Wireless & Mobile Communication (EEC-801)

UNIT-IV

GSM system for mobile: Services and features, System Architecture, Radio Sub system Channel types, Frame Structure. CDMA Digital Cellular Standard (IS 95): Frequency and Channel specifications, Forward CDMA channel and reverse CDMA channel

GSM SYSTEM FOR MOBILE

GSM :

Formerly: Groupe Speciale Mobile (founded 1982)

- now: Global System for Mobile Communication
- Pan-European standard (ETSI, European Telecommunications Standardization Institute)
- simultaneous introduction of essential services in three phases (1991,1994, 1996) by the European telecommunication administrations seamless roaming within Europe possible
- today many providers all over the world use GSM (more than 200 countries in Asia, Africa, Europe, Australia, America)
- more than 1.2 billion subscribers in more than 630 networks
- more than 75% of all digital mobile phones use GSM (74% total)

With global coverage goals in mind, being compatible with GSM from day one is a prerequisite for any new system that would add functionality to GSM. As with other 2G systems, GSM handles voice efficiently, but the support for data and Internet applications is limited. A data connection is established in just the same way as for a regular voice call; the user dials in and a circuit-switched connection continues during the entire session. If the user disconnects and wants to re-connect, the dial-in sequence has to be repeated. This issue, coupled with the limitation that users are billed for the time that they are connected, creates a need for packet data for GSM.

The digital nature of GSM allows the transmission of data (both synchronous and asynchronous) to or from ISDN terminals, although the most basic service support by GSM is telephony.17 Speech, which is inherently analog, has to be digitized. The method employed by ISDN, and by current telephone systems for multiplexing voice lines over high-speed trunks and optical fiber lines, is Pulse Coded Modulation (PCM). From the start, planners of GSM wanted to ensure ISDN compatibility in services offered, although the attainment of the standard ISDN bit rate of 64 Kbit/s was difficult to achieve, thereby belying some of the limitations of a radio link.

Performance characteristics of GSM
(w.r.to. analog sys.):

Communication
- mobile, wireless communication; voice and data services

Total mobility
- international access, chip-card enables use of access points of

Different providers

Worldwide connectivity
- one number, the network handles localization

High capacity
- better frequency efficiency, smaller cells, more customers per cell

High transmission quality
- High audio quality and reliability for wireless, uninterrupted phone

Calls at higher speeds (e.g., from cars, trains)

Security functions
- access control, authentication via chip-card and PIN

Disadvantages of GSM:

There is no perfect system!!

- no end-to-end encryption of user data
- no full ISDN bandwidth of 64 k bit/s to the user, no transparent B channel
- reduced concentration while driving
- electromagnetic radiation
- abuse of private data possible
- roaming profiles accessible
- high complexity of the system
- several incompatibilities within the GSM standards

GSM: Mobile Services(GSM offers)

- Several types of connectionsvoice connections, data connections, short message Service
- Multi-service options (combination of basic services). Three service domains
  - Bearer Services
  - Telemetric Services
  - Supplementary Services

Bearer Services

- Telecommunication services to transfer data between access points
- Specification of services up to the terminal interface (OSI layers 1-3)
- Different data rates for voice and data (original standard)
- data service (circuit switched)
- synchronous: 2.4, 4.8 or 9.6 k bit/s
- asynchronous: 300 - 1200 bit/s
- data service (packet switched)
- synchronous: 2.4, 4.8 or 9.6 k bit/s
- asynchronous: 300 - 9600 bit/s

Tele Services I

- Telecommunication services that enable voice communication via mobile phones
- All these basic services have to obey cellular functions, security measurements etc.

Offered services

- mobile telephony primary goal of GSM was to enable mobile telephony offering thetraditional bandwidth of 3.1 kHz
- Emergency number common number throughout Europe (112); mandatory for all service providers; free of charge; connection with the highest priority (preemption of other connections possible)
- Multinumbering several ISDN phone numbers per user possible

Tele Services II

Additional services

- Non-Voice-Teleservices
- group 3 fax
- voice mailbox (implemented in the fixed network supporting the mobile terminals)
- electronic mail (MHS, Message Handling System, implemented in the fixed network)
- Short Message Service (SMS)

Alphanumeric data transmission to/from the mobile terminal (160 characters) using the signaling channel, thus allowing simultaneous use of basic services and SMS (almost ignored in the beginning now the most successful add-on!)

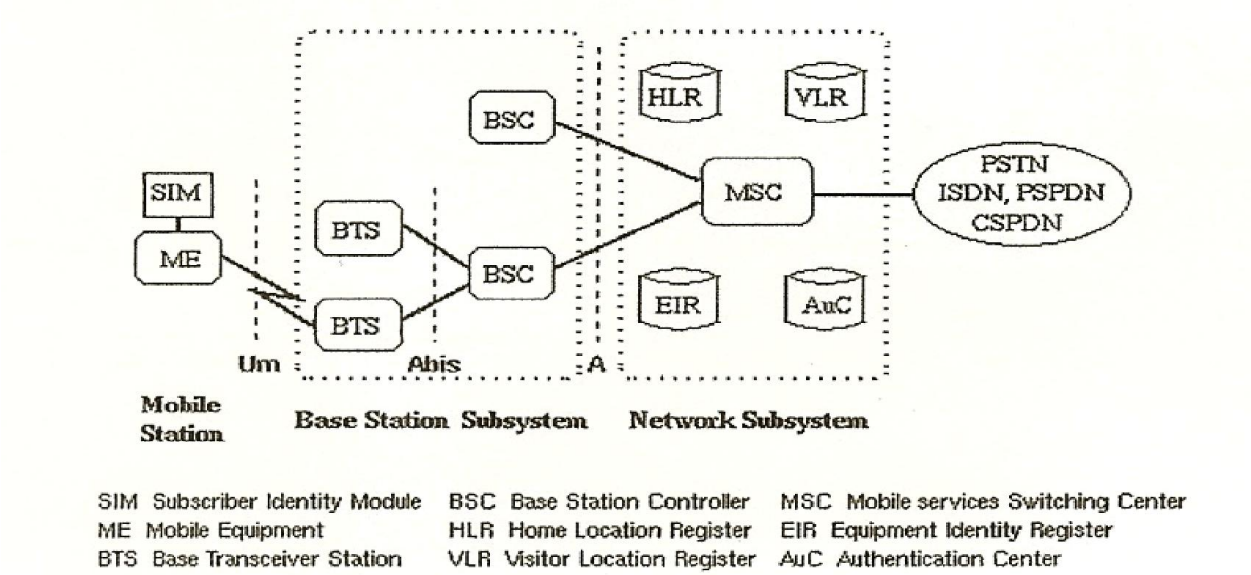
BASIC FEATURES PROVIDED BY GSM

Call Waiting	- Notification of an incoming call while on the handset
Call Hold	-Put a caller on hold to take another call
Call Barring	- All calls, outgoing calls, or incoming calls
Call Forwarding	- Calls can be sent to various numbers defined by the user
Multi Party Call Conferencing	- Link multiple calls together

ADVANCED FEATURES PROVIDED BY GSM

- Calling Line ID: incoming telephone number displayed
- Alternate Line Service: one for personal calls
  One for business calls
- Closed User Group: call by dialing last for numbers
- Advice of Charge: tally of actual costs of phone calls
- Fax & Data: Virtual Office / Professional Office
- Roaming: services and features can follow customer from market to market

SYSTEM ARCHITECTURE:



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

ARCHITECTURE OF THE GSM SYSTEM

GSM is a PLMN (Public Land Mobile Network)several providers setup mobile networks following the GSM standard within each country

- components
  1) MS (mobile station)
  2) BS (base station)
  3) MSC (mobile switching center)
  4) LR (location register)
- Subsystems
  1) RSS (radio subsystem): covers all radio aspects
  2) NSS (network and switching subsystem): call forwarding, handover, switching
  3) OSS (operation subsystem): management of the network

- Mobile Station (MS) :The Mobile Station is made up of two entities:

➢ **Mobile Equipment (ME)** :Mobile Equipment Produced by many different manufacturers Must obtain approval from the standardization body Uniquely identified by an IMEI (International Mobile Equipment Identity)

➢ **Subscriber Identity Module (SIM)** ;

1) Smart card containing the International Mobile Subscriber Identity (IMSI)
2) Allows user to send and receive calls and receive other subscribed services

3) Encoded network identification details
4) Protected by a password or PIN
5) Can be moved from phone to phone – contains key information to activate the phone

- **Base Station Subsystem (BBS)**

Base Station Subsystem is composed of two parts that communicate across the standardized Abis interface allowing operation between components made by different suppliers

➢ **Base Transceiver Station (BTS):**

1) Houses the radio transceivers that define a cell
2) Handles radio-link protocols with the Mobile Station
3) Speech and data transmissions from the MS are recoded
4) Requirements for BTS:
Ruggedness, reliability, portability, minimum costs

➢ **Base Station Controller (BSC) :**

1) Manages Resources for BTS
2) Handles call set up
3) Location update
4) Handover for each MS

- **Network Subsystem**

Mobile Switching Center (MSC)
Home Location Register (HLR)
Visitor Location Register (VLR)
Authentication Center (AUC)
Equipment Identity Register (EIR)

➢ **Mobile Switching Center (MSC)**

1) Switch speech and data connections between:
Base Station Controllers
Mobile Switching Centers
GSM-networks
Other external networks
2) Heart of the network
3) Three main jobs: connects calls from sender to receiver, collects details of the calls made and received, supervises operation of the rest of the network components

- **Home Location Registers (HLR)**

➢ contains administrative information of each subscriber
➢ current location of the mobile

Visitor Location Registers (VLR)

Contains selected administrative information from the HLR

- authenticates the user
- tracks which customers have the phone on and ready to receive a call
- periodically updates the database on which phones are turned on and ready to receive calls

Authentication Center (AUC)

- mainly used for security
- data storage location and functional part of the network
- Ki is the primary element

Equipment Identity Register (EIR)

- Database that is used to track handsets using the IMEI (International Mobile Equipment Identity)
- Made up of three sub-classes: The White List, The Black List and the Gray List
- Optional database

GSM criteria –

- Good subjective speech quality
- Low terminal and service cost
- Support for international roaming – one system for all of Europe
- Ability to support handheld terminals
- Support for range of new services and facilities
- Enhanced Features
- ISDN compatibility
- Enhance privacy
- Security against fraud

RADIO SUBSYSTEM

The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers

Components

- Base Station Subsystem (BSS):

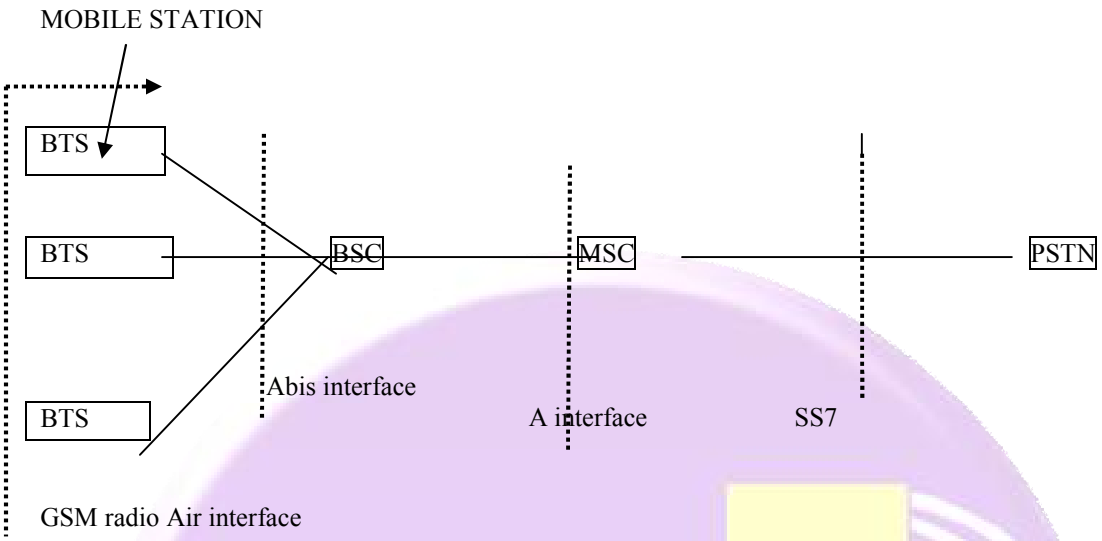
- Base Transceiver Station (BTS): radio component including sender, receiver, antenna - if directed antennas are used one BTS can cover several cells
- Base Station Controller (BSC): switching between BTSs, controlling BTSs, managing of network resources, mapping of radio channels (Um) onto terrestrial channels (A interface)
- BSS = BSC + sum(BTS) + interconnection

- Mobile Stations (MS)

GSM: CELLULAR NETWORK

- use of several carrier frequencies
- not the same frequency in adjoining cells
- cell sizes vary from some 100 m up to 35 km depending on user density, geography, Transceiver power etc.
- hexagonal shape of cells is idealized (cells overlap, shapes depend on geography)
- if a mobile user changes cellshandover of the connection to the neighbor cell

GSM Interfaces:-



GSM RADIO SPECTRUM

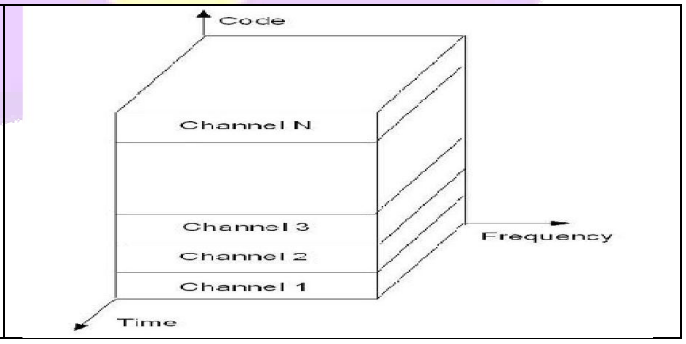
The ITU, which manages the international allocation of radio spectrum, allocated the 890-915 MHz bands for the uplink (mobile station to base station) and 935-960 MHz bands for the downlink (base station to mobile station) for mobile networks in Europe. "…Since this range was already being used in the early 1980s by the analog systems of the day, the CEPT had the foresight to reserve the top 10 MHz of each band for the GSM network that was still being developed." It should be noted that the World Radio-Communications Conference (WRC) in 1992 identified frequency bands for FPLMTS (Future Public Land Mobile Telecommunications Systems), which is in fact the original name of IMT-2000 (UMTS). The existing second-generation bands for second-generation GSM services consist of spectrum between 862 and 960 MHz and the totality of the GSM1800 band 1710 - 1880 MHz

CODE DIVISION MULTIPLE ACCESS (CDMA)

In CDMA, the same bandwidth is occupied by all the users, however they are all assigned separate codes, which differentiates them from each other (shown in Fig.) . CDMA utilize a spread spectrum technique in which a spreading signal (which is uncorrelated to the signal and has a large bandwidth) is used to spread the narrow band message signal.

Direct Sequence Spread Spectrum (DS-SS)

This is the most commonly used technology for CDMA. In DS-SS, the message signal is multiplied by a Pseudo Random Noise Code. Each user is given his own codeword which is orthogonal to the codes of other users and in order to detect the user, the receiver must know the codeword used by the transmitter.



CDMA/FDD IN IS-95:

In this standard, the frequency range is: 869-894 MHz (for Rx) and 824-849 MHz (for Tx). In such a system, there are a total of 20 channels and 798 users per channel. For each channel, the bit rate is 1.2288 Mbps. For orthogonality, it usually combines 64 Walsh codes and a m-sequence.

CDMA and Self-interference Problem

In CDMA, self-interference arises from the presence of delayed replicas of signal due to multipath. The delays cause the spreading sequences of the different users to lose their orthogonality, as by design they are orthogonal only at zero phase offset. Hence in despreading a given user's waveform, nonzero contributions to that user'ssignal arise from the transmissions of the other users in the network. This is distinct from both TDMA and FDMA, wherein for reasonable time or frequency guardbands, respectively, orthogonality of the received signals can be preserved.

CDMA and Near-Far Problem

The near-far problem is a serious one in CDMA. This problem arises from the fact that signals closer to the receiver of interest are received with smaller attenuation than are signals located further away. Therefore the strong signal from the nearby transmitter will mask the weak signal from the remote transmitter. In TDMA and FDMA, this is not a problem since mutual interference can be filtered. In CDMA, however, the near-far effect combined with imperfect orthogonality between codes (e.g. due to different time sifts), leads to substantial interference. Accurate and fast power control appears essential to ensure reliable operation of multiuser DS-CDMA systems.

THIRD GENERATION

As noted above, a key definition of 3G systems is that a packet-switched data rate of at least 144 kbps is provided. 3G systems must support both voice and data (some 2G systems did not support data). To promote international interoperability of mobile phone equipment, the International Telecommunication Union (ITU) oversees the development of 3G standards. This effort is known as International Mobile Telecommunications-2000 (IMT-2000). Under IMT-2000, there are five defined air interface standards. Two of these operate in Canada.

The first is the Universal Mobile Telecommunications System (UMTS). UMTS uses Wideband Code Division Multiple Access (W-CDMA) as the air interface. W-CDMA uses the CDMA technique, but is not technologically related to, or compatible with, cdmaOne or CDMA2000. The development of UMTS standards is coordinated by a group of manufacturers, network operators, and standards organizations known as the Third Generation Partnership Project (3GPP). UMTS is a successor to GSM and aims to re-use as much of the GSM infrastructure as possible to minimize transition costs. As such, UMTS is prevalent in Europe and parts of Asia. The first UMTS network was launched in 2003. Rogers Wireless had plans to launch UMTS in Canada in the third quarter of 2006, but has since decided to focus on a 4G technology called High-Speed Downlink Packet Access (HSDPA).

The second 3G technology in Canada is 1xEvoluation-Data (1x EVDO), also known as CDMA2000 1xEV-DO or Interim Standard 856 (IS-856). As the name suggests, 1xEV-DO is part of the CDMA2000 family of standards, and is a successor to cdmaOne/IS-95. A group called the Third Generation Partnership Project Two (3GPP2) oversees development of this standard. 3GPP2 is, like 3GPP, a group of manufacturers, operators, and standards bodies. 1xEV-DO is most common in Asia-Pacific and North America, but is also found in other regions. There are over 30 million 1xEV-DO subscribers around the world.

Another 3G standard within the scope of this study is CDMA2000 1xEvolution Data and Voice (1XEV-DV). 1xEV-DV increases the capacity of data and voice channels as compared to CDMA2000 1x, whereas 1xEV-DO only provides improvements to the data channel. However, the standards for 1xEV-DV were developed several years after the 1xEV-DO standards and after many operators had implemented 1xEV-DO networks. Few manufacturers or network operators showed significant interest in 1xEV-DV, so Qualcomm, which was leading the development of the 1xEV-DV standard, terminated the development work and focused on 1xEV-DO. This report will not discuss 1xEV-DV any further.

Beyond Third Generation

Network operators and manufacturers are already planning for the fourth generation of mobile technology, referred to as 4G. 4G networks are unlikely to launch much before 2010. However, some advances in 3G systems have already been defined and are referred to as 3.5G. One such advance is High-Speed Downlink Packet Access (HSDPA). HSDPA is an

extension to UMTS in much the same way that 1xEV-DO was an extension to CDMA2000 1x. HSDPA introduces a new, high-speed downlink channel (from the base station to the mobile station).

Mobile Generation Summary

To summarize, there are two main mobile telephony "families": GSM-based and CDMA-based. Table summarizes the evolution of both families.

Table : Summary of Mobile Generations and Technologies

Standard (Interface)	GSM Family	CDMA Family
2G	GSM (TDMA)	cdma One (CDMA)
2.5G	GPRS (TDMA)	None
2.75G	EDGE (TDMA)	CDMA2000 1x (CDMA)
3G	UMTS (W-CDMA)	CDMA2000 1xEV-DO (CDMA)
3.5G	HSDPA (W-CDMA)	None defined yet
Development	3GPP	3GPP2
Standards Publisher	ETSI	TIA
Canadian Operators	Rogers Wireless	Bell Mobility, TELUS

CONTROL AND HANDLING:

Most wireless services operate in a Frequency Division Duplex (FDD) mode, whereby the Forward Channel (Base Station to Mobile Station "down-link") is typically offset at a higher radio frequency to the Reverse Channel (Mobile Station to Base Station "up-link"). Tableprovides an overview of the PCS and Cellular Air Interfaces used in Canada.

Table - PCS and Cellular Air Interfaces in Canada

Interface	Frequency Band	Standard/ Protocol	Security	Services Supported
Advanced Mobile Phone System (AMPS)	800-900 MHz	EIA-553 IS-54	Electronic Serial Number (ESN)	Voice
Code Division Multiple Access (CDMA)	800 MHz (Digital Cellular) 1.9 GHz (PCS)	IS-95	CAVE CMEA ECMEA VPM	Voice SMS Wireless Modem WAP
Time Division Multiple Access (TDMA)	800 MHz (Digital Cellular) 1.9 GHz (PCS)	IS-54 IS-136	CAVE CMEA ECMEA VPM ORYX	SMS Wireless Modem Two-way Messaging
Global System for Mobile Communications (GSM)	1.9 GHz (SCP)	GSM Standard	IMSI Authentication Algorithm A8CipherKeyGeneration Algorithm A5Encryption Algorithm	Voice SMS Wireless Modem WAP
Integrated Digital Enhanced Network (iDEN)	800 MHz Enhanced Specialized Mobile Radio (ESMR)	Motorola Proprietary Standard	None	SMS WAP Wireless
Mobitex	900 MHz Wireless Wide Area Network (WAN)	Mobitex Proprietary Standard	None	Wireless Modem Two-way Messaging
DataTAC	900 MHz Wireless Wide Area Network (WAN)	Data TAC Proprietary Standard	None	Wireless Modem Two-way Messaging

OVERVIEW

The IS-95 CDMA air interface employs direct-sequence, spread-spectrum modulation techniques, which spread the information contained in a particular signal of interest over a much greater bandwidth than the original signal.

IS-95 is a second generation, digital wireless standard that may be implemented in the digital cellular (800 MHz) or PCS (1.9 GHz) frequency range.

Major Canadian wireless service providers that employ CDMA (IS-95) include: • Bell Mobility • Telus	CDMA (IS-95) can support voice and the following wireless data services: • Short Message Service (SMS) • Wireless modem service (IS-95b packet data) • Wireless Application Protocol (WAP) service

CDMA Security:

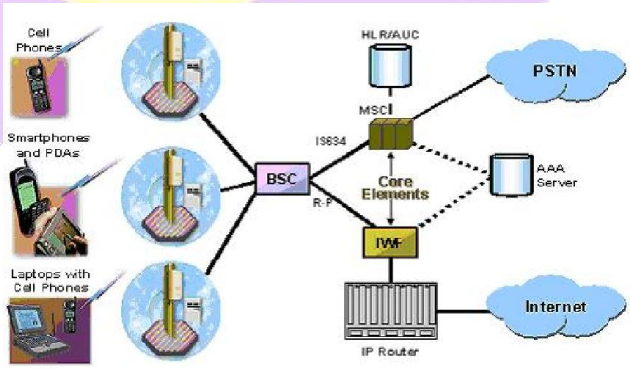
The IS-95 standard Mobile Station-Base Station Compatibility Standard for Wideband Spread Spectrum Cellular Systems does offer a voice privacy option that attempts to secure voice communications. Annex A - Interface Specification for Common Cryptographic Algorithms of this standard specifies the algorithms that can be used for authentication and confidentiality.

Although the CDMA standard does specify all the above algorithms, many service providers have chosen **not** to implement these algorithms into their system(s). Service providers are more interested in avoiding fraud than securing the voice aspect of the communications, and rely on the inherent complexity of the system (spread spectrum) for security. However, spread spectrum is designed to ensure that devices can communicate in noisy environments and is not intended to be a security mechanism. In addition, none of the algorithms discussed above are approved for use in the GC for protecting designated or classified information.

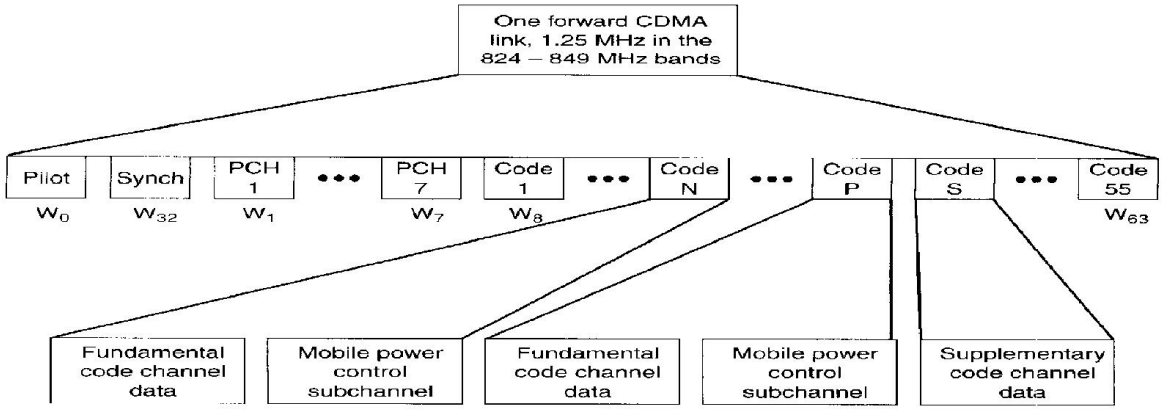
CDMA2000 1x

Overview: *CDMA2000 1x is the core air interface in the CDMA2000 family, and is an evolutionary upgrade to cdmaOne (also known as IS-95). As such, CDMA2000 1x is backward compatible with cdmaOne. CDMA2000 1x operates in a pair of 1.25 MHz radio channels. CDMA2000-based systems are defined to operate in frequency bands at 400 MHz, 800 MHz, 900 MHz, 1700 MHz, 1800 MHz, 1900 MHz, and 2100 MHz.*

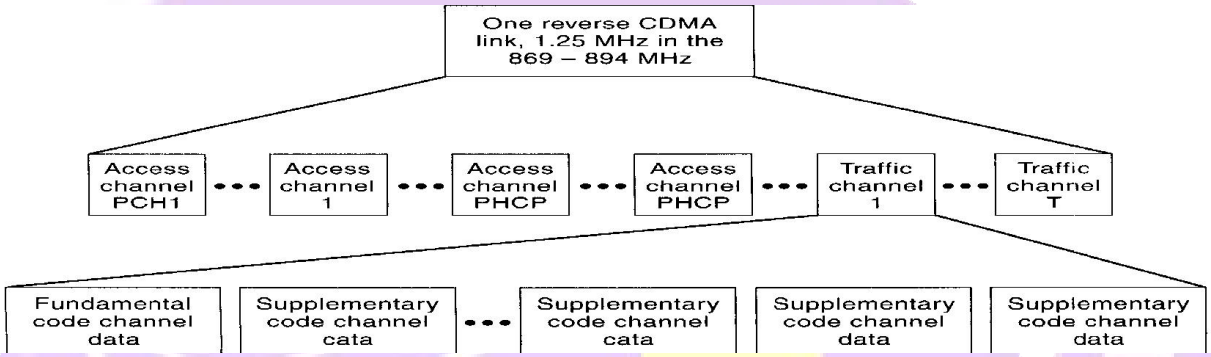
CDMA2000 1x nearly doubles the voice capacity of cdma one networks. In most deployments, a peak data rate of 144 kbps is provided.

Figure shows a generic CDMA2000 network architecture. In the figure, the BSC is a Base Station Controller, and the MSC is a Mobile Switching Centre. The IWF is an Interworking Function gateway, which is a gateway for data traffic between a wireless network and a wired network. The AAA Server handles authentication, authorization, and accounting. The PSTN is the Public Switched Telephone Network. IS-634 is the interface standard for communications between the BSC and the MSC. The R-P interface is the radio-PDSN interface; PDSN is Packet Data Serving Node.	

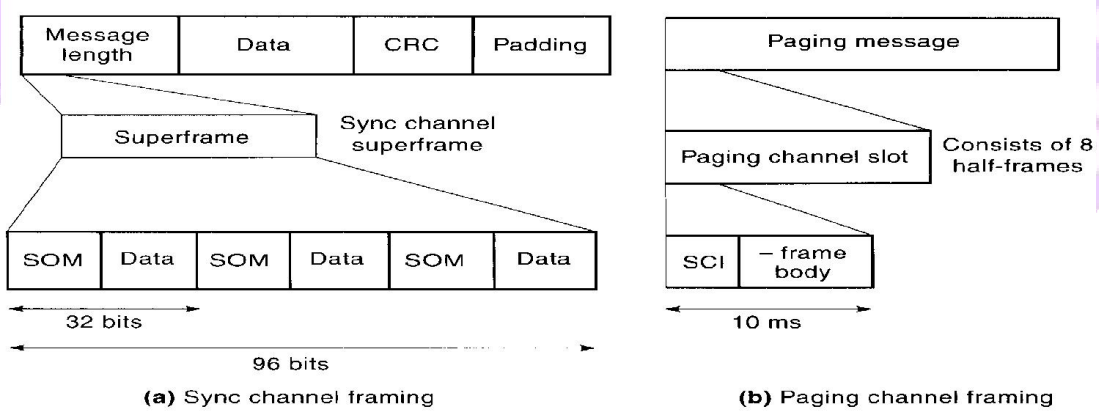
The IS -95 CDMA Forward Channel



The IS -95 CDMA Reverse Channel



Framing in IS-95



(a) Sync channel framing

(b) Paging channel framing