

- Carries only overhead messages and possible SMS broadcast messages.
- It improves the performance of the system by separating overhead messages from the paging channels and passing them on to a separate broadcast channel.

Forward Quick Paging Channel (F-QPCH)

- This channel uses a different type of modulation to quickly inform the mobile device about its assigned slot in a paging channel. It is sent in advance (80 ms) before the paging channel to save time. This channel is a new channel, which is available in cdma2000 and in IS-95.

Forward Dedicated Auxiliary Pilot Channel (F-DAPICH)

- This is an optional pilot, which can be generated for a particular mobile.
- Its application is also in improving coverage or data rate toward a particular mobile.

Reverse Access and Common Control Channel

- They are used for communication of layer 3 and MAC messages from the mobile to the base station.
- Different access channels are separated by different long PN codes.

Reverse Pilot Channel

- This channel assists in forward link power control.
- A fixed reference value is multiplexed with forward power control information, also called the power control subchannel, which is a kind of feedback and helps the forward channel to increase or decrease its power. The power control subchannel is a single bit transmitted every 1.25 ms.
- Apart from power control measurements, the pilot channel is used for initial acquisition, time tracking, RAKE receiver and coherent reference recovery.

Reverse Dedicated Control Channel. (R-DCCH)

- Since the physical channel is spread with a Walsh code sequence to provide orthogonal channelization, the R-DCCH is mapped to the in-phase (I) data channel.

4.2.2 Link Layer

This forms the second layer in the OSI model and its main functions are to provide reliability and QoS as per the service desired by the upper layers. The link layer is divided into two main parts [7], [12];

4.2.2.1 Link Access Control (LAC) Sublayer.

The LAC Sublayer and layer communicate signaling information through the logical channels. The LAC Sublayer performs the following functions [30]:

- Delivery of SDUs (Service Data Units) to the Layer 3 peer entity using ARQ techniques, when needed, to provide reliability.

- Assembling and validating well-formed Protocol Data Unit's (PDU), appropriate for carrying the SDUs.
- Segmentation of encapsulated PDUs into encapsulated PDU fragments of sizes 19 suitable for transfer by the MAC Sublayer
- Reassembly of encapsulated PDU fragments into encapsulated PDUs.
- Access control through "global challenge" authentication, message integrity validation or both. Conceptually, some messages failing authentication or message integrity check on a common channel may not necessarily need to be delivered to the Upper Layers for processing.
- Address control to ensure delivery of PDUs based upon addresses that identify particular mobile stations.
- Internal signaling, by exchanging notifications and data with Layer 3 and the supervisory and configuration entities, resulting from the processing of LAC Sublayer level information.

4.2.2.2 MAC (Medium Access Control) Sublayer.

It controls the access of data services between multiple users and also for a single user accessing different services.

4.2.2.3 The Upper Layers (Layer 3 to 7).

These layers are present in the mobile and carry numerous functions. Layer 3 originates and terminates signaling data unit (SDU) between the base station and the mobile station. Layer 3 processing consists of the following,

- Mobile station initialization.

  In this state, the mobile station selects the system to be used then acquires the pilot channel, system configuration and timing information and synchronizes its timing to that of a CDMA system.

- Mobile station in idle state.

  In this state, the mobile performs supervision and monitoring of the common channel, the paging channel and the Forward Common Control Channel. It also performs the message acknowledgement, soft handoff, registration procedures and also the network reselection procedure if needed.

- System Access State.

  The mobile communicates with the base station to check for broadcast messages of just monitors the paging channels. While in this state the mobile also checks for soft handoffs if required.

- Mobile station control of traffic channel State.

  In this state the mobile first verifies and then begins communicating with the base station using forward and reverse traffic channels according to the service configuration. It also communicates with the base station for soft handoff, CDMA-to-CDMA hard handoff or CDMA-to-Analog Handoff.

- Registration.

  After control of the traffic channel, the mobile informs the base station about its location, identification and slot cycle (which time slot is it monitoring). There are other different types of registrations. Power up and down registration to inform the base station about turn on, switching to a different frequency block or from a different system. It also registers with the base station, when the distance between the current base station and the one in which it last registered exceeds a threshold.

4.3 Future Advancements.

Moving on further towards the future capabilities and services that await the user to avail, a concept which allows the user to stay connected all the time, at any place and through any device. This idea will provide seamless connectivity to user for accessing the 3G cellular network, the Wireless LAN or the DSL, even Bluetooth through either a 3G-cell phone, a laptop or a PDA (Personal Data Assistant) in the home, the way to work, inside the office or even in a remote location like restaurants, airports, subways or even movie theaters [17].

This smart system seems easy to bring into existence but there are lot of details that have to be considered from the user and the service provider’s point of view. Parameters like personal preferences, size and capabilities of the device, application requirements, security, operator or corporate policies, available network resources, and network coverage. There are various elements that form this new network, they being the terminal the user is using (laptop, PDA, handset), the network (GSM, CDMA, 3G, Bluetooth, WLAN), the service provider network and the application server [18].

These elements can be related in various ways,

- In this case the user gets access to all networks from a single provider on a package basis or an as needed basis. This case is not complicated as the user needs just one subscription and will receive just one bill. There is a common identifier, which will identify the user even when in different networks and will assist in billing, authentication and authorization.
- In this case the provider has tie-ups with other providers. This situation might create some complexity but will provide the user the discretion to choose either the network that he or she has subscribed to or just stay move to a better network on a needed basis. The same scenario can apply to the final two situations as well.
- The provider might not have any network of his own, but might have tie-ups with all necessary providers for the user to access.
- In the final case the user himself decides which network he wants to access and pays according to it in his package.

While selecting such a package the user might want to setup a personal profile, define parameters like cost, bandwidth (speed) or applications. These parameters should be easy to understand and also he should have total control to edit them from time-to-time. One way to implement seamless information exchange would be to either use to user profile to vary the access of the network to meet a certain minimum QoS threshold, or the applications will vary according to the devices and optimize the presentation and delivery of the information.
Now from the technical point, lets consider a network and how would all the parameters would fit in.

4.3.1 Compatibility

First and for most there has to a compatibility between the technology of the service provider and the handset, which means a handset which works on GSM technology cannot work on a CDMA network.

During initialization or turning on of the device, a procedure called the location update has to carried out where the device looks out for the best network that is available. The location update has to be constantly carried out so that the device can shift in case there is any other network, which can provide better service. Location updates can be carried out in three different ways. The device itself has a memory of the user's profile and a list of default settings to select a network. This is necessary not only for location update but also incase there is a loss of network connectivity, the device must choose access without support from the network. The network can also vary its characteristics like QoS or load for better throughput or incase the device is incapable of doing so. Finally the user can intervene and select any particular network from multiple options according to his package [17].

4.3.2 AAA (Authentication, Authorization and Accounting).

The second detail to be covered is Authentication, Authorization and Accounting. After the user has carried out a location update, the network has to verify the identity of the user specially when the user is in different network. Incase the user is latched on to a different network, which is not owned by the parent provider, then the authorization message is sent from the present network to the parent network, whose details are embedded in the device and after all the details are clarified, the device is allowed to access the network. Then finally the billing details have to be passed on from the parent network to this network for maintenance of billing records.

4.3.3 Continuity and Transfer.

The third aspect that is involved is continuity and transfer. This could mean change of device in the same network or change of networks when the same device is in use. Enhancing the IP layer and making it transparent to higher layers can maintain continuity [17].

CHAPTER 5

INTEROPERABILITY BETWEEN TDMA AND CDMA

After considering both the Access methods and their pros and cons, the condition arises that the end user is not expected to know all the technicalities and details while using the basic speech service, data service, the SMS (Short Message Service) or even when roaming (National or International) from one network/system to another. The only concern is to get the best service, connectivity, better voice and data quality and less call drops, in short a method which satisfies network transparency and number portability has to be found. So the question that arises is whether we can use the advantages of both the methods and incorporate them in a way, which will not cause the service provider to bear heavy expenses of software and hardware modifications and providing the best service to its customers. This can be achieved in two ways.

1. Incorporate GSM system into an already existing CDMA system or vice-versa. Thus advantages of both the systems can be achieved [2]. Or in other words develop a novel method, which combines different Multiple Access methods [5].
2. Implement both the systems separately and have interoperability between them.

Consider the first method in which CDMA operation can be integrated within the operative GSM system [2].

Several options can be considered for integrating CDMA on an existing GSM system.

- Coincident time-slots on a set of carriers may be pooled to form a single wide-band time-slot which users can occupy using code division multiple access techniques.
- The time-slots of a single carrier may be allocated to sets of T/CDMA users.
- The same time-slots over different carriers can also be allocated using CDMA technique.

The performance can be evaluated by testing under worst-case scenarios of interference for example: A GSM user subject to only CDMA interference and vice-versa. To avoid the problems of adjacent channel interference and frequency planning the receiver should be able to operate for an adjacent (200 kHz) interference with a C/Ic ratio of –9 dB. The main techniques that can be considered as candidates are Joint Detection CDMA and Multi-Carrier DS-CDMA (MC-DS-CDMA). The crucial test that the system has to overcome is the interference the user of one system has to face from the other system. So if it can be proved that the for e.g. a GSM user can cope up with interference from only CDMA users and still maintain the speech quality and vice-versa, then the combined system is a valid option.

Joint Detection CDMA (JD-CDMA):

Joint Detection CDMA is a multi-user detection technique based on the application of advanced separation algorithms to adaptively eliminate multiple access interference [3].

Multi-Carrier Direct-Sequence CDMA (MC-DS-CDMA):

In this scheme, the original data stream is multiplexed into several sub streams, each of which is separately spread by the same user specific code and transmitted on separate sub carriers. There are two implementations of MC-DS-CDMA that can be considered. The first uses a single time-slot and multiple carriers to form a wideband CDMA channel; the other uses adjacent time-slots on the same carrier to implement CDMA operation [2]. The factors that need to be considered are intercell interference, intracell interference, the cluster size and the number of slots/carrier. Even though with MC-DS-CDMA Intracell interference is reduced, JD-CDMA shows higher tolerance. So for each system working in either environment as the number if users per channel increase, the number of slots that can be pooled on a channel reduces. So a trade-off has to be reached so as to provide the threshold Eb/No. It can be stated that use of CDMA in a GSM environment greatly reduces interference. With the reduction in interference, the cluster size can be reduced resulting in greater number of users in the GSM system.

To implement this concept of providing CDMA services on an existing GSM network, it is obvious that some form of mutual interference suppression is necessary. Introduction of simple notch filters at the CDMA transmitter and receiver is a viable solution [6]. On the downlink, the

CDMA transmitter inserts a notch filter with a sharp cut-off centered on the frequency the GSM network in using for that cell.

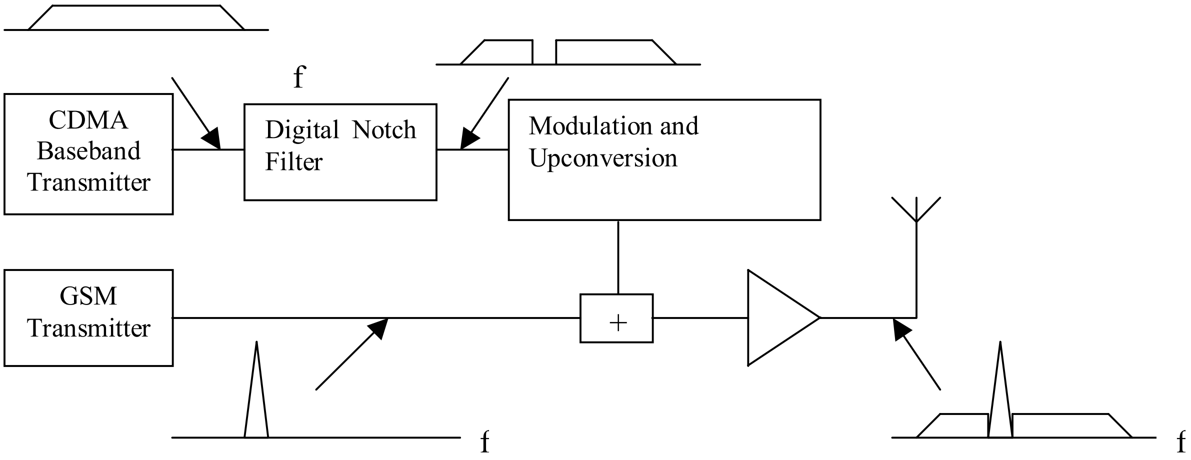

Figure No 20- How notch filters can be used to reduce interference.

It is undemanding to use a notch filter for a particular cell, but the real challenge arises when the user is at the border of three cells and thus three different frequencies have to notch out.
Similarly at the receiver, suppression filters need to be introduced to suppress the interference from GSM signals.

One of the possible options is to introduce a protocol conversion node between the two networks, however such a solution cannot meet the requirements due to inherent technical constraints imposed by the different standards. The other possibility is a network architecture based on dual stack concept [1]. GSM and its present version UMTS (Universal Mobile Telecommunication Systems) are candidates for TDMA whereas cdmaOne and cdma2000 are their counterparts.

GSM Mobile Application Part (MAP) is an intersystem operations protocol that supports mobility management, call delivery, and subscriber profile management for GSM networks; is it upgraded for UMTS MAP and ANSI/TIA/EIA-41 MAP is the counterpart signaling protocol in cdmaOne and cdma2000 networks. So the integrated network should support *protocol conversion function,* which translates messages and parameters between the two dissimilar networks. It should also support *database-mapping function,* which supports mapping between identifiers and translation of profile information. And finally it should also support *transaction* *association function,* used to maintain and reoriginate MAP transactions and responses to the other networks.

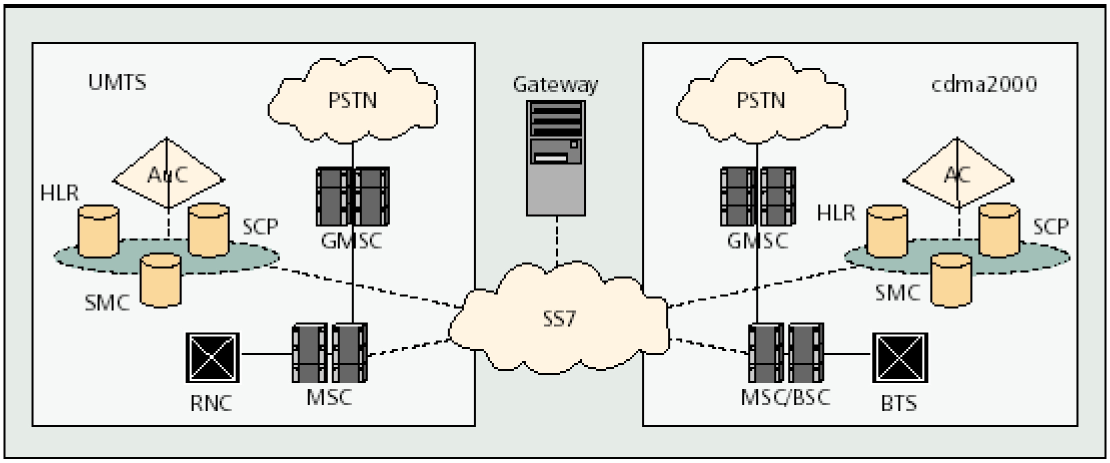

Figure 21- Network configuration based on the gateway solution [1].

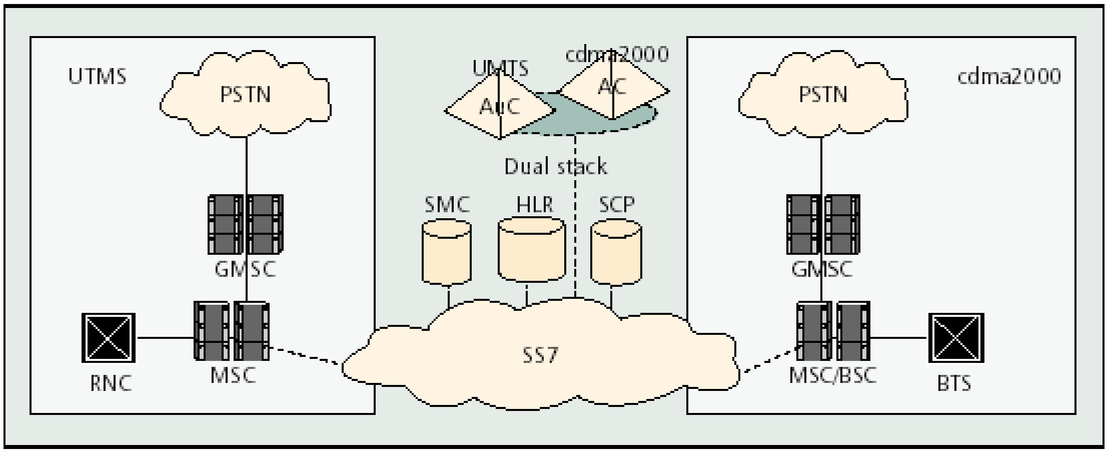

Figure 22- Network architecture based on the dual-stack solution.

The dual stack solution requires the HLR (Home Location Register), SCP (Service Control Point) and SMC (Short Message Center) to be modified and upgraded to support the protocol stacks required by the cdma2000 and UMTS technologies. Authentication centers (AuC and AC) carry out their functions for UMTS and cdma2000 respectively. Individual protocol stacks performs their own mobility management, call delivery, supplementary service management, but the coordination of these functions in between the two networks is done by the dual-stack HLR, SCP and SMC. The transparency can be achieved by using triggering information, which would distinguish whether the function called for (Location Update, Authentication, Call Origination and Termination) is from the UMTS or the cdma2000 network [1].

CHAPTER 6

CONCLUSION AND SCOPE FOR FUTURE STUDY

So it can be concluded from the analysis and detailed theoretical study that the technology for mobile communication is changing, evolving and improving at an enormous rate, and lot of research is being carried out. It was realized that since the GSM channel is just 200 KHz, it could not provide high-speed data transmission beyond GPRS. So for the radio interface, CDMA is selected. But the core networks can still be used from the previous generation. The prime areas for scope of improvement are QoS, capacity enhancement, mobility, data rate, and user friendliness. Considering a particular model of fading and interference pattern, with desired values of SNR and S/I, capacity of a coverage area and QoS can be simulated using MATLAB and OPNET. With the growth of the technology several applications are envisioned and many of some are already into implementations like, games, multimedia, camera and web-cam enabled phones, GPS applications to locate landmarks and finally m-commerce. The vision for the future is to bring all the technology that the user could avail from the computer or from the Internet down to the mobile phone and also enjoy high-speed data transfer like fax, WAP along with the freedom to roam in almost any network.

The study covered many crucial topics right from the basics of multiple accesses, the evolution of cellular technology and the basics of the protocol architecture. The study also encompassed the differences in both technologies, their individual advantages and finally it covered how both CDMA and GSM operate together and where are they both headed in the future towards 3G and beyond. The thorough study of each topic is the part of the future study and will also include other services and technologies like Voice over Internet Protocol (VoIP), 802.11, WLL (Wireless Local Loop), WLAN (Wireless Local Area Network).

REFERENCES

[1] Soojin Kim, HyungJoon Cho, HeeHyuck Hahm, SangYun Lee, and Myung Sung Lee SK telecom Co. “Interoperability between UMTS and cdma2000 Networks”, 3G Mobile Network Technologies and Experiences.

[2] J.A. Pons Puig and J. Dunlop- Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow G1 1XW, Scotland, UK. “Potential of GSM air interface to support CDMA operation”- Wireless Networks Volume 6 2000.

[3] Peter Jung, Friedbert Berens and Jorg Plechinger, University of Kaiserslantern. “Joint Detection for Multicarrier CDMA Mobile Radio Systems”- IEEE 1996. Volume –8.

[4] K. Hamidian and J. Payne, Electrical Engineering CSU. “Combined CDMA with TDMA increases the capacity of a Cellular Communication System”- IEEE 1993. Volume 5.

[5] Karl Kammerlander, SIEMENS Mobile Networks. “Benefits of Combined TDMA/CDMA operation for third generation mobile radio systems”.

[6] Terry Widdowson, BT Laboratories, Ipswich, England. “A CDMA Overlay Of the GSM Network”- Personal, Indoor and Mobile Radio Communications, 1997. 'Waves of the Year 2000'. PIMRC '97. The 8th IEEE International Symposium on, Volume: 1, 1-4 Sept. 1997 vol.1.

[7] Vijay Garg, “IS-95 CDMA and cdma2000”- Prentice Hall, New Jersey, 2000.

[8] Saleh Farque, “Cellular Mobile Systems Engineering”- Artech House, Norwood MA, 1996.

[9] Theodore S. Rappaport, Brian D. Woerner, Jeffery H. Reed, “Wireless Personal Communications”- Kluwer Academic Publishers, Massachusetts, 1996.

[10] Rifaat A. Dayem, “PCS and Digital Cellular Technologies”- Prentice Hall, 1997.

[11] Uyless Black, “X.25 and Related Protocols”- IEEE Computer Society Press, California, 1991.

[12] Samuel C. Yang, “CDMA RF System Engineering”- Artech House Publishers, Massachusetts, 1998.

[13] Gunnar Heine, “GSM Networks: Protocols, Terminology, And Implementation”- Artech House Publishers- Massachusetts, 1998.

[14] GSM Advanced- Agilent Technologies, India, 2000.

[15] Olav berg, Tore Berg, Svein Haavik, Jens Hjelmstad and Reider Skaug, “Spread Spectrum In Mobile Communication”- The Institute of Electrical Engineers, United Kingdom, 1998.

[16] Juha Korhonen, “Introduction to 3G Mobile Communications”- Artech House, Boston, 2001.

[17] Eva Gustafsson and Annika Johnsson, “Always Best Connected”- IEEE Wireless Communications, February 2003.

[18] Martin Haardt and Werner Mohr, “The Complete Solution for Third-Generation Wireless Communications: Two Modes on Air, One Winning Strategy”- IEEE Personal Communications, December 2000.

[19] Per-Goran Andermo and Lars-Magnus Ewerbring, “A CDMA-Based Radio Access Design for UMTS”- IEEE Personal Communications, February 1995.

[20] Sami Uskela, “Key Concepts for Evolution toward beyond 3G Networks”- IEEE Wireless Communications, February 2003.

[21] Juha Rapeli, “Future Directions for Mobile Communications Business, Technology and Research”- Wireless Personal Communications, 2001.

[22] Magda El Zarki, “Digital Multiple Access Techniques” www.seas.upenn.edu, Pennsylvania, spring 1998.

[23] Hughes Software Systems,
http://www.adax.com/whitepapers/gsm_to_3g_white_paper.pdf, Reading, UK.

[24] Wei, Ching, University of Birmingham,
http://webteam.eee.bham.ac.uk/Members/WeiChing/g5c2d.htm, UK.

[25] Michel Daoud Yacoub, “Wireless Technology: Protocols, Standards, and Techniques”, DECOM/FEE/UNICAMP, Brazil, 2001.

[26] University of Manchester, U.K.
http://www.cs.man.ac.uk/Study_subweb/Ugrad/coursenotes/CS6242/Stephen/Slides_SKB_5.pdf,

[27] Vijay Garg, Kenneth Smolik, Joseph E. Wilkes “Applications of CDMA in Wireless/ Personal Communications”, Prentice Hall, October 1996.

[28] Nokia "A History of Third Generation Mobile 3G". www.nokia.com.

[29] www.3GPP.org

[30] www.3GPP2.org

[31] www.GSMWorld.com

[32] www.mobilegprs.com

[33] Stüber, Gordon L, "Principles of mobile communication", Section 4.4, Kluwer Academic Publishers, Boston, 2001.

[34] John Scourias, "Overview of GSM Communications", http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html

[35] www.agilent.com

[36] Nishith D. Tripathi, Nortel, Jeffrey H. Reed and Hugh F Vanlandingham. MPRG, Virginia Tech, "Handoff in Cellular Systems", IEEE Personal Communications, Dec 1998.

BIOGRAPHICAL SKETCH

Arun Ananth Bhatji was born on the 5th of September 1978, in Mumbai, India. After completing his High School from St. Thomas Academy, Mumbai in 1993, he went on to get his Undergraduate degree in Electrical Engineering with distinction from K.K.Wagh College of Engineering in Nashik. He then joined Hutchison Max Telecom Ltd, Mumbai as a Switch/Telecom Engineer for a period of two years. He was involved in many successful projects with the company and was a major team player. He later joined Florida State University in Fall 2001 for his Master of Science program in the Electrical and Computer Engineering Department and graduated in spring of 2004. His area of specialization is in Wireless Communications and Mobile Technology.