Chapter 1

- **Unit I**
- **Fundamentals of Mobile Communication:** Introduction to mobile communication systems, GSM architecture and subsystems, Mobile network components, GSM frame structure and channel types, Overview of GSM and GPRS architecture, Call setup and mobility management, Handoff types and algorithms.

Introduction to Wireless Communication

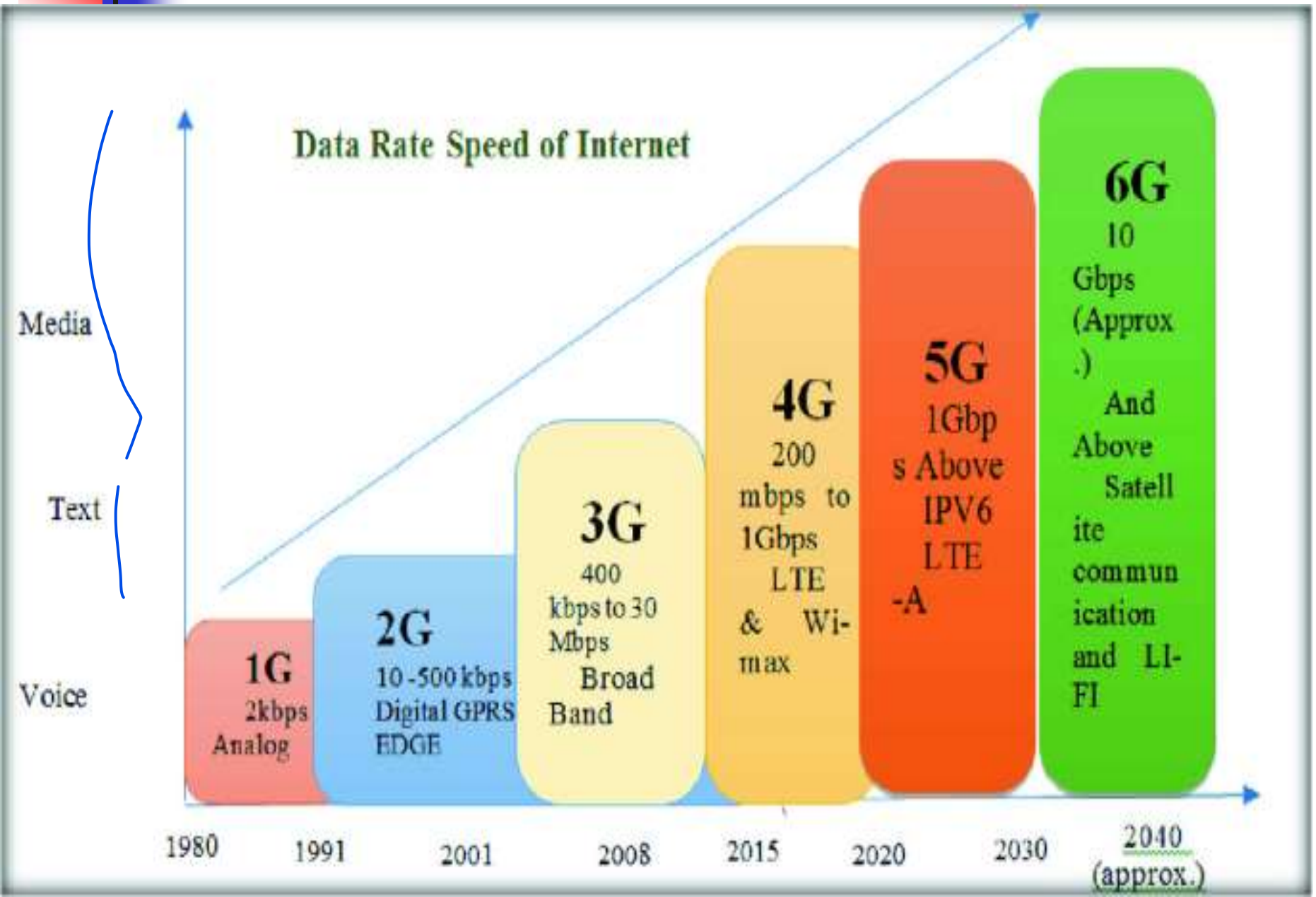
1. **Definition:**
   - Wireless communication is the transfer of information between two or more points that are not physically connected by an electrical conductor. Instead, it uses electromagnetic waves to transmit signals over the air.
2. **How It Works:**
   - Data is converted into electromagnetic signals and transmitted via antennas.
   - The receiving antenna captures these signals, which are then converted back into usable data.
3. **Examples of Wireless Technologies:**
   - **Cellular Networks**: Mobile phones use a network of cell towers to communicate.
   - **Wi-Fi**: Wireless local area networks (WLANs) that connect devices to the internet without cables.

- **Bluetooth**: Short-range communication between devices, such as phones and headphones.
- **Satellite Communication**: Long-distance wireless communication using satellites in orbit.

The Evolution of Wireless Communication

Bullet Points:

1. Historical Development:
   - 1G (Analog voice) → 2G (Digital voice, SMS) → 3G (Mobile internet) → 4G (High-speed data, video streaming) → 5G (Ultra-fast speeds, IoT, low-latency)
2. From Analog to Digital:
   - Early wireless communication systems were analog, but digital systems became dominant due to better quality, security, and efficiency.
3. Current Trends:
   - 5G and Beyond: The rise of the Internet of Things (IoT), smart cities, and connected vehicles.


Data Rate Speed of Internet
Media
Text
Voice
1G
2kbps
Analog
2G
10 -500 kbps
Digital GPRS
EDGE
3G
400
kbps to 30
Mbps
Broad
Band
4G
200
mbps to
1Gbps
LTE
& Wi-
max
5G
1Gbp
s Above
IPV6
LTE
-A
6G
10
Gbps
(Approx
.)
And
Above
Satell
ite
commun
ication
and LI-
FI
1980
1991
2001
2008
2015
2020
2030
2040
(approx.)

Advantages of Wireless Communication

1. Mobility:
    - Users can communicate from almost anywhere, enhancing freedom and convenience.
2. Cost-Effectiveness:
    - Eliminates the need for physical cables, reducing infrastructure costs in large-scale networks.
3. Scalability:
    - Easily extend networks without complex and costly rewiring.

Challenges in Wireless Communication

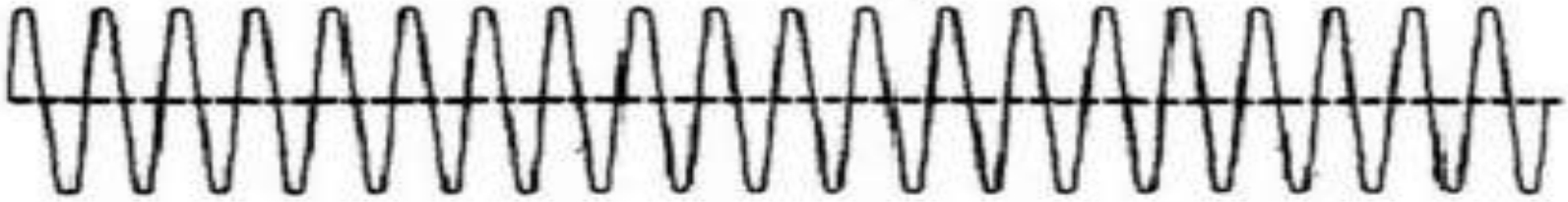
1. **Interference:**
   - Wireless signals are susceptible to interference from other devices or environmental factors (buildings, weather).
2. **Bandwidth Limitations:**
   - Limited frequency spectrum leads to competition and congestion, particularly in crowded areas.
3. **Security Concerns:**
   - Wireless networks are more vulnerable to hacking, eavesdropping, and data breaches compared to wired systems.
4. **Signal Degradation:**
   - Factors such as distance, obstacles, and atmospheric conditions can cause signal attenuation or fading.

Introduction to Modulation Techniques

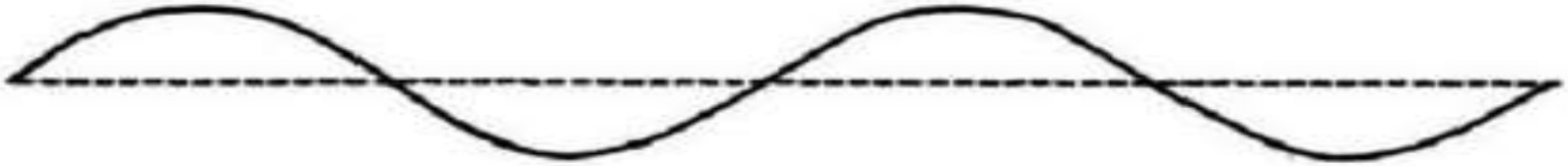
1. **Definition:**
   - Modulation is the process of varying a carrier signal in order to transmit data. The carrier signal is usually a high-frequency wave, and modulation helps to encode information (voice, data, video, etc.) onto it.
2. **Purpose of Modulation:**
   - Enables long-distance communication by adapting signals to travel efficiently over different mediums (air, cables, etc.).
   - Reduces interference and allows multiple signals to coexist (frequency allocation).
3. **Types of Modulation:**
   - **Analog Modulation**
   - **Digital Modulation**

Analog Modulation Techniques

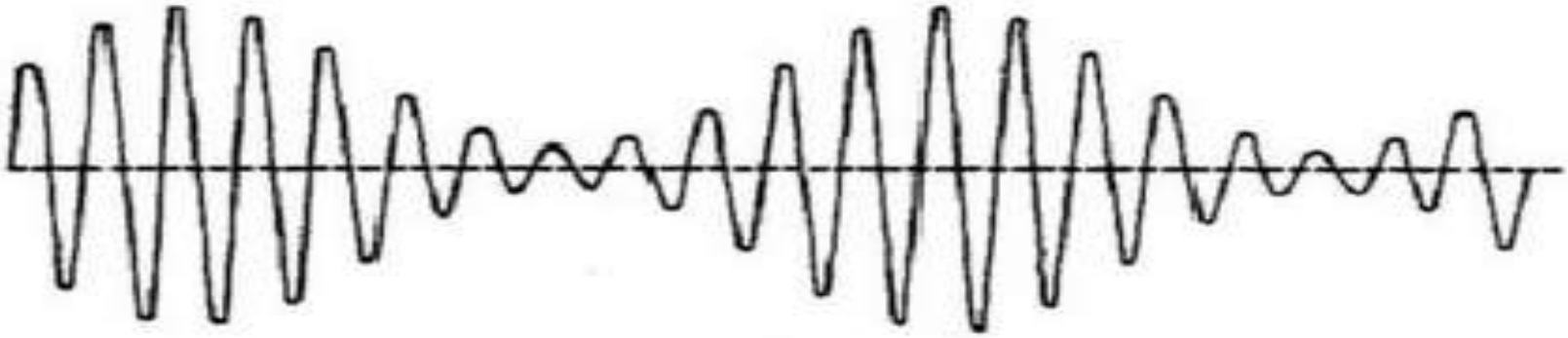
1. **Amplitude Modulation (AM):**
   - The amplitude of the carrier signal is varied in proportion to the information being sent.
   - **Applications:** AM Radio, early TV broadcasting.
   - **Advantages:** Simple and easy to implement.
   - **Disadvantages:** Susceptible to noise and signal distortion.
2. **Frequency Modulation (FM):**
   - The frequency of the carrier signal is varied according to the information signal.
   - **Applications:** FM Radio, sound transmission for TV.
   - **Advantages:** Higher noise immunity compared to AM, better sound quality.
   - **Disadvantages:** Requires more bandwidth than AM.
3. **Phase Modulation (PM):**
   - The phase of the carrier wave is varied to represent the data.
   - **Applications:** Satellite communication, some wireless systems.
   - **Advantages:** Resilient to interference and noise.
   - **Disadvantages:** More complex demodulation process.



A CARRIER



B SIGNAL



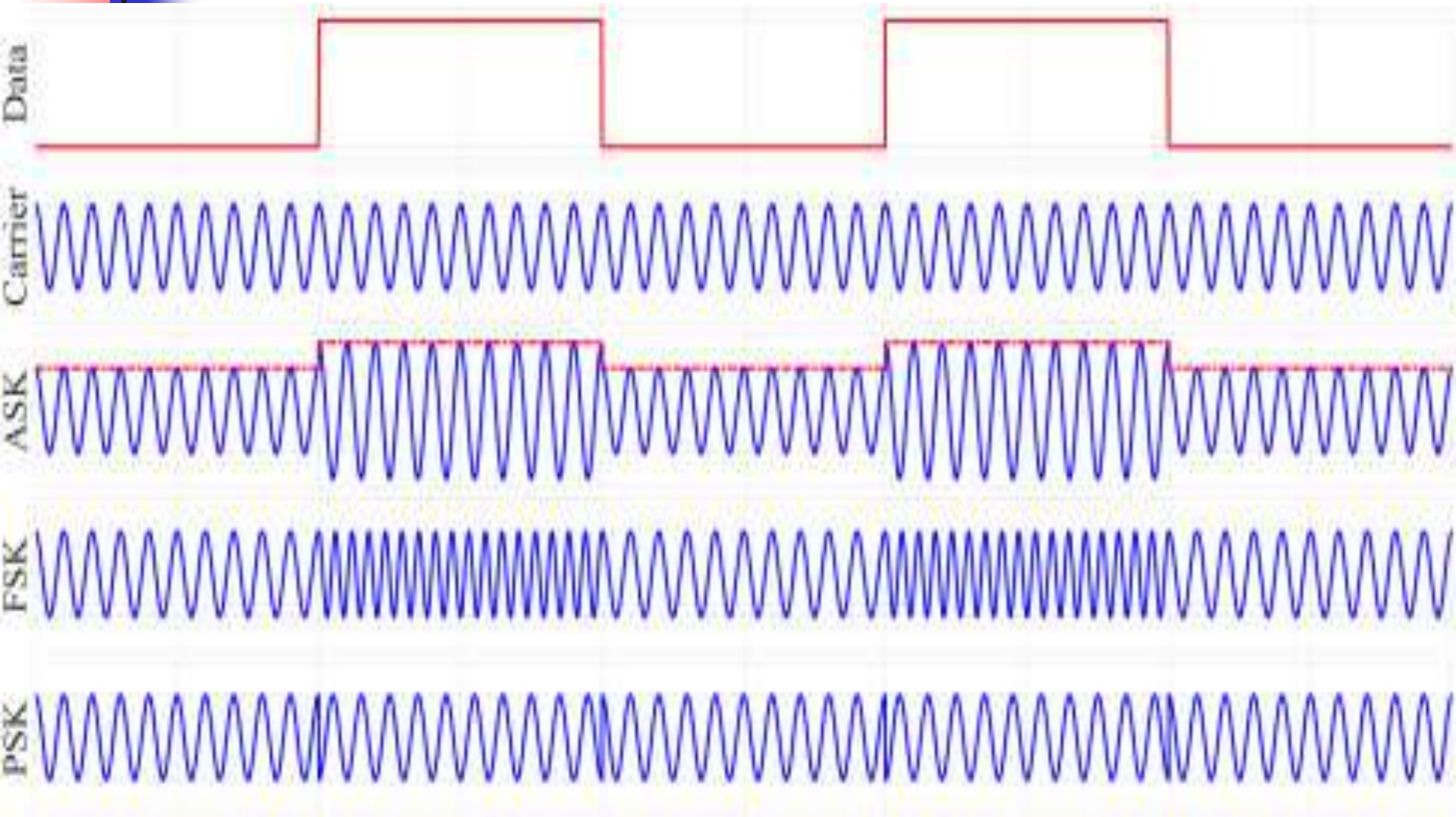
C AMPLITUDE MODULATED WAVE

D FREQUENCY MODULATED WAVE

Digital Modulation Techniques

1. **Amplitude Shift Keying (ASK):**
   - The amplitude of the carrier signal is changed according to the digital data (0 or 1).
   - **Applications:** RFID systems, optical fiber communication.
   - **Advantages:** Simple implementation.
   - **Disadvantages:** Sensitive to noise and interference.
2. **Frequency Shift Keying (FSK):**
   - The frequency of the carrier signal is switched between two values to represent binary data.
   - **Applications:** Modems, Bluetooth, RFID.
   - **Advantages:** More robust to noise compared to ASK.
   - **Disadvantages:** Requires more bandwidth than ASK.

3. **Phase Shift Keying (PSK):**
    - The phase of the carrier wave is changed to represent the digital data.
    - **Applications**: Wi-Fi, satellite communication, RFID.
    - **Advantages**: Efficient use of bandwidth.
    - **Disadvantages**: More complex receiver design.
4. **Quadrature Amplitude Modulation (QAM):**
    - Combines both amplitude and phase modulation to carry data, allowing for more bits per symbol.
    - **Applications**: High-speed data transmission like in 4G/5G networks, DSL, and cable modems.
    - **Advantages**: High spectral efficiency, capable of transmitting more data.
    - **Disadvantages**: More complex to implement, requires high signal-to-noise ratio.



Comparison of Modulation Techniques

Modulation Type	Advantages	Disadvantages	Applications
AM	Simple, easy to implement	Susceptible to noise	AM Radio
FM	Higher noise immunity	Requires more bandwidth	FM Radio, TV Sound
PM	Resilient to interference	Complex demodulation	Satellite Communication
ASK	Simple	Sensitive to noise	RFID, Optical Communication
FSK	Robust to noise	Requires more bandwidth	Bluetooth, Modems
PSK	Bandwidth efficient	Complex receiver	Wi-Fi, Satellite Communication
QAM	High data rate	Complex, requires high SNR	4G/5G, DSL, Cable Modems

Key Considerations for Choosing a Modulation Technique

1. **Bandwidth Efficiency:**
   - How efficiently the technique uses available bandwidth.
   - Digital techniques like QAM and PSK offer higher bandwidth efficiency.
2. **Power Efficiency:**
   - How much power is required for reliable transmission.
   - Techniques like AM are less power-efficient compared to FM or QAM.
3. **Noise Immunity:**
   - Resistance to interference and noise.
   - Digital modulation techniques like FSK and QAM have better noise immunity than analog ones like AM.
4. **Complexity:**
   - Some techniques require more complex equipment for modulation/demodulation (e.g., QAM, PSK).

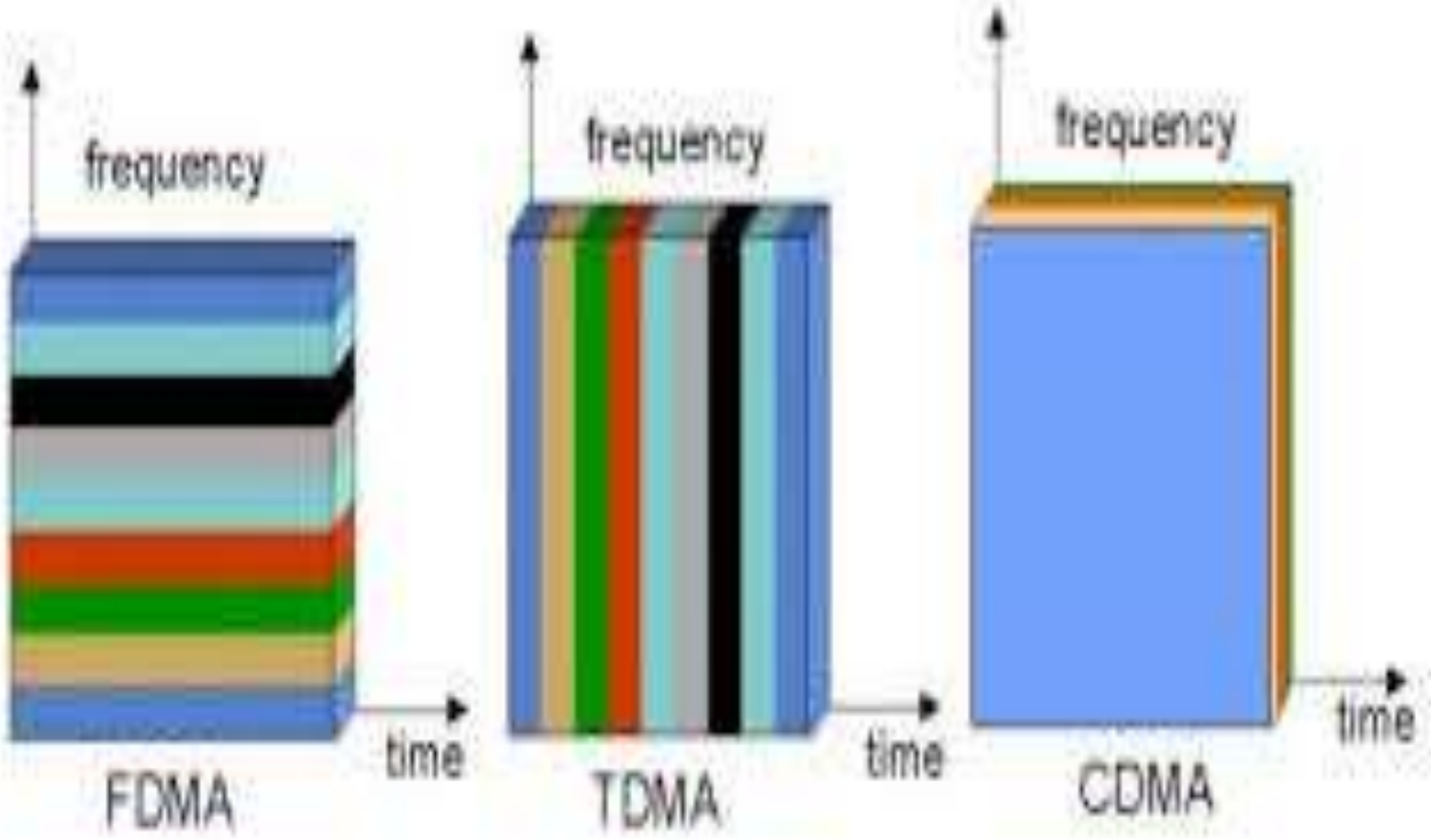
Introduction to Multiple Access Techniques

1. What is Multiple Access?

   - Multiple access techniques allow multiple users or devices to share the same communication channel (e.g., frequency band, time slot) without significant interference.
   - Essential for efficient utilization of limited bandwidth in wireless communication systems.

2. Why is Multiple Access Important?

   - Enables multiple users to communicate simultaneously within the same network.
   - Ensures fair and efficient allocation of network resources.
   - Critical for cellular networks, satellite communication, Wi-Fi, etc.


frequency
time
FDMA
frequency
time
TDMA
frequency
time
CDMA

Frequency Division Multiple Access (FDMA)

1. **How FDMA Works:**
   - The available bandwidth is divided into non-overlapping frequency bands or channels.
   - Each user is assigned a specific frequency band for the duration of their communication.
   - Users transmit simultaneously, but each within their designated frequency band.
2. **Key Features:**
   - Simple to implement in hardware (analog systems).
   - Users are isolated from each other by frequency, minimizing interference.
3. **Advantages:**
   - Suitable for continuous transmission (e.g., voice communication).
   - Well-suited for analog systems.
4. **Disadvantages:**
   - Requires guard bands to prevent interference, leading to inefficient use of bandwidth.
   - Limited capacity due to fixed channel allocation.
5. **Applications:**
   - Analog cellular systems (1G), radio and TV broadcasting.

(TDMA)

1. **How TDMA Works:**
   - The communication time is divided into time slots.
   - Each user is assigned a specific time slot within a repeating frame to transmit data.
   - Only one user transmits at a time within their time slot, avoiding interference.
2. **Key Features:**
   - Time-sharing of a single frequency channel.
   - Users share the same frequency band but transmit in different time slots.
3. **Advantages:**
   - Efficient use of bandwidth since frequency spectrum is shared.
   - Digital systems benefit from easier synchronization.
4. **Disadvantages:**
   - Requires precise time synchronization between users.
   - Not suitable for real-time communication (latency can be an issue).
5. **Applications:**
   - GSM (2G) networks, DECT (Digital Enhanced Cordless Telecommunications), some satellite systems.

Code Division Multiple Access (CDMA)

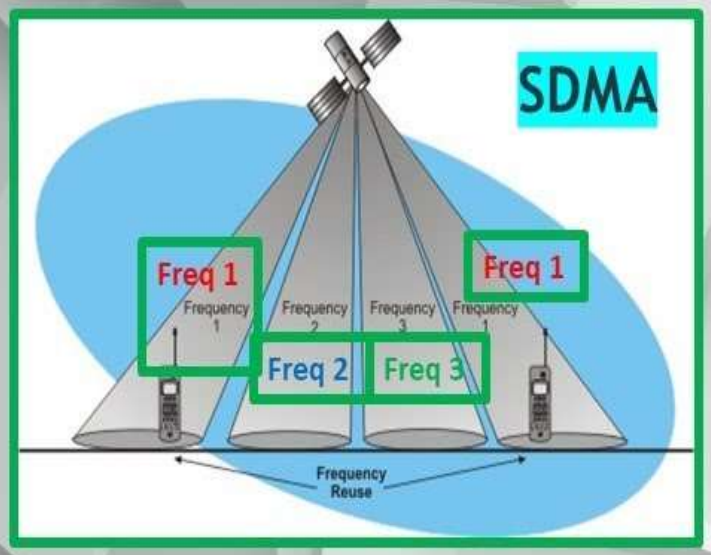
1. **How CDMA Works:**
   - All users share the same frequency band simultaneously.
   - Each user's data is encoded with a unique code (spreading code), and the receiver uses this code to separate signals.
   - Based on **spread spectrum** technology: the data signal is spread across a wide range of frequencies.
2. **Key Features:**
   - Each user's signal is spread over the entire available bandwidth.
   - Signals are distinguished using unique pseudo-random codes, allowing simultaneous transmissions.
3. **Advantages:**
   - Highly resistant to interference and eavesdropping.
   - Efficient use of bandwidth due to overlap of signals.
   - Greater capacity than FDMA and TDMA, especially for mobile communications.
4. **Disadvantages:**
   - Complex receiver design, requires high computational power for decoding.
   - Requires precise power control to avoid the **near-far problem** (stronger signals can drown out weaker ones).
5. **Applications:**
   - 3G cellular networks (e.g., WCDMA), GPS, some Wi-Fi systems.

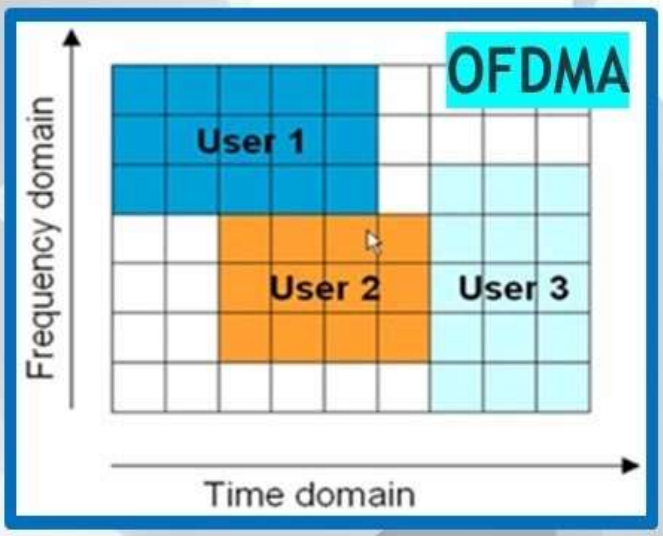
Orthogonal Frequency Division Multiple Access (OFDMA)

1. **How OFDMA Works:**
   - A form of multi-carrier transmission where users are assigned subsets of subcarriers.
   - The available spectrum is divided into orthogonal (non-overlapping) subcarriers, and multiple users transmit over different subcarriers simultaneously.
2. **Key Features:**
   - Combines both frequency and time domains for multiplexing.
   - Users transmit on orthogonal frequencies, reducing interference and allowing efficient use of bandwidth.
3. **Advantages:**
   - Highly efficient in handling high data rates.
   - Resistant to multipath fading and interference.
   - Allows dynamic bandwidth allocation based on user demand (flexibility).
4. **Disadvantages:**
   - More complex than FDMA/TDMA due to frequency synchronization requirements
   - High Peak-to-Average Power Ratio (PAPR) requires more efficient amplifiers.
5. **Applications:**
   - 4G LTE, 5G NR, WiMAX, Wi-Fi (802.11a/g/n/ac).

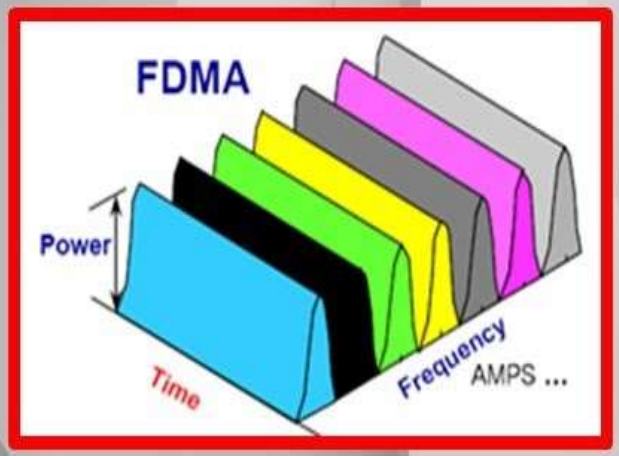
Space Division Multiple Access (SDMA)

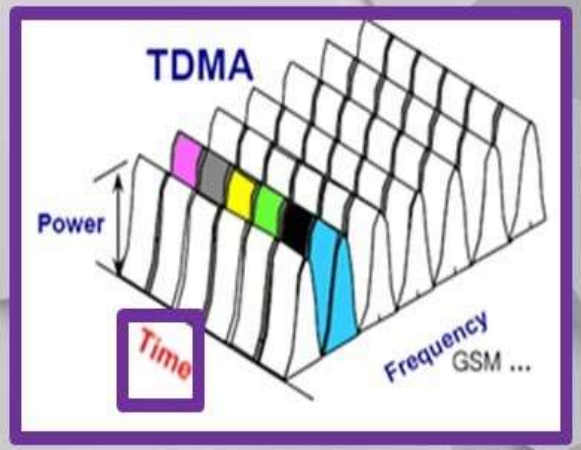
1. **How SDMA Works:**
   - Uses spatial separation to allocate channels based on the location of users.
   - Different users in different locations (sectors) can use the same frequency at the same time without interference.
2. **Key Features:**
   - Employs multiple antennas (beamforming or MIMO) to direct signals in specific directions, creating spatially separate communication paths.
3. **Advantages:**
   - Increases network capacity by reusing frequencies in different spatial sectors.
   - Improves signal quality and reduces interference by focusing signal power on intended users.
4. **Disadvantages:**
   - Complex implementation, requires advanced antenna technologies and algorithms.
   - Limited by physical location of users.
5. **Applications:**
   - Used in modern cellular systems (5G), satellite communications, and Wi-Fi (beamforming technology).

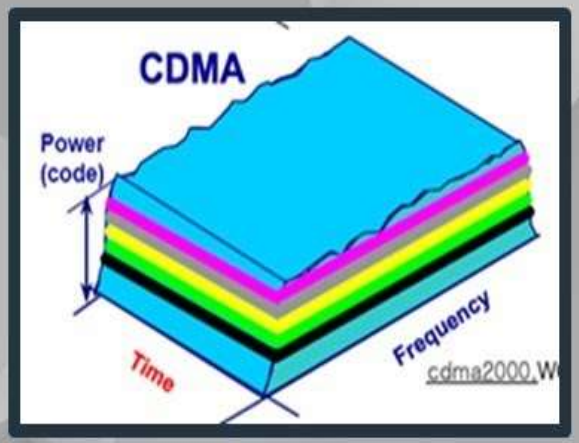




Multiple Access (FDMA, TDMA, CDMA, OFDMA & SDMA)

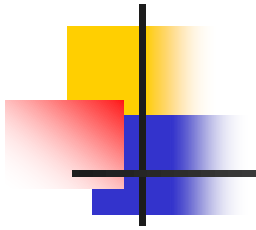






Comparison of Multiple Access Techniques

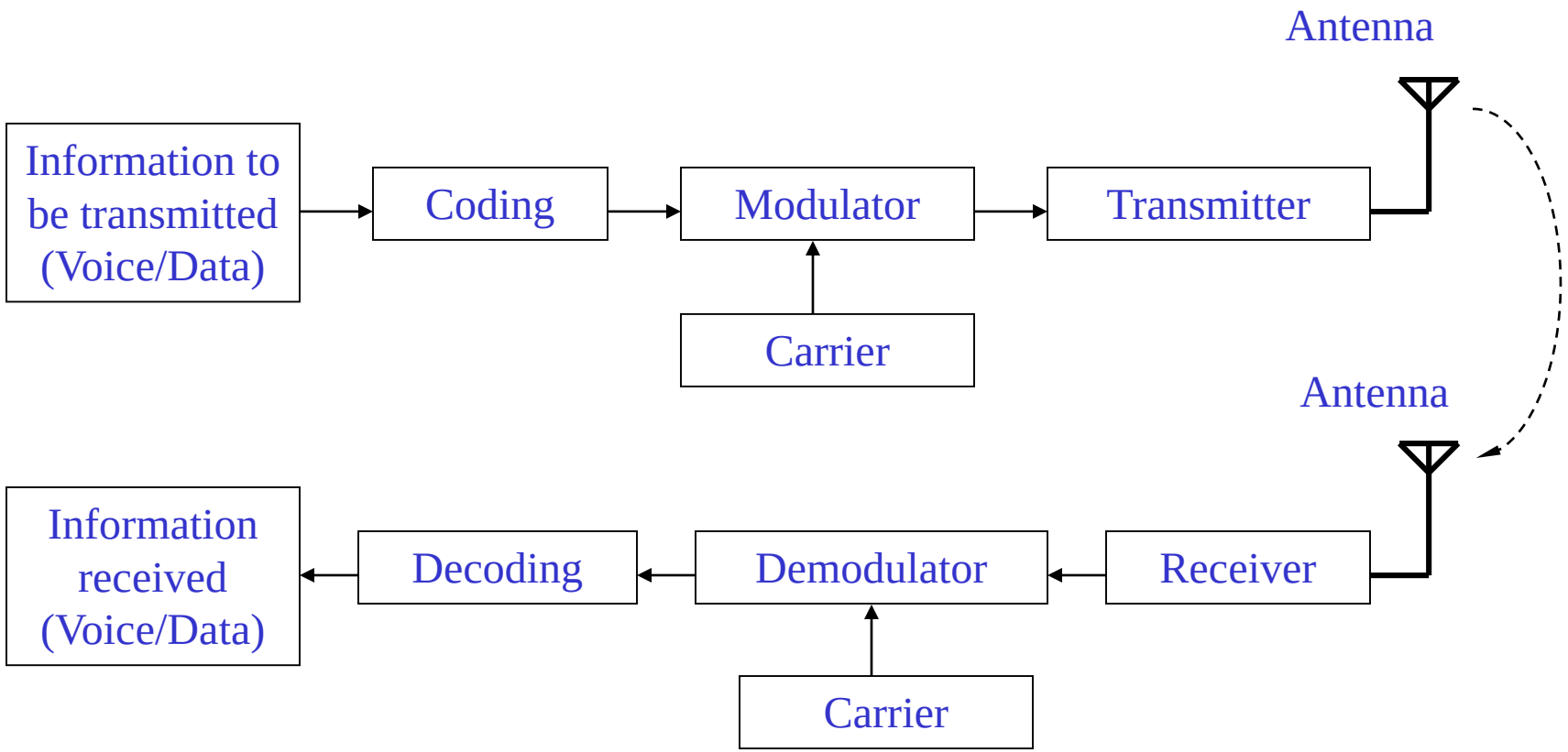
Technique	Resource Allocation	Advantages	Disadvantages	Applications
FDMA	Frequency	Simple, no timing issues	Requires guard bands, limited capacity	Analog cellular systems, radio
TDMA	Time	Efficient use of bandwidth, lower interference	Synchronization needed, latency	GSM (2G), DECT, satellite
CDMA	Code	High capacity, secure, resistant to interference	Complex decoding, near-far problem	3G, GPS
OFDMA	Frequency + Time	High data rates, flexible allocation	Complex implementation, high PAPR	4G LTE, 5G, WiMAX, Wi-Fi
SDMA	Space	Increased capacity, reduced interference	Complex antenna technology	5G, satellite, beamforming Wi-Fi



Summary

1. **Choice of Multiple Access Technique:**
   - Depends on the application, system complexity, required data rate, and interference tolerance.
2. **Trend Towards OFDMA and SDMA:**
   - Modern systems like 4G/5G heavily rely on OFDMA for high data rates and spectrum efficiency.
   - SDMA and MIMO are key for enhancing network capacity and spatial diversity in 5G systems.

A Simplified Wireless Communication System Representation



Fundamentals of Cellular Systems

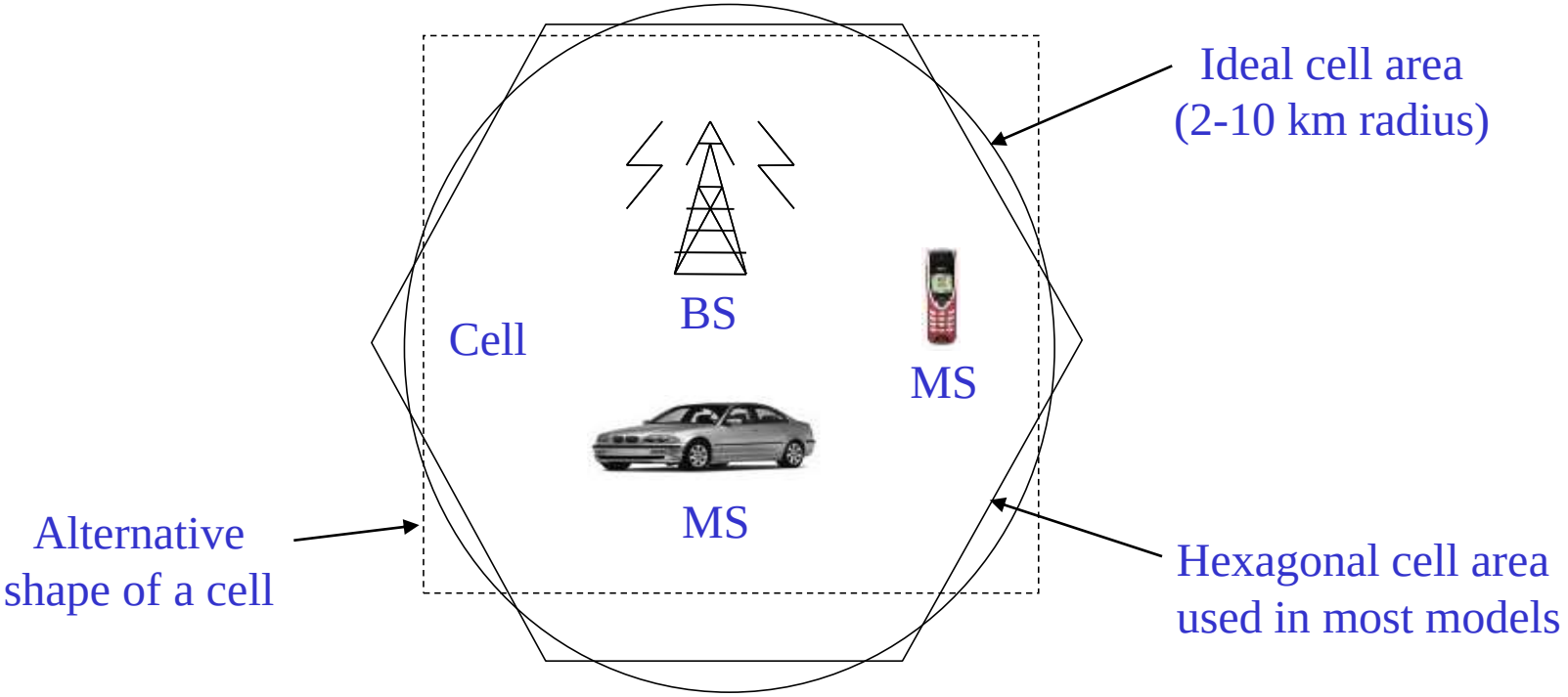


Illustration of a cell with a mobile station and a base station

GSM RF

- RF Spectrum

GSM 900

Mobile to BTS (uplink): 890-915 Mhz
BTS to Mobile(downlink):935-960 Mhz
Bandwidth : 2* 25 Mhz

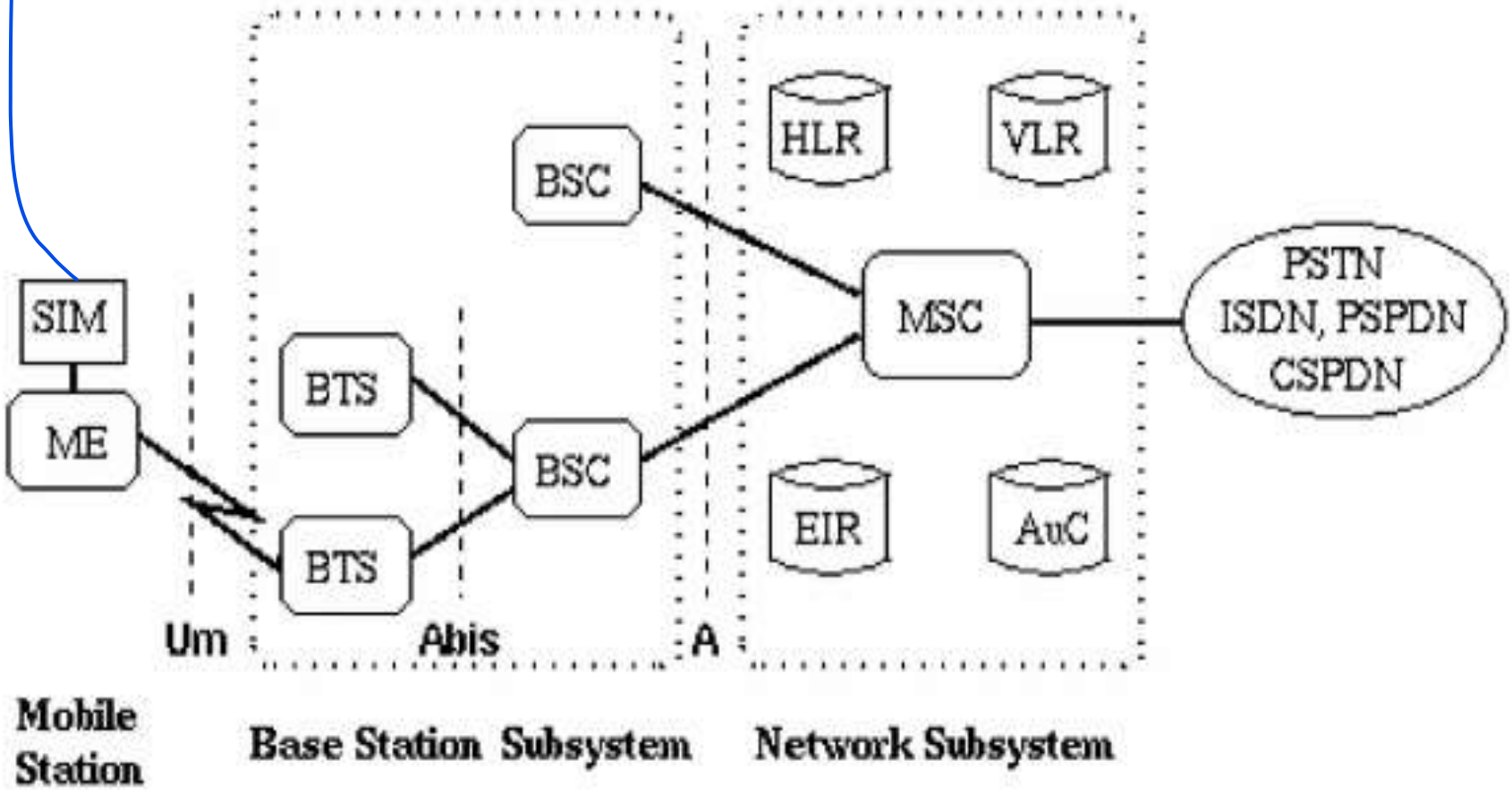
GSM 1800

Mobile to BTS (uplink): 1710-1785 Mhz
BTS to Mobile(downlink) 1805-1880 Mhz
Bandwidth : 2* 75 Mhz

GSM 850, 1900 also used

- Carrier Separation : 200 Khz
- Duplex Distance : 45 Mhz
- No. of RF carriers : 124
- Access Method : TDMA/FDMA
- Modulation Method : GMSK
- Modulation data rate : 270.833 Kbps

GSM System Architecture



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

GSM System Architecture-I

- **Mobile Station (MS)**
  - Mobile Equipment (ME)
  - Subscriber Identity Module (SIM)
- **Base Station Subsystem (BSS)**
  - Base Transceiver Station (BTS)
  - Base Station Controller (BSC)
- **Network Switching Subsystem(NSS)**
  - Mobile Switching Center (MSC)
  - Home Location Register (HLR)
  - Visitor Location Register (VLR)
  - Authentication Center (AUC)
  - Equipment Identity Register (EIR)

System Architecture
Mobile Station (MS)

The Mobile Station is made up of two entities:

1. Mobile Equipment (ME)
2. Subscriber Identity Module (SIM)

Mobile Equipment

- Portable, vehicle mounted, hand held device
- Uniquely identified by an **IMEI** (International Mobile Equipment Identity)
- Voice and data transmission
- Monitoring power and signal quality of surrounding cells for optimum handover
- Power level : 0.8W – 20 W
- 160 character long SMS.

SUBSCRIBER IDENTITY MODULE(SIM)

- Smart card contains the International Mobile Subscriber Identity (**IMSI**)
- Allows user to send and receive calls and receive other subscribed services
- Protected by a password or PIN
- Can be moved from phone to phone – contains key information to activate the phone

SYSTEM ARCHITECTURE
BASE STATION SUBSYSTEM (BSS)

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

1. Base Transceiver Station (**BTS**)
2. Base Station Controller (**BSC**)

BASE TRANSCEIVER STATION (BTS):

- Encodes, encrypts, multiplexes, modulates and feeds the RF signals to the antenna.
- Communicates with Mobile station and BSC
- Consists of Transceivers (TRX) units

BASE STATION CONTROLLER (BSC)

- Manages Radio resources for BTS
- Assigns Frequency and time slots for all MS's in its area
- Handles call set up
- Handover for each MS
- It communicates with MSC and BTS

System Architecture Network Switching Subsystem(NSS)

- The system contains the following functional units

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

Mobile Switching Center (MSC)

- Heart of the network
- Manages communication between GSM and other networks
- Billing information and collection
- Mobility management
  - Registration
  - Location Updating
  - Inter BSS and inter MSC call handoff

Home Location Registers (HLR)

- Stores information about each subscriber that belongs to it MSC in permanent and temporary fashion.
- As soon as mobile subscriber leaves its current local area, the information in the HLR is updated.
- database contains IMSI, MSISDN, prepaid/ postpaid, roaming restrictions, supplementary services.

Visitor Location Registers (VLR)

- Temporary database which updates whenever new MS enters its area, by HLR database
- Assigns a TMSI to each MS entering the VLR area which keeps on changing.
- Controls those mobiles roaming in its area
- Database contains IMSI, MSISDN, Location Area, authentication key

MSISDN (Mobile Station International Subscriber Directory Number) is the unique phone number assigned to a mobile subscriber or device, used for communication, call routing, billing, and network identification. It is the publicly visible phone number that you dial to reach someone.

IMSI stands for International Mobile Subscriber Identity, a unique number stored on a SIM card that identifies a mobile subscriber to a telecom network, enabling authentication and communication services. It consists of a Mobile Country Code (MCC), Mobile Network Code (MNC), and a Mobile Subscriber Identification Number (MSIN) to identify the individual user.

AUTHENTICATION CENTER (AUC)

- Contains the algorithms for authentication as well as the keys for encryption.
- Protects network operators from fraud.
- Situated in special protected part of the HLR.

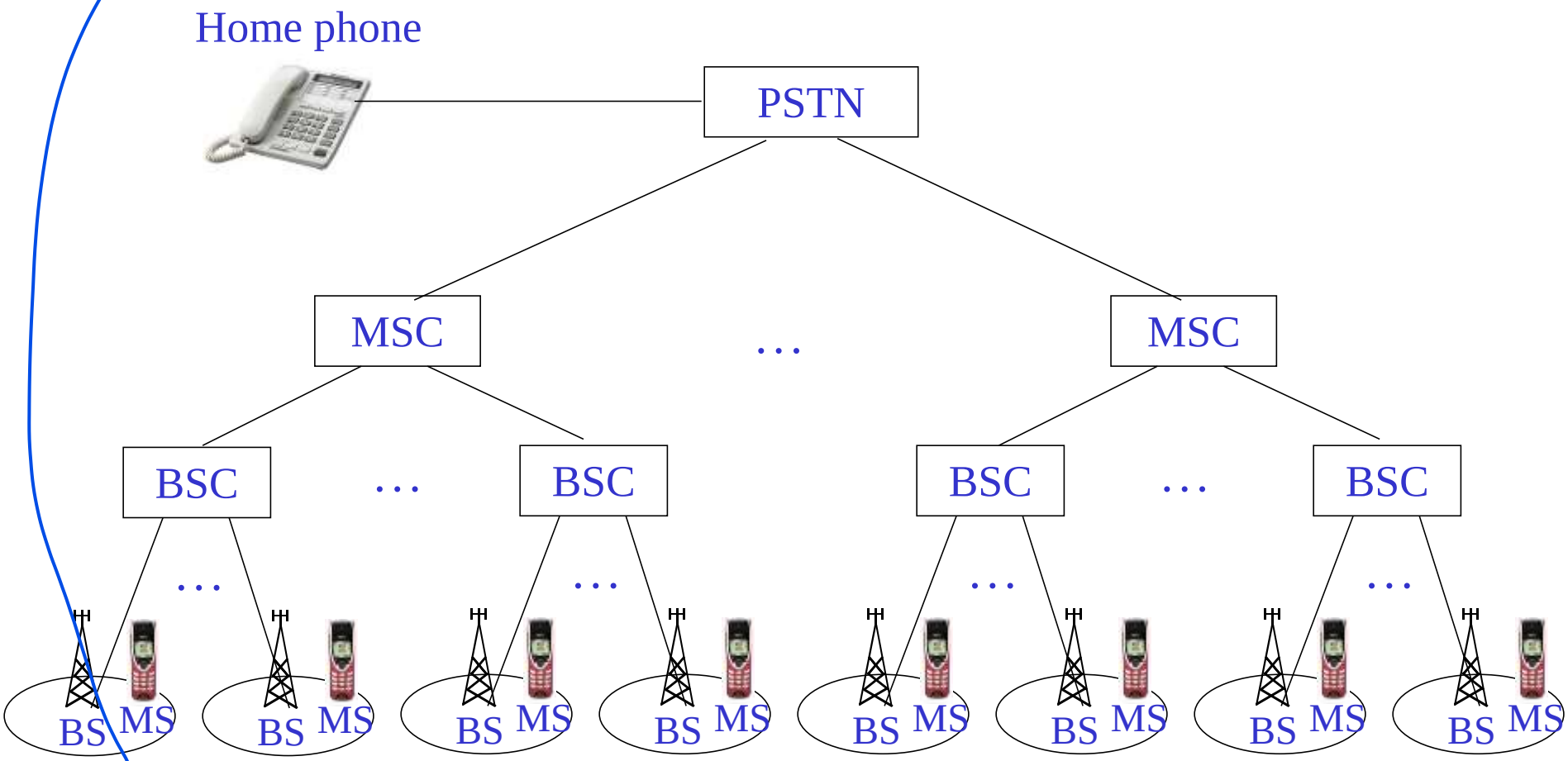
EQUIPMENT IDENTITY REGISTER (EIR)

- Stores all devices identifications registered for this network.
- Database that is used to track handsets using the IMEI (International Mobile Equipment Identity)
- Prevents calls from stolen, unauthorised or defective mobile devices

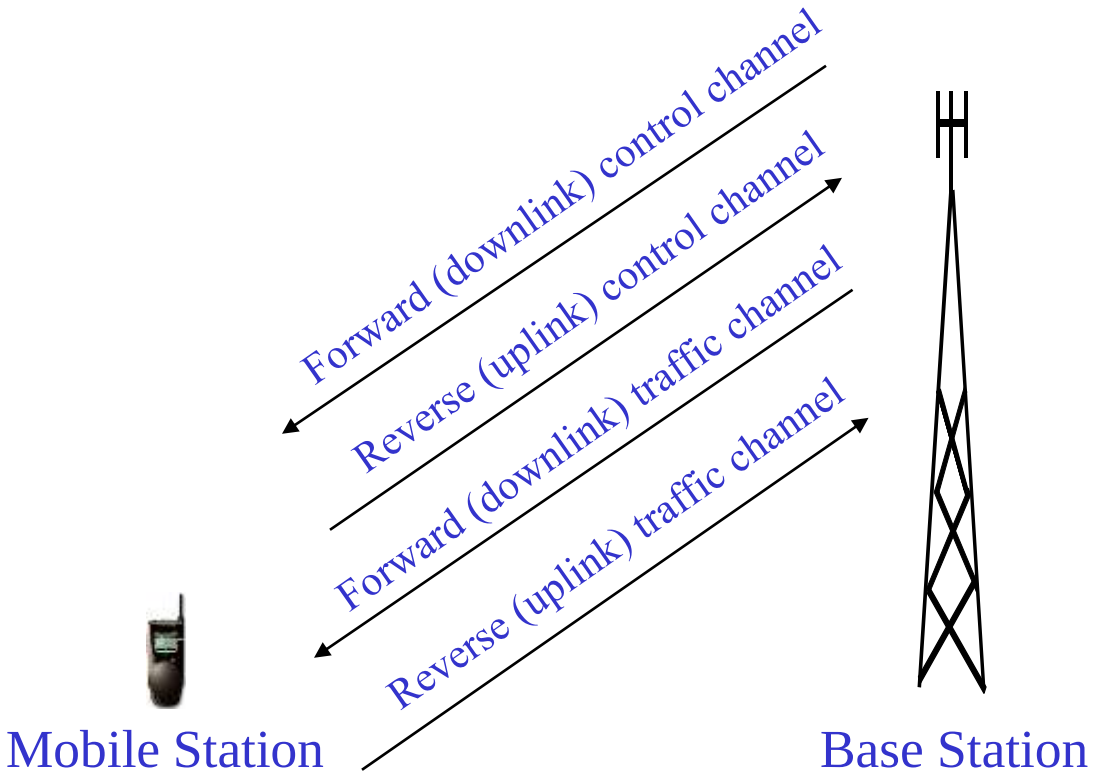
OPERATION AND MAINTENANCE CENTRE (OMC)

- The centralized operation of the various units in the system and functions needed to maintain the subsystems.
- Dynamic monitoring and controlling of the network.
- Functions :
  - configuration management
  - fault report and alarm handling
  - performance supervision/management
  - storage of system software and data

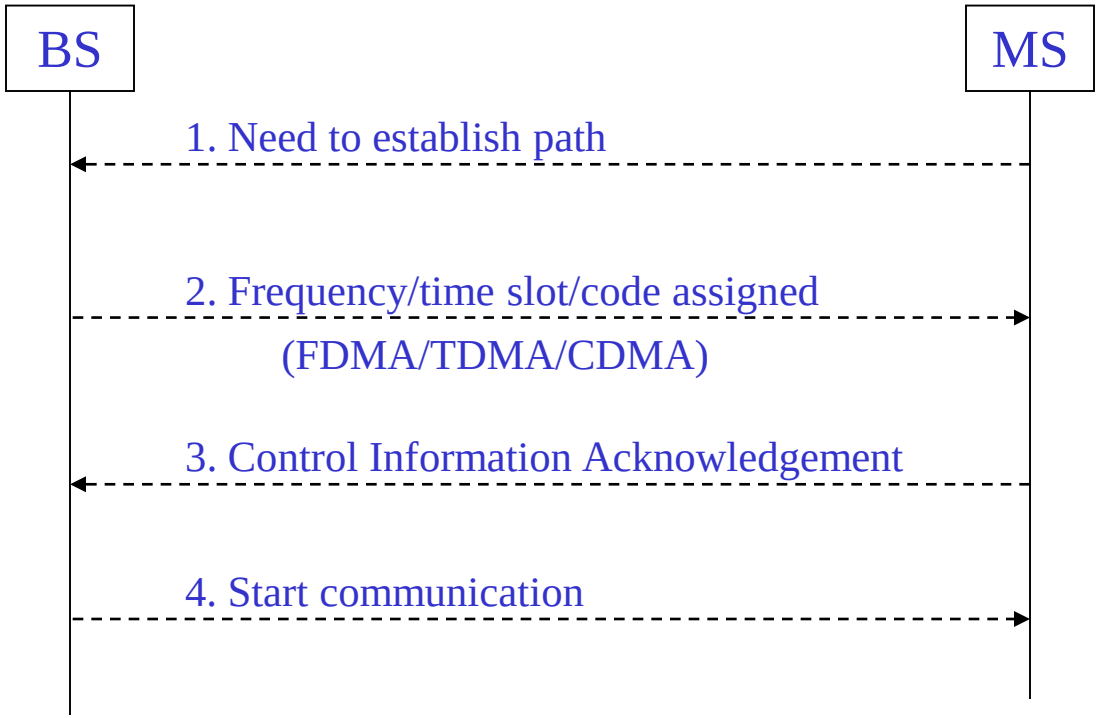
MS, BS, BSC, MSC, and PSTN



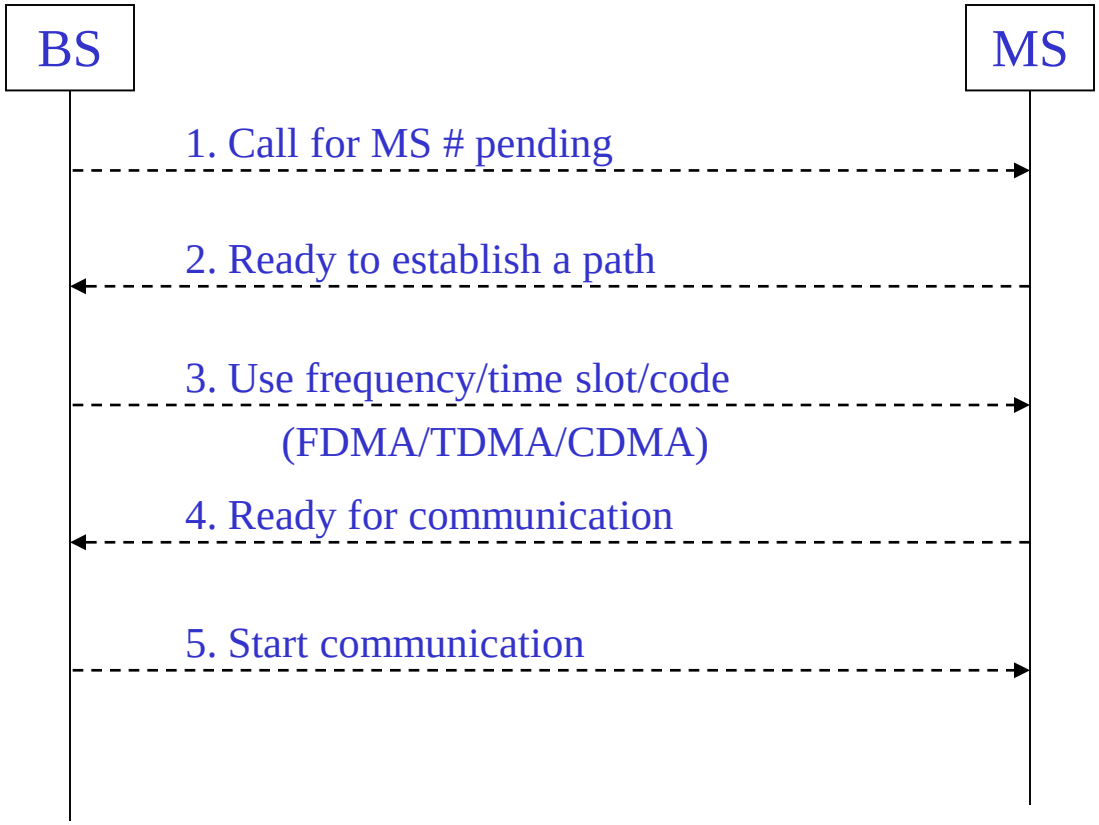
Control and Traffic Channels



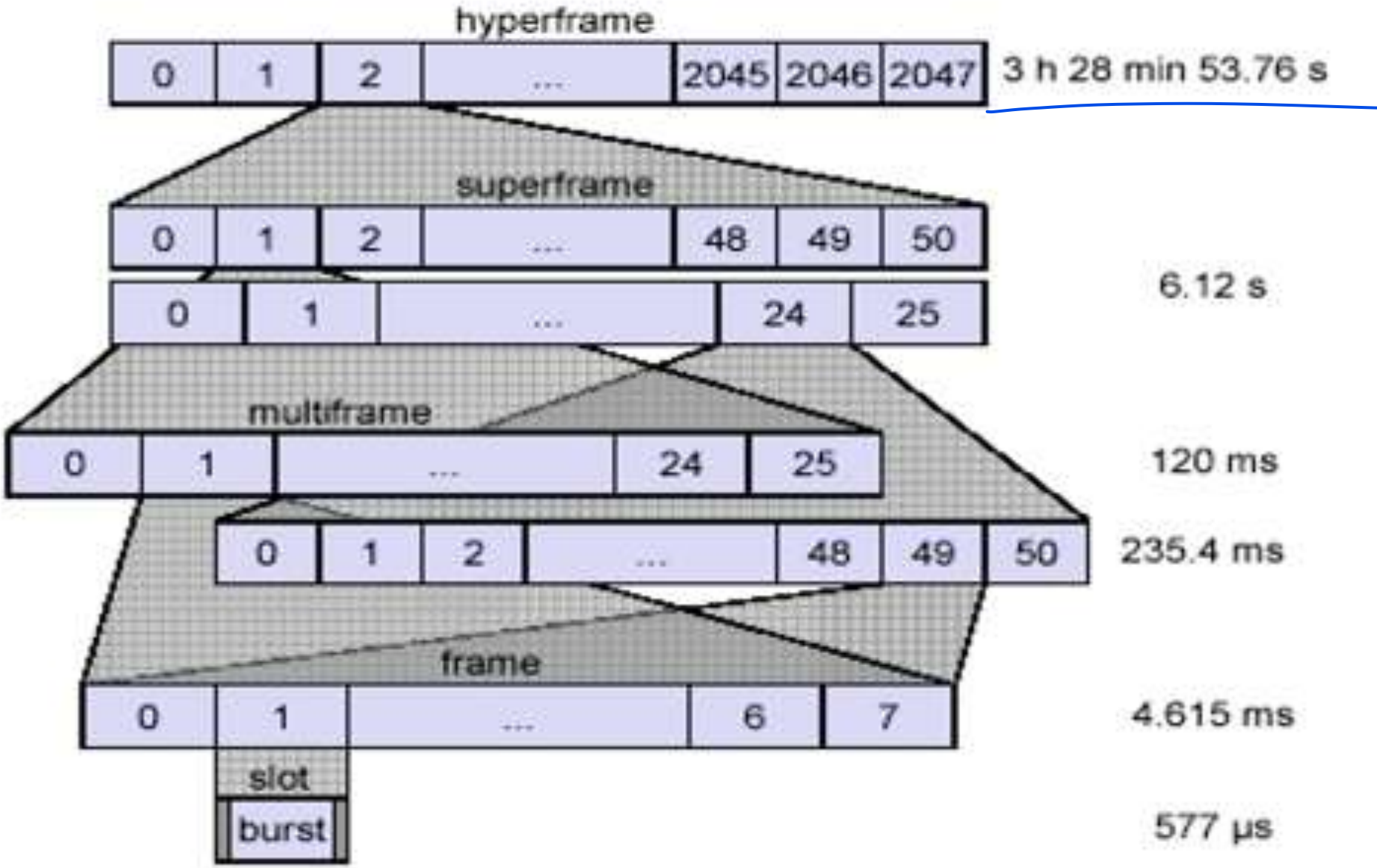
Steps for a Call Setup from MS to BS



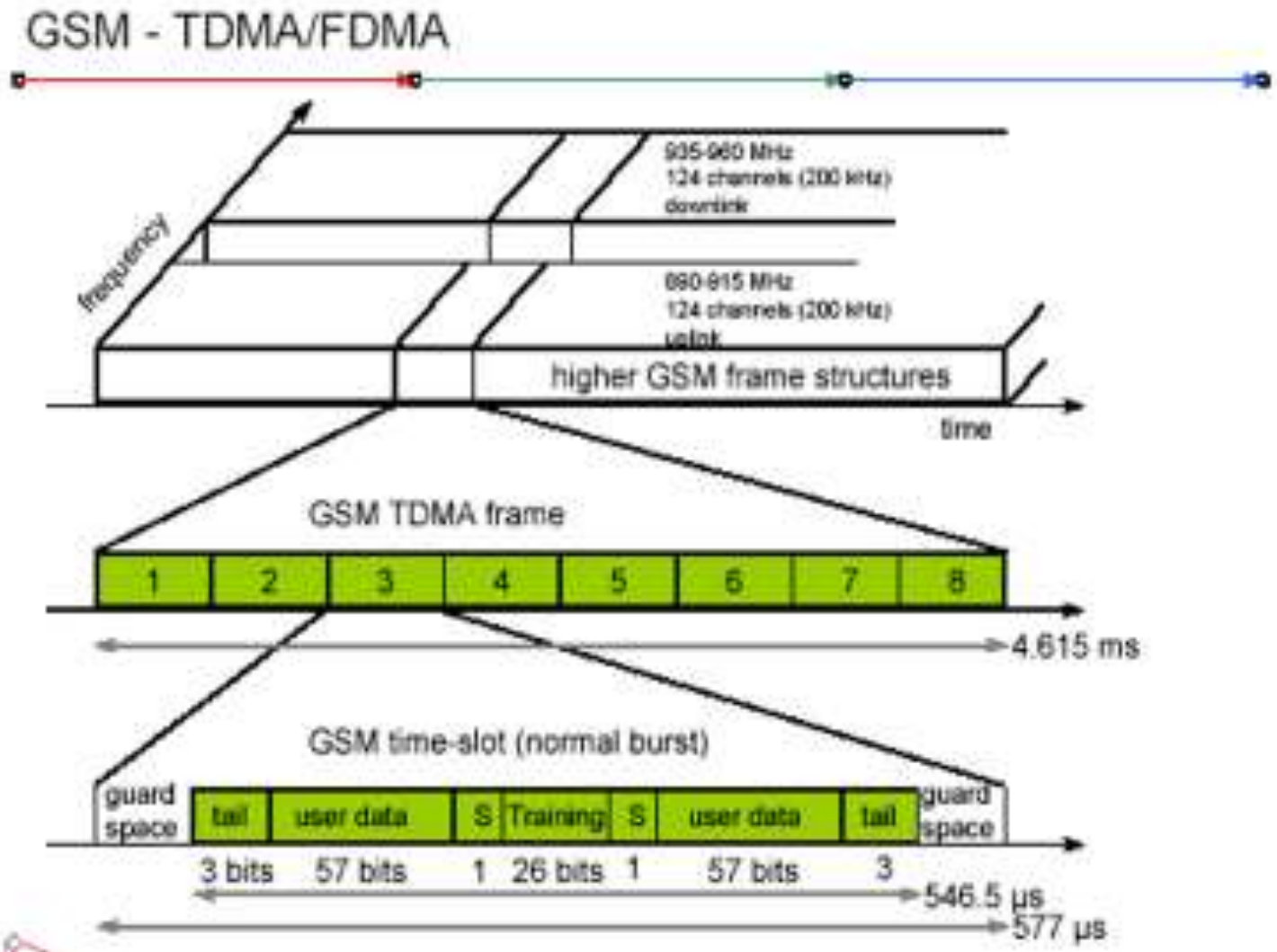
Steps for a Call Setup from BS to MS



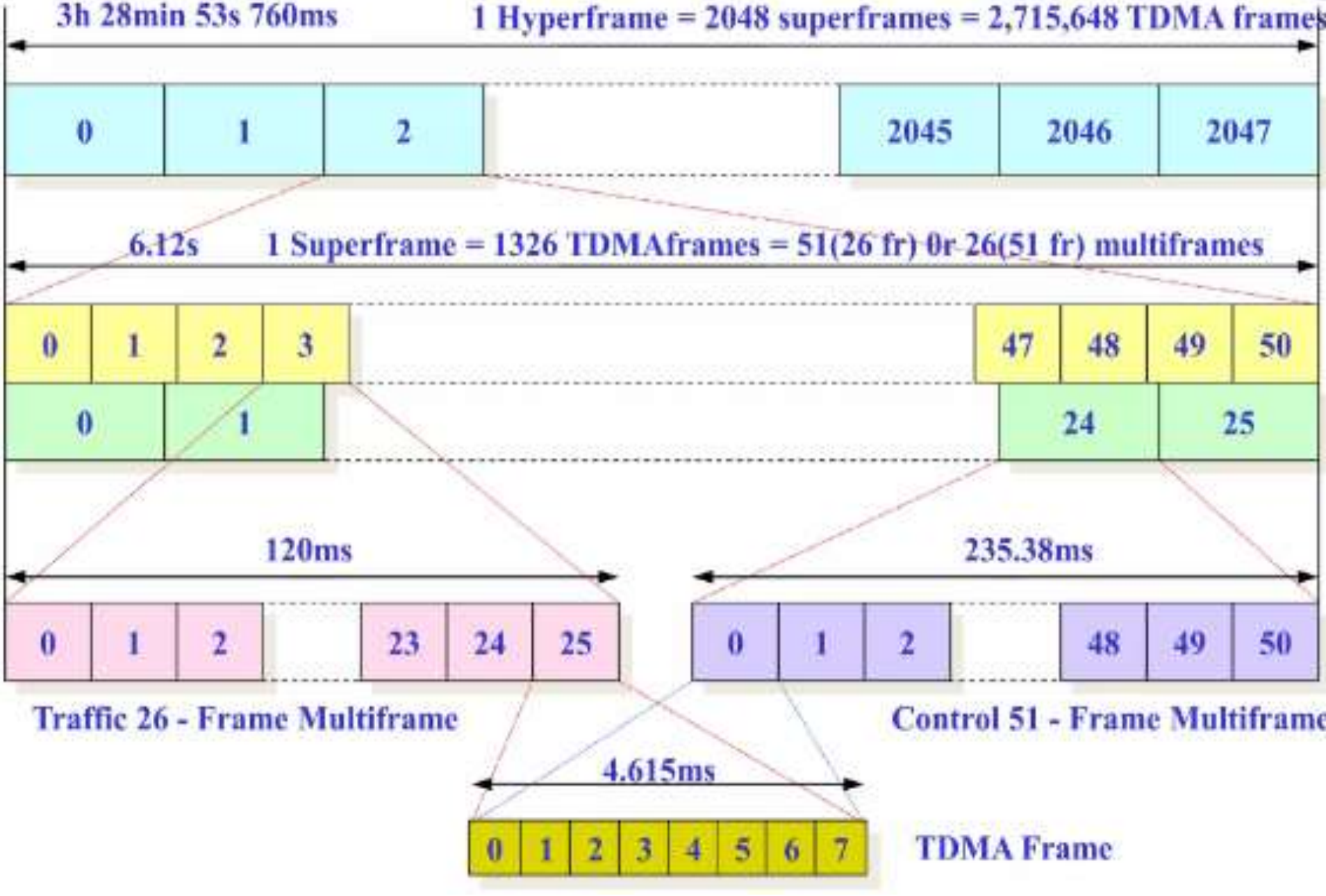
Physical Channel



GSM-Frame Structure

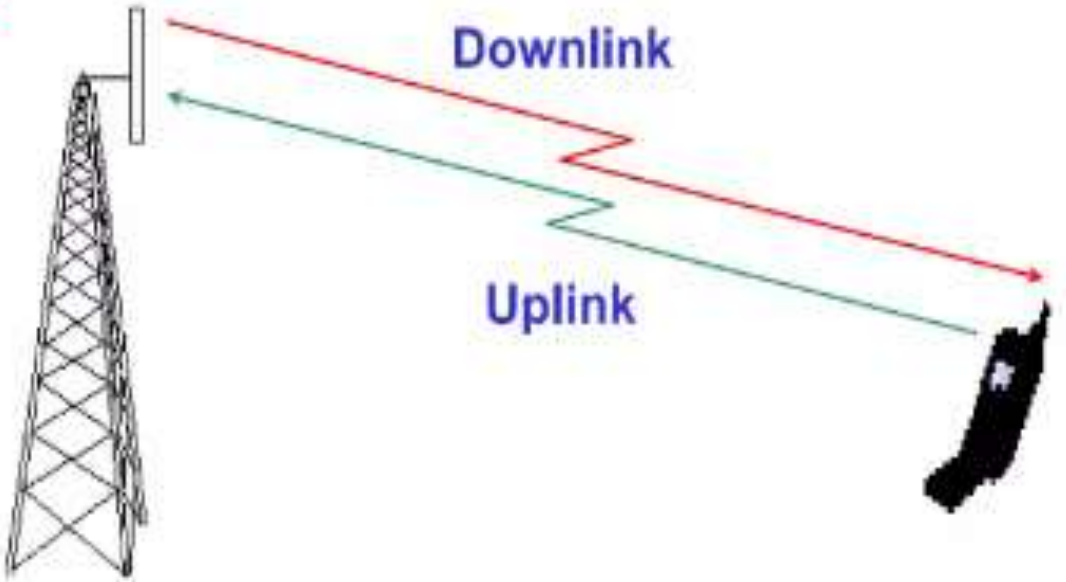


HYPERFRAME AND SUPERFRAME STRUCTURE



CHANNEL CONCEPT

CHANNELS



Physical channel - Each timeslot on a carrier is referred to as a physical channel. Per carrier there are 8 physical channels.

Logical channel - Variety of information is transmitted between the MS and BTS. There are different logical channels depending on the information sent. The logical channels are of two types

- Traffic channel
- Control channel

GSM Channel Types

1. Physical Channels

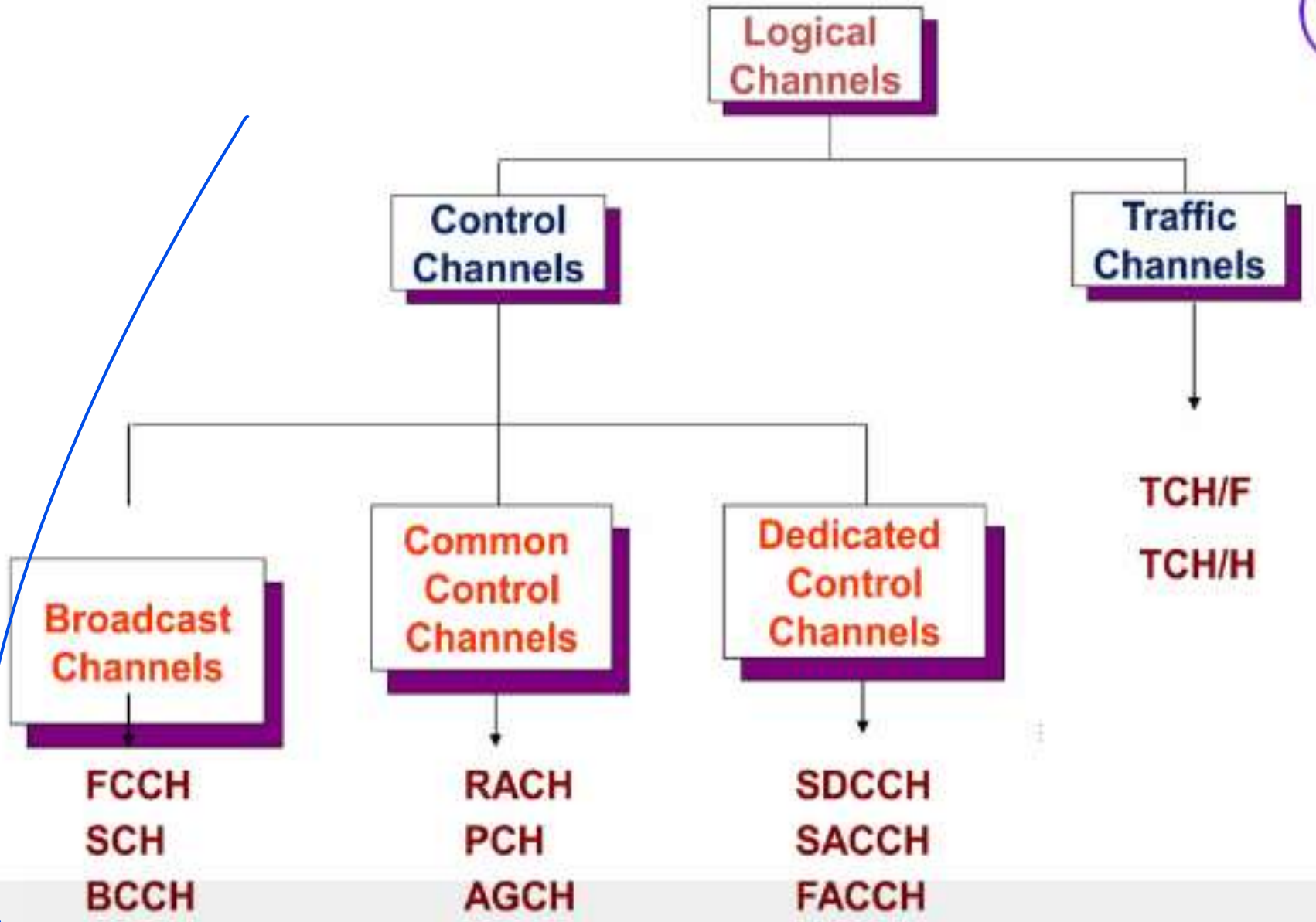
- Defined by: carrier frequency + timeslot
- Each GSM carrier (200 kHz wide) is divided into **8 time slots** using TDMA.
- Each time slot = **1 physical channel.**
- Physical channels carry **logical channels** (traffic or control information).

2. Logical Channels

Logical channels define **what type of information** is carried over a physical channel.

They are grouped into **Traffic Channels (TCH)** and **Control Channels (CCH).**

Logical Channels



A. Traffic Channels (TCH)

Used to **carry user information**: voice or data.

- **Full-Rate TCH (TCH/F)**: 1 time slot per frame (speech/data @ 13 kbps).
- **Half-Rate TCH (TCH/H)**: 2 users share 1 slot (speech/data @ 6.5 kbps).
- **TCH/Data**: 2.4, 4.8, 9.6 kbps user data.

B. Control Channels (CCH)

Used for signalling, synchronization, paging, and call setup.

Divided into **Broadcast**, **Common**, and **Dedicated** control channels.

(i) Broadcast Channels (BCH)

Transmit **system information** from BTS to all mobiles in the cell.

- **BCCH (Broadcast Control Channel):** cell identity, frequency lists, system parameters.
- **FCCH (Frequency Correction Channel):** helps MS tune to the BTS frequency.
- **SCH (Synchronization Channel):** frame number + BS identity, enables synchronization.

(ii) Common Control Channels (CCCH)

Shared between MSs in a cell, used for **access procedures.**

- **PCH (Paging Channel):** network informs MS of incoming call/SMS.
- **RACH (Random Access Channel):** MS requests channel (uplink).
- **AGCH (Access Grant Channel):** BTS assigns channel to MS (downlink).

(iii) Dedicated Control Channels (DCCH)

Assigned to a specific MS for call setup & maintenance.

- **SDCCH (Standalone Dedicated Control Channel)**: authentication, location update, SMS before a TCH is assigned.
- **SACCH (Slow Associated Control Channel)**: always paired with TCH/SDCCH; carries power control, timing advance, link quality reports.
- **FACCH (Fast Associated Control Channel)**: used for urgent signalling (e.g., handover); temporarily steals a TCH slot.

General Packet Radio Service

- General -> not restricted to GSM use (DECT ?, 3rd generation systems ?)
- Packet Radio -> enables packet mode communication over air
- Service, not System -> existing BSS (partially also NSS) infrastructure is used

Main benefits

- Resources are reserved only when needed and charged accordingly
- Connection setup times are reduced
- Enables new service opportunities

GPRS Characteristics

GPRS uses packet switched resource allocation

- resources allocated only when data is to be sent/received

Flexible channel allocation

- one to eight time slots
- available resources shared by active users
- up and down link channels reserved separately
- GPRS and circuit switched GSM services can use same time slots alternatively

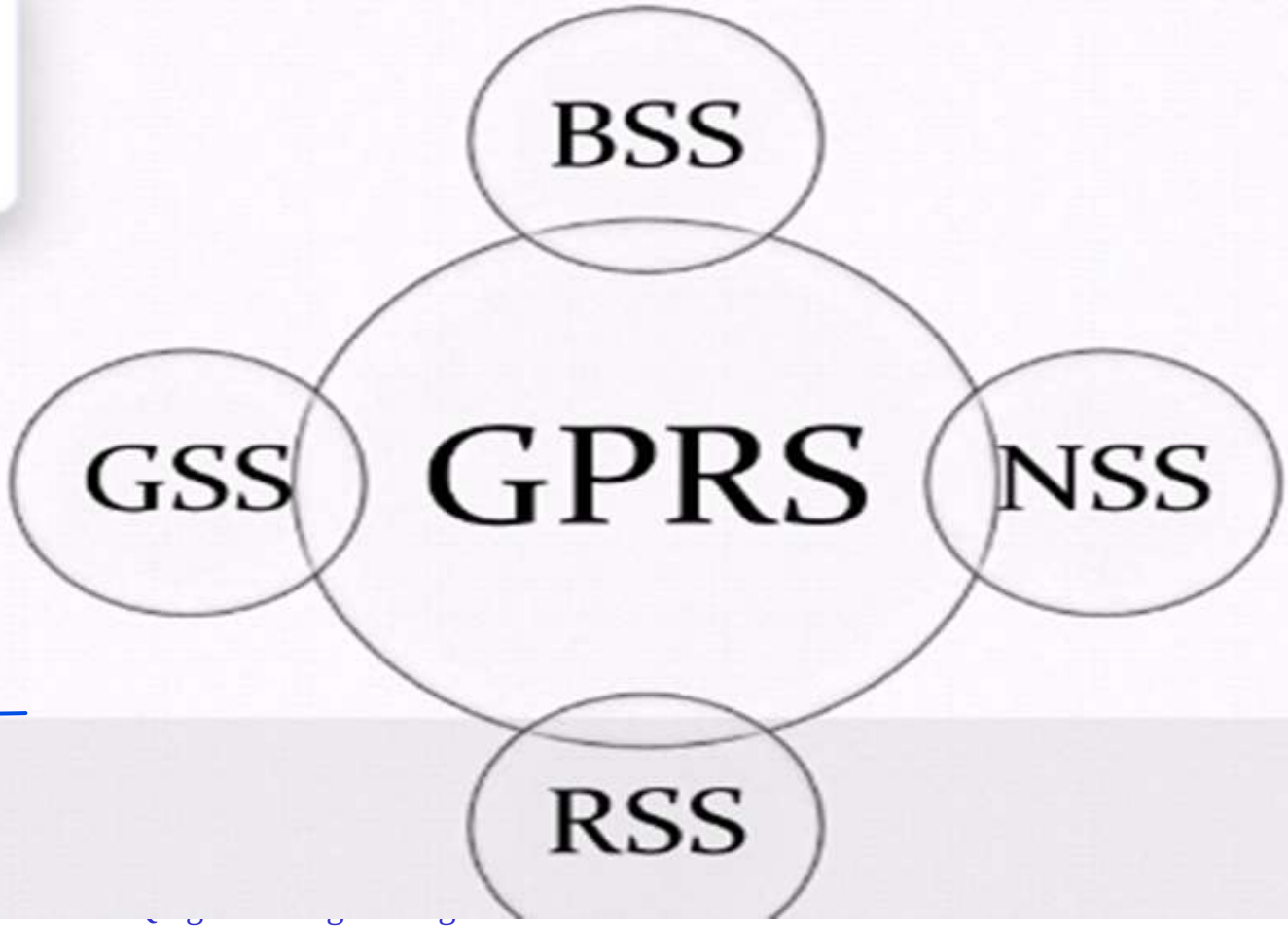
Traffic characteristics suitable for GPRS

- Intermittent, bursty data transmissions
- Frequent transmissions of small volumes of data
- Infrequent transmission of larger volumes of data

GPRS Architecture

HAVING 4 SUBSYSTEMS

PRS BSS NSS RSS

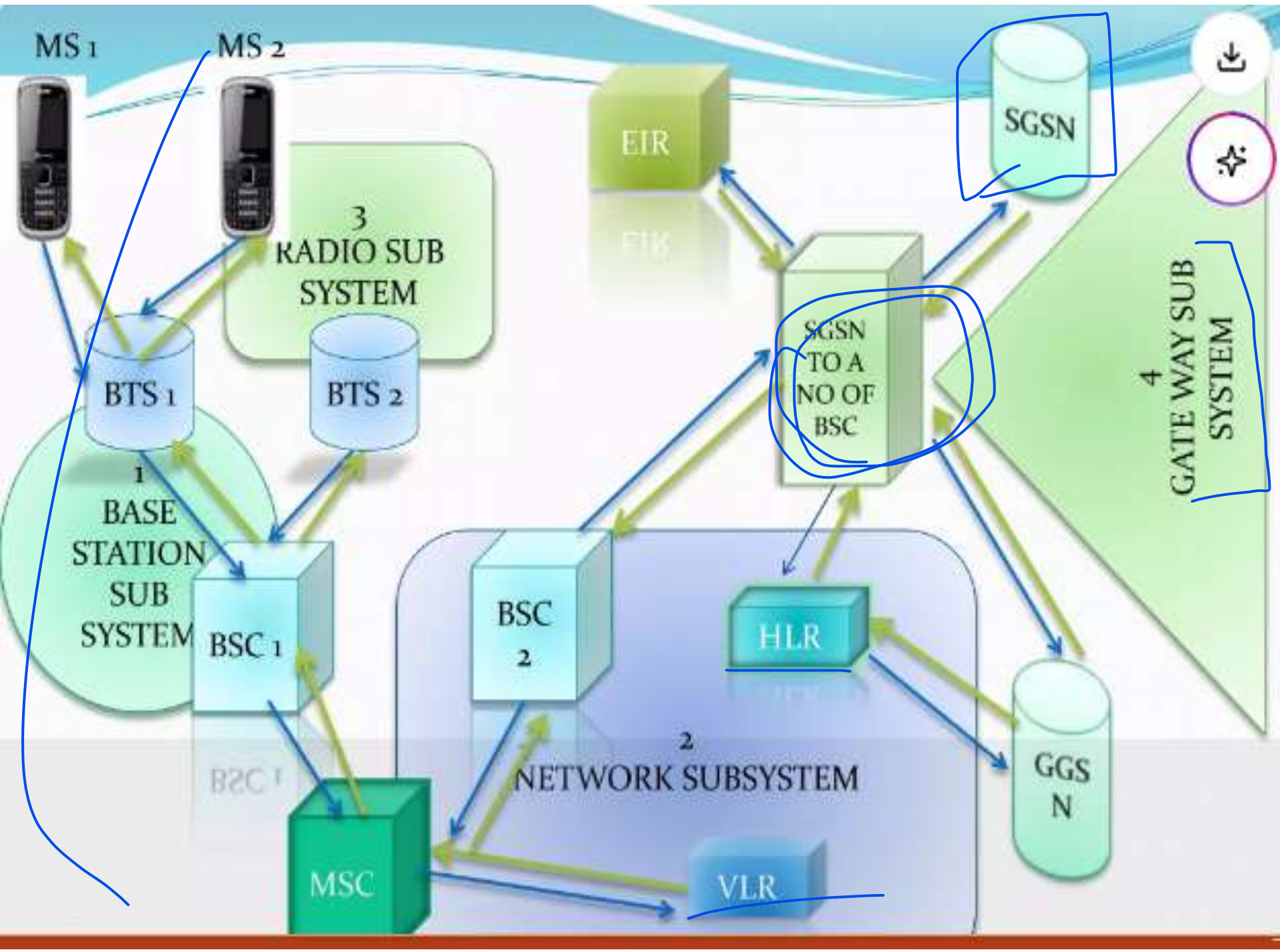


Base Station System(BSS)

- BSS system needs to enhancement to recognize and send packet data.
- BSS includes BTS and MS.

Network Subsystem(NSS)

- It consist of a number of sgsns
- Also consist of a number of msc
- helps in – authentication, operation & maintenance of subsystems


MS 1
MS 2
EIR
SGSN
3
RADIO SUB
SYSTEM
BTS 1
BTS 2
SGSN
TO A
NO OF
BSC
4
GATE WAY SUB
SYSTEM
1
BASE
STATION
SUB
SYSTEM
BSC 1
BSC
2
HLR
2
NETWORK SUBSYSTEM
GGS
N
MSC
VLR

GPRS support nodes

- There are two network nodes use to offer packet data service called GPRS support nodes
  1) Serving GPRS Support Node (SGSN)
  2) Gateway GPRS Support Node (GGSN)

Serving GPRS Support Node(SGSN)

Serving GPRS Support Node(SGSN) is one of the GPRS support node

- Routing the packet switched data to and from the ms
- Mobility management
- Location management
- Authentication and charging for calls
- Stores the location information of the user
- User's profile

Gateway GPRS Support Node(GGSN)

- Provide a gateway b/w gprs & pdn
- Convert data from sgsn to pdp format(packet data protocol)
- Store the current sgsn address
- Stores the location of user in its location register
- Perform authentication & charging functions

🔷 1. Mobile-Originated Call (MOC)

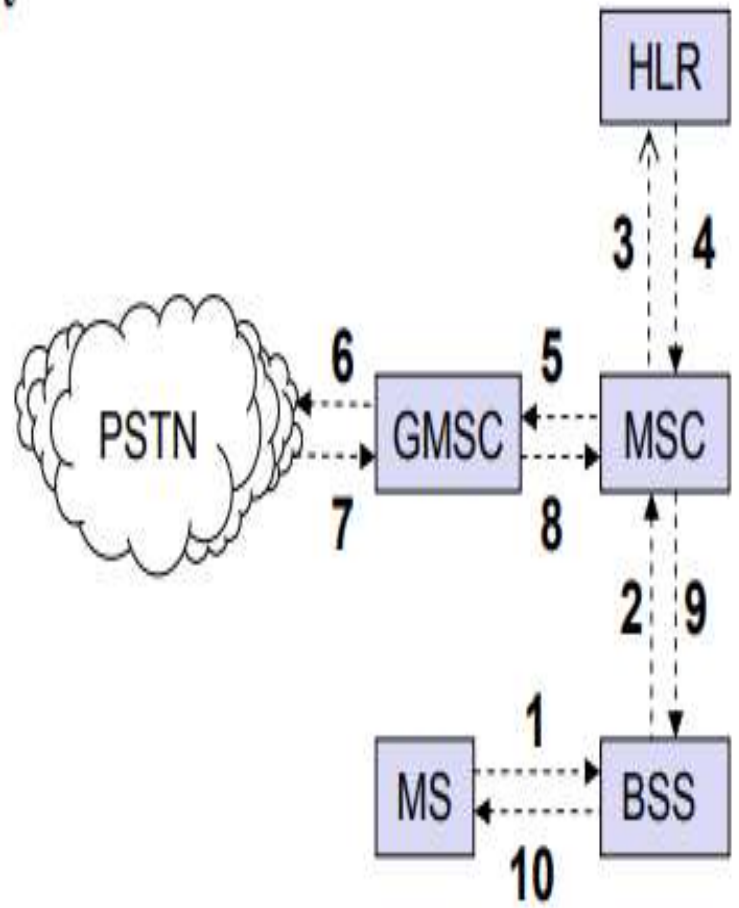
When a subscriber **initiates a call**:

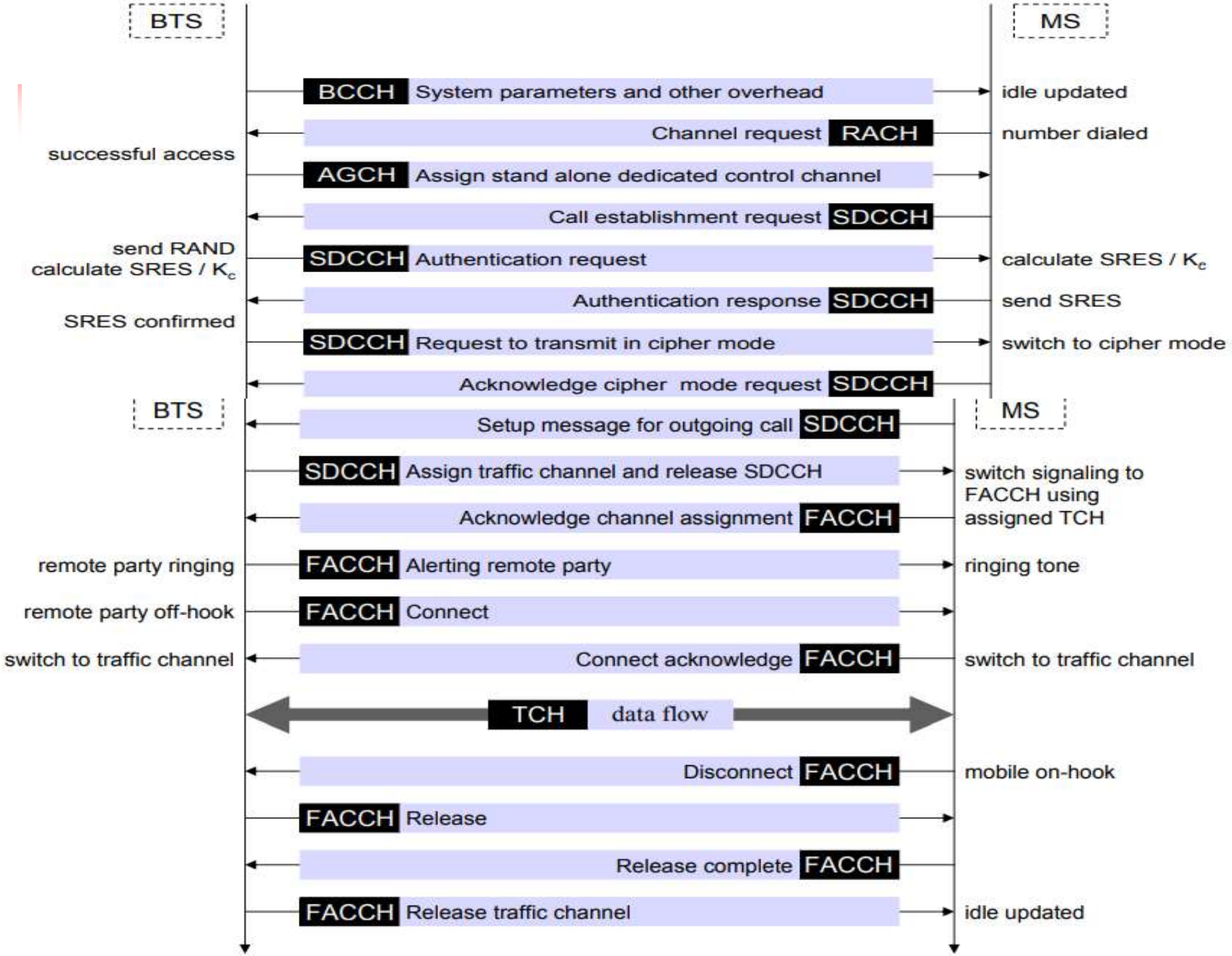
Step-by-Step Flow

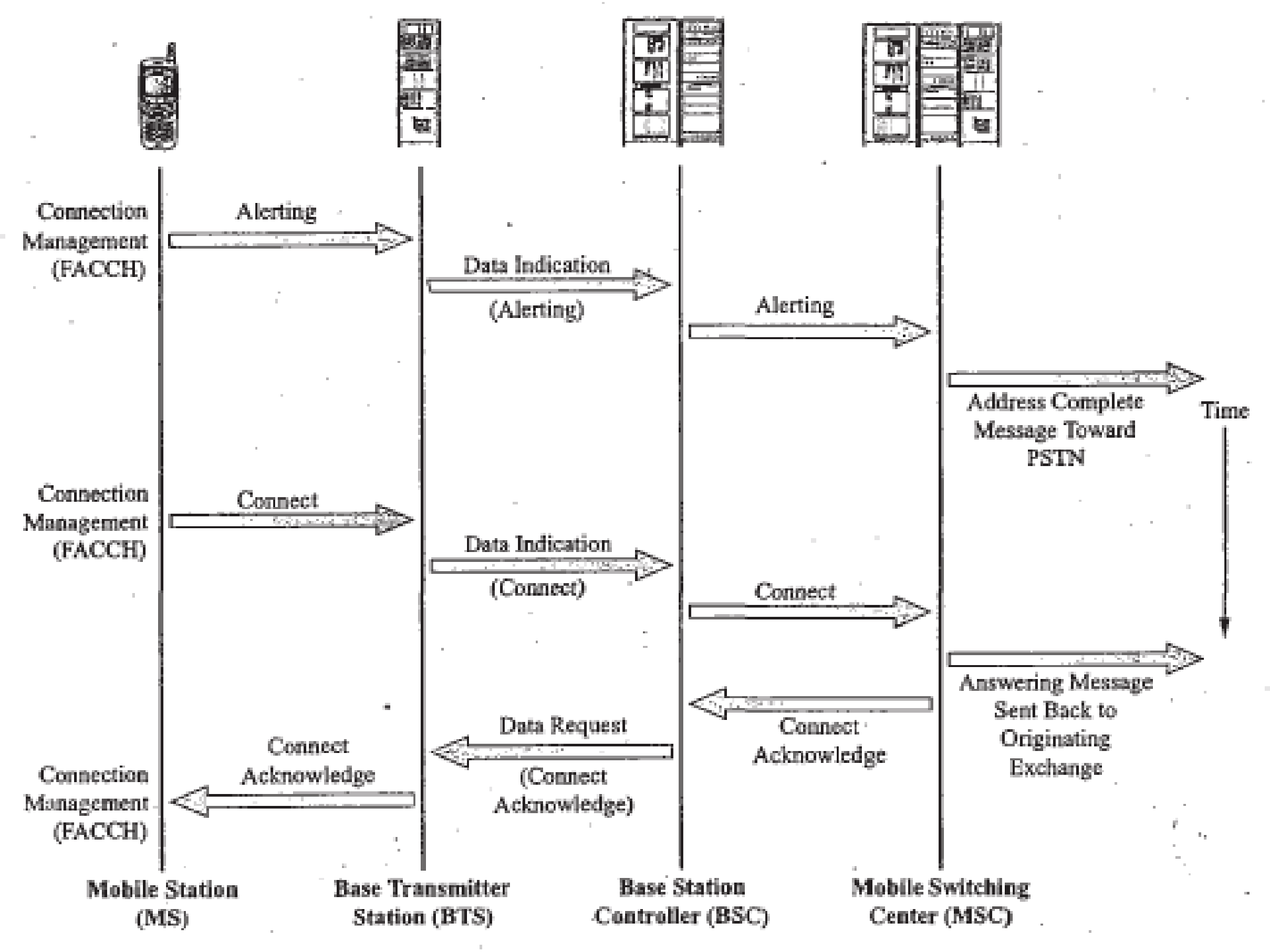
1. **Channel Request**
   - MS sends request on **RACH (Random Access Channel)**.
   - BSS forwards to MSC.
2. **Channel Assignment**
   - BTS/BSC assigns an **SDCCH (Standalone Dedicated Control Channel)** via **AGCH**.
3. **Authentication & Security**
   - Network authenticates MS using **AUC & HLR**.
   - Ciphering (encryption) may be activated.
4. **Call Setup Request**
   - MS sends dialed number to MSC over SDCCH.
   - MSC checks subscriber validity (HLR/VLR).
5. **Call Routing**
   - MSC routes call to PSTN / another MSC / another MS.
6. **Alerting**
   - Called party is alerted (ringing).
7. **Traffic Channel Assignment**
   - A **TCH (Traffic Channel)** is allocated.
   - Signaling switches to SACCH/FACCH for control.
8. **Conversation Phase**
   - Speech/data carried over TCH.

Mobile Originated Call

- 1, 2: connection and authentication request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call




BTS
MS
BCCH System parameters and other overhead
idle updated
Channel request RACH
number dialed
successful access
AGCH Assign stand alone dedicated control channel
Call establishment request SDCCH
send RAND
calculate SRES / Kc
SDCCH Authentication request
calculate SRES / Kc
Authentication response SDCCH
send SRES
SRES confirmed
SDCCH Request to transmit in cipher mode
switch to cipher mode
Acknowledge cipher mode request SDCCH
BTS
MS
Setup message for outgoing call SDCCH
SDCCH Assign traffic channel and release SDCCH
switch signaling to
FACCH using
assigned TCH
Acknowledge channel assignment FACCH
remote party ringing
FACCH Alerting remote party
ringing tone
remote party off-hook
FACCH Connect
switch to traffic channel
Connect acknowledge FACCH
switch to traffic channel
TCH data flow
Disconnect FACCH
mobile on-hook
FACCH Release
Release complete FACCH
FACCH Release traffic channel
idle updated


Connection Management (FACCH)
Alerting
Data Indication
(Alerting)
Alerting
Address Complete Message Toward PSTN
Time
Connection Management (FACCH)
Connect
Data Indication
(Connect)
Connect
Answering Message Sent Back to Originating Exchange
Connect Acknowledge
Data Request
(Connect Acknowledge)
Connect Acknowledge
Connection Management (FACCH)
Mobile Station (MS)
Base Transmitter Station (BTS)
Base Station Controller (BSC)
Mobile Switching Center (MSC)

Mobility Management

Definition

Mobility Management (MM) ensures that a mobile user can **move freely** while maintaining **continuous communication** — allowing the network to track and locate the mobile station (MS) at all times.

It is part of the **Network Switching Subsystem (NSS)** and works closely with **Location Management** and **Handoff Management**.

Major Functions of Mobility Management

1. **Location Management** – Finding and updating where the mobile station is.
2. **Authentication & Security Management** – Verifying and protecting the subscriber identity.
3. **Handover (Handoff) Management** – Ensuring ongoing calls are maintained while moving between cells.

🗺️ 1. Location Management

Helps the network **know where the subscriber is located** to deliver calls or messages.

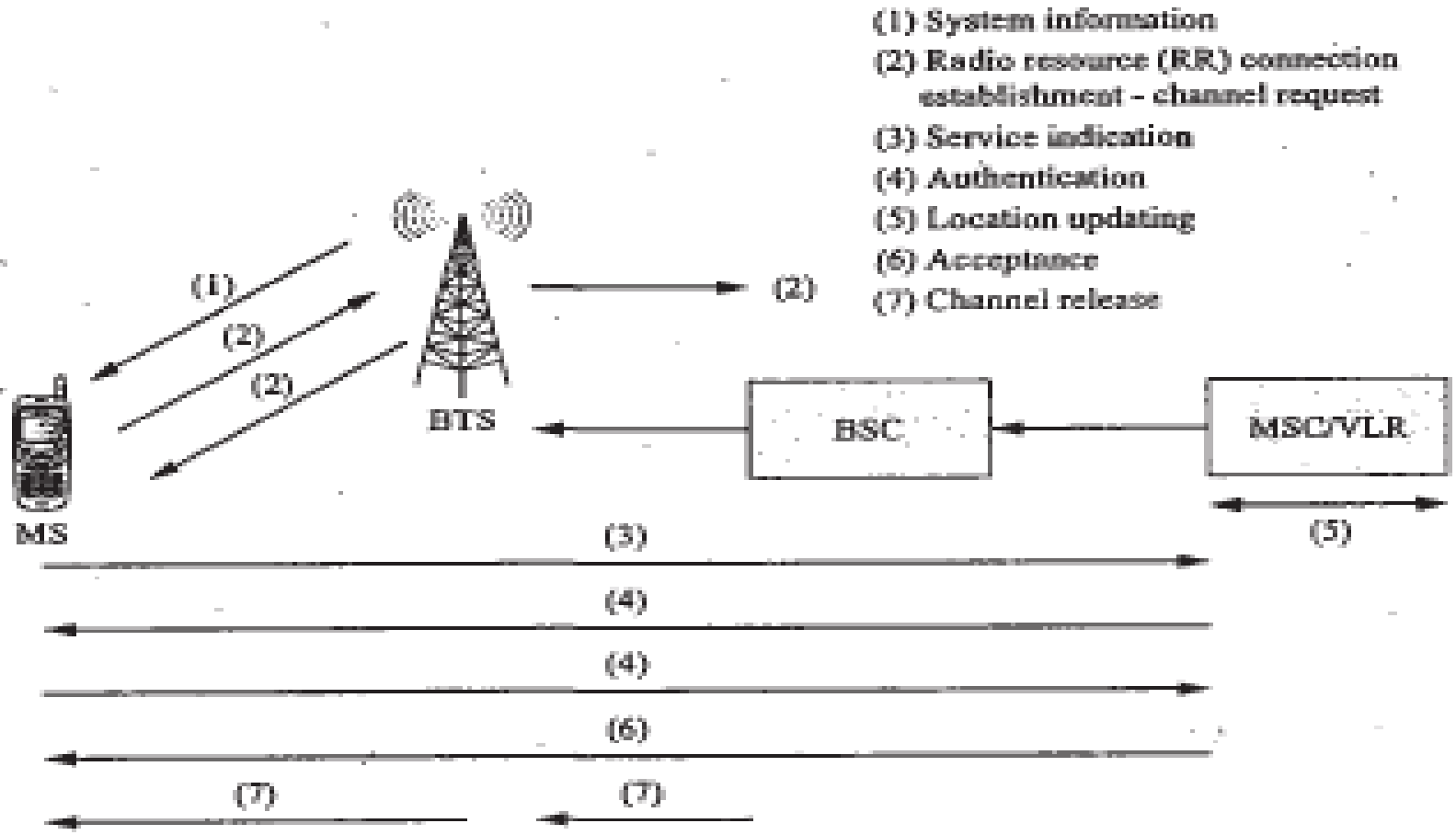
Components:

- **HLR (Home Location Register):** Stores permanent subscriber data (IMSI, services, authentication keys).
- **VLR (Visitor Location Register):** Temporary record of MS currently in its area.

Procedures:

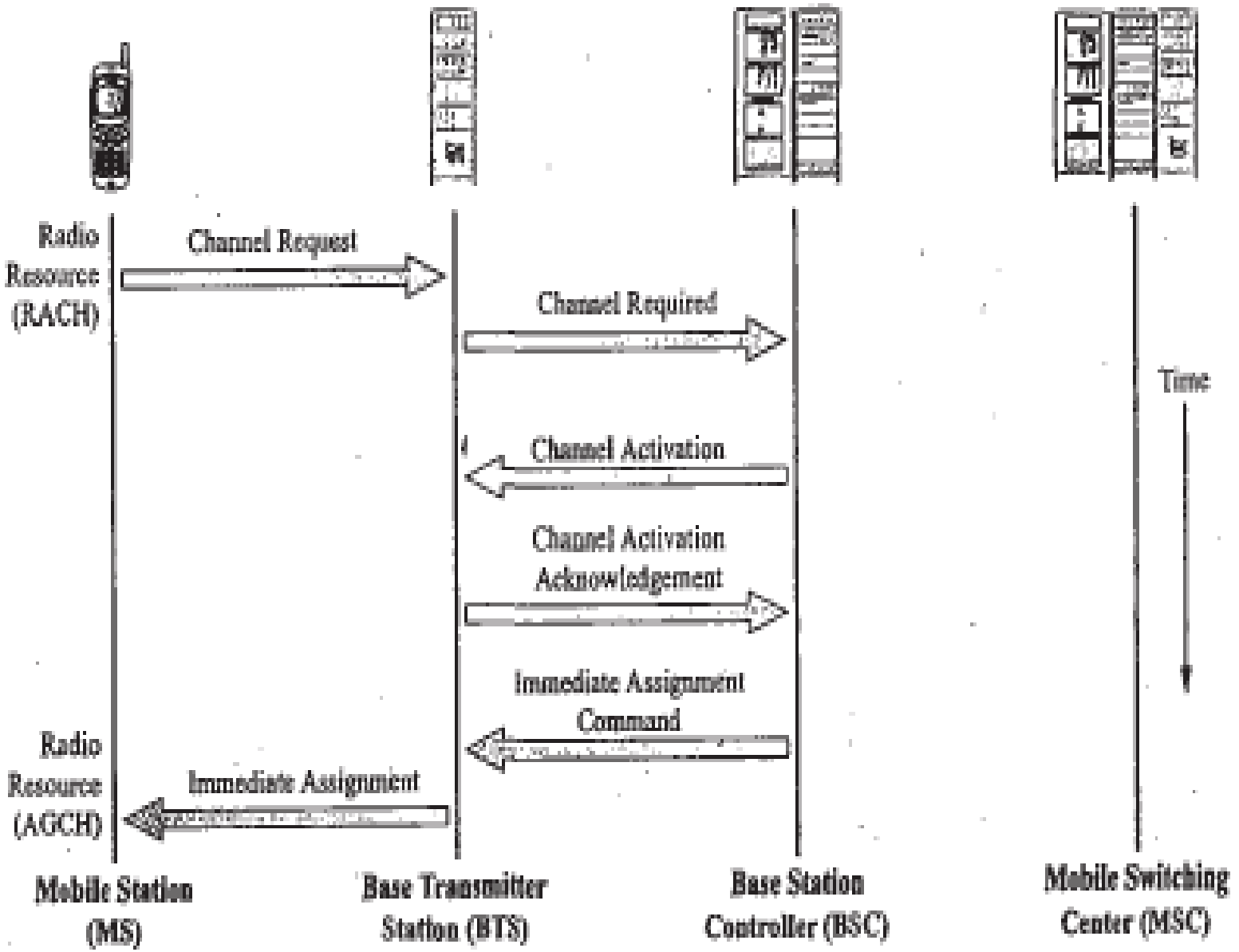
- **Location Update:**
  - MS informs the network of its new location area when:
    - Power is turned ON
    - Moving to a new Location Area (LA)
    - Periodic timer expires
  - MSC updates the **VLR**, and VLR updates **HLR**.

- **Paging:**
  - When there's an incoming call, MSC pages the MS in the **Location Area** using **Paging Channel (PCH)**.
  - MS responds via **RACH (Random Access Channel)**.



35 GSM location updating (Courtesy of Ericsson).

Normal Location Updating (Idle Mode) The basic steps involved with location updating look very similar to those used for call setup. The steps are radio resource connection establishment, service request, authentication (except for the case of periodic registration), cipher mode setting (depending upon the circumstances), location updating, and then radio resource connection release.



ire 5–36 GSM location updating.

🔐 2. Authentication & Security

Protects network and subscriber identity.

Steps:

1. **Authentication:**
    - MSC requests **AUC (Authentication Center)** to verify subscriber using **IMSI** and a random challenge.
    - MS uses a secret key (Ki) from its SIM to compute a response.
    - Network compares it with AUC's response — if matched, MS is authenticated.
2. **Ciphering (Encryption):**
    - Ensures confidentiality of transmitted data over the air interface (Um).
3. **Temporary Identity (TMSI):**
    - To protect subscriber's IMSI, a **Temporary Mobile Subscriber Identity** (TMSI) is assigned by the VLR.
    - Reduces chances of identity interception.

3. Handover (Handoff) Management

When a user moves between cells, the network performs **handover** to maintain call continuity.

Types:

- **Intra-BTS** (within same BTS)
- **Intra-BSC** (different BTS, same BSC)
- **Inter-BSC** (different BSC, same MSC)
- **Inter-MSC** (between different MSCs)

Handover decision is based on:

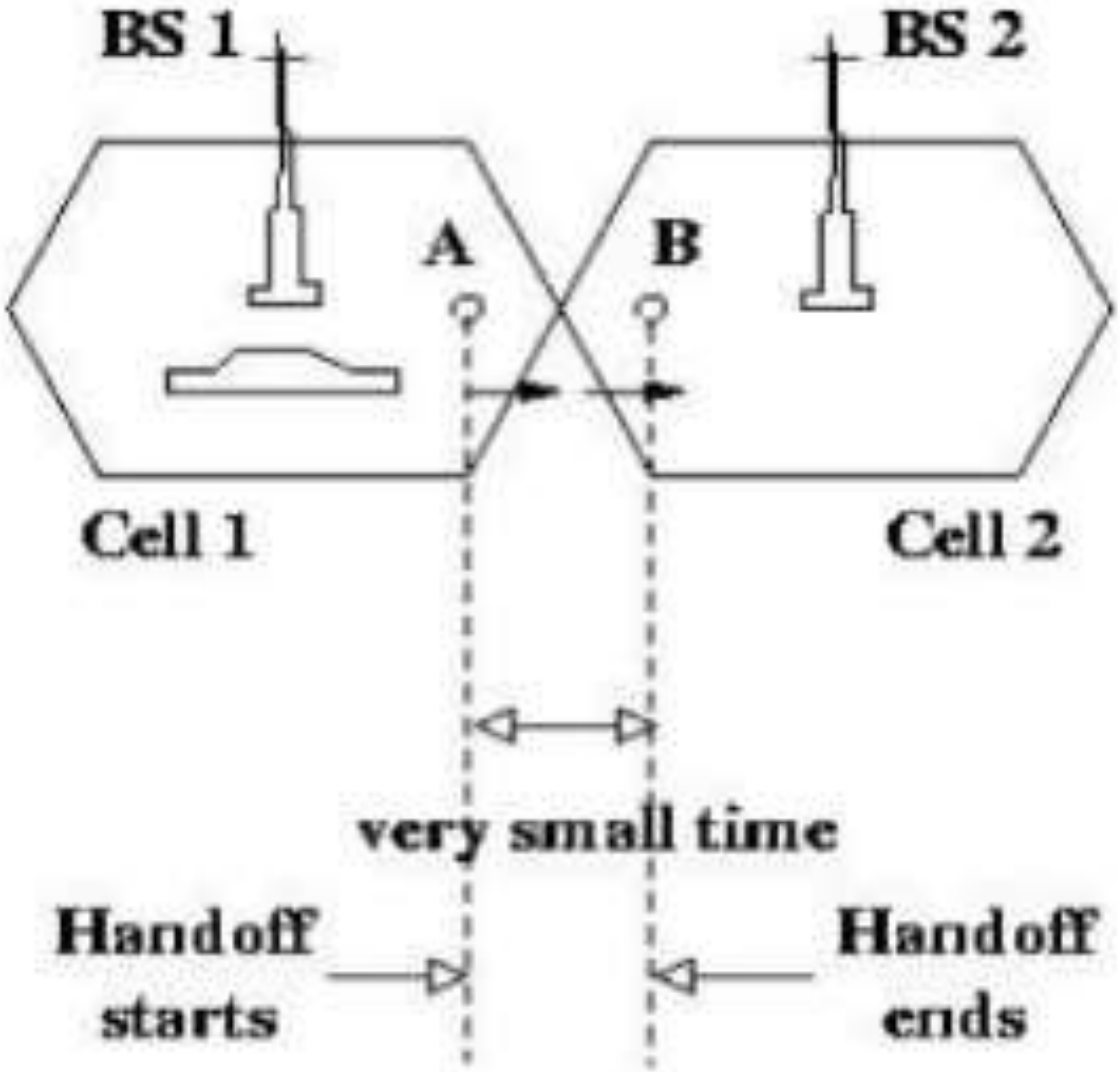
- Signal strength
- Signal quality
- Distance or timing advance
- Traffic load

Handoff

- Mobiles may move out of coverage area of a cell and into coverage area of a different cell during a call
- MSC must identify new BS to handle call
  - MSC must seamlessly transfer control of call to new BS
  - MSC must assign call new forward and reverse channels within the channels of new BS
- Some important performance metrics in handoff:
  - Seamless – user should not know handoff occurring
  - Minimum unnecessary Handoff due to short time fading
  - Low probability of blocking new calls in the new cell
  - Handoff to a good SNR channel so that an admitted call is not dropped

Intra-BTS handover This form of GSM handover occurs if it is required to change the frequency or slot being used by a mobile because of interference, or other reasons. In this form of GSM handover, the mobile remains attached to the same base station transceiver, but changes the channel or slot.

Intra-BTS handover



Inter-BTS Intra BSC handover This for of GSM handover or GSM handoff occurs when the mobile moves out of the coverage area of one BTS but into another controlled by the same BSC. In this instance the BSC is able to perform the handover and it assigns a new channel and slot to the mobile, before releasing the old BTS from communicating with the mobile.

Inter-BSC handover When the mobile moves out of the range of cells controlled by one BSC, a more involved form of handover has to be performed, handing over not only from one BTS to another but one BSC to another. For this the handover is controlled by the MSC.

Inter-MSC handover This form of handover occurs when changing between networks. The two MSCs involved negotiate to control the handover.