WIRELESS NETWORKS

by

Ananth Ravindran

Assistant Professor

UNIT I

MULTIPLE RADIO ACCESS

- Medium Access Alternatives*:*
  - Fixed-Assignment for Voice Oriented Networks
  - Random Access for Data Oriented Networks ,
- Handoff and Roaming Support,
- Security and Privacy

Wireless Medium Access

Alternatives

Wireless Medium Access

1. **Fixed-Assignment Access for Voice-Oriented Networks**
   a. Frequency Division Multiple Access (FDMA)
   b. Time Division Multiple Access (TDMA)
   c. Code-Division Multiple Access (CDMA)
2. **Random Access for Data-Oriented Networks**
   a. ALOHA-Based Wireless Random Access Techniques
   b. CSMA-Based Wireless Random Access Techniques

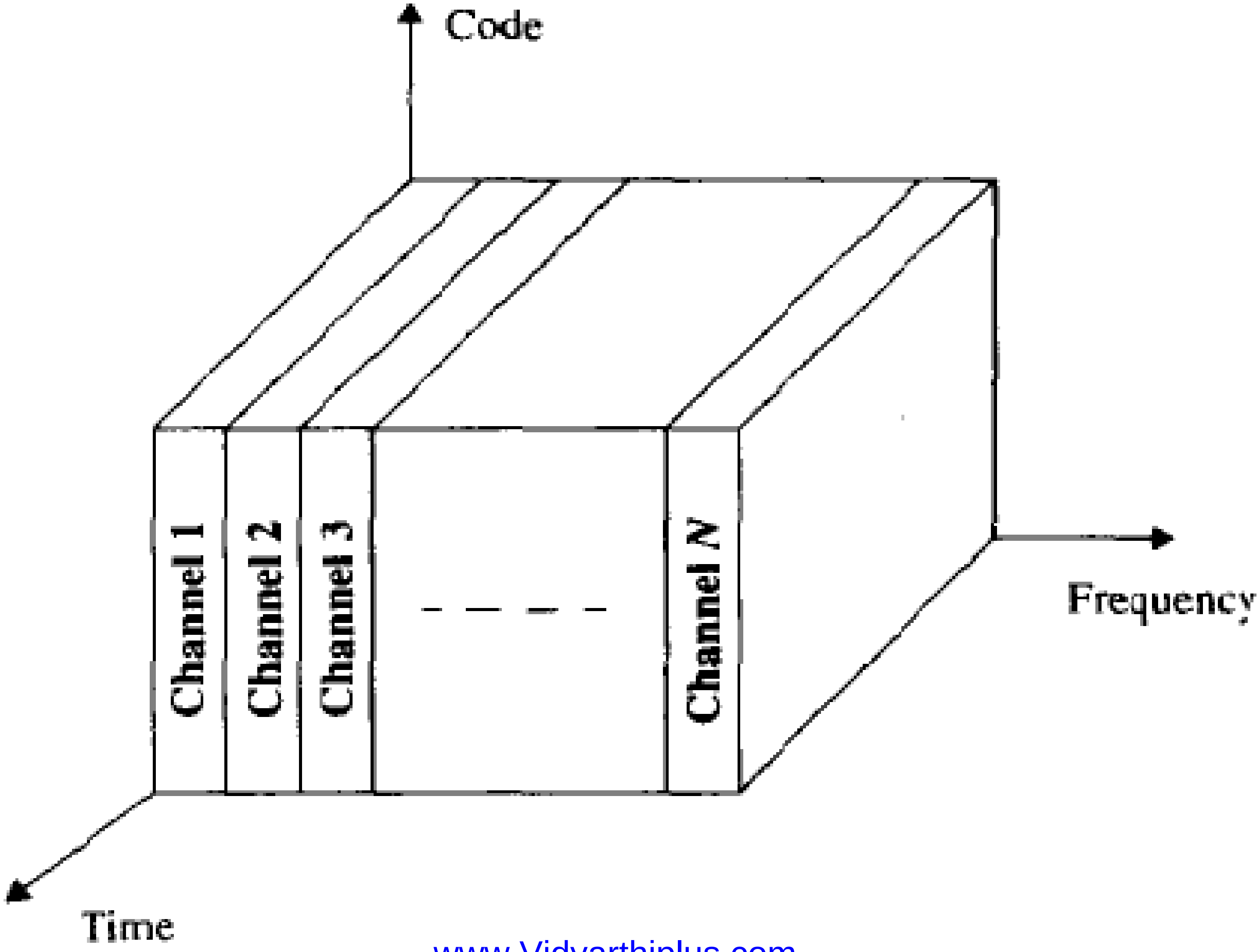
Fixed-Assignment Multiple Access Techniques

- The available spectrum bandwidth for our wireless communication is limited.
- Multiple access techniques enable multiple signals to occupy a single communications channel.

Major Types

- Frequency division multiple access (FDMA)
- Time division multiple access (TDMA)
- Code division multiple access (CDMA)

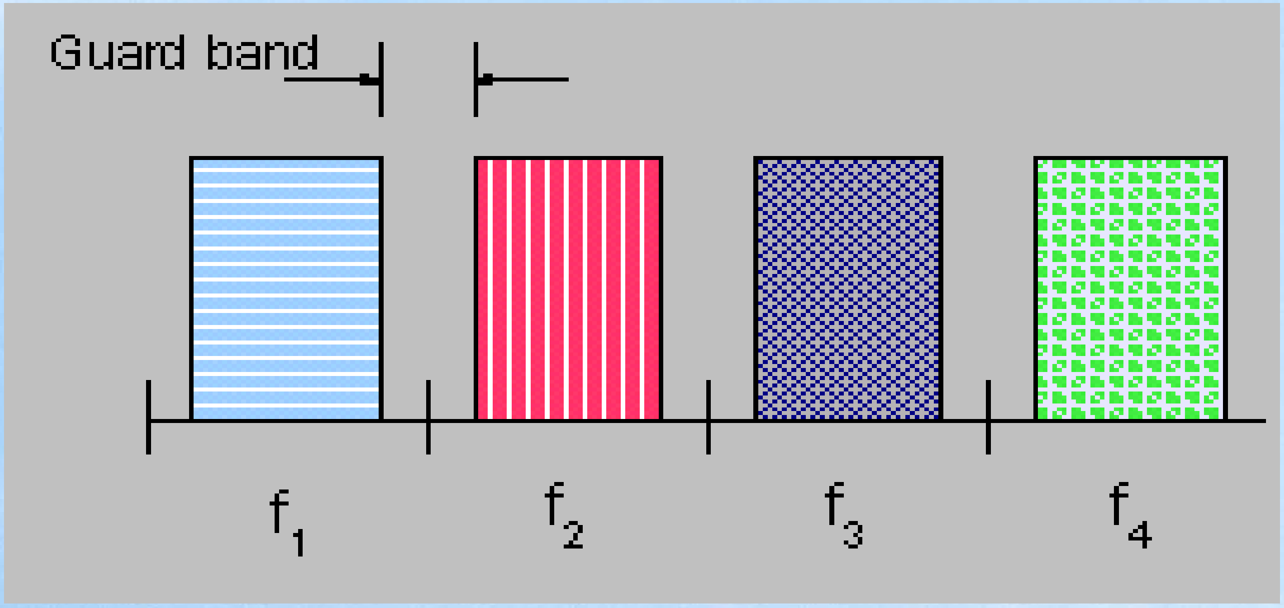
Frequency Division Multiple Access



Frequency Division Multiple Access

- It assigns individual frequency to individual users. (i.e) accommodates one user at a time.
- Each user is separated by Guard Bands.
- The complexity of FDMA mobile systems is lower when compared to TDMA systems

- A guardband is a narrow frequency band between adjacent frequency channels to avoid interference from the adjacent channels



- **The number of channels that can be simultaneously supported in a FDMA system is given by**

$$N = \frac{B_t - 2B_{guard}}{B_c}$$

- B_T **-> total spectrum allocation,**
- B_{GUARD} **-> the guard band**
- B_C **-> the channel bandwidth**

Key Features

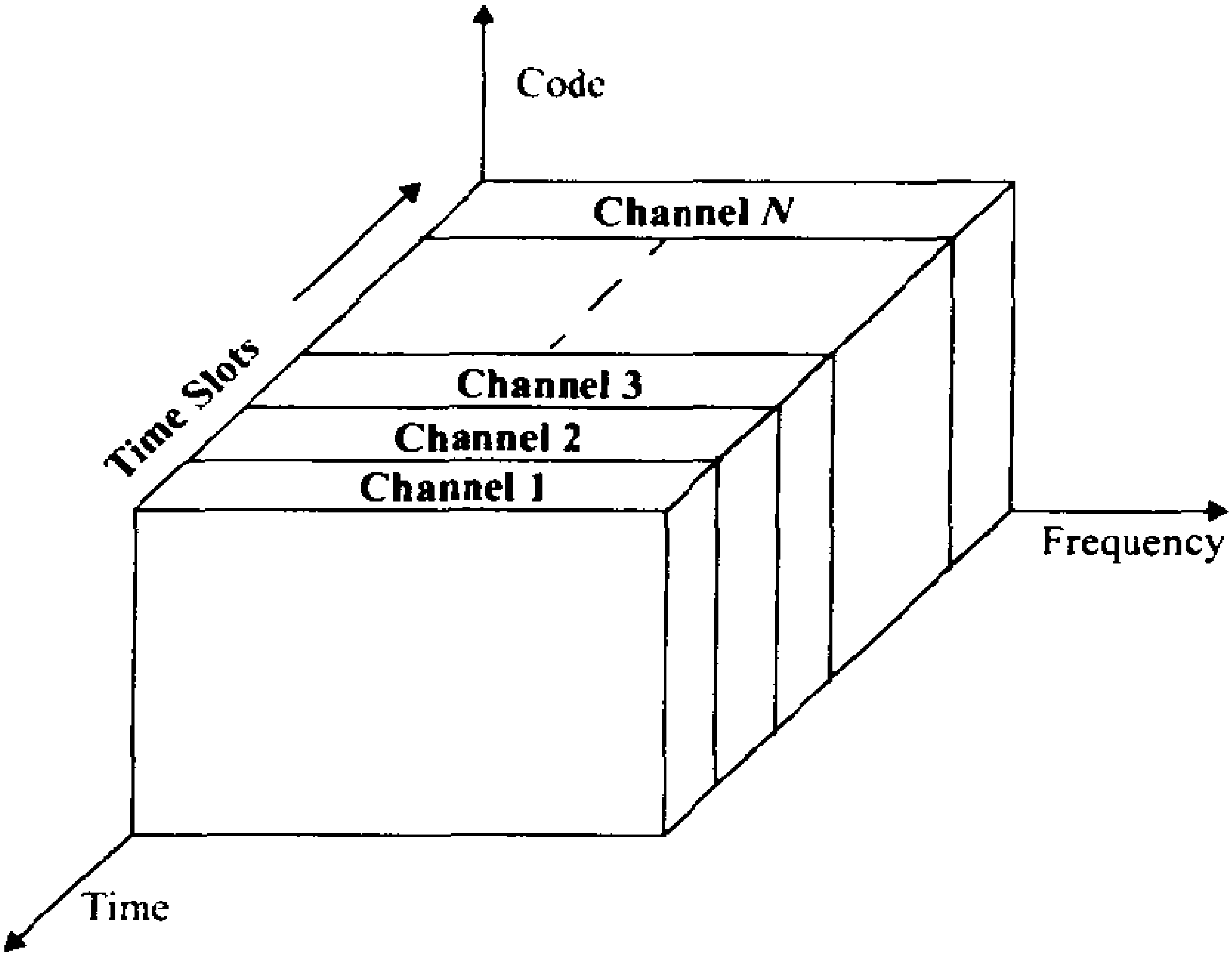
- If an FDMA channel is not in use, then it sits idle and cannot be used by other users
- The bandwidths of FDMA channels are narrow (30 kHz)
- Intersymbol interference is low
- It needs only a few synchronization bits

De Merits

- FDMA systems are costlier because of the single channel per carrier design,
- It need to use costly bandpass filters to eliminate spurious radiation at the base station.
- The FDMA mobile unit uses duplexers since both the transmitter and receiver operate at the same time. This results in an increase in the cost of FDMA subscriber units and base stations.
- FDMA requires tight RF filtering to minimize adjacent channel interference.

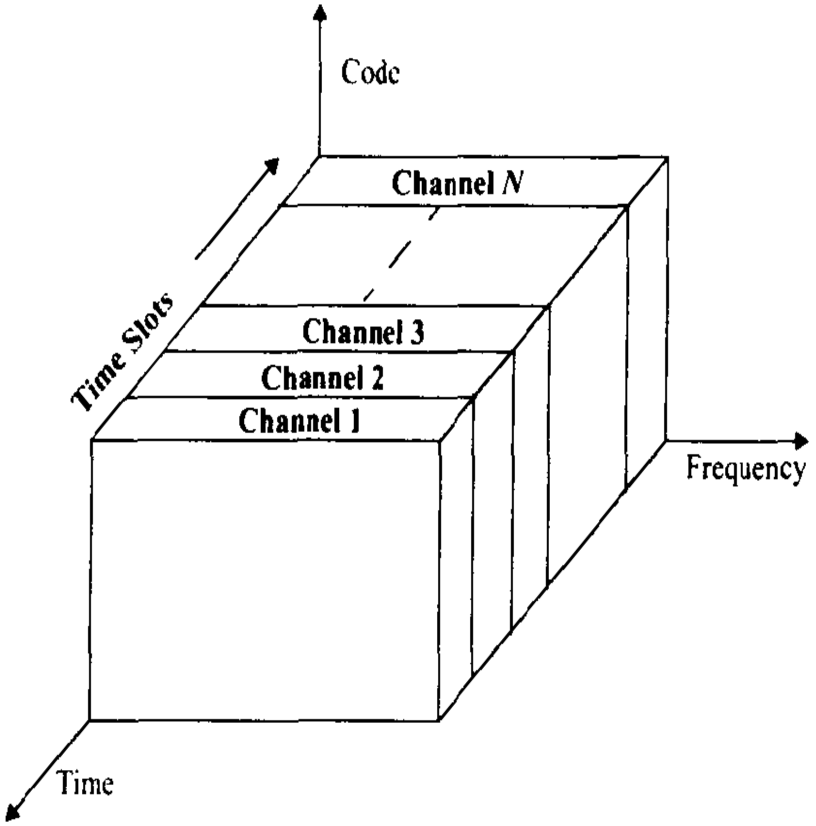
Time Division Multiple Access

Time division multiple access

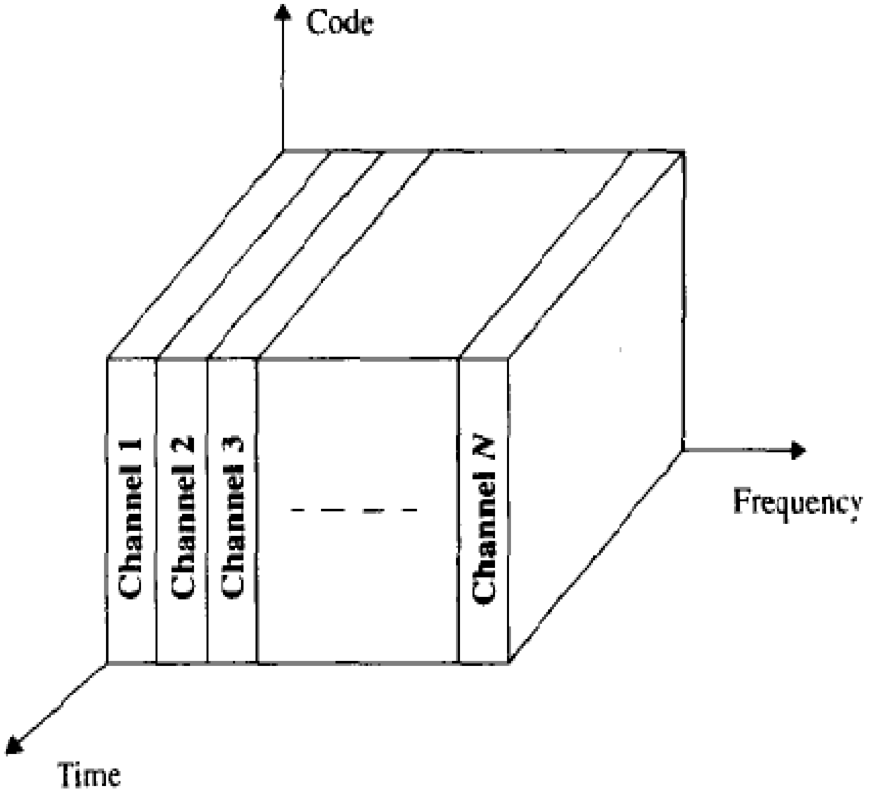


TDMA vs FDMA

TDMA



FDMA

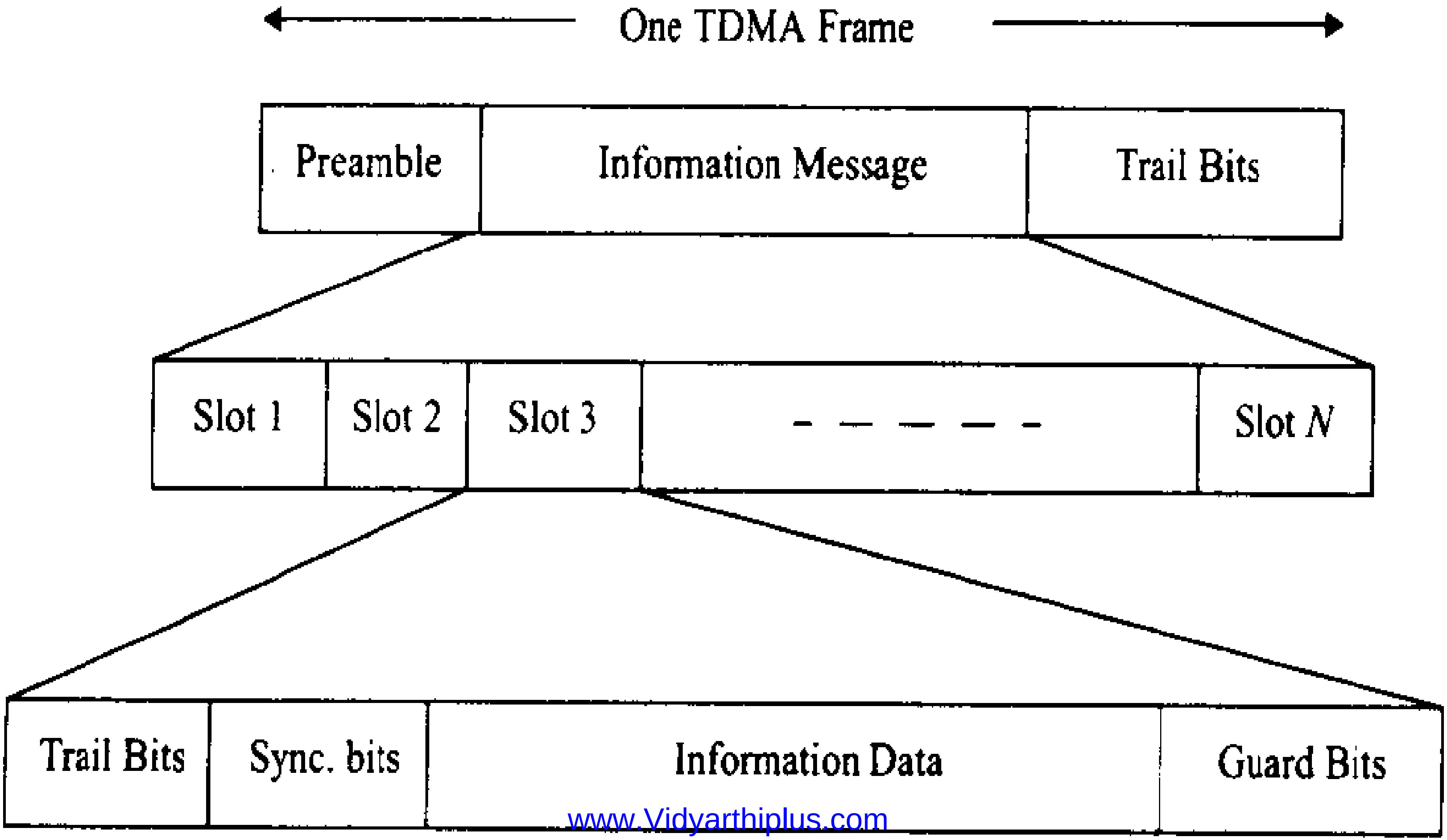


- Time division multiple access (TDMA) systems divide the radio spectrum into time slots
- Each user occupies a cyclically repeating time slot
- A set of ‘N’ slots form a Frame.
- Each frame is made up of a preamble, an information message, and tail bits
- TDMA systems transmit data in a buffer-and-burst method

- TDMA shares a single carrier frequency with several users, where each user makes use of non-overlapping time slots
- TDMA uses different time slots for transmission and reception
- Adaptive equalization is usually necessary in TDMA systems, since the transmission rates are generally very high as compared to FDMA channels

- High synchronization overhead is required in TDMA systems because of burst transmissions
- Guard Bands are necessary to ensure that users at the edge of the band do not "bleed over" into an adjacent radio service.

Frame Structure



- The preamble contains the address and synchronization information that both the base station and the subscribers use to identify each other.
- Trial bits specify the start of a data.
- Synchronization bits will intimate the receiver about the data transfer.
- Guard Bits are used for data isolation.

Efficiency of TDMA

- The efficiency of a TDMA system is a measure of the percentage of transmitted data that contains information as opposed to providing overhead for the access scheme

$$b_{OH} = N_r b_r + N_t b_p + N_t b_g + N_r b_g$$

where

b_{0H} – no over head bits per frame

b_r - no of overhead bits per

b_p - no overhead bits per preamble in each slot

b_g - no equivalent bits in each guard time interval

N_r - reference bursts per frame,

N_t- traffic bursts per frame

- The total number of bits per frame, b_T, is

$$b_T = T_f R$$

- T_f is the frame duration, and R is the channel bit rate
- Then the frame efficiency is

$$\eta_f = \left(1 - \frac{b_{OH}}{b_T}\right) \times 100\%$$

- And the no of frames

$$N = \frac{m\,(B_{tot} - 2B_{guard})}{B_c}$$

m - maximum number of TDMA users supported on each radio channel

Spread spectrum multiple access (SSMA)

- *Frequency Hopped Multiple Access* (FHMA)
- *Direct Sequence Multiple Access* (DSMA)

Direct sequence multiple access is also called code division multiple access (CDMA).

Frequency Hopped Multiple Access

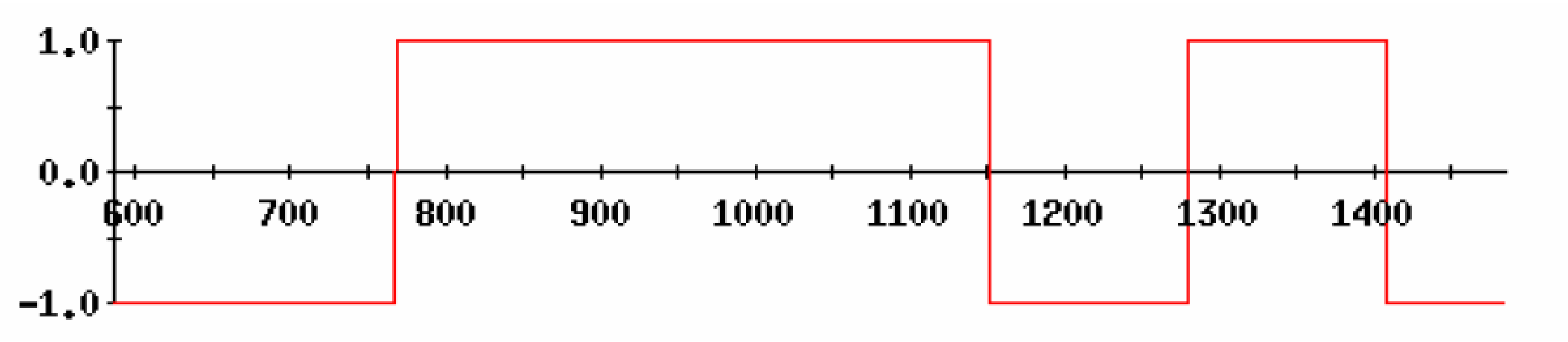
- The carrier frequencies of the individual users are varied in a pseudorandom fashion within a wideband channel
- The digital data is broken into uniform sized bursts which are transmitted on different carrier frequencies

- Fast Frequency Hopping System -> the rate of change of the carrier frequency is greater than the symbol rate
- Slow Frequency Hopping -> the channel changes at a rate less than or equal to the symbol rate

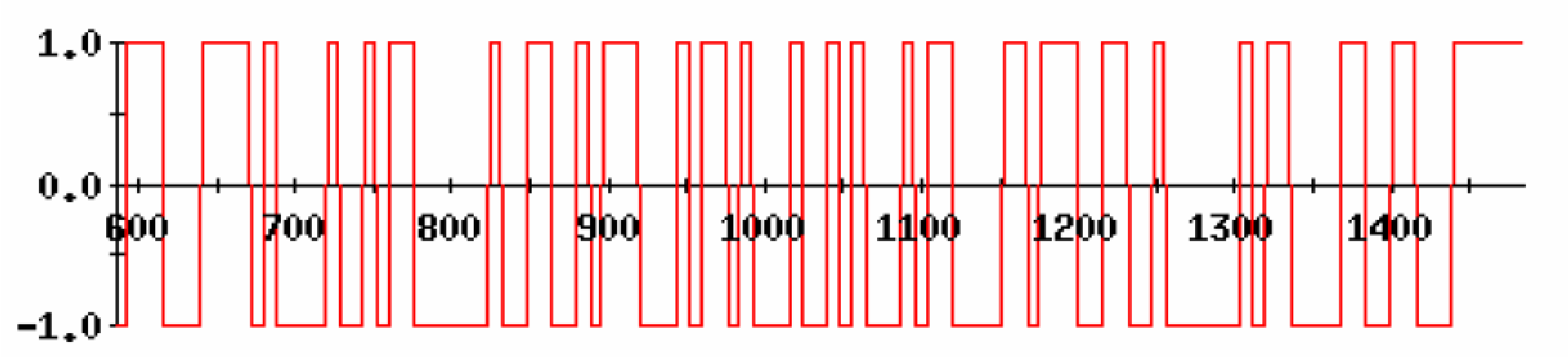
Code Division Multiple Access (CDMA)

- The narrowband message signal is multiplied by a very large bandwidth signal called the spreading signal (pseudo-noise code)
- The chip rate of the pseudo-noise code is much more than message signal.
- Each user has its own pseudorandom codeword.

Message



PN sequence



- CDMA uses CO-Channel Cells
- All the users use the same carrier frequency and may transmit simultaneously without any knowledge of others.
- The receiver performs a time correlation operation to detect only the specific desired codeword.
- All other code words appear as noise

- Multipath fading may be substantially reduced because the signal is spread over a large spectrum
- Channel data rates are very high in CDMA systems
- CDMA supports Soft handoff MSC can simultaneously monitor a particular user from two or more base stations. The MSC may chose the best version of the signal at any time without switching frequencies.

- In CDMA, the power of multiple users at a receiver determines the noise floor.
- In CDMA, stronger received signal levels raise the noise floor at the base station demodulators for the weaker signals, thereby decreasing the probability that weaker signals will be received. This is called Near- Far problem.
- To combat the Near- Far problem, power control is used in most CDMA

Random Access for Data-Oriented Networks

Random Access for Data-Oriented Networks

- In all wireless networks all voice-oriented operations use fixed-assignment channel access and data related traffic is carried out using Random Access Techniques.
- When the information to be transmitted is bursty in nature, fixed-assignment channel access methods result in wasting communication resources
- Random-access protocols provide flexible and efficient methods for managing a channel access to transmit short messages.
- It provides each user station with varying degrees of freedom in gaining access to the network whenever information is to be sent.

1. ALOHA - Based Wireless Random Access Techniques
2. Carrier Sense Multiple Access (CSMA) - Based Wireless Random Access Techniques

ALOHA-Based Wireless Random Access Techniques

1. Pure ALOHA
2. Slotted ALOHA
   a. Reservation ALOHA (R- ALOHA)
   b. Packet Reservation Multiple Access (PRMA)

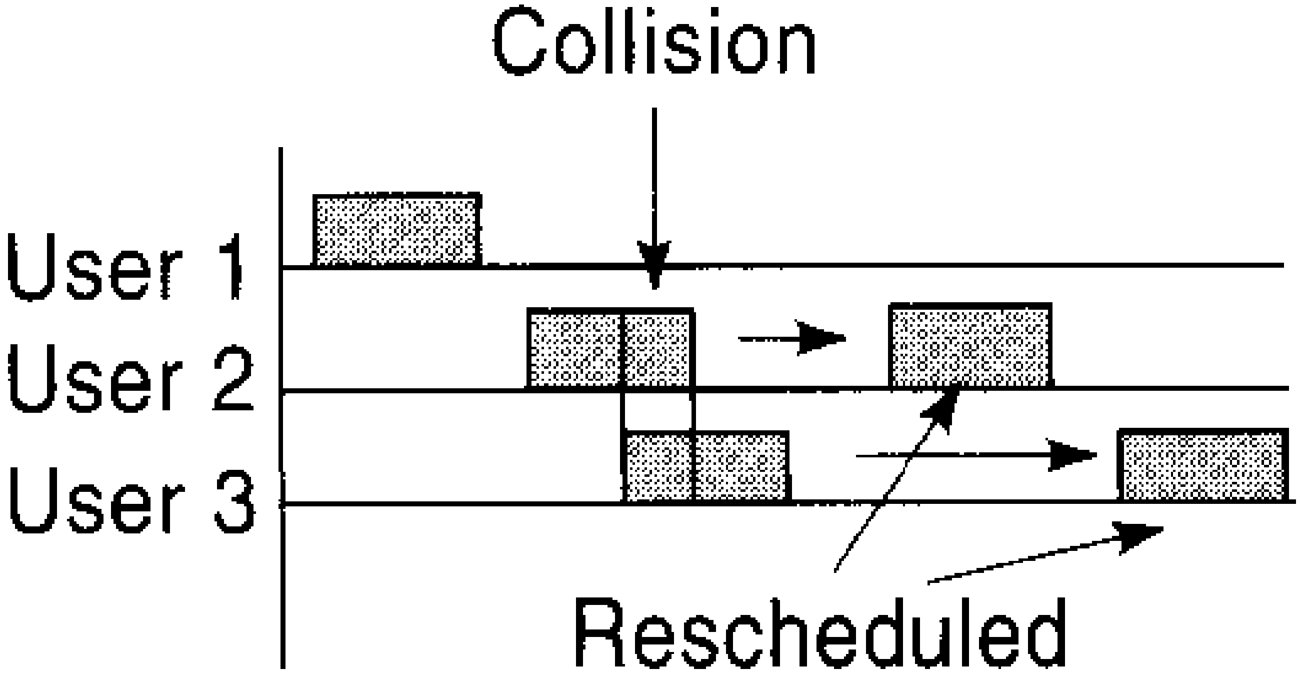
Pure ALOHA

- The original ALOHA protocol is also called pure ALOHA.
- ALOHA Protocol is developed by University of Hawaii. The word ALOHA means "hello" in Hawaiian.
- The initial system used ground-based UHF radios to connect computers on several of the island campuses with the university's main computer center on Oahu, by use of a random access protocol which has since been known as the ALOHA protocol

Basic Concept

- A mobile terminal transmits an information packet when the packet arrives from the upper layers of the protocol stack.
- A user accesses a channel as soon as a message is ready to be transmitted.
- Each packet is encoded with an error-detection code.
- After a transmission, the user waits for an acknowledgment on either the same channel or a separate feedback channel.
- The BS checks the parity of the received packet. If the parity checks properly, the BS sends a short acknowledgment packet to the MS.

Pure ALOHA



Collision

- The message packets are transmitted at arbitrary times, so there is a possibility of collisions between packets.
- After sending a packet the user waits a length of time more than the round-trip delay for an acknowledgment from the receiver.
- If no acknowledgment is received, the packet is assumed lost in a collision, and it is transmitted again with a randomly selected delay to avoid repeated collisions.
- As the number of users increase, a greater delay occurs because the probability of collision increases

Merits :

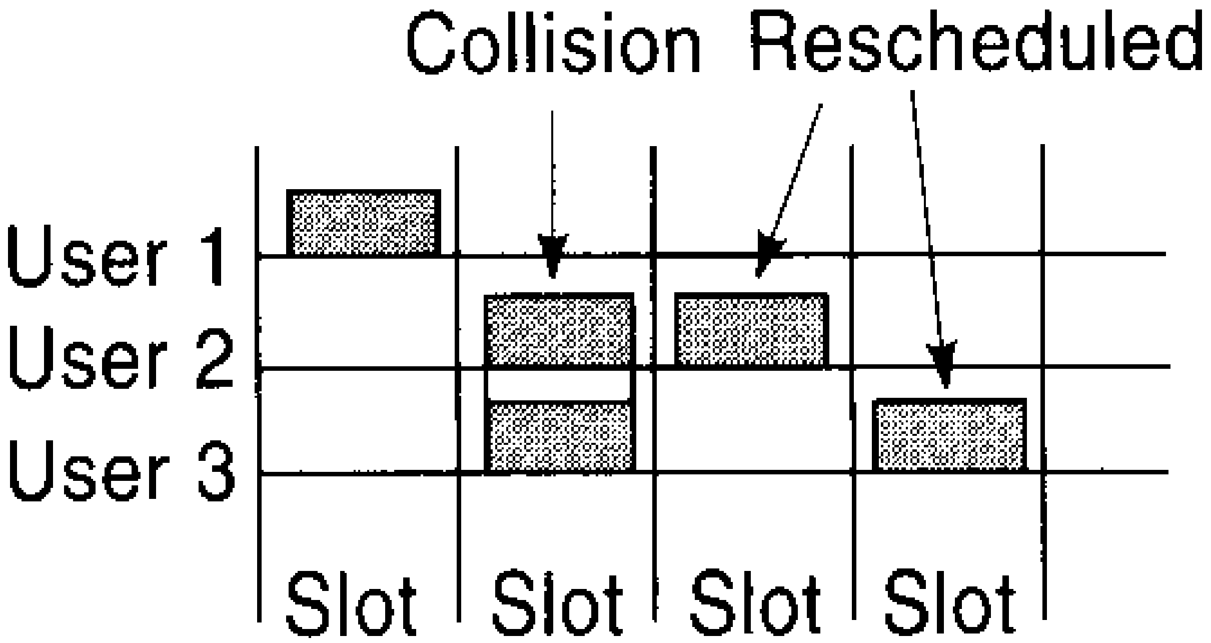
- The advantage of ALOHA protocol is that it is very simple, and it does not impose any synchronization between mobile terminals

De-Merits:

- Its has low throughput under heavy load conditions.
- The maximum throughput of the pure ALOHA is **18 percent.**

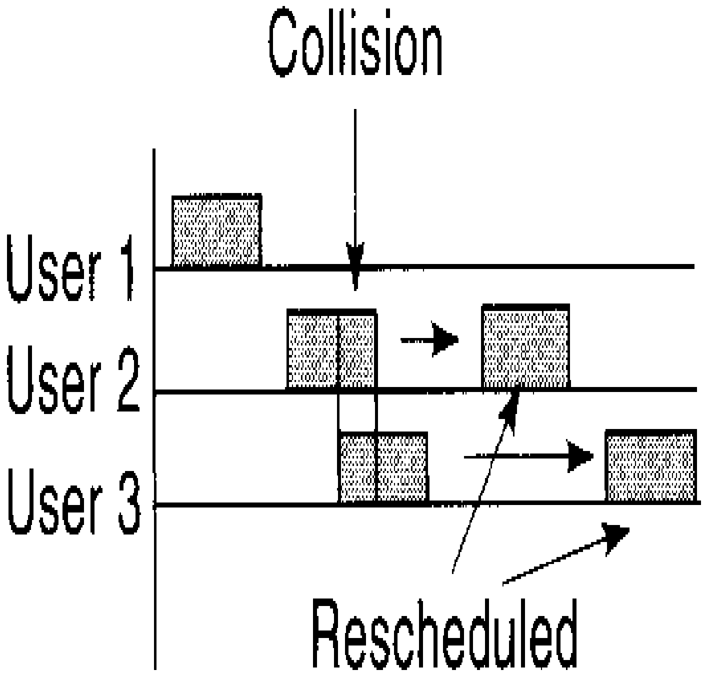
Slotted ALOHA

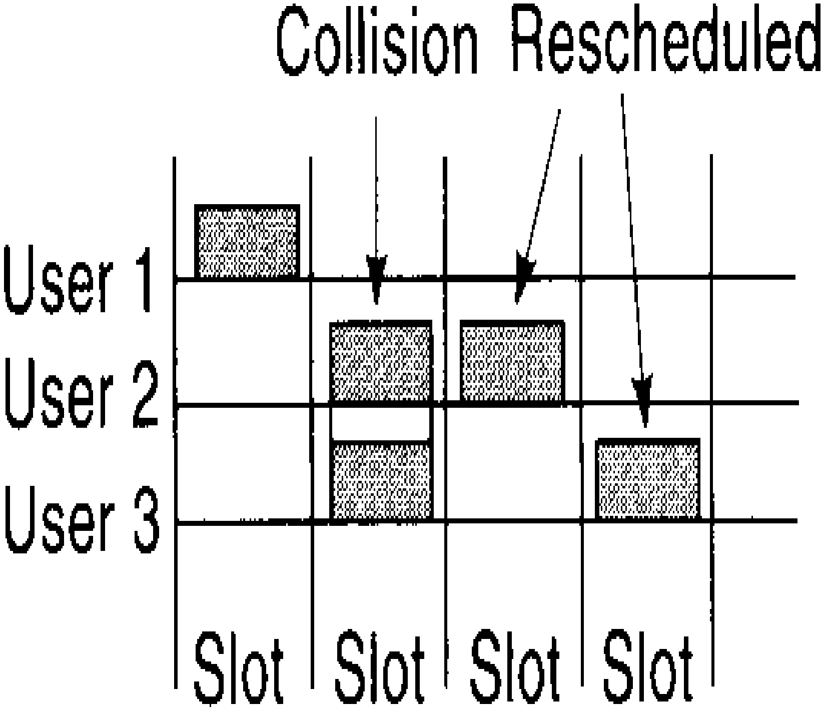
- The maximum throughput of a slotted ALOHA is 36 percent.
- In slotted ALOHA, time is divided into equal time slots of length greater than the packet duration t.
- The subscribers have synchronized clocks and each user will be synchronized with the BS clock.
- The user message packet is buffered and transmitted only at the beginning of a new time slot. This prevents partial collisions.



New transmissions are started only at the beginning of new slot

Pure ALOHA Slotted ALOHA





Application;

- In GSM the initial contact between BS and MS for voice communication is carried out by slotted ALOHA.

De-Merit;

- Even though the throughput is higher than pure ALOHA it is still low for present day wireless communication needs.

Reservation ALOHA

- Reservation ALOHA is the combination of slotted ALOHA and time division multiplexing.
- In this certain packet slots are assigned with priority, and it is possible for users to reserve slots for the transmission of packets.
- For high traffic conditions, reservations on request offers better throughput.

Packet Reservation Multiple Access (PRMA)

- PRMA is a method for transmitting a variable mixture of voice packets and data packets.
- This allows each time slot to carry either voice or data, where voice is given priority.
- PRMA merges characteristics of slotted ALOHA and TDMA protocols.
- It is used for short-range voice transmission where a small delay is acceptable.

- The transmission format in PRMA is organized into frames, each containing a fixed number of time slots.
- Each slot as named as either "reserved" or "available“
- Only the user terminal that reserved the slot can use a reserved slot.
- Other terminals not holding a reservation can use an ‘available’ slot.
- Terminals can send two types of information, referred to as periodic and random.
- Speech packets are always periodic. Data packets can be random.

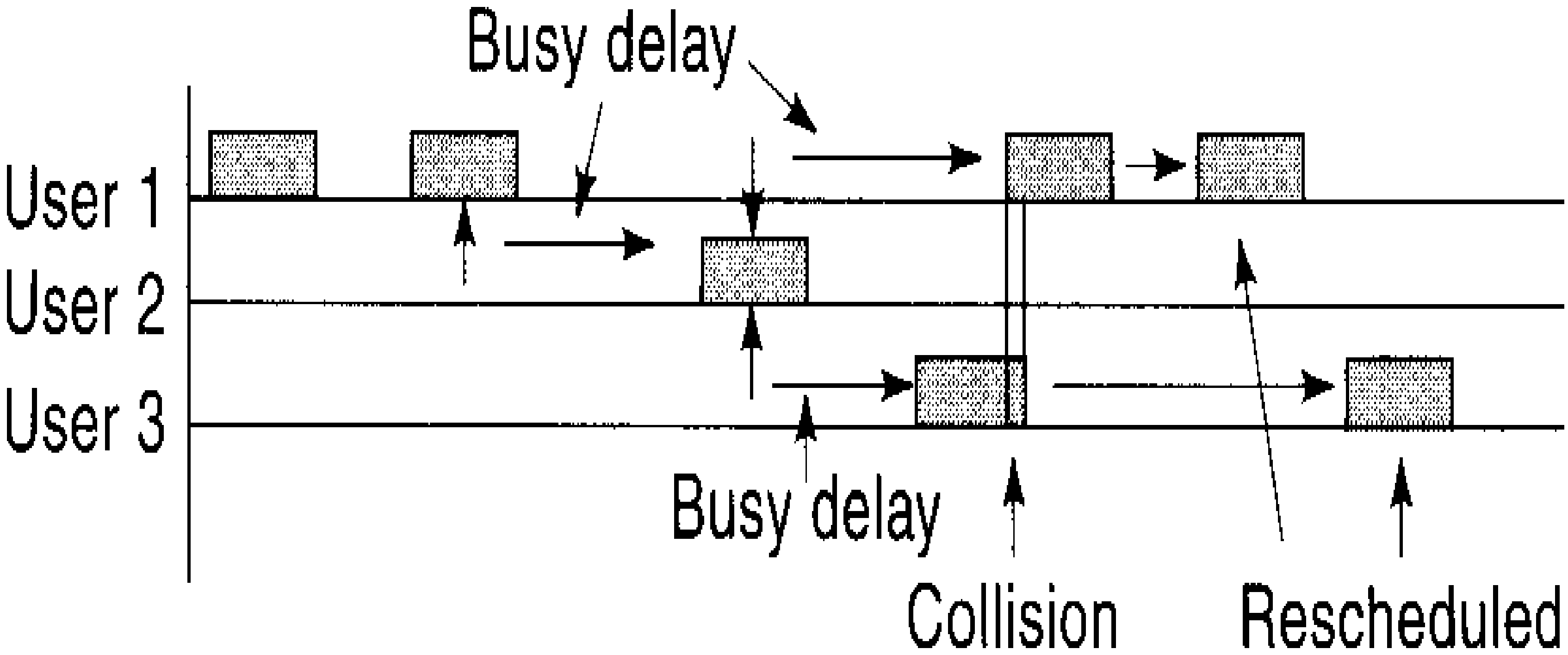
De-Merits of ALOHA

1. ALOHA protocols do not listen to the channel before transmission, the users will start transmitting as soon as the message is ready.
2. Efficiency is reduced by the collision and retransmission process.
3. There are no mechanisms to avoid collisions.

CSMA-Based Wireless Random Access Techniques

CSMA- Carrier Sense Multiple Access

- In this each terminal will monitor the status of the channel before transmitting information.
- If there is another user transmitting on the channel, it is obvious that a terminal should delay the transmission of the packet.
- If the channel is idle, then the user is allowed to transmit data packet without any restrictions.
- The CSMA protocol reduces the packet collision significantly compared with ALOHA protocol. But not eliminate entirely.


Busy delay
User 1
User 2
User 3
Busy delay
Collision
Rescheduled

Parameters in CSMA protocols

1. **Detection delay** - is a function of the receiver hardware and is the time required for a terminal to sense whether or not the channel is idle
2. **Propagation delay-** is a relative measure of how fast it takes for a packet to travel from a base station to a mobile terminal.

- Propagation delay is important, since just after a user begins sending a packet, another user may be ready to send and may be sensing the channel at the same time.
- If the transmitting packet has not reached the user who is poised to send, the latter user will sense an idle channel and will also send its packet, resulting in a collision between the two packets.

Propagation delay (t_d)

$$t_d = \frac{t_p R_b}{m}$$

where

- t_p -> propagation time in seconds,
- R_b -> channel bit rate
- m -> expected number of bits in a data packet

Various strategies of the CSMA

1. **NON-PERSISTENT CSMA** — In this type of CSMA strategy, after receiving a negative acknowledgment the terminal waits a random time before retransmission of the packet.
2. **1-PERSISTENT CSMA** — The terminal senses the channel and waits for transmission until it finds the channel idle. As soon as the channel is idle, the terminal transmits its message with probability one.
3. **p-PERSISTENT CSMA** —When a channel is found to be idle, the packet is transmitted with probability p . It may or may not be immediate.

4. ***CSMA/CD*** – In this the user monitors the channel for possible collisions. If two or more terminals start a transmission at the same time the transmission is immediately aborted in midway.

5. **Data sense multiple access (DSMA) -** is a special type of CSMA that is used to serve the hidden terminals. Cellular networks uses different frequencies for forward and reverse channel. Each MS may not have the knowledge about other MS operating in that area. So it may not know when the channel is idle. For this the BS can announce the availability of the reverse channel through the forward control channel. The BS uses Busy-Idle bit to announce.

6. **Busy tone multiple access (BTMA)**- this is a special type of technique where the system bandwidth is divided into message channel and busy channel. Whenever a terminal sends data through message channel it will also transmits a busy-tone in busy channel. If another terminal senses the busy channel it will understand that the message channel is busy and it will also turns its busy tone. This acts as an alarm for other terminals.

CSMA/CD

Carrier Sense Multiple Access/ Collision Detection

- CSMA/CD is a modification of pure carrier sense multiple access (CSMA). CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected
- Collision detection is easy in wired LANs - measure signal strengths, compare transmitted and received signals

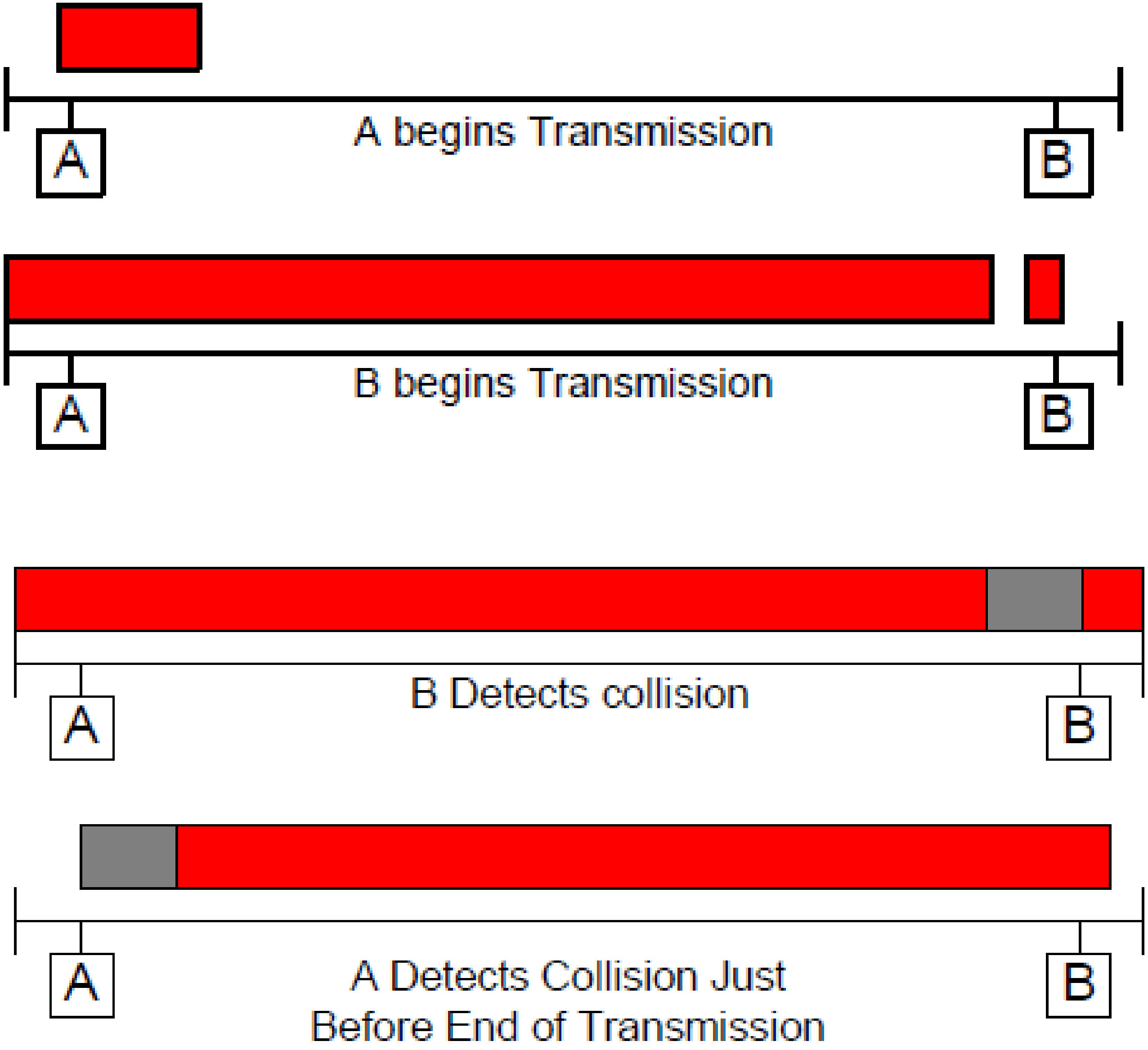
Example: Ethernet

- In CSMA/CD, station listens while transmitting if a station hears something different than what it is sending, it immediately stops (this happens when 2 or more transmitting signals collide with each other)
- In addition, if a collision is detected, a short jamming signal is subsequently sent to ensure that other stations know that collision has occurred (all stations discard the part of frame received)
- After sending the jam signal, back off for a random amount of time, then start to transmit again

CSMA/CD Reaction Time (Time to Detect Collision)

- Because of ‘propagation’ latency, collisions cannot be detected immediately
- Suppose nodes A and B are placed at two extreme ends of the network, and B initiates a transmission just before the transmission arrival from A station A will not be aware of the collision until time $2*t_{prop}$

http://media.pearsoncmg.com/aw/aw_kurose_network_2/applets/csmacd/csmacd.html

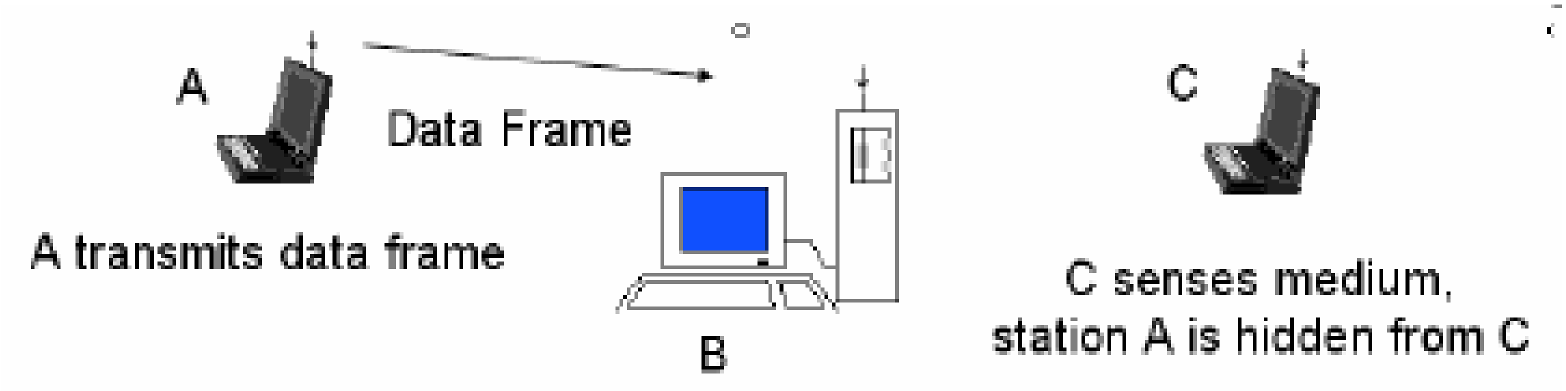

A
B
A begins Transmission
A
B
B begins Transmission
A
B
B Detects collision
A
B
A Detects Collision Just
Before End of Transmission

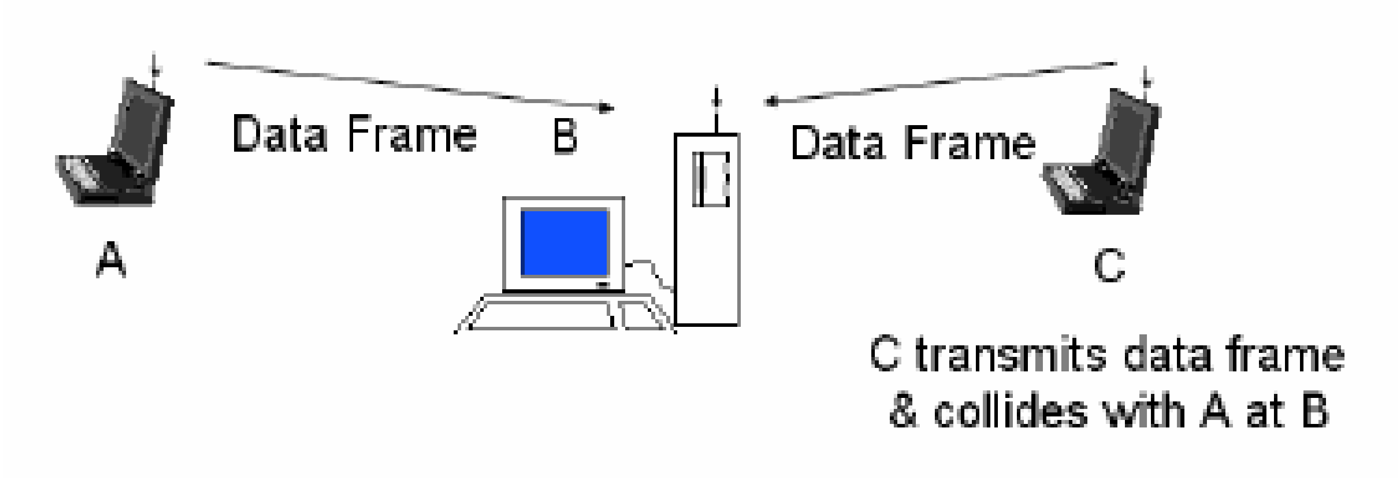
CSMA/CD in Wireless Domain

CSMA/CD is not successful in Wireless domain because of two main reasons:

1. Difficult to detect collision in Wireless radio environment
2. ‘Hidden terminal problem’ – transmitting stations out of each other’s range

- A and C want to send to B
- A starts transmitting – C cannot hear and assumes medium
- available
- C starts transmitting as well, signals collide at B !


A
Data Frame
C
A transmits data frame
C senses medium,
station A is hidden from C
B

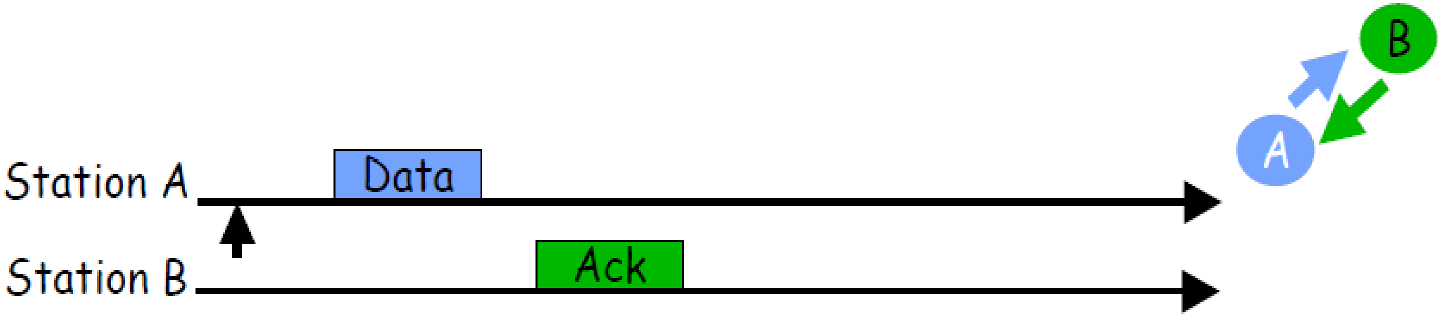

Data Frame
B
Data Frame
A
C
C transmits data frame
& collides with A at B

CSMA/CA

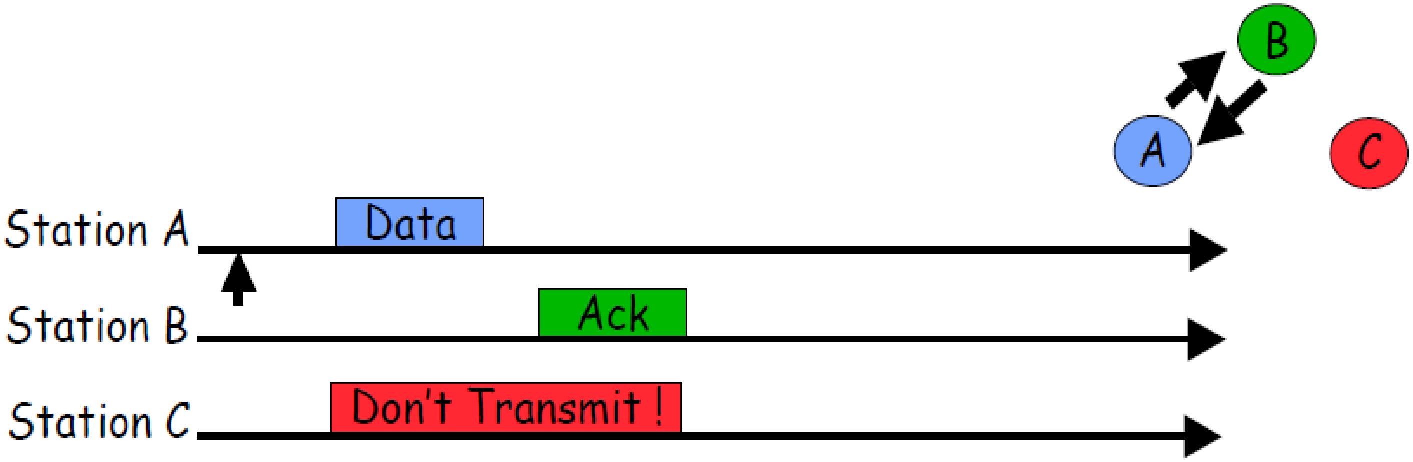
Carrier Sense Multiple Access / Collision Avoidance

- Collision detection is difficult in Wireless environment because it is very challenging for a wireless node to listen at the same time as it transmits.
- Hidden Node - A node that a station does not hear but can interfere with its transmissions

- Station wishing to transmit a Data packet senses the medium
- If it is idle for a given period - Transmits
- ACK packet is sent by the receiving station
- Collision assumed if sending station doesn't get ACK
- Data is retransmitted after a random time



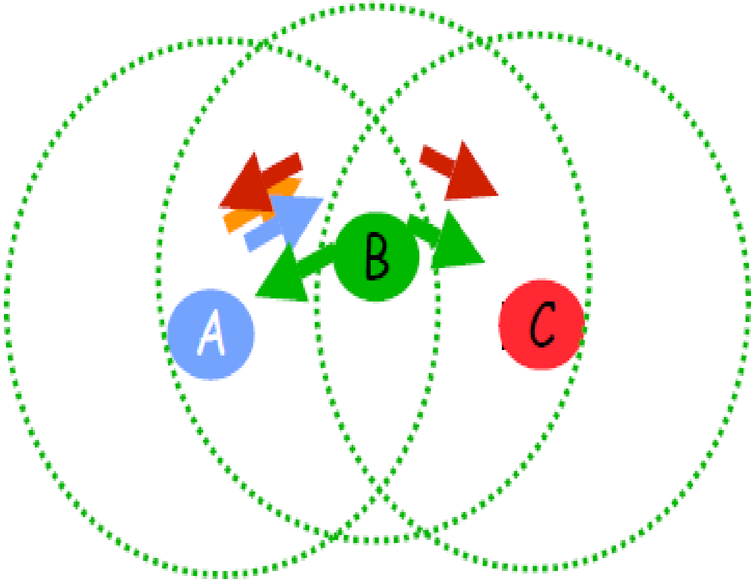
- Station “C” heard the Data or the ACK in the channel, and will not try to transmit during that time



Hidden Node Problem- Solution

- The Hidden Node Problem is solved by the use of Request to Send (RTS) & Clear to Send (CTS) frames

- Procedure
  - A → B Request to Send (RTS)
  - B → A Clear to Send (CTS)
  - A → B Data
  - B → A ACK



- Neighboring nodes will keep quiet for the duration of the transfer
- Network allocation vector (NAV) - specifies duration of transfer
- Node “C” is the hidden node for Node “A”, and both nodes are about to send frames to node B.
- Under normal circumstances both would have sent randomly without the knowledge of each other causing a collision at “B”

- In CSMA/CA the transmission will happen only by the use of Request to Send (RTS) & Clear to Send (CTS) frames
- Node A Requests for sending its data by using RTS frame.
- Node B analyses and permits by sending CTS frame.
- When C tries requests RTS frame it will be rejected by B, since its involved in an active transmission.
- C will be allowed for transmission only after A & B finishes their transmission.

Handoff

- Process of transferring a moving active user from one base station to another without disrupting the call.

Handoff Strategies

1. Ist generation handoff
2. MAHO (Mobile Assisted HandOff)
3. Inter system handoff
4. Guard channel concept
5. Queuing
6. Umbrella approach
7. Soft and hard handoff
8. Cell dragging.

I^{st} generation handoff-

- In this almost all the work were carried out by MSC with the help of Base Station.
- Using the Locator Receiver the MSC will measure the signal strength of the moving mobile.
- If the level decreases it will perform handoff by its own.

MAHO (Mobile Assisted HandOff)

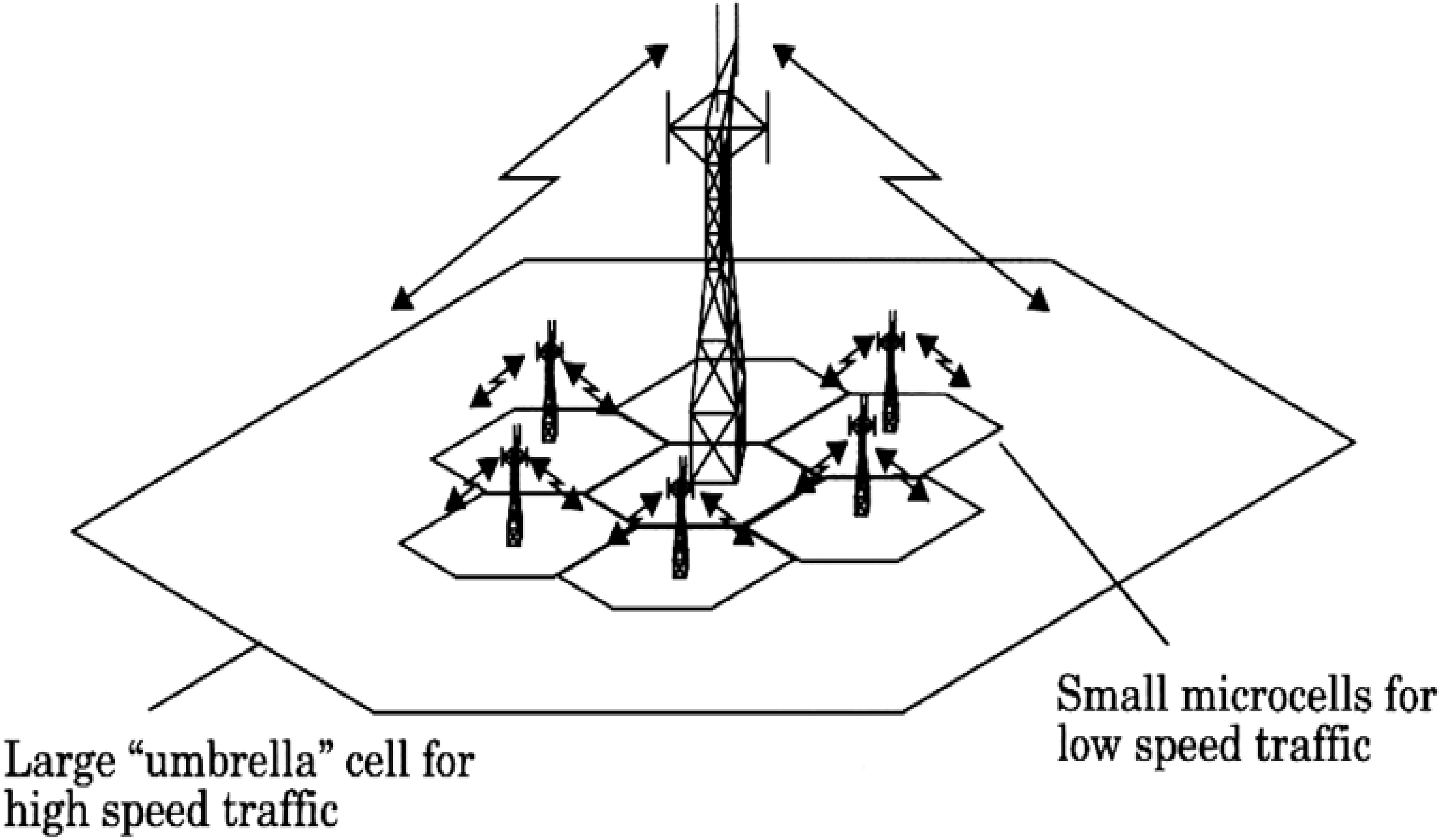
- In this every mobile station measures the received power from surrounding base stations and continually reports the results of these measurements to the serving base station.
- When the power received from the base station of a neighboring cell begins to exceed the power received from the current base station by a certain level or for a certain period of time a handoff is initiated.
- Since all the measurements were done by the mobile, the load of the MSC is reduced considerably

- Inter system handoff -occurs if a mobile moves from one cellular system to a different cellular system controlled by a different MSC (service provider) or while roaming
- Guard channel concept – In this some channels are reserved only for handoff.
- Queuing – If more number of users request handoff the they will be placed in queue before allotting channels

Umbrella approach

- Speed of the user is a main factor in deciding a successful handoff.
- In urban areas the cell size will be very small and high speed users will cross quickly.
- To perform handoff on these high speed users we use Micro and Macro cells concurrently.

Umbrella approach



Cell dragging

- Cell dragging occurs in an urban environment when there is a line-of-sight (LOS) radio path between the pedestrian subscriber and the base station.
- Even after the user has traveled well beyond the designed range of the cell, the received signal at the base station does not decay rapidly resulting in Cell Dragging

Soft and hard handoff

- Hard handoff- when the user moves to a new cell, he will be assigned with a new set of channels.
- Soft Handoff- when the user moves to a new cell, the channel itself will be switched to the new base station. CDMA uses soft Handoff.

WIRELESS SECURITY AND PRIVACY

- The broadcast nature of wireless communications renders it very susceptible to malicious interception and wanted or unintentional interference.
- Analog techniques are extremely easy to tap.
- Digital systems such as TDMA and CDMA are much harder to tap.
- Wireless security is necessary to prevent the unauthorized access or damage to computers using wireless networks.

There are two names you need to know in a wireless network:

- **Station (STA) ->** is a wireless network client—a desktop computer, laptop, or PDA
- **Access point (AP)->** is the central point (like a hub) that creates a basic service set to bridge a number of STAs from the wireless network to other existing networks.

Modes of unauthorized access

1. Accidental association
2. Malicious association
3. Ad-hoc networks
4. Non-traditional networks
5. Identity theft (MAC spoofing)
6. Man-in-the-middle attacks
7. Denial of service
8. Network injection
9. Caffe Latte attack

http://en.wikipedia.org/wiki/Wireless_security

1. Accidental association

- Violation of security perimeter of corporate network unintentionally.

2. Malicious association

- when wireless devices can be actively made by attackers to connect to a company network through their devices cracking company access point (AP).
- These types of laptops are known as “soft APs” and are created when a cyber criminal runs some software that makes his/her wireless network card look like a legitimate access point.
- Once access is gained, he/she can steal passwords, launch attacks on the wired network, or plant Trojans

3. Ad-hoc networks

- Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

4. Non-traditional networks

- Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured

5. Identity theft (MAC spoofing)

- Identity theft occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges.

6. Man-in-the-middle attacks

- In this the hacker will include a soft AP in to a network. Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network

7. Denial of service

- A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted Access Point or network with bogus requests, premature successful connection messages, failure messages, and other commands.
- These cause legitimate users to not be able to get on the network and may even cause the network to crash

8. Network injection

- In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic.
- The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs.
- A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices

9. Caffe Latte attack

- The Caffe Latte attack is another way to defeat WEP.
- It is not necessary for the attacker to be in the area of the network using this exploit.
- By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client
- By sending a flood of encrypted Address Resolution Protocol (ARP) requests, the assailant takes advantage of the shared key authentication and the message modification flaws in WEP.

The Attack Methodology

1. **Footprint the wireless network-** Locate and understand your target.
2. **Passive attack -** Analyze the network traffic or break the WEP.
3. **Authentication and authorization -** Determine what methods are enforced and how they can be circumvented.
4. **Active attack -** Launch denial of service (DoS) attacks.

http://technet.microsoft.com/en-us/library/bb457019.aspx

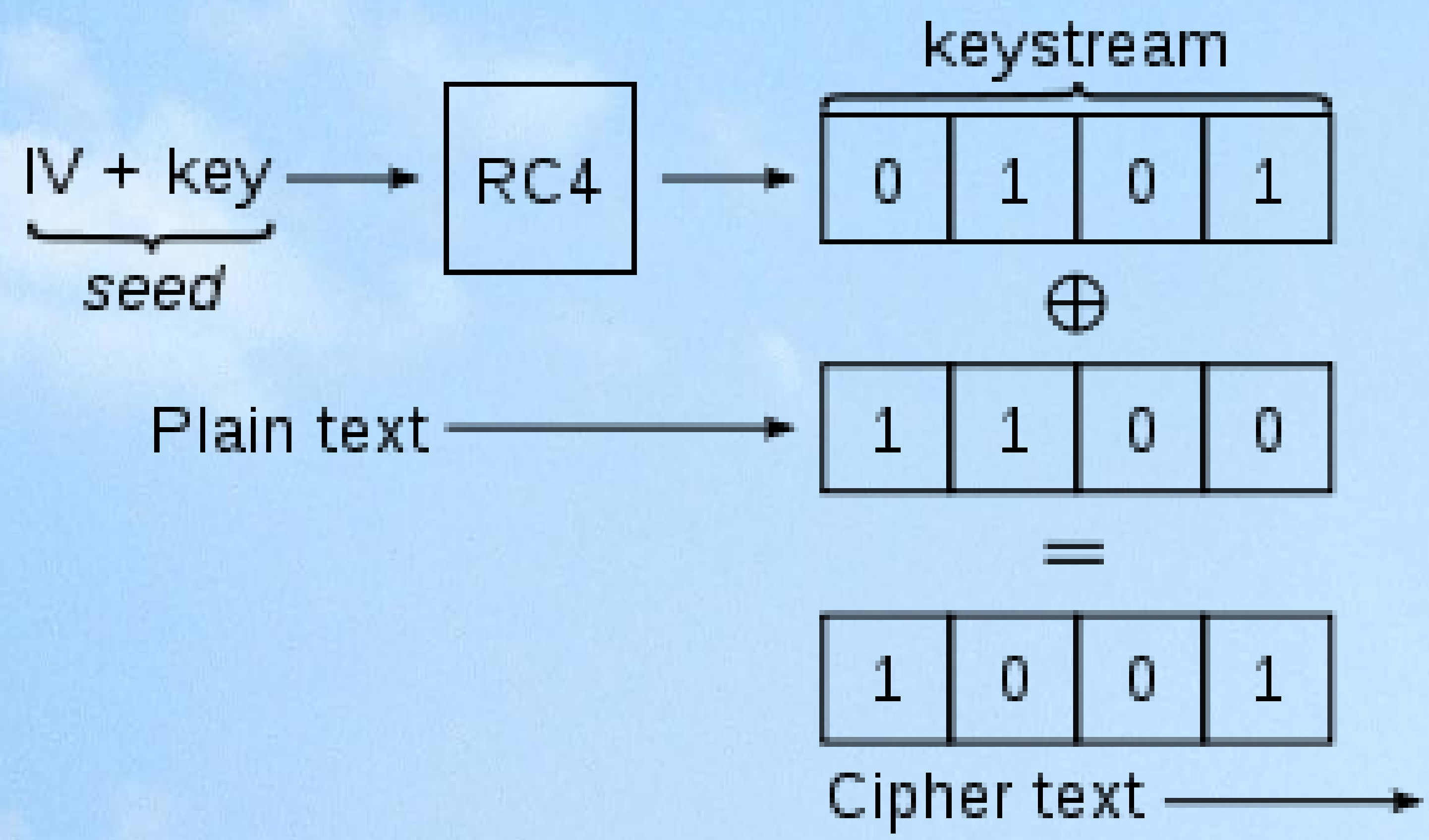
Defense Mechanisms

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access- 2 (WPA-2)
- …….

Wired Equivalent Privacy (WEP)

- **WEP** is a standard network protocol that adds security to wireless networks at the data link layer.
- WEP utilizes a data encryption scheme called **RC4** for data protection.
- **RC4** (also known as **ARC4** or **ARCFOUR**) is the most widely used software stream cipher and is used in popular protocols.

- RC4 generates a pseudorandom stream of bits.
- Standard 64-bit WEP uses a 40 bit key (WEP-40) and a 24 bit initialization vector .
- 128-bit WEP protocol using a 104-bit key size (WEP-104) and a 24 bit initialization vector.
- Initialization vector (IV) is a fixed-size input which is used for randomization of key. The purpose of an IV is to prevent any repetition.


IV + key
seed
RC4
keystream
0 1 0 1
⊕
Plain text
1 1 0 0
=
1 0 0 1
Cipher text

Authentication

1. The client sends an authentication request to the Access Point.
2. The Access Point replies with a clear-text challenge.
3. The client encrypts the challenge-text using the configured WEP key, and sends it back in another authentication request.
4. The Access Point decrypts the response. If this matches the challenge-text the Access Point sends back a positive reply.

Dis Advantages

- The same traffic key must never be used twice.
- But a 24-bit IV is not long enough to ensure this on a busy network.
- In August 2001, Scott Fluhrer, Itsik Mantin, and Adi Shamir published a cryptanalysis of WEP that decodes the way the RC4 cipher and IV is used in WEP.
- Using a passive attack they were able to recover the RC4 key after eavesdropping on the network.
- A successful key recovery could take as little as one minute depending on the traffic.
- WEP is replaced by WPA(Wi-Fi Protected Access)

Wi-Fi Protected Access(WPA)

- The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP.
- WPA uses Temporal Key Integrity Protocol (TKIP) to bolster encryption of wireless packets.

TKIP

- TKIP encryption replaces WEP's 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change
- TKIP uses a 128-bit per-packet key, it dynamically generates a new key for each packet and prevents attacks.
- It has an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA with TKIP provides 3 levels of security

1. TKIP implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 initialization.
2. WPA implements a sequence counter to protect against replay attacks. Packets received out of order will be rejected by the access point.
3. TKIP implements a 64-bit Message Integrity Check (MIC)

Message integrity check.

- This is designed to prevent an attacker from capturing, altering and/or resending data packets.
- This replaces the cyclic redundancy check (CRC) that was used by the WEP standard.
- CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled

Merits and Demerits

- TKIP uses the same underlying mechanism as WEP, and consequently is vulnerable to a number of similar attacks.
- But the message integrity check, per-packet key hashing, broadcast key rotation, and a sequence counter prevents many attacks.
- The key mixing function also eliminates the WEP key recovery attacks
- Beck-Tews attack has successfully extracted the keystream

Ohigashi-Morii attack

- Japanese researchers Toshihiro Ohigashi and Masakatu Morii reported a simpler and faster implementation of a similar attack.
- It utilizes a similar attack method, but uses a man-in-the-middle attack

WPA 2

- WPA2 (Wireless Protected Access 2) replaced the original WPA technology on all certified Wi-Fi hardware since 2006.
- WPA2 is based on Advanced Encryption Standard (AES) block cipher, whereas WEP and WPA use the RC4 stream cipher.
- WPA2 uses Pre-Shared Key (PSK) instead of TKIP
- WPA2 Pre-Shared Key (PSK) utilizes keys with 256 bits

There are two versions of WPA2

1. **WPA2-Personal-** protects unauthorized network access by utilizing a set-up password
2. **WPA2-Enterprise-** verifies network users through a server. WPA2 is backward compatible with WPA.

Security in GSM

In GSM, security is implemented in three entities:

- Subscriber identity module (SIM) contains IMSI, TMSI, PIN, MSISDN, authentication key Ki (64-bit), ciphering key (Kc) generating algorithm A8, and authentication algorithm A3.
- GSM handset contains ciphering algorithm A5.
- Network uses algorithms A3, A5, A8; Ki and IDs are stored in the authentication center

- **IMSI** - International mobile subscriber identity
- **TMSI** - Temporary Mobile Subscriber Identity
- **MSISDN** - Mobile Subscriber Integrated Services Digital Network-Number

- SIM is a single chip computer containing the operating system (OS), the file system, and applications. SIM is protected by a PIN and owned by an operator. SIM applications can be written with a SIM tool kit.
- Both A3 and A8 algorithms are implemented on the SIM

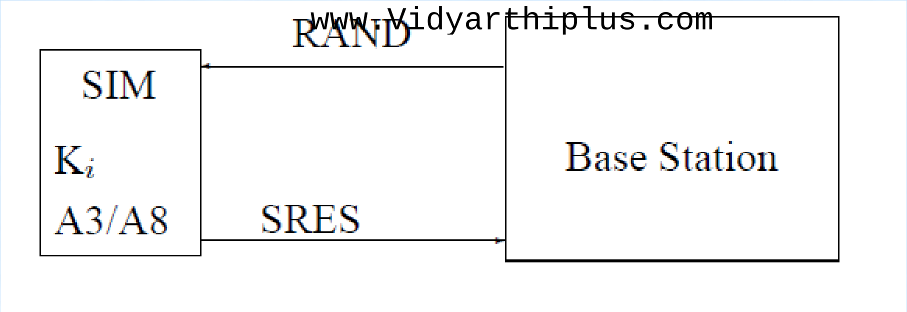
  http://en.wikipedia.org/wiki/COMP128
- COMP128 is an implementation of the A3 and A8 algorithms defined in the GSM standard

- A3 is used to authenticate the mobile station to the network. A8 is used to generate the session key used by the A5 algorithm to encrypt the data transmitted between the mobile station and the BTS.
- The algorithm was originally confidential. A partial description was leaked in 1997 and completed via reverse engineering. This led to a full publication in 1998
- Updated versions COMP128-2, COMP128-3, COMP128-4
- A5 is a stream cipher. It can be implemented very efficiently on hardware. Its design was never made public

- The authentication center contains a database of identification and authentication information for subscribers including IMSI, TMSI, location area identity (LAI), and authentication key (Ki).
- It is responsible for generating (RAND), response (RES), and ciphering key (Kc) which are stored in HLR / VLR for authentication and encryption processes

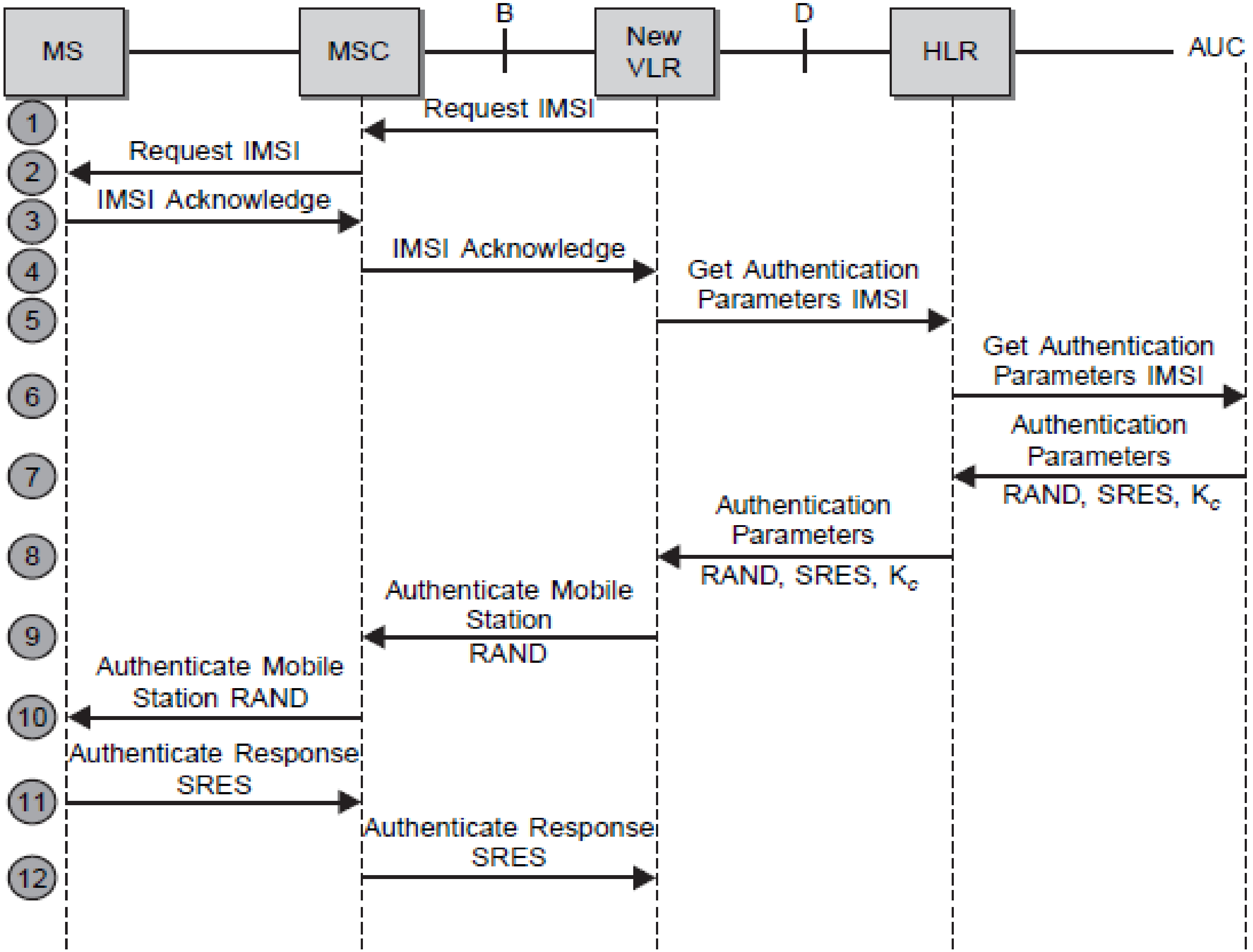
GSM Authentication

- RAND is a 128-bit random challenge issued from the base station to the mobile
- SRES is a 32-bit signed response generated by A3 issued from the mobile to the base station
- K_i is the SIM's 128-bit individual subscriber key (located only on the SIM and the GSM network). The K_i is securely burned into the SIM during manufacture.



- A3 - Authentication / A8 - Key Generator
  - The Ki and RAND are fed into the A3 algorithm and the signed response (SRES) is calculated.
  - The Ki and RAND are fed into the A8 algorithm and a session key called Kc is calculated.
- This *Ki* is never transmitted between the AuC and SIM, but is combined with the IMSI to produce a challenge/response for identification purposes and an encryption key called *Kc* for use in over the air communications.

GSM Authentication- Detailed


MS
MSC
B
New VLR
D
HLR
AUC
1
Request IMSI
2
Request IMSI
3
IMSI Acknowledge
4
IMSI Acknowledge
5
Get Authentication Parameters IMSI
6
Get Authentication Parameters IMSI
7
Authentication Parameters
RAND, SRES, K_c
8
Authentication Parameters
RAND, SRES, K_c
9
Authenticate Mobile Station
RAND
10
Authenticate Mobile Station RAND
11
Authenticate Response SRES
12
Authenticate Response SRES

GSM token-based unique challenge with ciphering.

Steps- Summary

1. The serving system sends a RAND to the MS.
2. The MS computes the SRES using RAND and the authentication key (Ki) in the encryption algorithm.
3. The MS transmits the SRES to the serving system.
4. The MSC sends a message to the VLR requesting authentication.
5. The VLR checks the SRES for validity.
6. The VLR returns the status to the MSC.
7. The MSC sends a message to the MS with a success or failure indication.

References

1. Andrea Goldsmith, Wireless Communications, Cambridge University Press, 2007.
2. Andreas.F. Molisch, “Wireless Communications”, John Wiley – India, 2006.
3. Rappaport. T.S., “Wireless communications”, Pearson Education, 2003.
4. Vijay. K. Garg, “Wireless Communication and Networking”, Morgan Kaufmann Publishers,
5. Kaveth Pahlavan,. K. Prashanth Krishnamuorthy, "Principles of Wireless Networks", Prentice Hall of India, 2006.
6. William Stallings, "Wireless Communications and networks" Pearson / Prentice Hall of India, 2nd Ed., 2007.

WIRELESS NETWORKS

by

Ananth Ravindran
Assistant Professor

UNIT II

WIRELESS WANS

First Generation Analog, Second Generation TDMA – GSM, Short Messaging Service in GSM, Second Generation CDMA – IS-95, GPRS - Third Generation Systems (WCDMA/CDMA 2000)

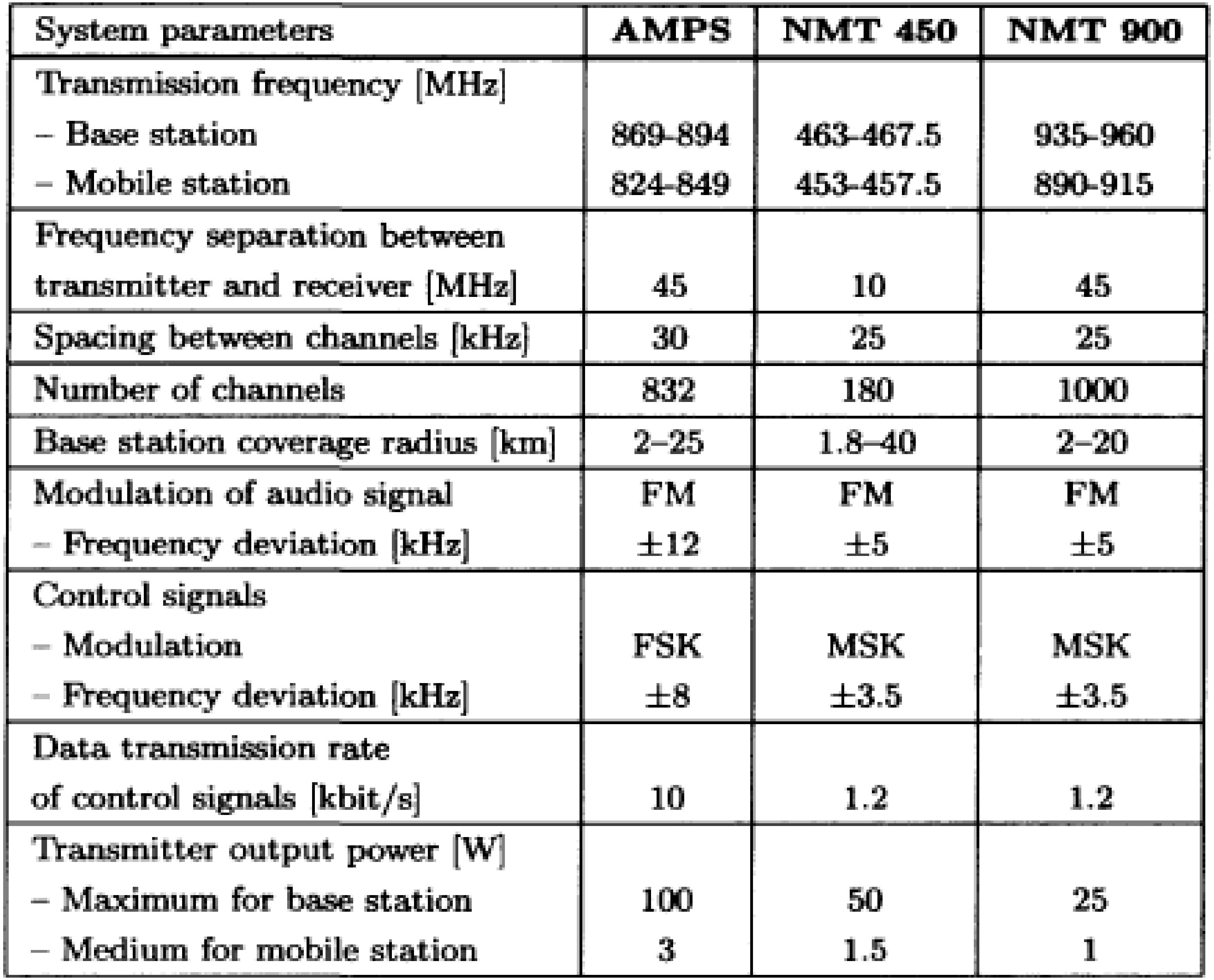
1G - First Generation networks

1 G

- These are the analog telecommunications standards that were introduced in the 1980s.
- It is mainly used for voice calls only
- Their signals were transmitted by frequency modulation.
- The first commercially automated 1G cellular network was launched in Japan by NTT (Nippon Telegraph and Telephone) in 1979

Popular 1G Networks

1. Nordic Mobile Telephone (NMT 450 & NMT-900)
   - Nordic Countries -Denmark, Finland, Iceland, Norway and Sweden
   - Switzerland, Netherlands, Eastern Europe and Russia
2. Advanced Mobile Phone System (AMPS)
   - North America and Australia



System parameters	AMPS	NMT 450	NMT 900
Transmission frequency [MHz]			
– Base station	869-894	463-467.5	935-960
– Mobile station	824-849	453-457.5	890-915
Frequency separation between transmitter and receiver [MHz]	45	10	45
Spacing between channels [kHz]	30	25	25
Number of channels	832	180	1000
Base station coverage radius [km]	2–25	1.8–40	2–20
Modulation of audio signal	FM	FM	FM
– Frequency deviation [kHz]	±12	±5	±5
Control signals			
– Modulation	FSK	MSK	MSK
– Frequency deviation [kHz]	±8	±3.5	±3.5
Data transmission rate of control signals [kbit/s]	10	1.2	1.2
Transmitter output power [W]			
– Maximum for base station	100	50	25
– Medium for mobile station	3	1.5	1

Nordic Mobile Telephone- Architecture

History

- It was opened for service in 1 October 1981.
- NMT is based on first generation analog technology
- It has two variants NMT-450 and NMT-900.
- The numbers indicate the frequency bands uses
- By 1985 the network had grown to 110,000 subscribers which made it the world's largest mobile network at the time

Technology

- The cell sizes in an NMT network range from 2 km to 30 km
- NMT used full duplex transmission, allowing for simultaneous receiving and transmission of voice.
- Car phone versions of NMT used transmission power of up to 15 watt (NMT-450) and 6 watt (NMT-900), handsets up to 1 watt

- NMT had automatic switching (dialing) and handover of the call
- NMT standard specified billing as well as national and international roaming.

Signaling

- NMT voice channel is transmitted with FM modulation
- Fast Frequency Shift Keying (FFSK) modulation is used for signaling between the base station and the mobile station.

Data transfer

- NMT supported a simple integrated data transfer mode called DMS (Data and Messaging Service) or NMT-Text.
- It uses the network's signaling channel for data transfer.
- Using DMS, text messaging was possible between two NMT handsets before SMS service started in GSM.
- But this feature was never commercially available except in Russian, Polish and Bulgarian NMT networks

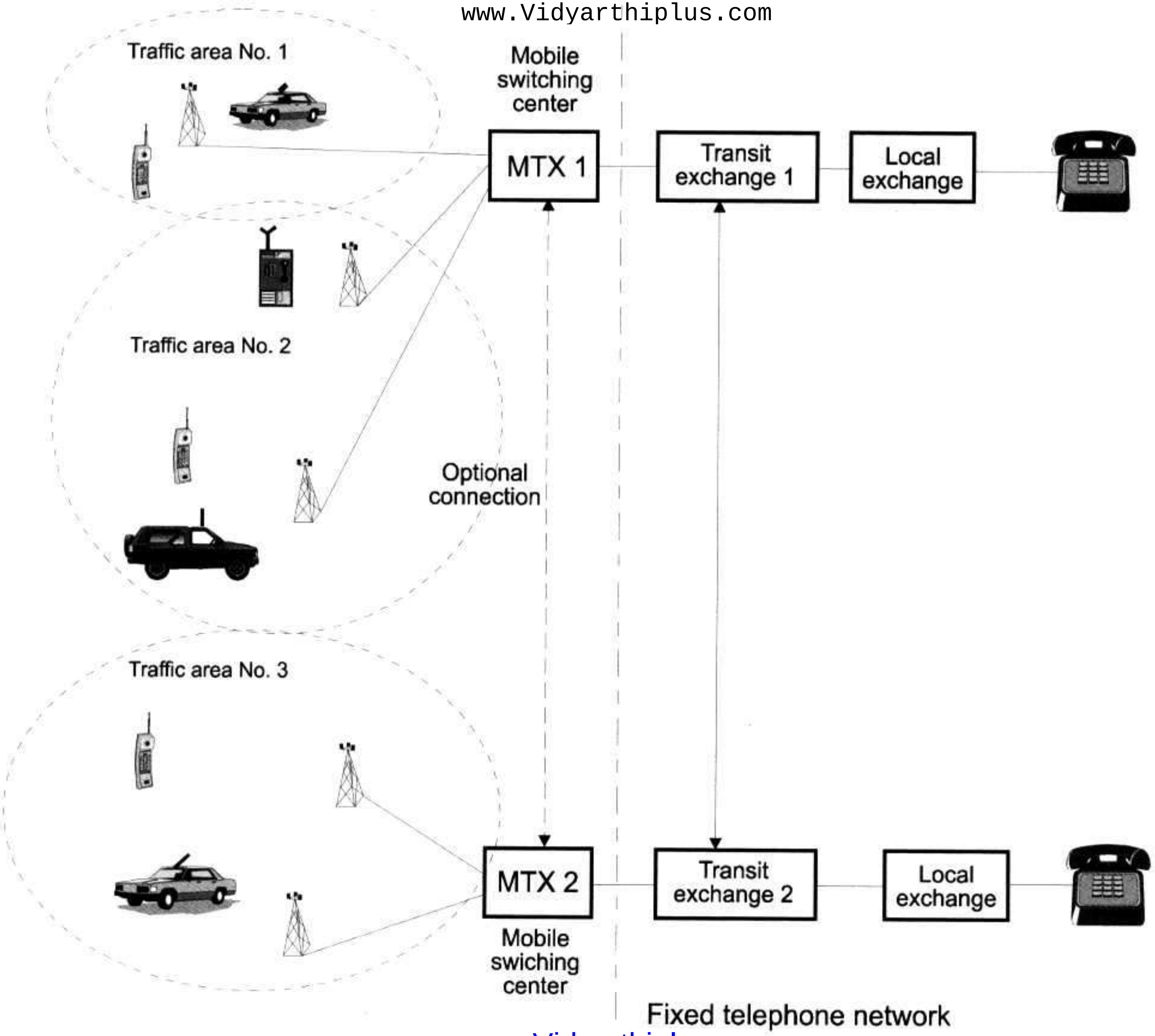
Security

- The voice traffic was not encrypted, therefore it was possible to listen to calls using a scanner.
- To prevent this the later versions of the NMT specifications defined optional analog scrambling .
- If both the base station and the mobile station supported scrambling, they could agree upon using it when initiating a phone call
- If two users had mobile stations supporting scrambling, they could turn it on during conversation even if the base stations didn't support it

SYSTEM ARCHITECTURE

The NMT system consists of three basic group of elements:

- *Mobile Telephone Exchanges*(MTX),
- *Base Stations* (BS) and
- *Mobile Stations* (MS).


Traffic area No. 1
Mobile switching center
MTX 1
Transit exchange 1
Local exchange
Traffic area No. 2
Optional connection
Traffic area No. 3
MTX 2
Mobile swiching center
Transit exchange 2
Local exchange
Fixed telephone network

- The MTX is the main control element of the system. It provides the interface with the PSTN. The interface is possible on the local, transit or international exchange levels. The preferred level of interface is a transit exchange.
- The base stations realize the interface between the fixed part of the system and mobile stations.
- The areas covered by base stations are grouped into *traffic areas.* Each traffic area is connected through the MTX with the fixed network
- MTX can control a few traffic areas. The area covered by base stations controlled by a single MTX is called a *service area*

Channels

- Each base station manages a subset of channels assigned to the cell according to the channel distribution plan. each base station has
  - A single paging (calling) channel,
  - Traffic channels,
  - A single access channel (in NMT 900),
  - Combined paging and traffic channel,
  - A single data channel.

- Paging Channel
  - The paging channel is used by the base station for transmission of a continuous identification signal.
  - Mobile stations located in a given traffic area and remaining in the *idle state* are locked to the paging channel
- Traffic channels
  - Traffic channels are used to perform calls and to manage a part of the call request. A traffic channel can remain in three different states,
    - **in a free state** - the mobile station can use it to initiate a call request to the base station,
    - **in a busy state** - the call is currently performed
    - **in an idle state** - the channel is neither in a free state nor in a busy state

- Combined Paging And Traffic Channel
  - The combined paging and traffic channel has the features of both channels. In a regular mode it is used as a paging channel.
  - However, if all traffic channels are occupied, it can be temporarily used by selected, high priority subscribers as a traffic channel
- Data channel
  - The data channel allows measurement of the power level of the signal of the mobile station being in the active connection state.
  - The measurement results are used by the MTX in the handover process

- Access Channel
  - The access channel is a special channel in the NMT 900 version of the system used to perform a call request instead of a traffic channel marked "free".

Features

- The NMT 450 operates in the FDMA/FDD mode
- It has 180 channels in NMT 450 and 1000 channels in NMT 900
- Cell splitting was used
- Near-far effect was present

MOBIRA

NOKIA
NOKIA
NOKIA
MOBIRA

Advanced Mobile Phone System (AMPS)

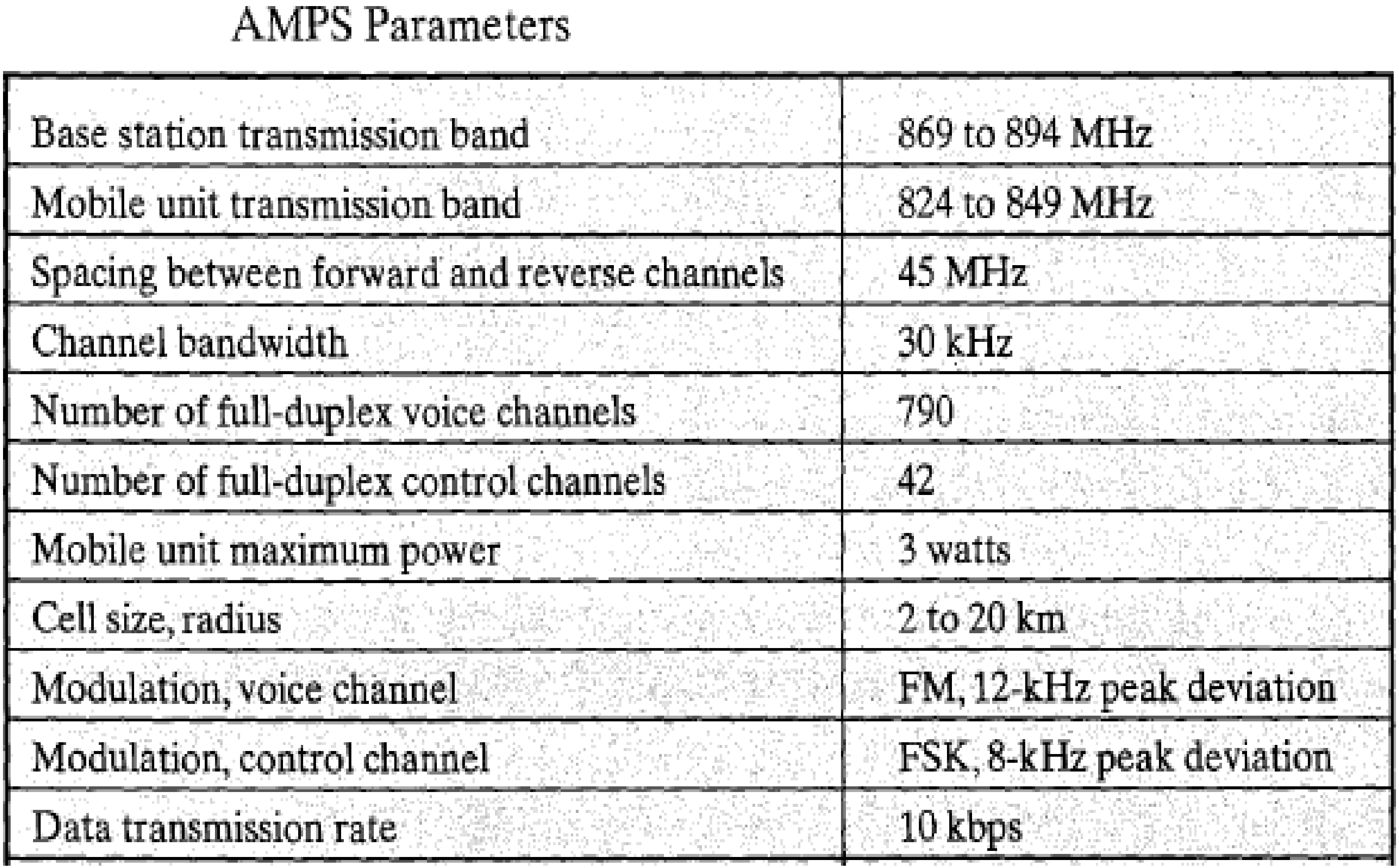
- AMPS is a first generation analog cellular telephone system that originated in the USA in the 1980s.
- AMPS can be found in countries such as Canada, Australia, Hong Kong, New Zealand, South Korea, Singapore, Taiwan, Thailand and Israel
- It is not compatible with European mobile phone standards

Technology

- AMPS was a first-generation cellular technology that uses separate frequencies or channels.
- AMPS operates in the 800 and 900 MHz frequency bands
- FDMA is used to divide each band of operating frequencies into 30 kHz channels
- Adjacent cells will then employ different channels for their transmitted and received signals, so that one cell does not interfere with another, and as a user moves between cells the channels

Frequency bands

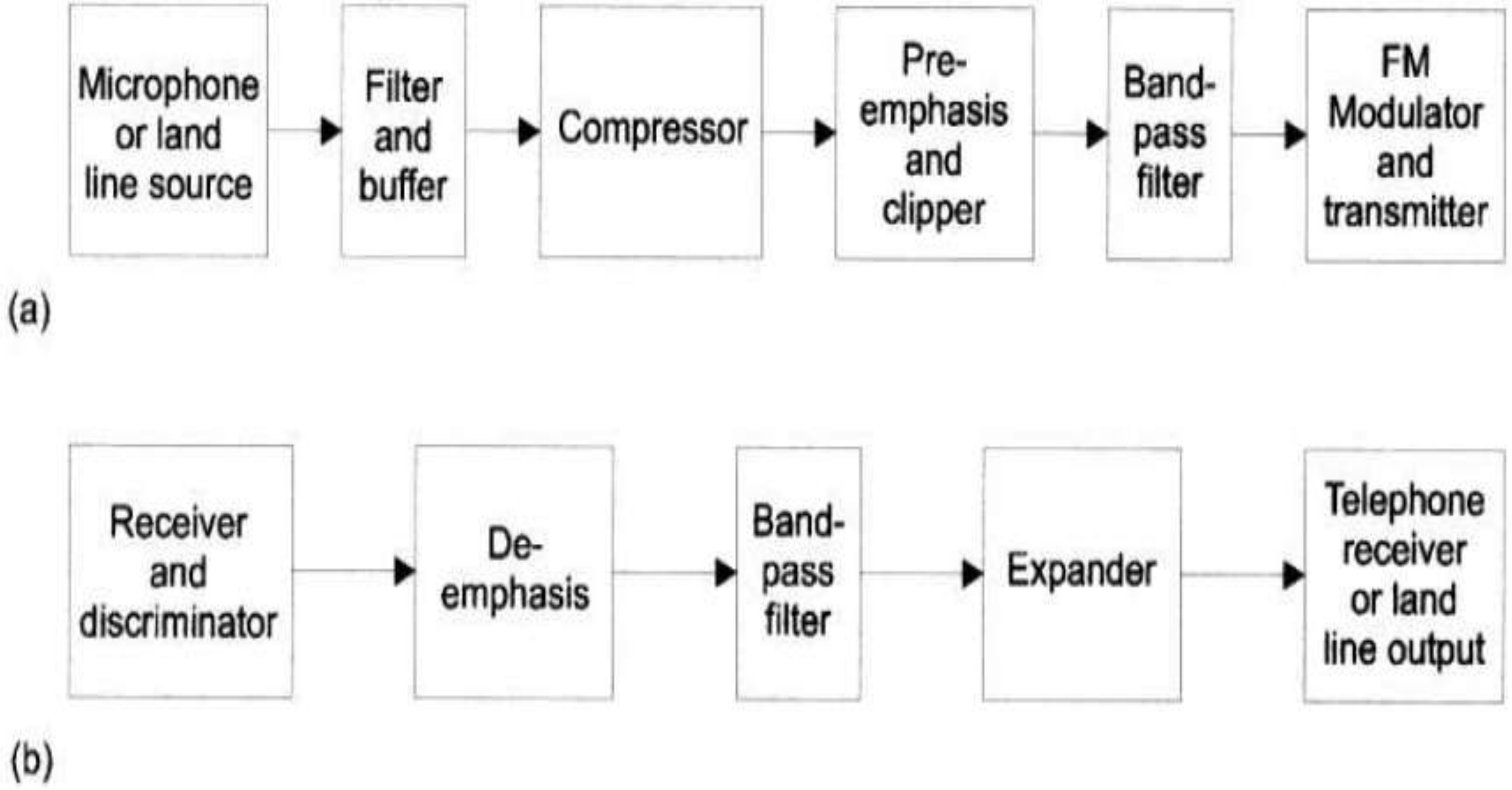
- The United States Federal Communications Commission (FCC) allowed two licensee (networks) known as “A (824–849 MHz)" and "B (869–894 MHz)" carriers.
- Each "block" of frequencies consisting of 21 control channels and 395 voice channels.
- Each channel is composed of 2 frequencies 1 for forward and 1 for reverse.



AMPS Parameters

Base station transmission band	869 to 894 MHz
Mobile unit transmission band	824 to 849 MHz
Spacing between forward and reverse channels	45 MHz
Channel bandwidth	30 kHz
Number of full-duplex voice channels	790
Number of full-duplex control channels	42
Mobile unit maximum power	3 watts
Cell size, radius	2 to 20 km
Modulation, voice channel	FM, 12-kHz peak deviation
Modulation, control channel	FSK, 8-kHz peak deviation
Data transmission rate	10 kbps

AMPS Radio Interface


Microphone or land line source
Filter and buffer
Compressor
Pre-emphasis and clipper
Band-pass filter
FM Modulator and transmitter
(a)
Receiver and discriminator
De-emphasis
Band-pass filter
Expander
Telephone receiver or land line output
(b)

(a) Transmitter (b) receiver

- The voice signal is received from a microphone or a PSTN source.
- The signal is filtered and limited in amplitude and fed to a compressor.
- The compressor is a variable gain circuit which controls the effect of speech level variability and decreases the dynamic range of the speech signal.
- The compression is performed in such a way that a 2 dB increase in input power level produces a 1 dB increase in output power level.

- The compressed signal is then pre- emphasized and amplitude limited in order not to exceed the specified frequency deviation of 12 kHz.
- In the receiver, the received FM signal is discriminated, processed by the de-emphasis filter, bandpass filtered and expanded.
- The characteristics of the expander is reciprocal to that of the compressor, so both operations cancel each other

Operation

- Each AMPS-capable cellular telephone has a Numeric Assignment Module (NAM) in read-only memory.
- The NAM contains the telephone number of the phone, which is assigned by the service provider, and the serial number of the phone, which is assigned by the manufacturer
- When the phone is turned on, it transmits its serial number and phone number to the MSC or MTSO (Mobile Telephone Switching Office)

Steps in making a call- mobile originated

- The subscriber initiates a call by typing in the telephone number.
- The MSC verifies that the telephone number is valid and that the user is authorized to place the call
- The MSC issues a message to the user's cell phone indicating which traffic channels to use for sending and receiving.
- The MSC sends out a ringing signal to the called party. All of these operations (steps 2 through 4) occur within 10 s of initiating the call.

- When the called party answers, the MSC establishes a circuit between the two parties and initiates billing information.
- When one party hangs up, the MTSO releases the circuit, frees the radio channels, and completes the billing information

PSTN originated call

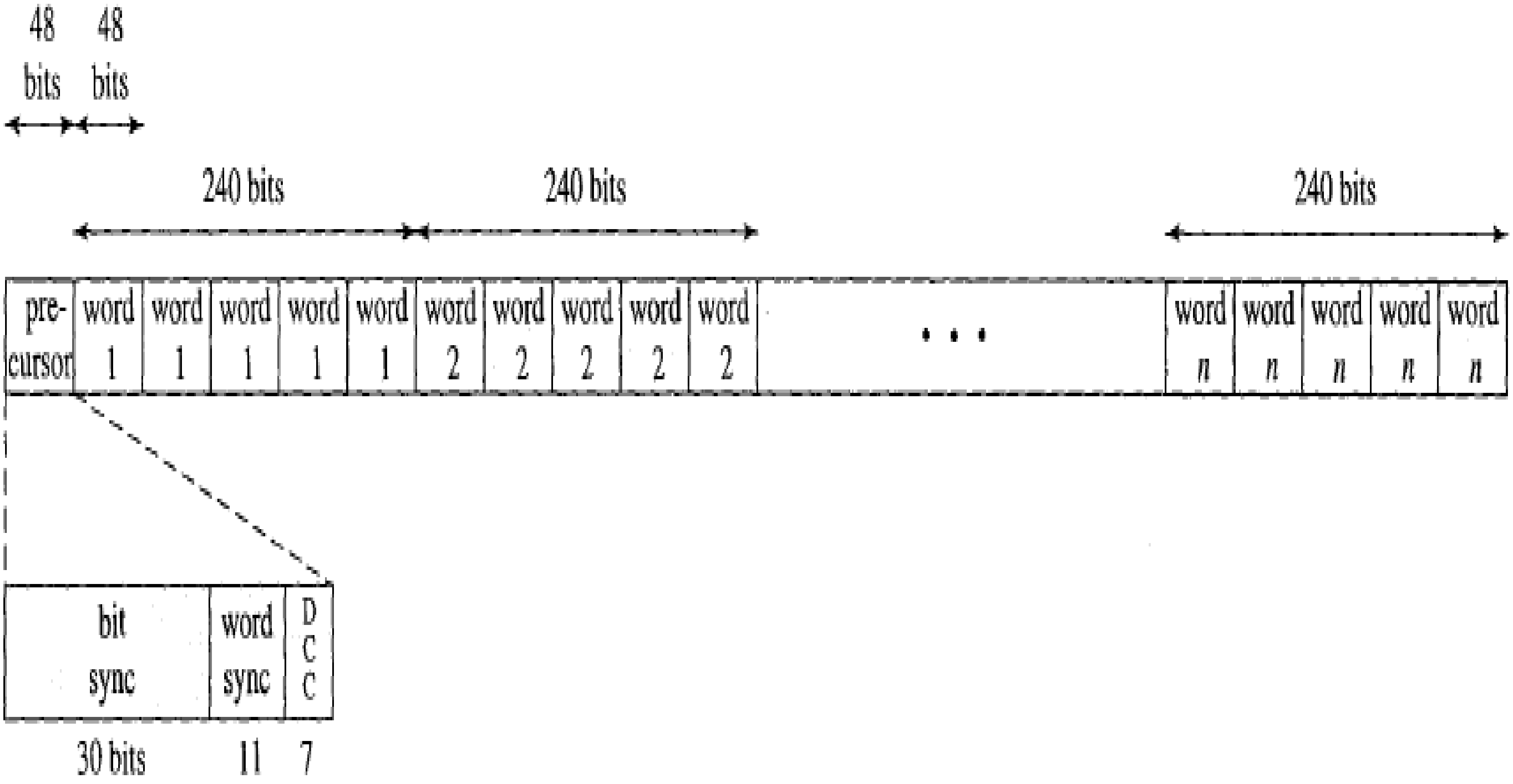
- The source of the call request is a PSTN subscriber.
- The PSTN network issues a call request sending the number of a mobile subscriber to the AMPS mobile switching center (MSC).
- The MSC sends the paging message, which includes the called subscriber's *Mobile Identification Number* (MIN), to all base stations.
- They emit the page on the forward control channels.

- If the called mobile station is in the idle mode, it is listening to one of these channels it acknowledges its reception on the reverse control channel by sending back to the base station its MIN, its serial number or the *Equipment Serial Number* (ESN).
- This way the MSC learns where the mobile station is currently located.
- In turn, the MSC instructs the selected base station to assign the unused voice channel pair to the connection with the mobile station

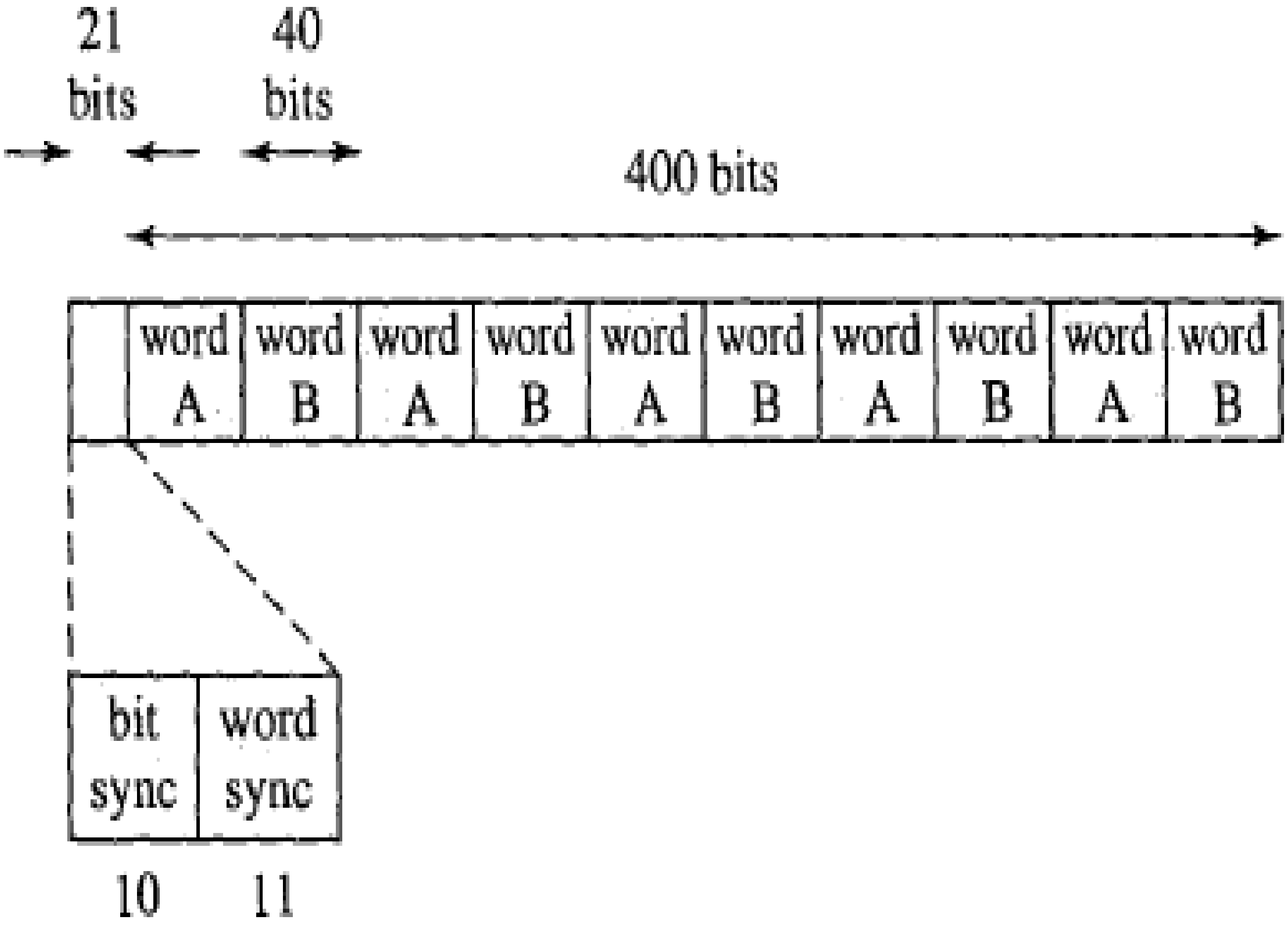
- The system uses 7-cell clusters, mostly with 120°-sector antennae, to ensure at least 18 dB of the signal-to-interference ratio
- The 30-kHz channels are divided into
  - *Forward Voice Channels* (FVC)
  - *Reverse Voice Channels* (RVC)
  - *Forward Control Channels* (FCC)
  - *Reverse Control Channels* (RCC)

AMPS Channels

- AMPS service includes 21 full-duplex 30-kHz control channels - 21 reverse control channels (RCCs) & 21 forward control channels (FCC)
- It has 395 FVC and 395 RVC



(a) Reverse control channel frame structure



(b) Forward control channel frame structure

Cloning Problem

- It has no protection from eavesdropping using a scanner.
- A hacker with a specialized equipment could intercept a handset's ESN (Electronic Serial Number) and MIN (Mobile Identification Number)
- An Electronic Serial Number is a packet of data which is sent by the handset to the cellular system for billing purposes, effectively identifying that phone on the network.
- If an ESN/MIN Pair is intercepted, it could then be cloned onto a different phone and used in other areas for making calls without paying.

Second Generation GSM

GSM Intro

- Global System for Mobile (GSM) is a 2G cellular standard.
- It is the most popular standard.
- GSM was first introduced into the European market in 1991

GSM Services

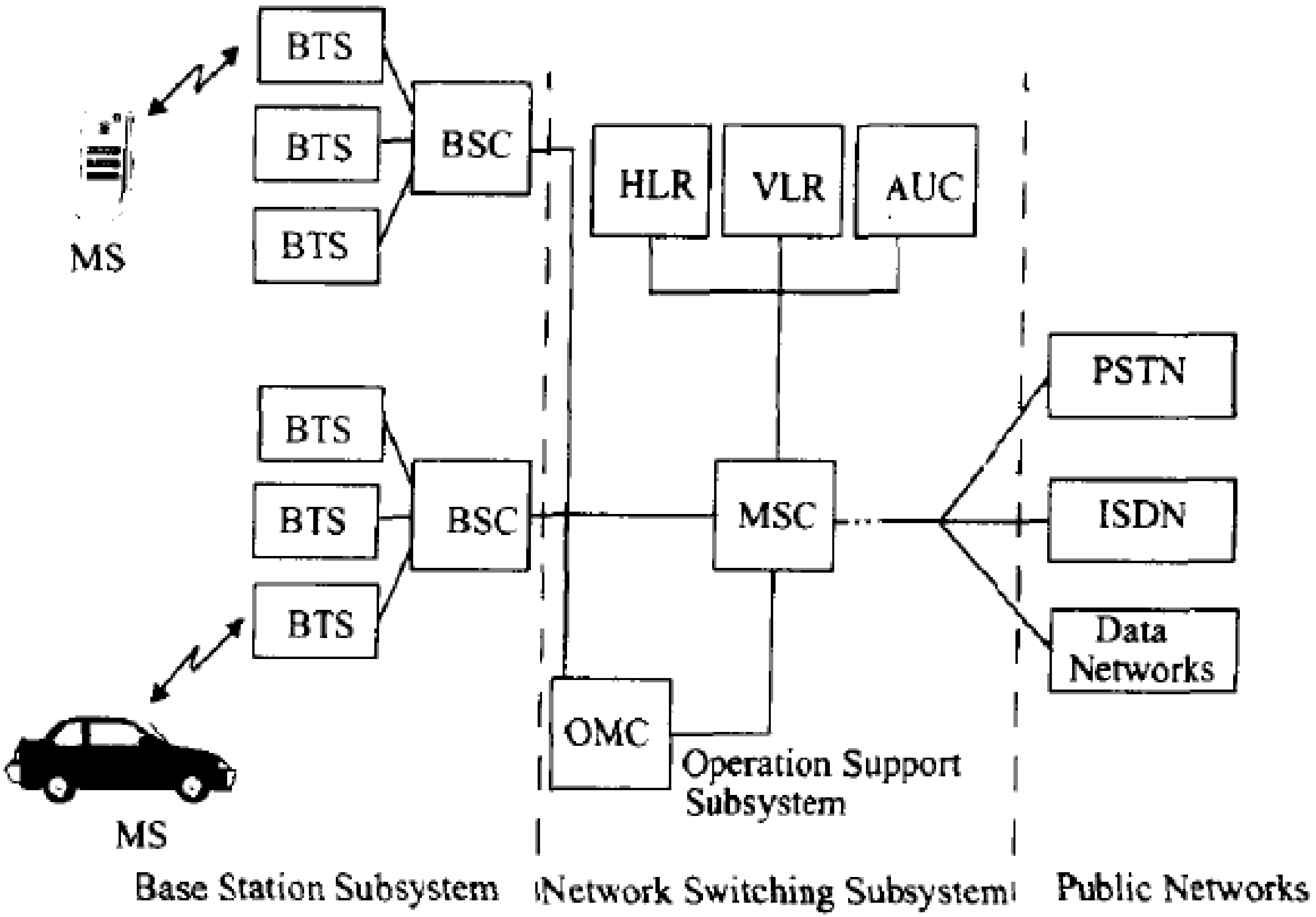
- The has 3 main services

1. Telephone services – this refers to the normal telephone services, in addition to that we have video calls and teleconferencing calls.
2. Bearer services or data services- GPRS & EDGE
3. Supplementary ISDN services- SMS, call diversion, closed user groups and caller identification

Key features

1. *Subscriber Identity Module* (SIM) - a memory device that stores all the user information
2. On air privacy- The privacy is made possible by encrypting the digital bit stream sent by a GSM transmitter. Each user is provided with a unique secret cryptographic key, that is known only to the cellular carrier. This key changes with time for each user

GSM System Architecture


BTS
BTS
BTS
BSC
MS
HLR
VLR
AUC
PSTN
BTS
BTS
BTS
BSC
MSC
ISDN
Data Networks
MS
OMC
Operation Support Subsystem
Base Station Subsystem
Network Switching Subsystem
Public Networks

GSM System Architecture

- It has 3 sub system

1. *Base Station Subsystem* (BSS),
2. *Network and Switching Subsystem* (NSS),
3. *Operation Support Subsystem* (OSS)

Base Station Subsystem (BSS)

- The Mobile Station (MS) is usually considered to be part of the BSS.
- The BSS is also known as the ***Radio Subsystem***
- BSS facilitates communication between the mobile stations and the Mobile Switching Center (MSC).
- The Mobile Stations (MS) communicate with the Base Station Subsystem (BSS) using radio air interface

- Each BSS consists of many Base Station Controllers (BSCs) which connect the MS to the Network and Switching Subsystem (NSS) via the MSCs
- Each BSC typically controls up to several hundred *Base Transceiver Stations* (BTSs).
- BTSs are connected to the BSC by microwave link or dedicated leased lines
- Handoffs between two BTSs (under same BSC)can be handled by the BSC instead of the MSC. This greatly reduces the switching burden of the MSC.

Network and Switching Subsystem (NSS)

- The NSS manages the switching functions of the system and allows the MSCs to communicate with other networks such as the PSTN and ISDN.
- The MSC is the central unit in the NSS and controls the traffic among all of the BSCs.
- Communication between the MSC and the BSS is carried out by using SS7 protocol.
- The NSS handles the switching of calls between external networks and the BSCs

- NSS maintains are three databases for switching operations.

  1. *Home Location Register* (HLR)
  2. *Visitor Location Register* (VLR)
  3. *Authentication Center* (AUC)

- The HLR contains subscriber information and location information for each user under a single MSC.
- Each subscriber is assigned a unique *International Mobile Subscriber Identity* (IMSI), and this number is used to track each user.

Visitor Location Register (VLR)

- This will oversee the operations of a ROAMING mobile.
- It temporarily stores the IMSI and customer information of the roamer.
- Once a roaming mobile is logged in the VLR, the MSC sends the necessary information to the roamer’s HLR so that calls to the roaming mobile can be appropriately routed over the PSTN by the *roaming* user's HLR

Authentication Center

- Authentication Center is a strongly protected database which handles the authentication and encryption keys for every user in the HLR and VLR.
- The Authentication Center contains a register called the *Equipment Identity Register* (EIR) which identifies stolen or fraudulently altered phones

Short Messaging Service

- SMS is defined in the supplementary services of GSM
- It can be alphanumeric messages of up to 160 characters (140 bytes).
- It operates by making use of the existing GSM infrastructure in addition with a SMS Center(SMSC).
- The physical layer, and the logical channels of the GSM system is used to transmit the short messages
- SMS has both an instant delivery service if the destination MS is active or it can be stored and forwarded if the MS is inactive

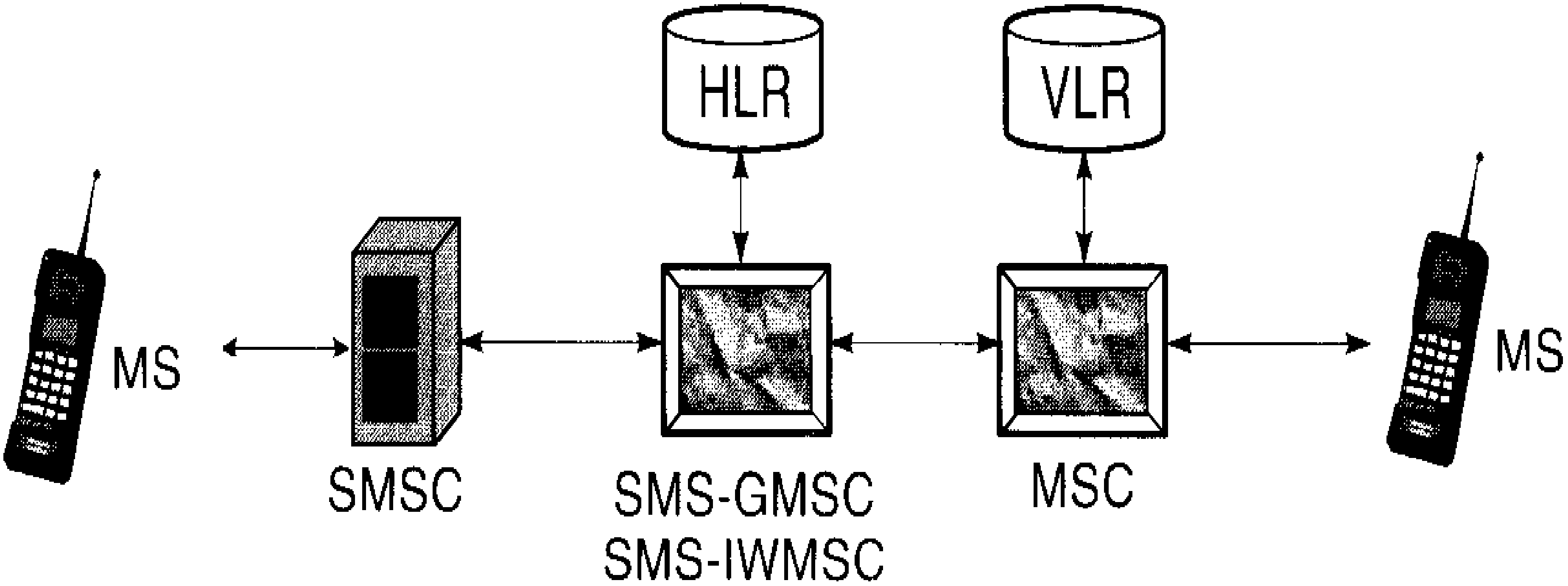
Two types of services

1. ***Cell Broadcast*** - the message is transmitted to all MSs that are active in a cell.
2. ***PTP- Peer-to-Peer –*** MS sending a message to another MS

Operation

- A short message (SM) can have a specified priority level, future delivery time, expiration time
- A sender may request acknowledgment of message receipt(Delivery Report).
- An SM will be delivered and acknowledged even when a call is in progress
- Each message is maintained and transmitted by the SMSC
- The SMSC sorts and routes the messages appropriately

Layered Architecture



- The short messages are transmitted through the GSM infrastructure using SS-7 protocol.
- A SM originating from an MS has to be first delivered to a service center.
- A dedicated function in the MSC called the ***SMS-interworking MSC*** (SMS-IWMSC) allows the forwarding of the SM to the SMSC using a global SMSC ID.
- *The **SMS-gateway MSC*** (SMS- GMSC) functions as an delivery point for the SM to reach the MS
  - it either queries the HLR or sends it to the SMS-GMSC function at the home MSC of the recipient

There are four layers in SMS

1. **The application layer (AL)-** can generate and display the alphanumeric message
2. **The transfer layer (TL)** - exchange SMs and receive confirmation of receipt of SMs. It can obtain a delivery report or status of the SM sent in either direction
3. **The relay layer (RL) -** relays the SMS through the LL.
4. **The link layer (LL) –** Manages the routing process

Transmission

- The SMs are transmitted in time slots that are freed up in the control channels.
- If the MS is in an idle state the short messages are sent over the Standalone Dedicated Control Channels (SDCCH) at 184 bits within approximately 240 ms.
- If the MS is in the active state (i.e., it is handling a call), the SDCCH is used for call set-up and maintenance
- In that case, the Slow Associated Control Channel *(*SACCH) has to be used for delivering the SM at around 168 bits every 480ms and this is much slower.

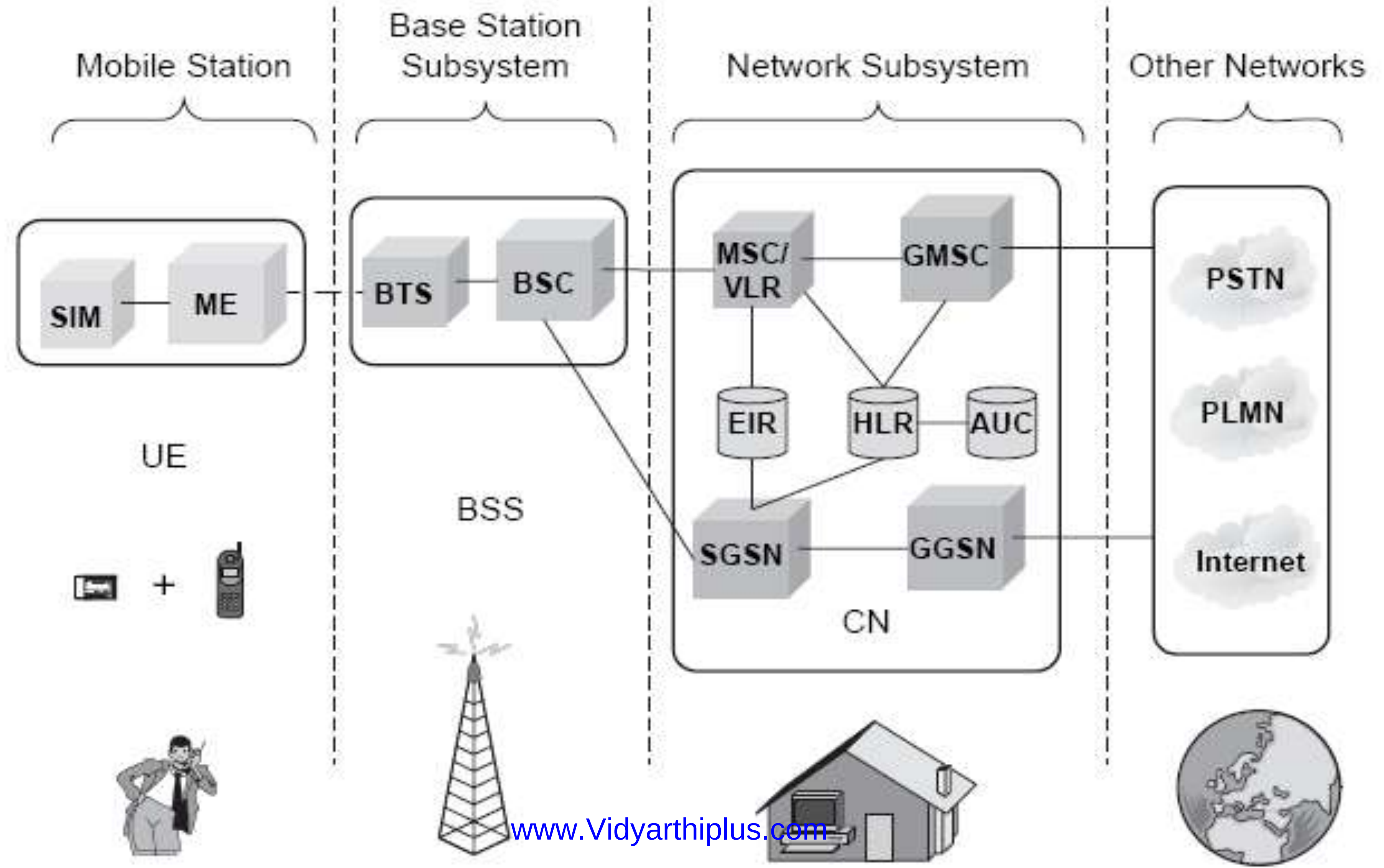
Cell Broadcast

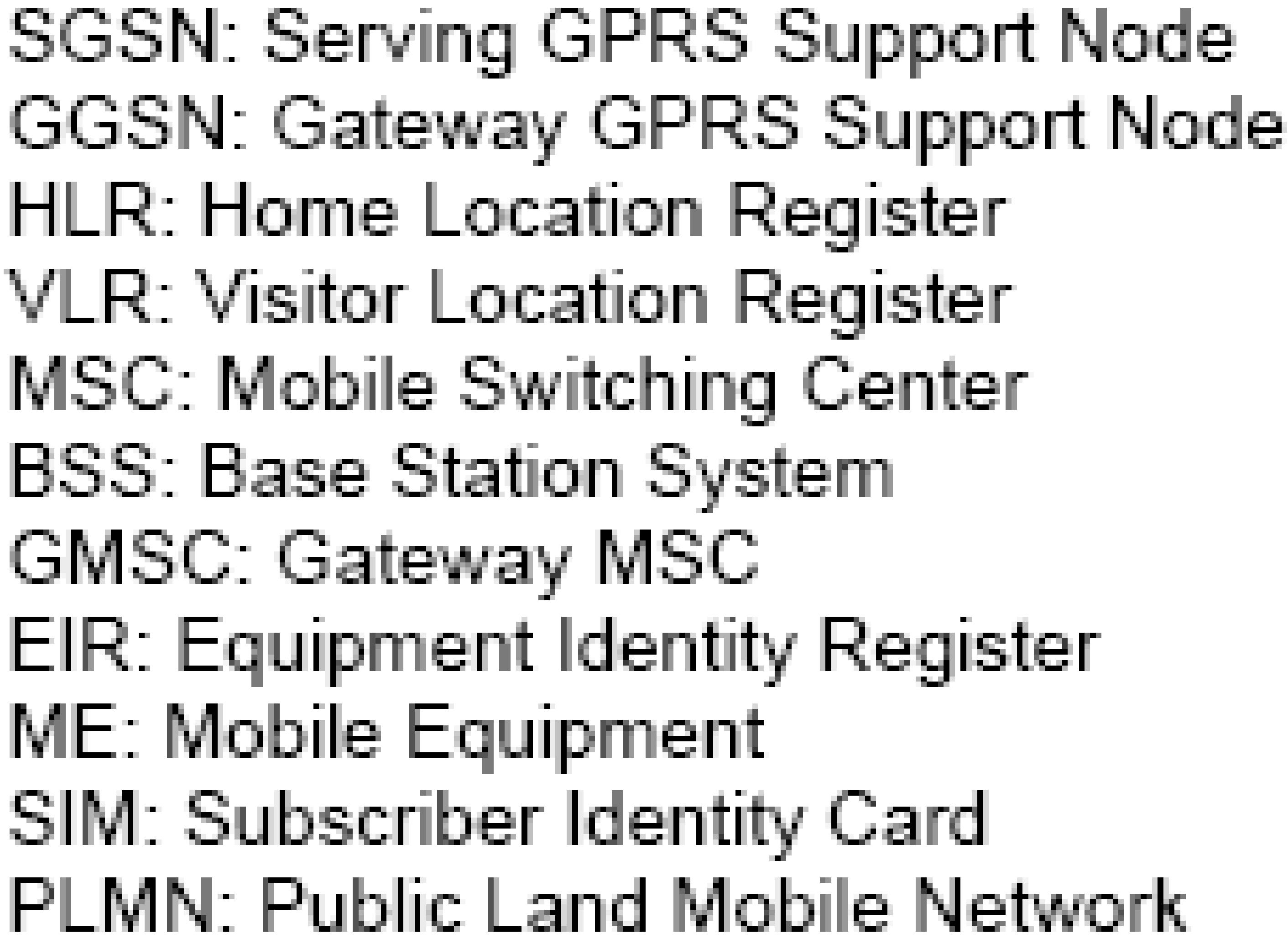
- In the case of cell broadcast, a cell broadcast entity and a cell broadcast center are used to send to multiple BSCs for delivery.
- The broadcasts contain the data and identities of mobiles that are to receive the message.
- The cell broadcast uses the Cell Broadcast Control Channel (CBCH).

General Packet Radio Service (GPRS)

- General packet radio service (GPRS) enhances GSM data services.
- It is specified as a 2.5 G standard
- Data transmission is in the form of short bursts(Packet Switching)
- GPRS does not require any dedicated end-to-end connection
- Radio bandwidth can be shared efficiently among many users simultaneously using multiplexing.
- This doesn’t need any extra installation of infrastructure.

GPRS Architecture





SGSN: Serving GPRS Support Node
GGSN: Gateway GPRS Support Node
HLR: Home Location Register
VLR: Visitor Location Register
MSC: Mobile Switching Center
BSS: Base Station System
GMSC: Gateway MSC
EIR: Equipment Identity Register
ME: Mobile Equipment
SIM: Subscriber Identity Card
PLMN: Public Land Mobile Network

- GPRS using TCP/IP and X.25 to offer speeds up to 115 kbps
- GPRS can be implemented in the existing GSM systems with minimal up-gradation (*GPRS backbone system (GBS))*
- The GBS is composed of the SGSN and the GGSN
- The implementation of GPRS has only a limited change on the GSM core network
- It simply requires the addition of new packet data switching and gateway nodes.
- GPRS supports all widely used data communications protocols, including IP.

BSS Operations

- The base station subsystem (BSS) consists of a base station controller (BSC) and packet control unit (PCU).
- The PCU supports all GPRS protocols for communication over the air interface.
- Its function is to set up, supervise, and disconnect packet switched calls.
- The base station transceiver (BTS) is a relay station without protocol functions. It performs modulation and demodulation

NSS Operations

- Two types of services are provided by GPRS:
  - Point-to-point (PTP)
  - Point-to-multipoint (PTM)
- The GPRS standard introduces two new nodes,
  - Serving GPRS Support Node (SGSN)
  - Gateway GPRS Support Node (GGSN)
- The home location register (HLR) is enhanced with GPRS subscriber data and routing information

Functions of GGSN

- Transfer within the Public Land Mobile Network (PLMN) is supported by the GPRS support node (GGSN).
- The GGSN acts as a logical interface to external packet data networks.
- Within the GPRS networks, protocol data units (PDUs) are encapsulated at the originating GSN and decapsulated at the destination GSN.
- IP is used to transfer PDUs, this process is referred to as tunneling in GPRS

- The GGSN provides the gateway to the external IP network, handling security and accounting functions.
- The GGSN contains routing information for the attached GPRS users.
- The GGSN also maintains routing information used to tunnel the data packets to the SGSN that is currently serving the mobile station (MS).

- All GPRS user related data required by the SGSN to perform the routing and data transfer functionality is stored within the HLR.
- Subscriber and equipment information is shared between GPRS and the switched functions of GSM by the use of a common HLR and coordination of data between the visitor location register (VLR) and the GPRS support nodes of the GBS.
- The GBS is composed of the SGSN and the GGSN

Functions of SGSN

- The SGSN serves the mobile and performs security and access control functions.
- The SGSN is connected to the BSS via frame-relay
- The SGSN provides packet routing, mobility management, authentication, and ciphering to and from all GPRS subscribers located in the SGSN service area.

IS-95 (CELLULAR-CDMA)

Intro

- Cellular CDMA is officially termed as Interim Standard 95 (IS-95), it is the first CDMA-based digital cellular standard by Qualcomm.
- The brand name for IS-95 is cdmaOne.
- CDMA-3G is CDMA2000

- IS-95 allows each user within a cell to use the same radio channel, and users in adjacent cells also use the same radio channel, since this is a direct sequence spread spectrum CDMA system.
- CDMA completely eliminates the need for frequency reuse.

- Each IS-95 channel occupies 1.25 MHz of spectrum on each one-way link.
- IS-95 uses a different modulation and spreading technique for the forward and reverse links.
- On the forward link, the base station simultaneously transmits the user data for all mobiles in the cell by using a different spreading sequence for each mobile.
- A pilot code is transmitted simultaneously and at a higher power level to all mobiles to synchronize with the carrier frequency.

- On the reverse link, all mobiles respond in an asynchronous fashion and have ideally a constant signal level due to power control applied by the base station.
- Received power is controlled at the base station to avoid Near-Far Problem.

Speech Coder

- The speech coder used in the IS-95 system is the Qualcomm 9600 bps Code Excited Linear Predictive (QCELP) coder
- Intermediate user data rates of 2400 and 4800bps are also used for special purposes
- QCELP13 uses 13.4 kbps of speech data .

CDMA Frequency

450MHz
BS receiver(Uplink): 450.0
BS sender(downlink): 460.0

800MHz
BS receiver(Uplink): 825.0
BS sender(downlink):870.0

1900MHz
BS receiver(Uplink): 1850.0
BS sender(downlink):1930.0

In India

- Reverse Link → 824 - 849 MHz band
- Forward Link →869 - 894 MHz
- A forward and reverse channel pair is separated by 45 MHz
- The maximum user data rate is 9.6 kb/s
- Channel Chip Rate of 1.2288 Mchip/s

Spreading and Modulation

IS-95 uses three types of spreading codes:

1. Walsh codes.
2. Short spreading codes,
3. Long spreading codes,

Walsh codes

- Walsh codes are strictly orthogonal codes that can be constructed systematically using

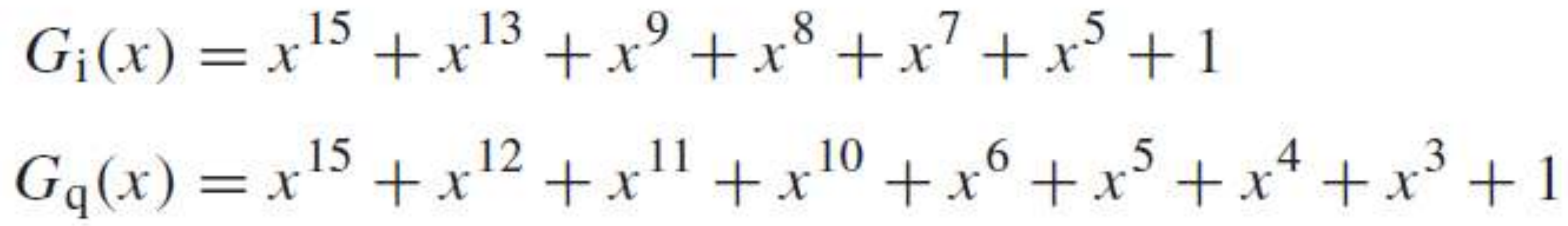
  Walsh–Hadamard matrix

$$\mathbf{H}_{\mathrm{had}}^{(n+1)} = \begin{pmatrix} \mathbf{H}_{\mathrm{had}}^{(n)} & \mathbf{H}_{\mathrm{had}}^{(n)} \\ \mathbf{H}_{\mathrm{had}}^{(n)} & \overline{\mathbf{H}}_{\mathrm{had}}^{(n)} \end{pmatrix}$$

- **Short spreading codes**

→are PN-sequences, generated with a shift register of length 15

This has two arms, I and Q and their generator polynomial is



$$G_{\mathrm{i}}(x) = x^{15} + x^{13} + x^{9} + x^{8} + x^{7} + x^{5} + 1$$

$$G_{\mathrm{q}}(x) = x^{15} + x^{12} + x^{11} + x^{10} + x^{6} + x^{5} + x^{4} + x^{3} + 1$$

Long Spreading Codes

→PN-sequences generated using shift registers having length 42

The generator polynomial is

$$G_1 = x^{42} + x^{35} + x^{33} + x^{31} + x^{27} + x^{26} + x^{25} + x^{22} + x^{21} + x^{19} + x^{18} + x^{17} + x^{16} + x^{10} + x^{7} + x^{6} + x^{5} + x^{3} + x^{2} + x^{1} + 1$$

Spreading and Modulation

- The source data rate of 8.6 kbit/s or 13.3 kbit/s is converted to a chip rate of 1.2288 Mchip/s
- Encoding is usually done with standard convolutional encoders.
- Spreading is done with “M-ary orthogonal keying” or multiplication by spreading sequences

Channels

Power Control Subchannel

- IS-95 strives to force each user to provide the same power level at the base station receiver to eliminate Near- Far Problem.
- Since both the signal and interference are continually varying, power control updates are sent by the base station every 1.25 ms.

- Power control commands are sent to each subscriber unit on the forward control subchannel which instruct the mobile to raise or lower its transmitted power in 1 dB steps.
- If the received signal is low, a ‘0' is transmitted over the power control subchannel, thereby instructing the mobile station to increase its mean output power level.
- If the mobile's power is high, a ‘1’ is transmitted to indicate that the mobile station should decrease its power level

Pilot Signal

- Each BS sends out a pilot signal that the MS can use for timing acquisition, channel estimation, and to help with the handover process.
- It is not power controlled
- It uses Walsh code 0 for transmission: this code is the all-zero code.
- It has higher transmit power than traffic channels

Synchronization Channel

- The synchronization channel transmits information about system details that are required for the MS to synchronize itself to the network.
- The synchronization channel transmits data at 1.2 kbit/s.

Paging Channel

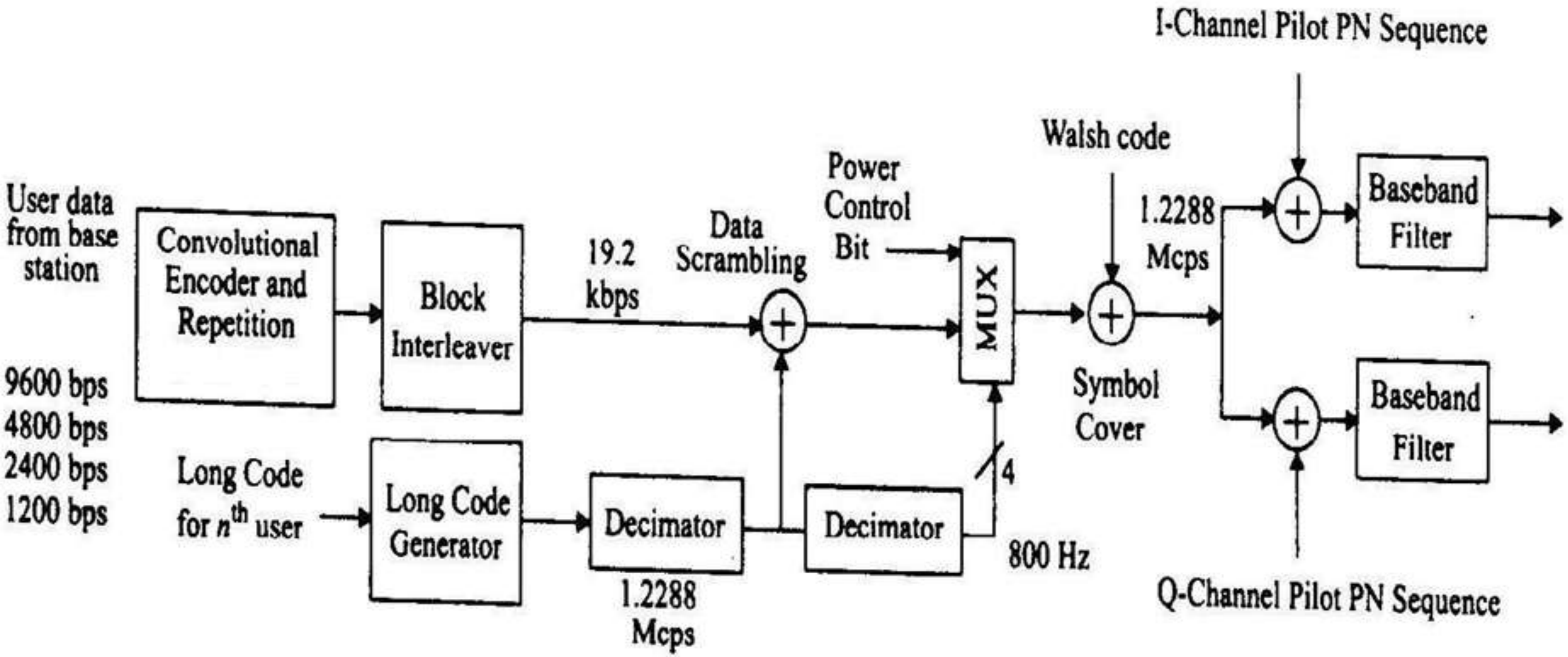
- The paging channel transmits system and call information from the BS to the MS like…
  - Message to indicate incoming call
  - System information and instructions
  - Handoff thresholds
  - Maximum number of unsuccessful access attempts
  - Channel assignment messages.
  - Acknowledgments to access requests.

Traffic Channels

- RAW User data-
  - 9.6kbps
  - 4.8 kbps
  - 2.4 kbps
  - 1.2 kbps
- After encoding - 19.2 kbps

Forward CDMA Channel

Forward CDMA channel



- The forward CDMA channel consists of a **pilot channel**, a **synchronization channel,** up to seven **paging channels**, and up to sixty-three forward **traffic channels**
- The pilot channel allows a mobile station to acquire timing for the Forward CDMA channel & provides a phase reference for coherent demodulation
- It also provide signal strength comparisons between base stations for determining when to handoff.
- The synchronization channel broadcasts synchronization messages to the mobile stations and operates at 1200 bps

- The paging channel is used to send control information and paging messages from the base station to the mobiles and operates at 9600, 4800, and 2400 bps
- The forward traffic channel (FTC) supports variable user data rates at 9600, 4800, 2400, or 1200 bps.

Convolutional Encoder and Repetition Circuit

- Data on the forward traffic channel is grouped into 20 ms frames.
- The user data is first convolutionally coded and then formatted and interleaved to adjust for the actual user data rate.
- The user data is encoded to baseband symbol rate of 19.2 kbps.
- Whenever the user rate is less than 9600 bps, each symbol from the convolution encoder is repeated before block interleaving.

- If the information rate is 4800 bps, each code symbol is repeated 1 time
- The repetition results in a constant coded rate of 19,200 symbols per second for all possible information data rates.

Block Interleaver

- After convolution coding and repetition, symbols are sent to a 20ms block interleaver, which is a 24 by 16 array.
- This is used to preserve a complete block of data.
- Data is fed row wise and read column wise.

Long PN Sequence

- In the forward channel, direct sequence is used for data scrambling.
- The long PN sequence is uniquely assigned to each user, and it is a periodic long code with period 2^{42}-1 chips
- The initial state of the generator is '1' after following 41 consecutive '0' outputs

- Data scrambling is performed after the block interleaver.
- The 1.2288 MHz PN sequence is applied to a decimator, which keeps only the first chip out of every sixty-four consecutive PN chips.
- The symbol rate from the decimator is 19.2 kbps
- The data scrambling is performed by modulo-2 addition of the interleaver output with the decimator output symbol
- The function of decimator is to down sample the 1.2288Mchps long code to 19.2 kbps sequence.

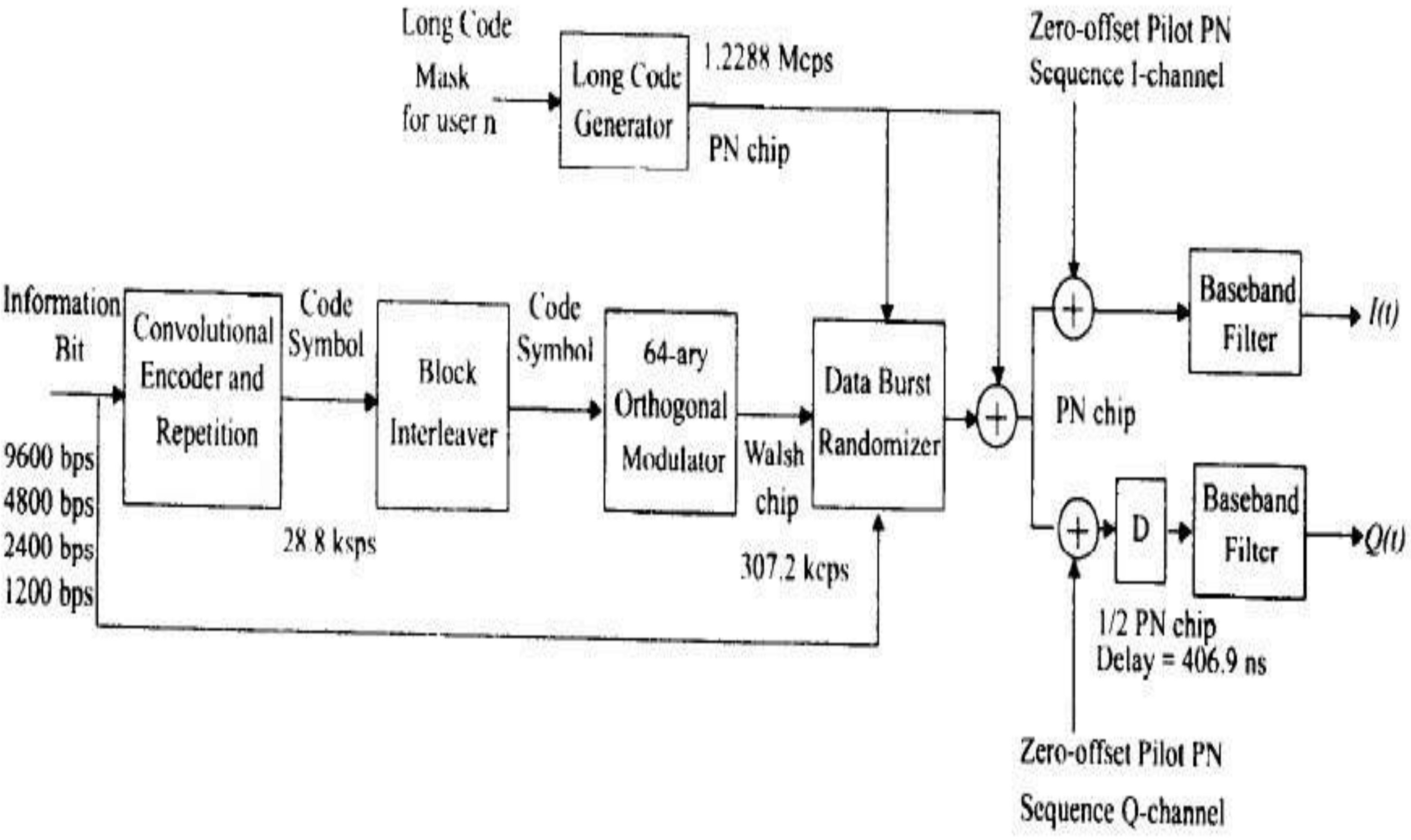
Orthogonal Covering

- The next step in the process is the DS-SS function, which spreads the 19.2 kbps to a rate of 1.2288 Mbps using one row of the 64x64 Walsh matrix.
- The Walsh functions comprise of 64 binary sequences, each of length 64, which are completely orthogonal to each other and provide orthogonal channelization for all users on the forward link.

Modulation

- The final bit rate is 1.2288 Mbps.
- This digital bit stream is then modulated onto the carrier using a **QPSK modulation** scheme.
- The data are split into I and Q (in-phase and quadrature) channels
- The data in each channel are XORed with a unique short code.
- The short codes are generated as pseudorandom numbers from a 15-bit long shift register

Reverse CDMA Channel



- The Reverse CDMA channels are made up of
  - Access Channels (AC)
  - Reverse Traffic Channels (RTC)

Access Channels (AC)

- The access channel is used by the mobile to initiate communication with the base station and to respond to paging channel messages.
- The access channel is a random access channel with each channel user uniquely identified by their long codes.
- The Reverse CDMA channel may contain a maximum of 32 Access Channels per supported paging channel
- The Reverse Traffic Channels operates on a variable data rate, the access channel works at a fixed data rate of 4800 bps.

- User data on the reverse channel are grouped into 20 ms frames.
- All data transmitted on the reverse channel are convolutionally encoded, block interleaved, modulated by a **Offset-QPSK modulation**

- Coded bits after the convolutional encoder are repeated before interleaving when the data rate is less than 9600 bps. This is identical to the method used on the forward channel. After repetition, the symbol rate out of the coder is fixed at **28,800 bps**
- The block interleaver is an array with 32 rows and 18 columns where code symbols are written into the matrix by columns and read out by rows

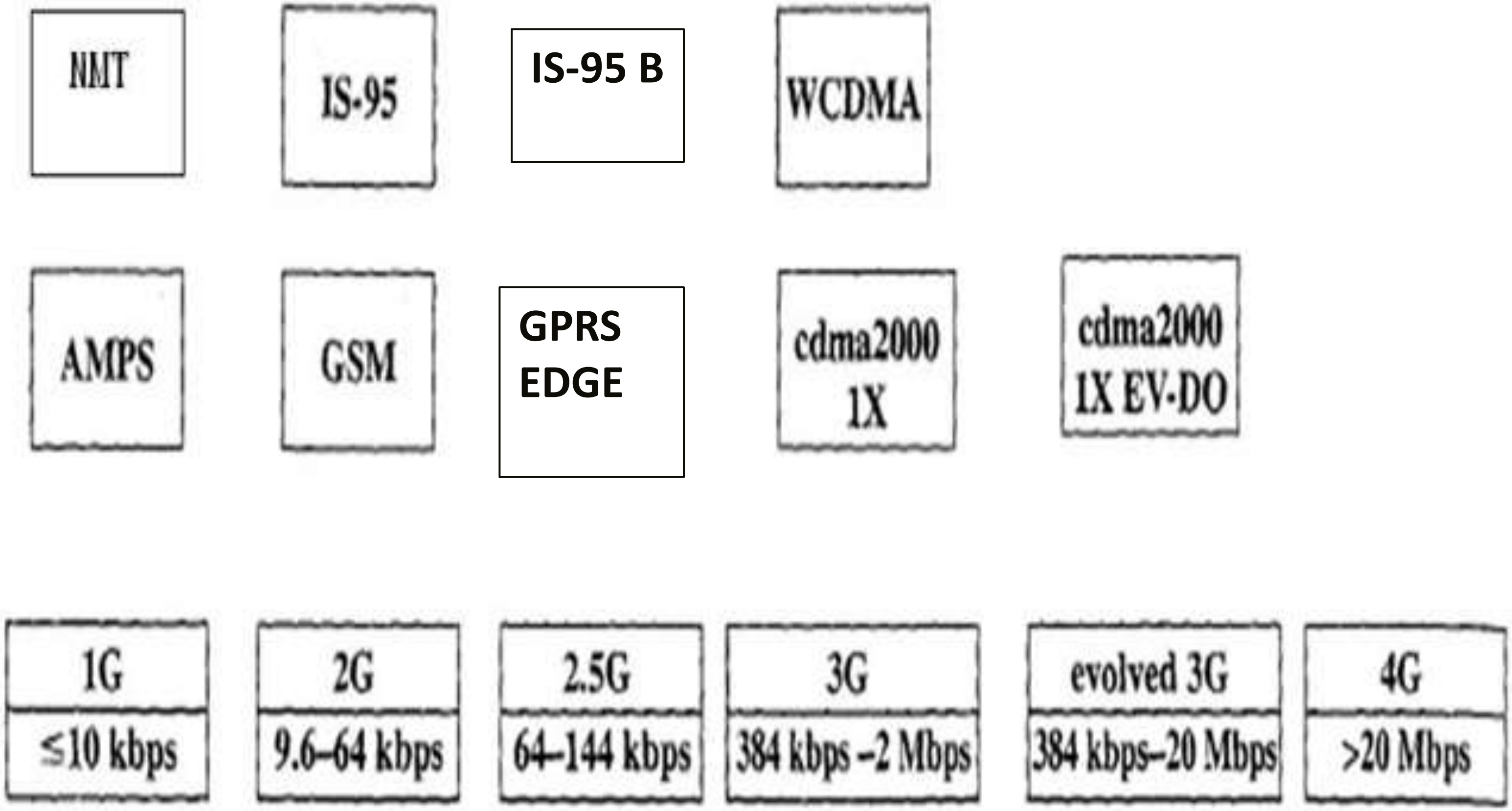
- On the reverse channel the Walsh functions are used for data modulation.
- A data randomizer is used to transmit certain bits while turning the transmitter off at other times.
- The data burst randomizer ensures that every repeated code symbol is transmitted exactly once
- The data burst randomizer generates a masking pattern of'0's and 'l's that randomly masks the redundant data generated by the code repetition process. This is called as Gating Off.

- When the data rate is 9600 bps, all interleaver output bits are transmitted.
- When the data rate is 4800 bps, half of the interleaver output bits are transmitted, and the mobile unit does not transmit 50% of the time

Spreading & Modulation

- The reverse traffic channel is spread by the long code PN sequence which operates at a rate of 1.2288 Mcps
- Prior to transmission, the reverse traffic channel is spread by I and Q channel pilot PN sequences which are identical to those used in the forward CDMA channel process.
- These pilot sequences are used for synchronization purpose.
- The reverse link modulation is **offset quadrature phase shift keying (OQPSK)**

Third Generation



1G	2G	2.5G	3G	evolved 3G	4G
≤10 kbps	9.6–64 kbps	64–144 kbps	384 kbps –2 Mbps	384 kbps–20 Mbps	>20 Mbps
NMT	IS-95	IS-95 B	WCDMA		
AMPS	GSM	GPRS EDGE	cdma2000 1X	cdma2000 1X EV-DO	

Evolution of Cellular Wireless Systems

- 2.5 G GSM- EDGE & GPRS
- 2.5 G CDMA – IS 95B
- 3G GSM- W-CDMA or UMTS (Universal Mobile Telecommunications Service) http://en.wikipedia.org/wiki/W-CDMA
- 3G CDMA- CDMA 2000 - 1xEV-DO (Evolution-Data Optimized)

- The data transfer rates for third generation mobile telecommunications is much more than 2G or 2.5 G
- You can conduct Video-conferencing
- Good Voice quality
- You can use map and positioning services
- You can play multiplayer games with co-players across the globe, right on your cell phone
- You can do online shopping, online banking.
- You can watch Online streaming and TV in your mobile

- The prices of 3G handsets and mobile units are relatively the same
- 144 kbps data rate available to users in high-speed motor vehicles over large areas
- 384 kbps available to pedestrians standing or moving slowly over small areas

Design Considerations

- **Bandwidth:**
  - An important design goal for all 3G systems is to limit channel usage to 5 MHz
- **Chip rate:** A chip rate of 3 Mcps
  - a **chip** is a pulse of a (DSSS) code.
  - The chip rate of a code is the number of pulses per second
- **Multirate:**
  - The system should be able to carry data with multiple rates.

Universal Mobile Telecommunications System

Universal Mobile Telecommunications System(UMTS)

- **UMTS** is a third generation mobile cellular technology for networks based on the GSM standard
- UMTS is a component of the International Telecommunications Union IMT-2000 standard
- It employs wideband code division multiple access (W-CDMA) to offer greater spectral efficiency and bandwidth to mobile network operators
- UMTS requires new base stations and new frequency allocations

- UMTS supports maximum theoretical data transfer rates of 45 Mbit/s
- Users can expect a transfer rate of up 21 Mbit/s for HSDPA (High Speed Downlink Packet Access) handsets.
- These speeds are significantly faster than the 9.6 kbit/s of a single GSM and 14.4 kbit/s of CDMAOne channels.
- HSPA+, or Evolved High-Speed Packet Access provides data rates up to 168 Megabits per second (Mbit/s) to the mobile device (downlink) and 22 Mbit/s from the mobile device (uplink)

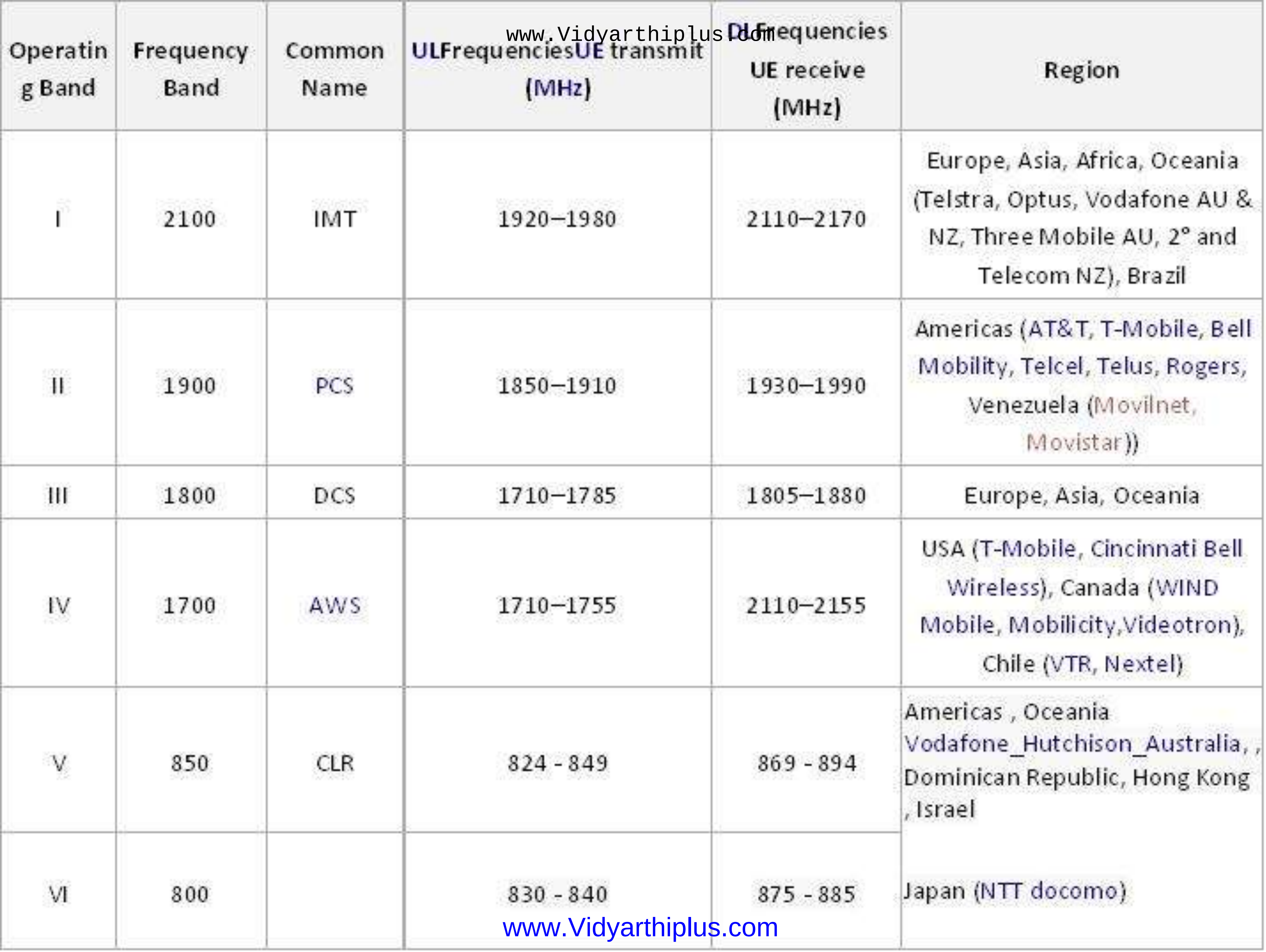
Frequency bands

- The specific frequency bands originally defined by the

  IMT - 2100 Band are

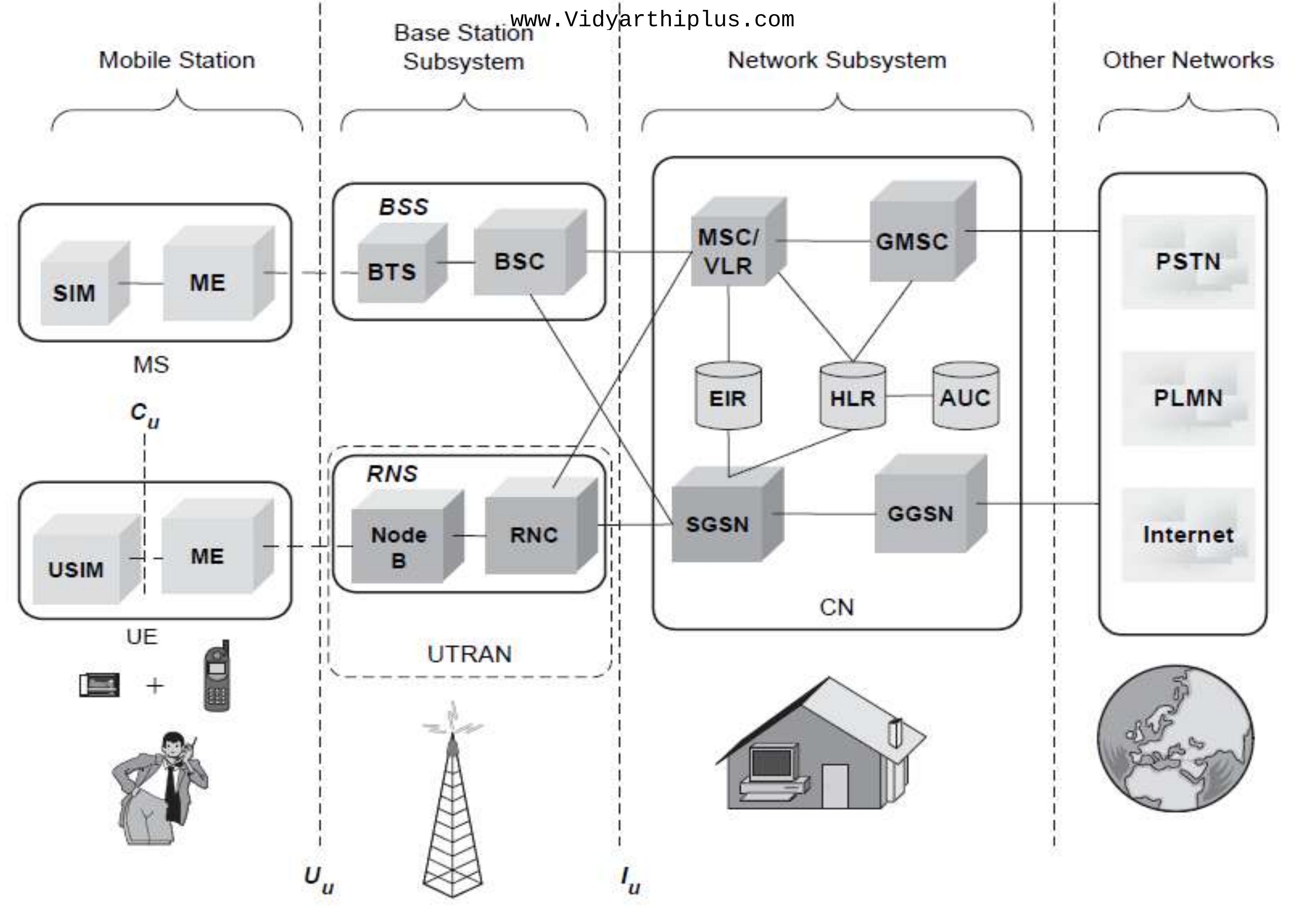
  - ➢ 1920 - 1980 MHz for the mobile-to-base (uplink)
  - ➢ 2110 – 2170 MHz for the base-to-mobile (downlink)

- But different countries uses different spectrum



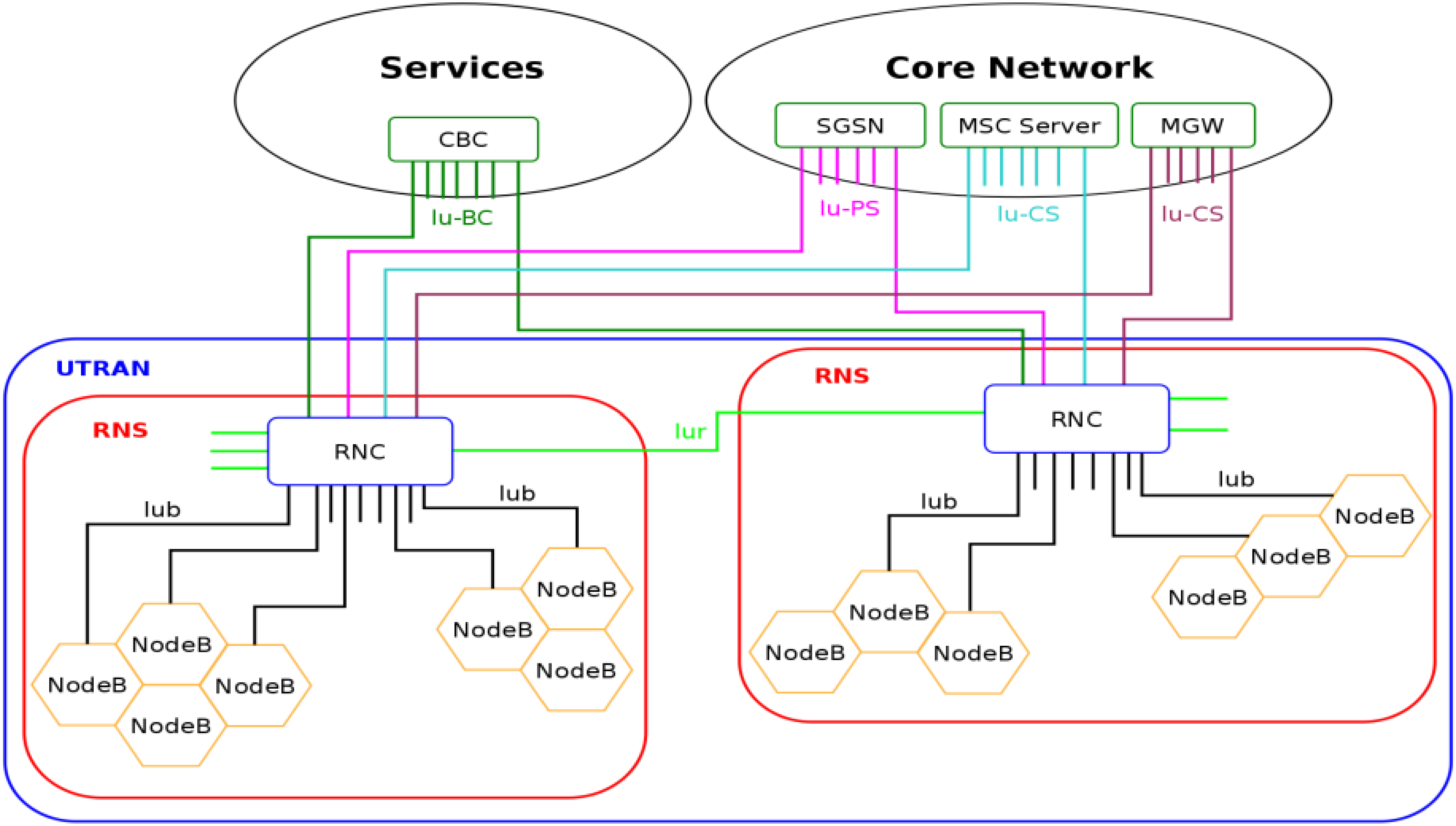
Operating Band	Frequency Band	Common Name	ULFrequenciesUE transmit (MHz)	DLFrequencies UE receive (MHz)	Region
I	2100	IMT	1920–1980	2110–2170	Europe, Asia, Africa, Oceania (Telstra, Optus, Vodafone AU & NZ, Three Mobile AU, 2° and Telecom NZ), Brazil
II	1900	PCS	1850–1910	1930–1990	Americas (AT&T, T-Mobile, Bell Mobility, Telcel, Telus, Rogers, Venezuela (Movilnet, Movistar))
III	1800	DCS	1710–1785	1805–1880	Europe, Asia, Oceania
IV	1700	AWS	1710–1755	2110–2155	USA (T-Mobile, Cincinnati Bell Wireless), Canada (WIND Mobile, Mobilicity,Videotron), Chile (VTR, Nextel)
V	850	CLR	824 - 849	869 - 894	Americas , Oceania Vodafone_Hutchison_Australia, , Dominican Republic, Hong Kong , Israel
VI	800		830 - 840	875 - 885	Japan (NTT docomo)

Architecture



UMTS—3G reference architecture.

Components and Hierarchy



- CBC - Cell Broadcast Center
- SGSN - Serving GPRS Support Node
- MGW- Media GateWay
- UTRAN- UMTS Terrestrial Radio Access Network
- RNC- Radio Network Controller
- RNS- Radio Network Subsystem
- Node B- Equivalent to the BTS (base transceiver station) in GSM

- International Mobile Telecommunications-2000 (IMT-2000)
- Public Land Mobile Network (PLMN)
- GGSN- Gateway GPRS Support Node
- GMSC- Gateway MSC
- EIR- Equipment Identity Register
- IMEI- International Mobile Station Equipment Identity
- IMSI- International mobile subscriber identity

- Universal Terrestrial Radio Access Network (UTRAN) is composed of multiple base stations using different terrestrial air interface standards and frequency bands.
- UMTS is based on an evolved GSM core network.
- UMTS and GSM/GPRS can share a Core Network (CN)
- UMTS uses a pair of 5 MHz wide channels
- UMTS provides backward compatibility with GSM in terms of network protocols and interfaces

- The core network supports both GSM and UMTS/IMT-2000 services, including handoff and roaming.
- This allows a simple migration for existing GSM operators. However, the migration path to UMTS is still costly:
- While much of the core infrastructure is shared with GSM, the cost of obtaining new spectrum licenses and overlaying UMTS at existing towers is high.
- UMTS phones are highly portable—they have been designed to roam easily onto other UMTS networks

- Almost all UMTS phones are UMTS/GSM dual-mode devices, so if a UMTS phone travels outside of UMTS coverage during a call the call may be handed off to available GSM coverage.
- UMTS phones can use a Universal Subscriber Identity Module (USIM)

Key Elements

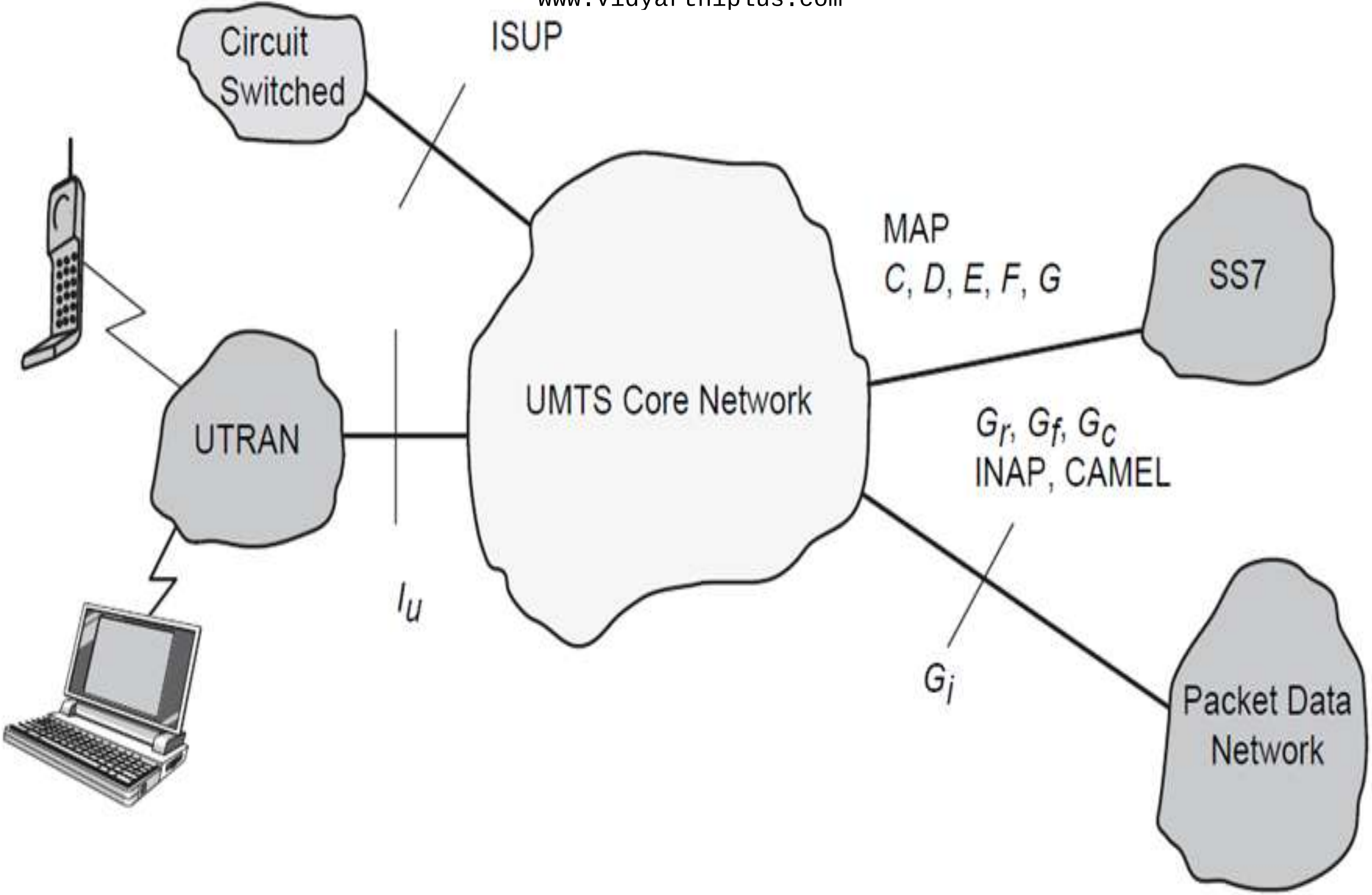
- GSM base station subsystem (BSS)
- GSM-UMTS core network (UCN)
- UMTS terrestrial radio access network (UTRAN)

Base Station Subsystem (BSS)

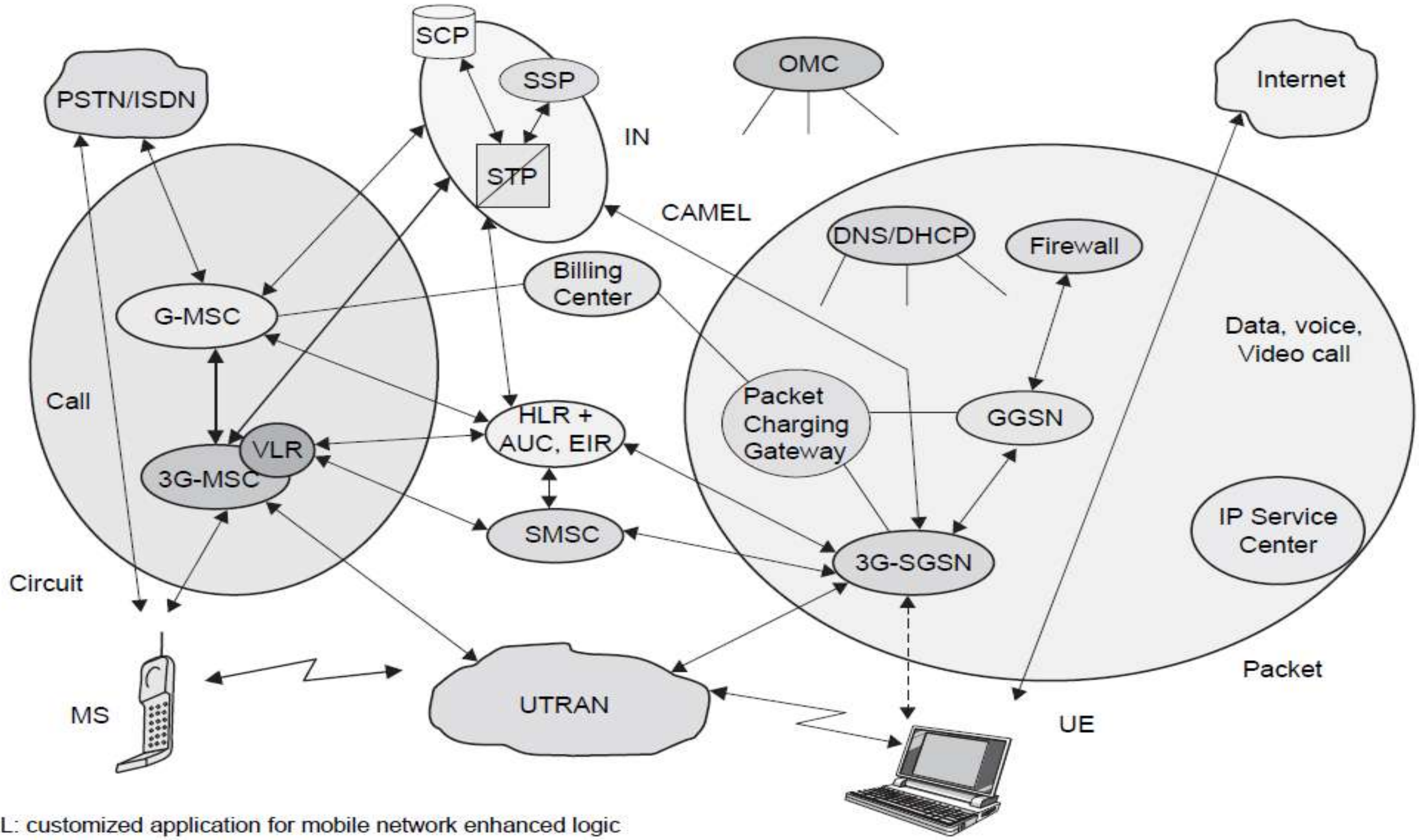
- The Mobile Station (MS) is usually considered to be part of the BSS.
- The BSS is also known as the ***Radio Subsystem***
- BSS facilitates communication between the mobile stations and the Mobile Switching Center (MSC).
- The Mobile Stations (MS) communicate with the Base Station Subsystem (BSS) using radio air interface

- Each BSS consists of many Base Station Controllers (BSCs) which connect the MS to the Network and the MSCs
- Each BSC typically controls up to several hundred *Base Transceiver Stations* (BTSs).
- BTSs are connected to the BSC by microwave link or dedicated leased lines
- Handoffs between two BTSs (under same BSC)can be handled by the BSC instead of the MSC. This greatly reduces the switching burden of the MSC.

UMTS Core Network Architecture



UMTS core network architecture.



CAMEL: customized application for mobile network enhanced logic
SMSC: short message service center
DNS: domain name server
DHCP: dynamic host configuration protocol

Logical architecture of the UMTS core network.

- The Core Network manages the switching functions of the system and allows the MSCs to communicate with other networks such as the PSTN and ISDN.
- The MSC is the central unit and controls the traffic among all of the BSCs.
- Communication between the MSC and the BSS is carried out by using SS7 protocol.
- The MSC handles the switching of calls between external networks and the BSCs

- MSC maintains are three databases for switching operations.

1. *Home Location Register* (HLR)
2. *Visitor Location Register* (VLR)
3. *Authentication Center* (AUC)

- Home Location Register (HLR)

  - A HLR contains user information such as account information, account status, user preferences, features subscribed to by the user, user's current location, etc
  - When a MSC detects a mobile user's presence in the area covered by its network, it first checks a database to determine if the user is in his/her home area or is roaming
  - Each subscriber is assigned a unique International Mobile Subscriber Identity (IMSI), and this number is used to track each user.

Visitor Location Register (VLR)

- This will oversee the operations of a ROAMING mobile.
- It temporarily stores the IMSI and customer information of the roamer.
- Once a roaming mobile is logged in the VLR, the MSC sends the necessary information to the roamer’s HLR so that calls to the roaming mobile can be appropriately routed over the PSTN by the *roaming* user's HLR

Authentication Center

- Authentication Center is a strongly protected database which handles the authentication and encryption keys for every user in the HLR and VLR.
- The Authentication Center contains a register called the *Equipment Identity Register* (EIR) which identifies stolen or fraudulently altered phones

3G-MSC

- The 3G MSC provides the interconnection to external networks like PSTN and ISDN
- Mobility management: Handles attach, authentication, updates to the HLR, SRNS relocation, and intersystem handover
- Call management: Handles call set-up messages from/to the UE.
- Supplementary services: Handles call-related supplementary services such as call waiting, etc.
- Short message services (SMS)
- VLR functionality

- SS7, MAP and RANAP interfaces: The 3G-MSC is able to complete originating or terminating calls in the network in interaction with other entities of a mobile network, e.g., HLR, AUC (Authentication center)
- Vocoding
- ATM/AAL2 Connection to UTRAN for transportation of user traffic

3G-SGSN

- The 3G-SGSN provides the necessary control functionality both toward the UE and the 3G-GGSN
- Session management: Handles session set-up messages from/to the UE and the GGSN and operates Admission Control and QoS mechanisms
- Mobility management: Handles attach, authentication, updates to the HLR and SRNS relocation, and intersystem handover.

- Subscriber database functionality: This database (similar to the VLR) is located within the 3G-SGSN and serves as intermediate storage for subscriber data to support subscriber mobility.
- Charging: The SGSN collects charging information related to radio network usage by the user.
- OAM (operation, administration, and maintenance) agent functionality

3G-GGSN

- It is connected with SGSN via an IP-based network
- Maintain information locations at SGSN level
- Gateway between UMTS packet network and external data networks (e.g. IP, X.25)
- Gateway-specific access methods to intranet
- User data screening/security can include subscription based, user controlled, or network controlled screening
- Charging: The GGSN collects charging information related to external data network usage by the user

The following network elements **can** be reused:

- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)
- Mobile Switching Center (MSC) (vendor dependent)
- Authentication Center (AUC)
- Serving GPRS Support Node (SGSN) (vendor dependent)
- Gateway GPRS Support Node (GGSN)

From Global Service for Mobile (GSM) communication radio network, the following elements **cannot** be reused

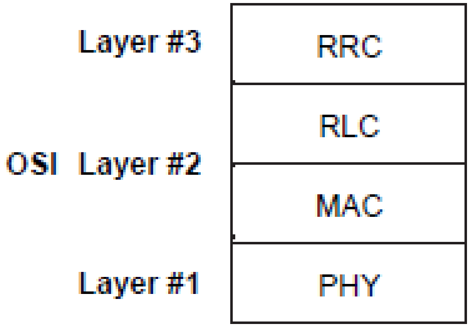
1. Base station controller (BSC)
2. Base transceiver station (BTS)

The UMTS network introduces new network elements

1. Node B (base transceiver station)
2. Radio Network Controller (RNC)
3. Media Gateway (MGW)

Channel Structure in UTRAN

- UTRAN consists of three protocol layers: physical layer, data link layer, and network layer



Layer #1:
- Physical Layer

Layer #2:
- Upper part: Radio Link Control (RLC)
- Lower part: Medium Access Control (MAC)

Layer #3:
- Lower part: Radio Resource Control (RRC)

OSI layer model and air interface protocols.

Physical layer functions

- Forward error correction, bit-interleaving, and rate matching
- Signal measurements
- Micro-diversity distribution/combining and soft handoff execution
- Multiplexing/mapping of services on dedicated physical codes
- Modulation, spreading, demodulation, despreading of physical channels
- Frequency and time (chip, bit, slot, frame) synchronization
- Fast closed-loop power control
- Power weighting and combining of physical channels
- Radio frequency (RF) processing

MAC Layer Functions

- Selection of appropriate transport format (basically bit rate)
- Service multiplexing on random access channel (RACH), forward access channel (FACH), and dedicated channel (DCH)
- Priority handling of data flow
- Access control on RACH and FACH
- Contention resolution on RACH

Radio link control (RLC) functions

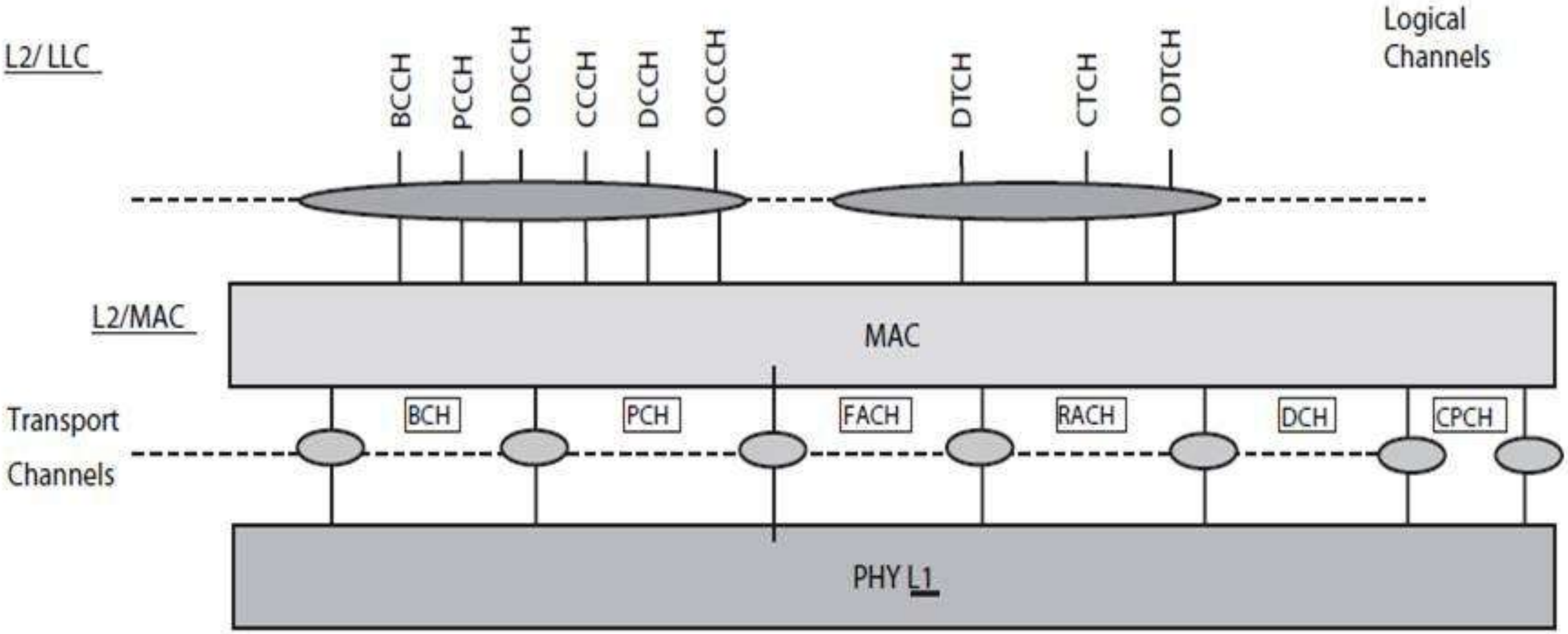
- Segmentation and assembly of the packet data unit
- Transfer of user data
- Error correction through retransmission
- Sequence integrity
- Duplication information detection
- Flow control of data

Radio resource control (RRC) functions

- Broadcasts system information,
- Handles radio resources (i.e., code allocation, handover, admission control, and measurement/control report)
  - General control (GC) service used as an information broadcast service
  - Notification (Nt) service used for paging and notification of a selected UE
  - Dedicated control (DC) service used to establish/release a connections and transfer messages

UTRAN Channels

1. **Logical channels** are used by MAC layer to provide data transport services
2. **Transport channels** offer information transfer services to the MAC layer
3. **Physical channels** are identified by code, frequency, phase and time slot (TDD only)



BCCH: Broadcast Control Channel
PCCH: Paging Control Channel
DCCH: Dedicated Control Channel
ODCCH: ODMA Dedicated Control Channel
OCCCH: ODMA Common Control Channel
DTCH: Dedicated Traffic Channel
ODTCH: ODMA Dedicated Traffic Channel
CTCH: Common Traffic Channel
CCCH: Common Control Channel

UTRAN channels.

1. Logical Channels in UTRAN

Logical control channel

a) Broadcast control channel (BCCH)

b) Paging control channel (PCCH)

c) Common control channel (CCCH)

d) Dedicated control channel (DCCH)

e) ODMA common control channel (OCCCH)

f) ODMA dedicated control channel (ODCCH)

Logical Traffic Channels

a) Dedicated traffic channel (DTCH)

b) ODMA traffic channel (ODTCH)

2. Transport Channels in UTRAN

Common transport channels

a) Broadcast channel (BCH)

b) Forward access channel (FACH)

c) Paging channel (PCH)

d) Random access channel (RACH)

e) Common packet channel (CPCH)

f) Downlink shared channel (DSCH)

Dedicated transport channels

a) Dedicated Channel (DCH)

b) Fast Uplink Signaling Channel (FAUSCH)

c) Opportunity driven multiple access dedicated channel (ODCH)

3. Physical Channel

- Dedicated physical channel (DPCH)
  - Dedicated physical data channel (DPDCH)
  - Dedicated physical control channel (DPCCH)
- Common physical channels
  - Physical random access channel (PRACH)
  - Physical common packet channel (PCPCH)

- **BCCH – Broadcast Control Channel**
  - Downlink (DL) channel for broadcasting system and control information
- **Paging control channel (PCCH)**
  - This Downlink channel is used to carry paging requests. It is used either when the network does not know the location cell of the mobile equipment, or when the mobile is in the RRC connected state (using sleep mode) procedures to preserve battery power

- **Common control channel (CCCH)**
  - CCCH is a channel used for transmitting control information between the network and mobiles, and is applicable in both the uplink and downlink directions.
  - It is commonly used by mobiles which currently have no RRC connection with the network, (idle mode) and by those accessing a new cell after cell re-selection.
- **Dedicated control channel (DCCH)**
  - DCCH is a multi-purpose, point-to-point bidirectional channel which is used to carry dedicated control information specific to a single mobile

- ODMA common control channel (OCCCH)
- ODMA dedicated control channel (ODCCH)
  - ODMA (Opportunity Driven Multiple Access) is really just a relaying protocol rather than a pure access scheme, whereby a terminal which lies outside cell coverage can use another mobile terminal as a relay to transmit to the base station
  - Both OCCCH & ODCCH are used for transmitting control information between terminals, the difference being that OCCCH carries information common to a number of terminals, whereas ODCCH is “point-to-point”, intended for a specific terminal

Logical traffic channels

- Dedicated traffic channel (DTCH)
  - Bidirectional point-to-point channel dedicated to just one mobile for the transfer of user information.
- ODMA traffic channel (ODTCH)
  - Point-to-point channel dedicated to one mobile to transfer user information between mobiles

Transport Channels

- Broadcast channel (BCH)
  - DL channel used to broadcast system and cell specific information, transmitted over the entire cell with low fixed bit rate
- Forward access channel (FACH)
  - DL channel transmitted over the entire or only a part of cell using beam-forming antennas, uses slow power control
- Paging channel (PCH)
  - DL channel transmitted over the entire cell, transmission of PCH is associated with the transmission of a physical layer signal, the paging indicator, to support efficient sleep mode procedure

- Random access channel (RACH)
  - Uplink channel characterized by a limited size data field, a collision risk, and by use of open loop power control
- Common packet channel (CPCH)
  - Uplink channel, contention-based random access channel used for transmission of bursty data traffic
- Downlink shared channel (DSCH)
  - DL channel shared by several mobiles, associated with a DCH

- Dedicated Channel (DCH)
  - Bidirectional transport channel that is used to carry user or control information between the network and the UE
- The Fast Uplink Signaling Channel (FAUSCH)
  - is an optional uplink transport channel that is used to carry control information from a user equipment.
- Opportunity driven multiple access dedicated channel (ODCH)
  - ODCH is used to relay control information to base station through other users

Physical channels

- A physical channel identified by code and frequency. They consist of radio frames and time slots
- The length of a radio frame is 10 ms and one frame consists of 15 time slots
- For DL channels two codes are used, one to identify the cell and the other to identify a particular channel within that cell.
- For UL a long code is used to identify the channel.

Uplink Dedicated Physical Channel

- Dedicated physical data channel (DPDCH)
  - Carry user data and signaling information generated at layer 2
- Dedicated physical control channel (DPCCH)
  - Carry control information generated at layer 1 (pilot bits, transmit power control (TPC) commands, feedback information (FBI) commands, and optional transport format combination indicator (TFCI))

Uplink Common Physical Channel

- Physical random access channel (PRACH)
  - used to carry the Random access channel (RACH) and fast uplink signaling channel (FAUSCH)
- Physical common packet channel (PCPCH)
  - to carry Common packet channel (CPCH)

Downlink Common Physical Channel

- **Primary common control physical channel (PCCPCH)** carries BCH, rate 30 kbps, continuous transmission; no power control
- **Secondary common control physical channel (SCCPCH)** carries FACH and PCH, transmitted when data is available
- **Synchronization channel (SCH)** is used for cell search
- **Physical downlink shared channel (PDSCH)** carries DSCH; shared by users based on code multiplexing; associated with DPCH.
- **Acquisition indicator channel (AICH)** carries acquisition indicators.
- **Page indicator channel (PICH)** carries a page for UE

Physical channels

- A physical channel identified by code and frequency. They consist of radio frames and time slots
- The length of a radio frame is 10 ms and one frame consists of 15 time slots
- For DL channels two codes are used, one to identify the cell and the other to identify a particular channel within that cell.
- For UL a long code is used to identify the channel.

Uplink Dedicated Physical Channel

- Dedicated physical data channel (DPDCH)
  - Carry user data and signaling information generated at layer 2
- Dedicated physical control channel (DPCCH)
  - Carry control information generated at layer 1 (pilot bits, transmit power control (TPC) commands, feedback information (FBI) commands, and optional transport format combination indicator (TFCI))

Uplink Common Physical Channel

- Physical random access channel (PRACH)
  - used to carry the Random access channel (RACH) and fast uplink signaling channel (FAUSCH)
- Physical common packet channel (PCPCH)
  - to carry Common packet channel (CPCH)

Downlink Common Physical Channel

- **Primary common control physical channel (PCCPCH)** carries BCH, rate 30 kbps, continuous transmission; no power control
- **Secondary common control physical channel (SCCPCH)** carries FACH and PCH, transmitted when data is available
- **Synchronization channel (SCH)** is used for cell search
- **Physical downlink shared channel (PDSCH)** carries DSCH; shared by users based on code multiplexing; associated with DPCH.
- **Acquisition indicator channel (AICH)** carries acquisition indicators.
- **Page indicator channel (PICH)** carries a page for UE

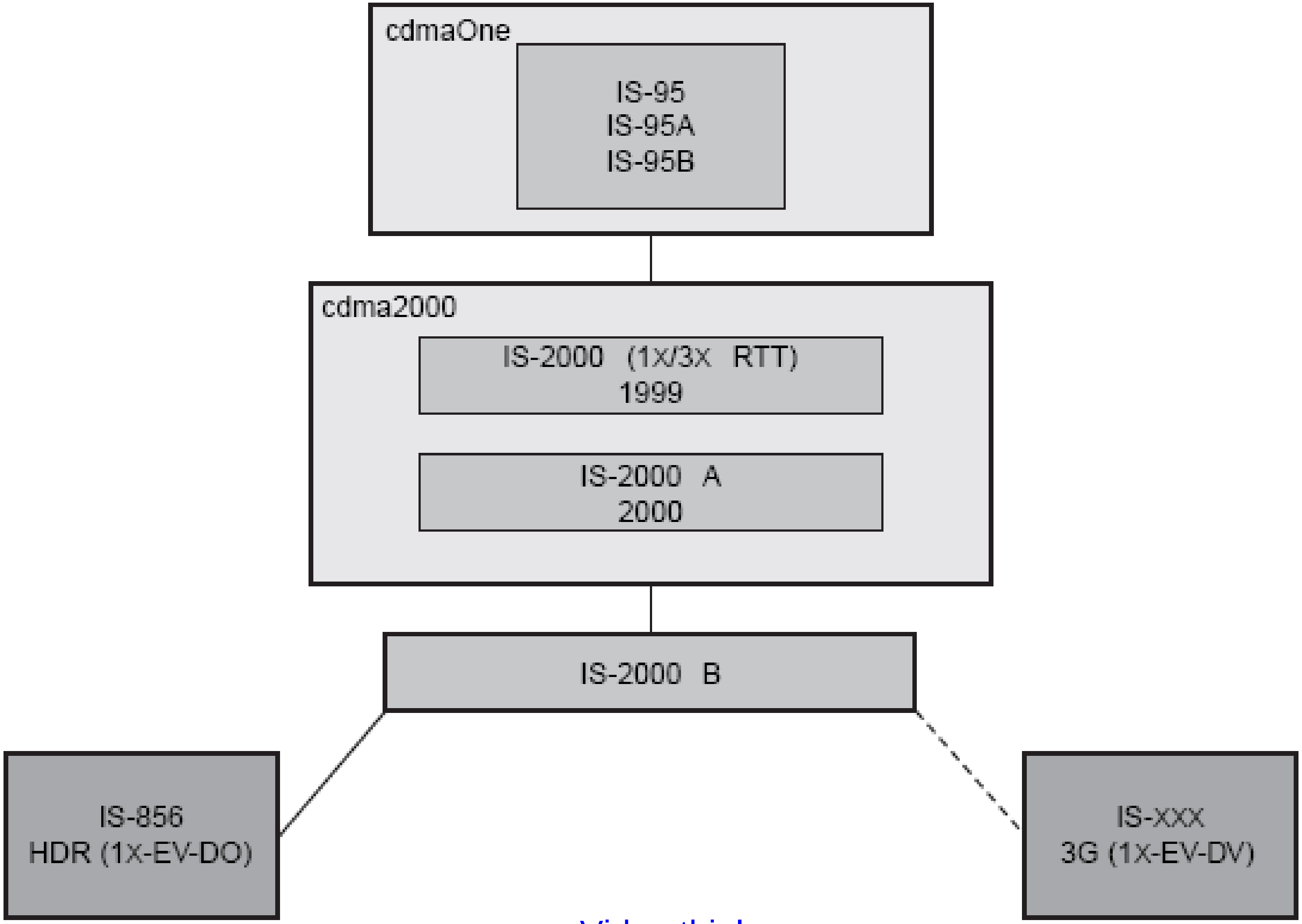
CDMA 2000 (3G- CDMA)

- The cdma2000 radio transmission technology (RTT) is a wideband, spread spectrum radio interface that uses CDMA (IS-95) technology
- The cdma2000 system is backward compatible with the current cdmaOne (IS-95) family of standards
- It uses channels of 1.25 MHz width.
- Cdma2000 reuse the existing TIA/EIA-95B standard

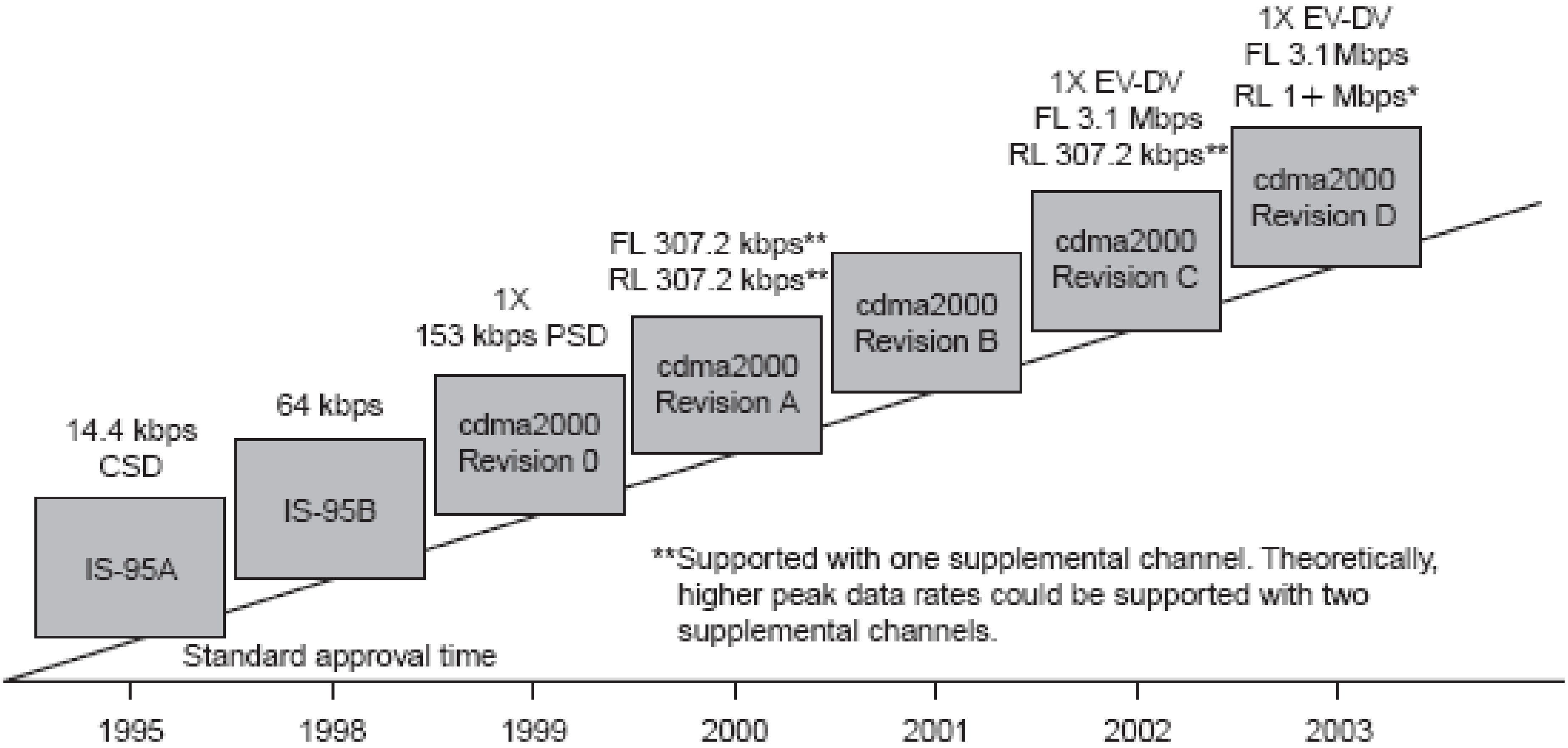
1. CDMA2000 1X,
2. 3G 1X EV-DO (evolution for data-only systems)
3. 3G 1X EV-DV (evolution for data and voice)

The designation "1x", meaning 1 times Radio Transmission Technology, indicates the same radio frequency (RF) bandwidth as IS-95.

CDMA Evolution



Data Rates



**Supported with one supplemental channel. Theoretically, higher peak data rates could be supported with two supplemental channels.

RL: Reverse Link

FL: Forward Link

CSD: Circuit Switched Data

PSD: Packet Switched Data

cdma2000 Layering Structure

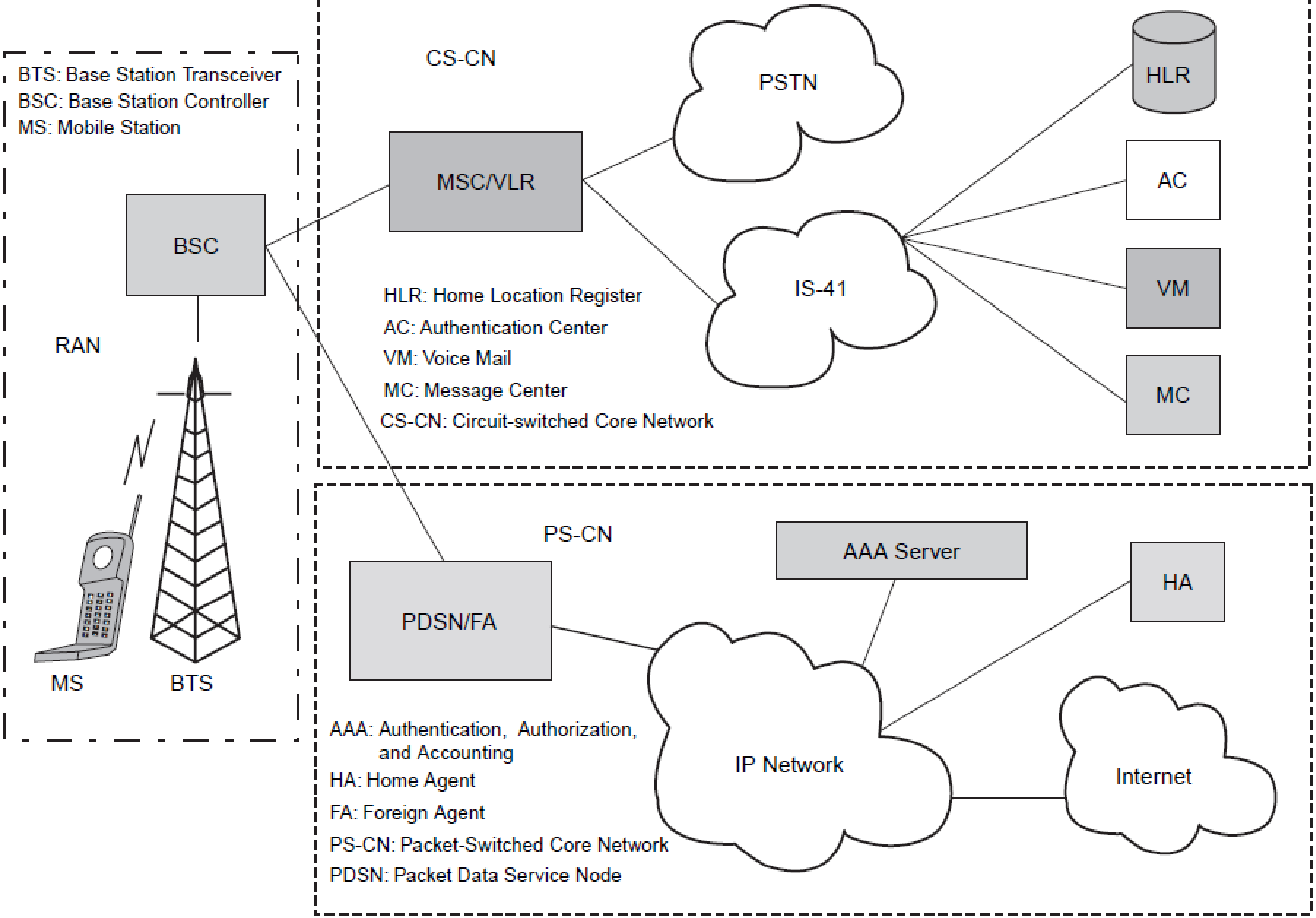
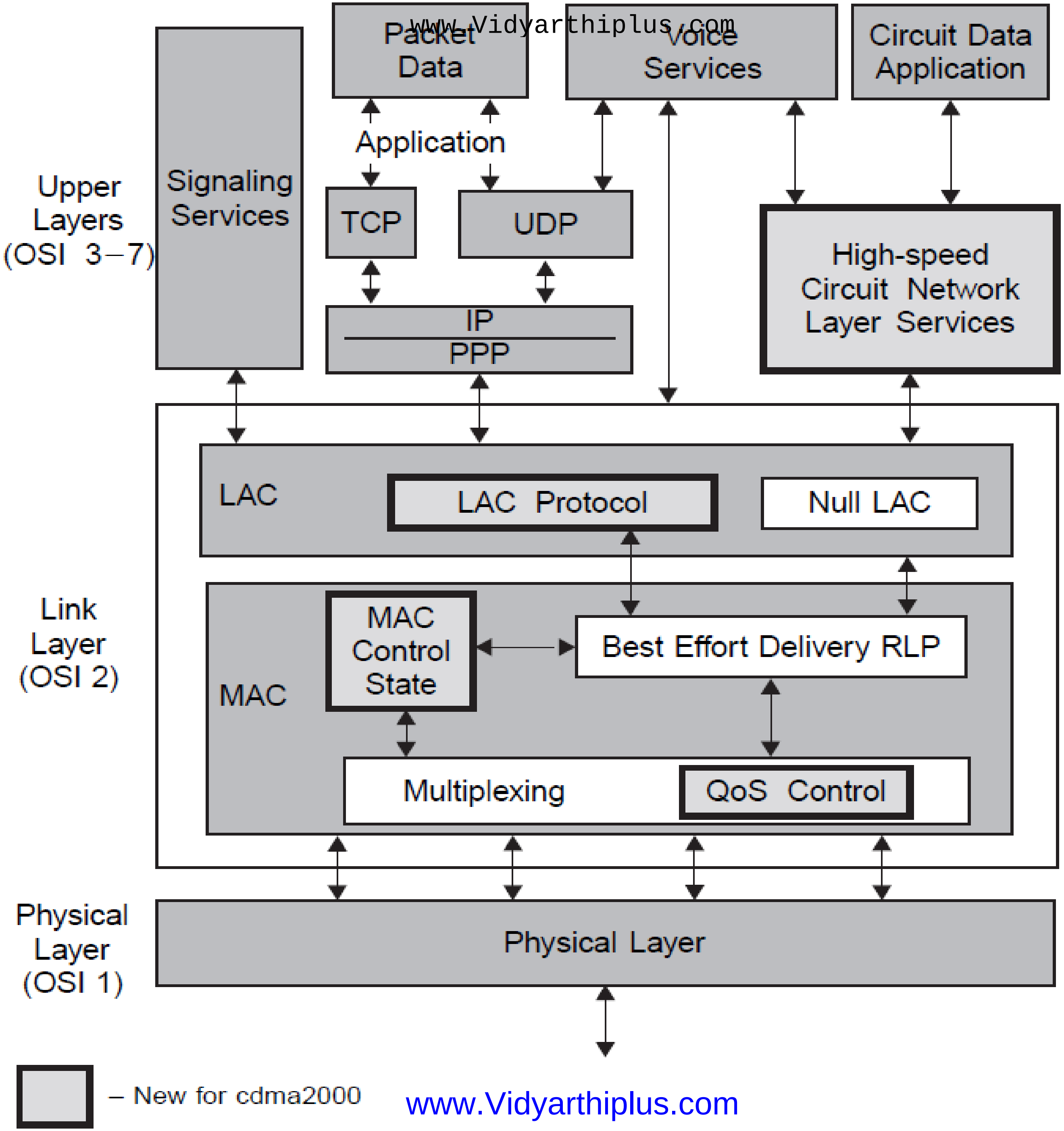

BTS: Base Station Transceiver
BSC: Base Station Controller
MS: Mobile Station
BSC
RAN
MS
BTS
CS-CN
MSC/VLR
PSTN
IS-41
HLR
AC
VM
MC
HLR: Home Location Register
AC: Authentication Center
VM: Voice Mail
MC: Message Center
CS-CN: Circuit-switched Core Network
PS-CN
PDSN/FA
AAA Server
HA
IP Network
Internet
AAA: Authentication, Authorization, and Accounting
HA: Home Agent
FA: Foreign Agent
PS-CN: Packet-Switched Core Network
PDSN: Packet Data Service Node

Figure 16.20 cdma2000 network architecture

Protocol Stack


Packet Data
Voice Services
Circuit Data Application
Upper Layers (OSI 3–7)
Signaling Services
Application
TCP
UDP
IP
PPP
High-speed Circuit Network Layer Services
LAC
LAC Protocol
Null LAC
Link Layer (OSI 2)
MAC
MAC Control State
Best Effort Delivery RLP
Multiplexing
QoS Control
Physical Layer (OSI 1)
Physical Layer
– New for cdma2000

IP: Internet Protocol

MAC: Medium Access Control

OSI: Open System Interconnect

RLP: Radio Link Protocol

UDP: User Data Protocol

LAC: Link Access Control

QoS: Quality of Service

PPP: Point-to-Point Protocol

TCP: Transmission Control Protocol

The upper layers open system interconnection (OSI layers 3–7) contain three basic services

1. **Voice services**.- Voice telephony services
2. **End user data-bearing services**. -Services that deliver any form of data on behalf of the mobile end user, including packet data and SMS .
3. **Signaling**.- Services that control all aspects of the operation of the mobile

Link Layer

- The link layer provides varying levels of reliability and QoS characteristics according to the needs of the specific upper layer service.
- It gives protocol support and control mechanisms for data transport services
- And performs all functions necessary to map the data transport needs of the upper layers into specific capabilities and characteristics of the physical layer

The link layer is divided into two sublayers:

- Link Access Control (LAC) and
- Medium Access Control (MAC)

  - The LAC sublayer manages point-to-point communication channels between peer upper layer entities and provides framework to support a wide range of different end-to-end reliable link layer protocols.

The MAC sublayer provides three important functions.

1. **MAC control state.-** Procedures for controlling the access of data service (packet and circuit) to the physical layer
2. **Best effort delivery**.- this uses the Radio Link Protocol (RLP) for providing a best level of reliability.
3. **Multiplexing and QoS control**. Enforcement of negotiated QoS levels by mediating conflicting requests from competing services and appropriately prioritizing access requests.

The MAC sub layer is subdivided into

1. Physical Layer Independent Convergence Function (PLICF)
2. Physical Layer Dependent Convergence Function (PLDCF)
   a. Instance specific PLDCF
   b. PLDCF MUX (multiplexing)
   c. QoS sublayer

PLICF

- The PLICF provides service to the LAC sublayer and includes all MAC operational procedures and functions that are not unique to the physical layer.
- PLICF uses services provided by PLDCF to implement actual communications activities in support of MAC sublayer service.

PLDCF

- The PLDCF performs mapping of logical channels from the PLICF to logical channels supported by the specific physical layer
- This performs multiplexing, demultiplexing, and consolidation of control information with bearer data.
- Perform any (optional) automatic repeat request (ARQ) protocol functions that are tightly integrated with the physical layer

PLDCF Protocols

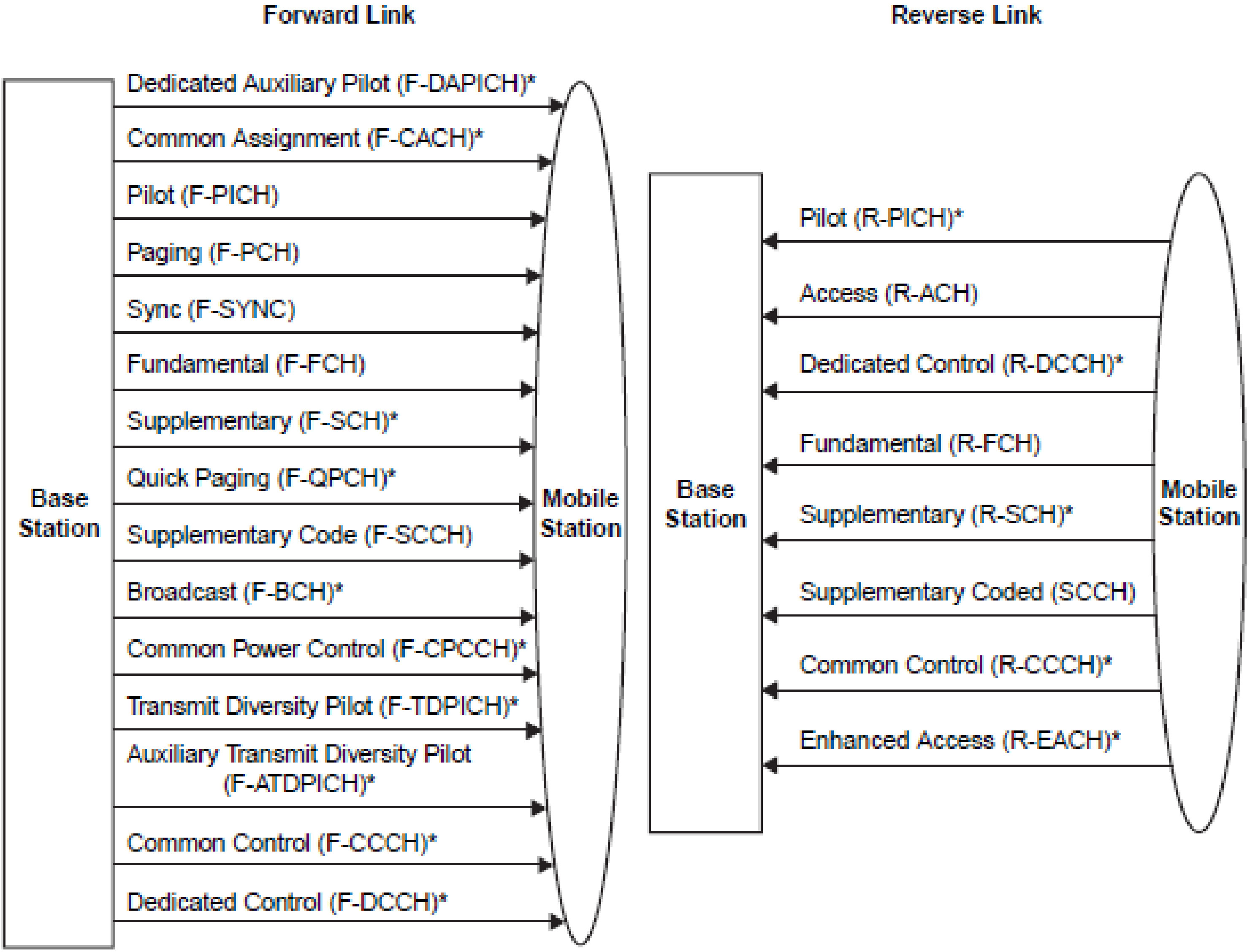
1. Radio link protocol (RLP)
2. Radio burst protocol (RBP)
3. Signaling radio link protocol (SRLP)
4. Signaling radio burst protocol (SRBP)

Radio link protocol (RLP).

- RLP provides both transparent and non transparent modes of operation.
- In the nontransparent mode, RLP uses ARQ protocol to retransmit data segments that were not delivered properly by the physical layer.
- In the transparent mode, RLP does not retransmit missing data segments.
- However, it maintains synchronization between the sender and receiver and notifies the receiver of the missing parts of the data stream. Transparent RLP does not introduce any transmission delay, and is useful for implementing voice services over RLP.

- **Radio burst protocol (RBP).** This protocol provides a mechanism for delivering relatively short data segments over a shared Access Common Traffic Channel (CTCH) .
- **Signaling radio link protocol (SRLP).** This protocol provides a best-effort streaming service for signaling the Dedicated Signaling Channel (DSCH).
- **Signaling radio burst protocol (SRBP).** This protocol provides a mechanism to deliver signaling messages through Common Signaling Channel (CSCH)

Cdma2000 Channels



Forward Link

Base Station

Dedicated Auxiliary Pilot (F-DAPICH)*

Common Assignment (F-CACH)*

Pilot (F-PICH)

Paging (F-PCH)

Sync (F-SYNC)

Fundamental (F-FCH)

Supplementary (F-SCH)*

Quick Paging (F-QPCH)*

Supplementary Code (F-SCCH)

Broadcast (F-BCH)*

Common Power Control (F-CPCCH)*

Transmit Diversity Pilot (F-TDPICH)*

Auxiliary Transmit Diversity Pilot (F-ATDPICH)*

Common Control (F-CCCH)*

Dedicated Control (F-DCCH)*

Mobile Station

Reverse Link

Base Station

Pilot (R-PICH)*

Access (R-ACH)

Dedicated Control (R-DCCH)*

Fundamental (R-FCH)

Supplementary (R-SCH)*

Supplementary Coded (SCCH)

Common Control (R-CCCH)*

Enhanced Access (R-EACH)*

Mobile Station

* New to cdma2000

cdma2000 physical channels

Forward Link Features

1. Transmit Diversity-
   - Antenna diversity can be implemented in a multicarrier forward link with no impact on the subscriber terminal, where a subset of carriers is transmitted on each antenna.
   - The rake receiver captures signal energy from all bands.
2. Orthogonal Modulation
   - To reduce or eliminate intracellular interference, each forward link physical channel is modulated by a Walsh code
3. Power Control
   - The forward link power control operates at a high rate to track and compensate accurately the fast Rayleigh fading on the forward link.

4. Walsh Code Administration
   - Cdma2000 require variable length Walsh codes for traffic channels. The Walsh codes used are from 128 chips to 2 chips in length

5. Modulation and Spreading
   - QPSK modulation is used
   - The forward link supports chip rates of N x 1.2288 Mcps (where N = 1, 3, 6, 9, 12).

Reverse Link Features

- Continuous waveform.
  - A continuous pilot and continuous data-channel waveform are used for all data rates
- Orthogonal spreading with different length Walsh sequences
- Rate matching
- Low spectral sidelobes
- Independent data channels

Reverse Link Features- Continued

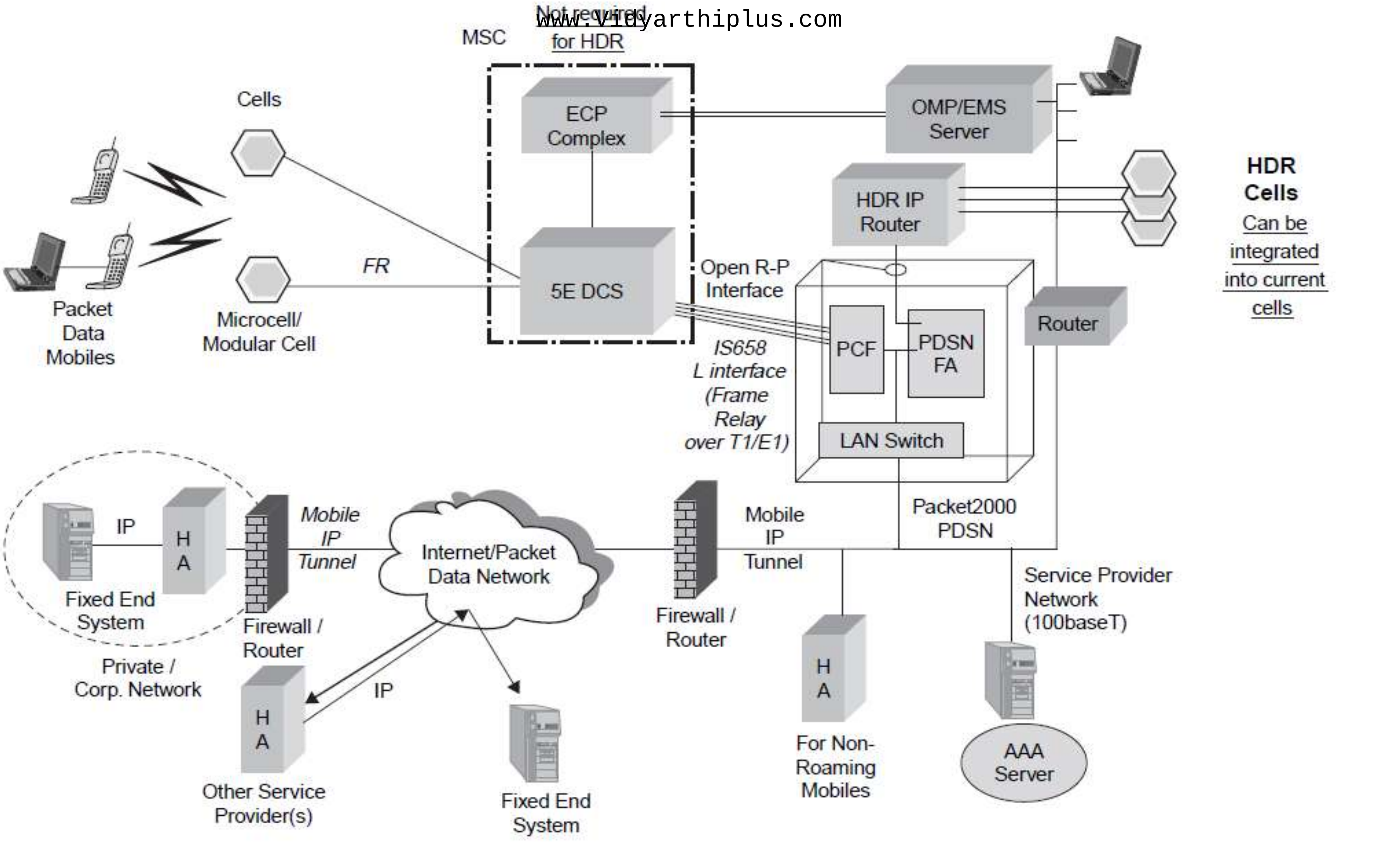
- Reverse Link Power Control
  - power control in the reverse link is to resolve the near-far problem
  - Fast reverse power control: 800 times per second
- Channels are primarily code multiplexed
- Transmission is continuous to avoid EMI
- Hybrid combination of QPSK and BPSK
- Forward error correction

CDMA 2000 1X EV-DO

cdma2000 1X EV-DO (Evolution-Data Optimized or Evolution-Data only)

- TIA/EIA-95B standard
- Telecommunications Industry Association (TIA)
- Electronic Industries Alliance(EIA)
- cdma2000 1X EV-DO is also called High Data Rate (HDR)
- This provides up to 2.4 Mbps in a 1.25 MHz channel
- Rev. A provides up to 3.1 Mbit/s
- The HDR is compatible with CDMA IS-95 networks

Architecture



AAA: Authentication, Authorization, Accounting
HA: Home Agent
PCF: Packet Control Function
PDSN: Packet Data Switching Node

FR: Frame Relay
MSC: Mobile Switching Center
HDR: High Data Rate

HDR and cdma2000 1X mobile IP architecture.

HDR network has three key elements:

1. Radio nodes (RNs),
2. Radio network controller (RNC),
3. Packet data serving node (PDSN)

- Each radio node has three sectors and serves one cell site.
- A dedicated transceiver in each sector will provide the HDR airlink between the user equipment (UE) and RN.
- Higher layers of the HDR protocol are processed at the RNC.
- The RNC also manages handoffs and passes user data between the RNs and the PDSN.
- The PDSN is a wireless edge router that connects the radio network to the Internet.

- HDR data center has an aggregation router, an element manager system (EMS), and several Internet service provider (ISP) servers.
- The aggregate router terminates IP traffic from the RNs and passes it to the RNC.
- The EMS manages the radio access network with commonly used ISP servers.
- It includes standard Domain Name Server (DNS), Dynamic Host Configuration Protocol (DHCP) and Authentication, Authorization, and Accounting (AAA)

Uplink & Downlink

- The downlink frames destined for same sector are time division multiplexed (TDM).
- The downlink rate can vary between 38.4 kbps and 2.4 Mbps.
- The uplink uses CDMA
- On the uplink, subscribers can transmit at data rates ranging from 9.6 to 153.6 kbps.

Comparison of HSDPA and cdma2000 1X EV-DO.

Features	HSDPA	cdma2000 1× EV-DO
Downlink frame size	2 ms transmission time interval (TTI) (3 slots)	1.25, 2.5, 5, 10 ms variable frame size (1.25 ms slot size)
Channel feedback	Channel quality reported at 2 ms rate or 500 Hz	SNR feedback at 800 Hz (every 1.25 ms)
Data user multiplexing	TDM/CDM	TDM/CDM (variable frame)
Adaptive modulation and coding	QPSK and 16-QAM mandatory	QPSK, 8-PSK and 16-QAM
Hybrid ARQ	Incremental redundancy	Async. incremental redundancy
Spreading factor (SF)	SF = 16 using OVSF channelization codes	Walsh code length 32
Control channel approach	Dedicated channel pointing to shared channel	Common control channel

Cdma2000 1X EV-DV

Evolution Data and Voice

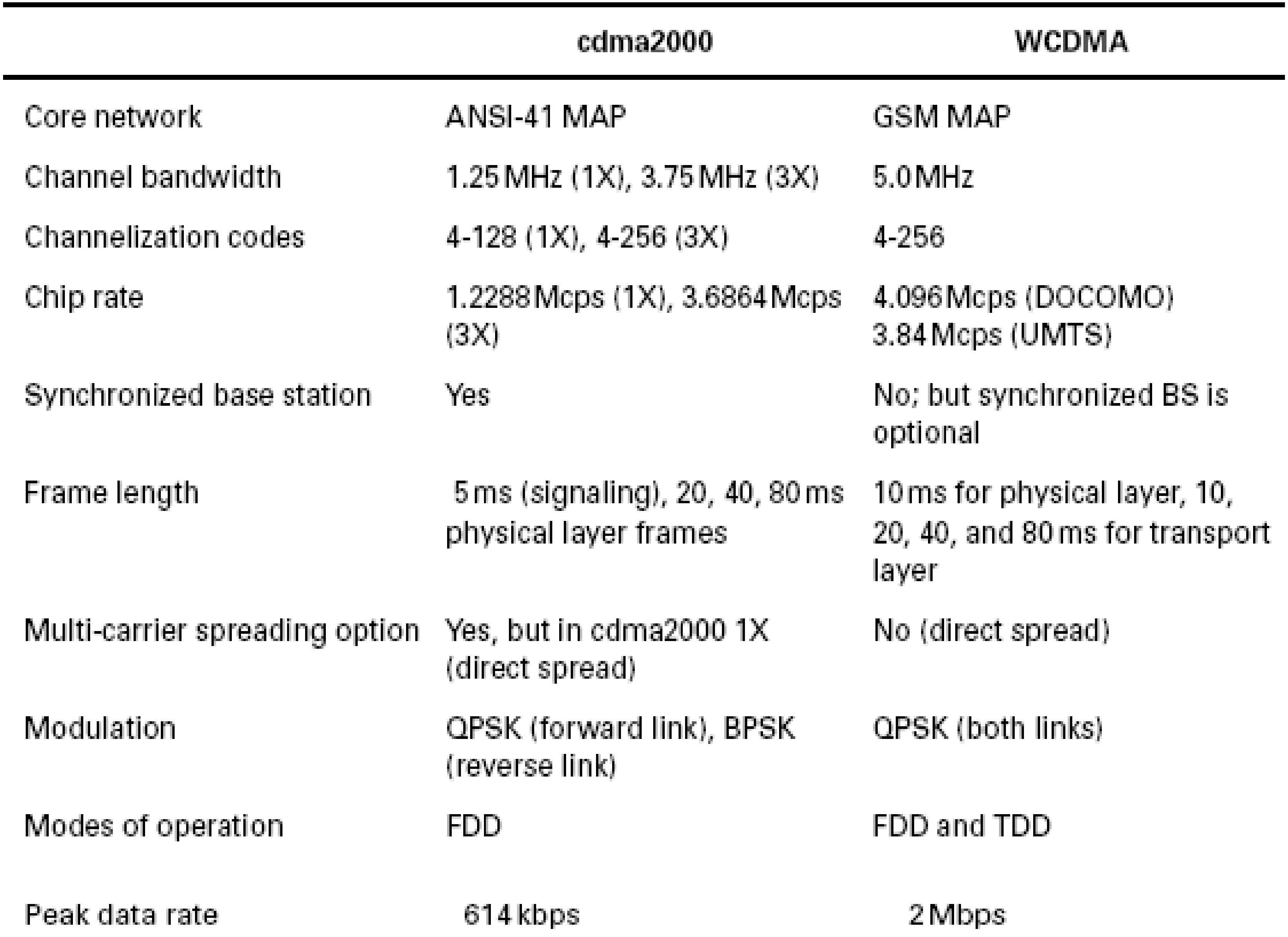
- EV-DV is part of the same family of CDMA connectivity as EV-DO.
- However, EV-DV also supports voice calls.
- EV-DV is a combination of EV-DO and 1xRTT
- The cdma2000 1X EV-DV system is designed to deliver greater spectrum usage efficiencies, backward compatibility for all previous versions of IS-95 and cdma2000

- The cdma2000 1X EV-DV delivers a peak data rate of 3.09 Mbps & and up to 451.2 kbps peak in reverse link.
- The cdma2000 1X EV-DV specifications incorporate three new control channels and one new traffic channel
  – Forward Packet Data Channel (F-PDCH).

1. Forward Packet Data Control Channel (F-PDCCH),
2. Reverse Channel Quality (R-CQICH),
3. REVERSE ACK CHANNEL (R-ACKCH)

Features

1. Forward link capacity.
   - use time division multiplexing (TDM) and code division multiplexing (CDM)
2. Backward compatibility
3. Concurrent voice and data
   - supports voice and data in same channel
4. Hybrid ARQ
5. Adaptive modulation and coding
6. Cell selection
   - the handset can select the best serving sector



	cdma2000	WCDMA
Core network	ANSI-41 MAP	GSM MAP
Channel bandwidth	1.25 MHz (1X), 3.75 MHz (3X)	5.0 MHz
Channelization codes	4-128 (1X), 4-256 (3X)	4-256
Chip rate	1.2288 Mcps (1X), 3.6864 Mcps (3X)	4.096 Mcps (DOCOMO) 3.84 Mcps (UMTS)
Synchronized base station	Yes	No; but synchronized BS is optional
Frame length	5 ms (signaling), 20, 40, 80 ms physical layer frames	10 ms for physical layer, 10, 20, 40, and 80 ms for transport layer
Multi-carrier spreading option	Yes, but in cdma2000 1X (direct spread)	No (direct spread)
Modulation	QPSK (forward link), BPSK (reverse link)	QPSK (both links)
Modes of operation	FDD	FDD and TDD
Peak data rate	614 kbps	2 Mbps