Unit 3

Telecommunication System - GSM

- ✓Mobile services
- ✓Architecture of a GSM System
- ✓Protocol Architecture
- ✓Radio Interface
- ✓Localization and calling - MTC, MOC
- ✓Handover
- ✓Security- Authentication, Encryption

Introduction to GSM

- Global System for Mobile Communication (GSM)
- Goal – Provide mobile phone system that allows users to roam.
- Its 2nd generation system replacing first generation analog system.
- Versions

Name	Uplink	Downlink	Description
GSM 900	**890 – 915 MHz**	**935- 960 MHz**	**Standard & Popular version**
GSM 1800	1710 – 1785 MHz	1805 – 1880 MHz	Digital Cellular System
GSM 1900	1850 – 1910 MHz	1930 – 1990 MHz	Personal Communication Service
GSM 400	450.4 – 457.6 MHz	460.4 – 467.6 MHz	Simple proposal

Characteristics of GSM

- Communication – mobile + wireless
- Total Mobility – International access
- Worldwide Connectivity – One number worldwide
- High capacity – small cells & more customers per cell
- High Transmission Quality – Uninterrupted calls
- Security functions – Access control, PIN

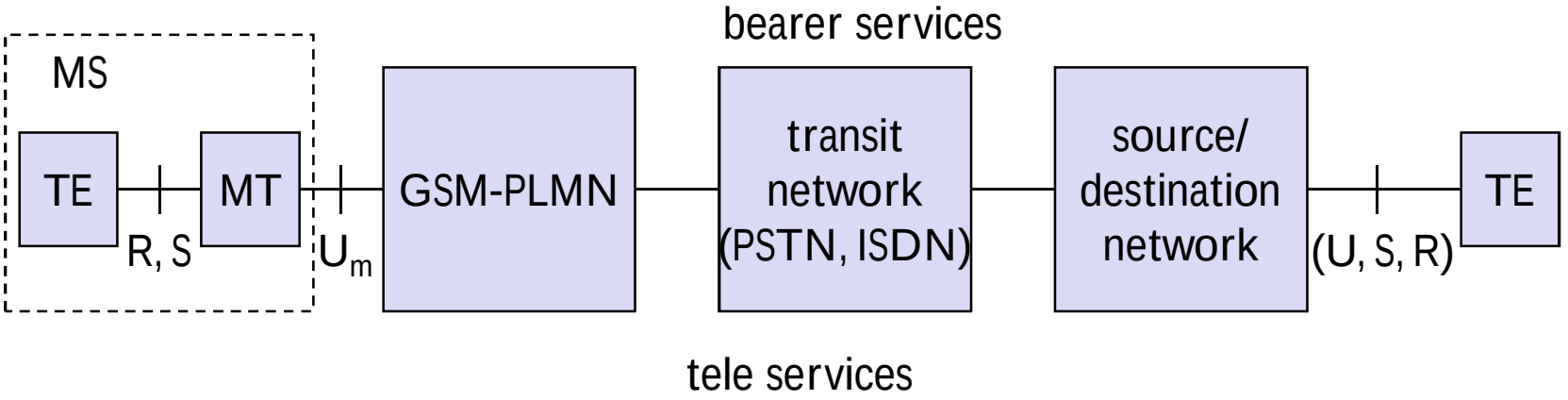
Disadvantages of GSM

- Electromagnetic radiation
- Abuse of private data is possible
- High complexity of system
- No end-to-end encryption of user

Mobile Services

Mobile Service Reference Model

- GSM permits integration of different voice and data services and their working with existing networks.



- MS is connected to PLMN via Um interface.
- It is connected to transit network of PSTN/ISDN.
- There might be additional network, source/destination before another TE is connected.
- Within MS, MT performs all network specific tasks.

Mobile Services

Three Types

1. Bearer Services – all services that enable transparent transmission between interfaces to network.

2. Teleservices – actual telecommunication services between source TE to destination TE.

3. Supplementary Services – extensive services.

Bearer Services

- Bearer Services permit transparent and non-transparent, synchronous and asynchronous transmission.

Transparent Bearer Services

- These services make use of only Physical Layer functions.
- To increase transmission quality it uses FEC (Forward Error Correction).

Non – Transparent Bearer Services

- Uses protocols of Layer 2 and Layer 3 for error correction and flow control.
- Radio Link Protocol (RLP) and High-Level data Link Control (HDLC).

Tele Services

- GSM focuses on voice-oriented tele-services.
- Deals with Encrypted voice transmission, message services and basic data communication.
- Various tele-services

1. Telephony - Provides high quality digital voice transmission, with 3.1 kHz bandwidth for analog phones.
2. Emergency Numbers – This service is mandatory for all operators and free of charge.
3. Short Message Service (SMS) – 160 characters
4. Enhanced Message Service (EMS) – 760 characters
5. Multimedia Message Service (MMS) – Text + Multimedia
6. Group 3 Fax – non voice telephony service.

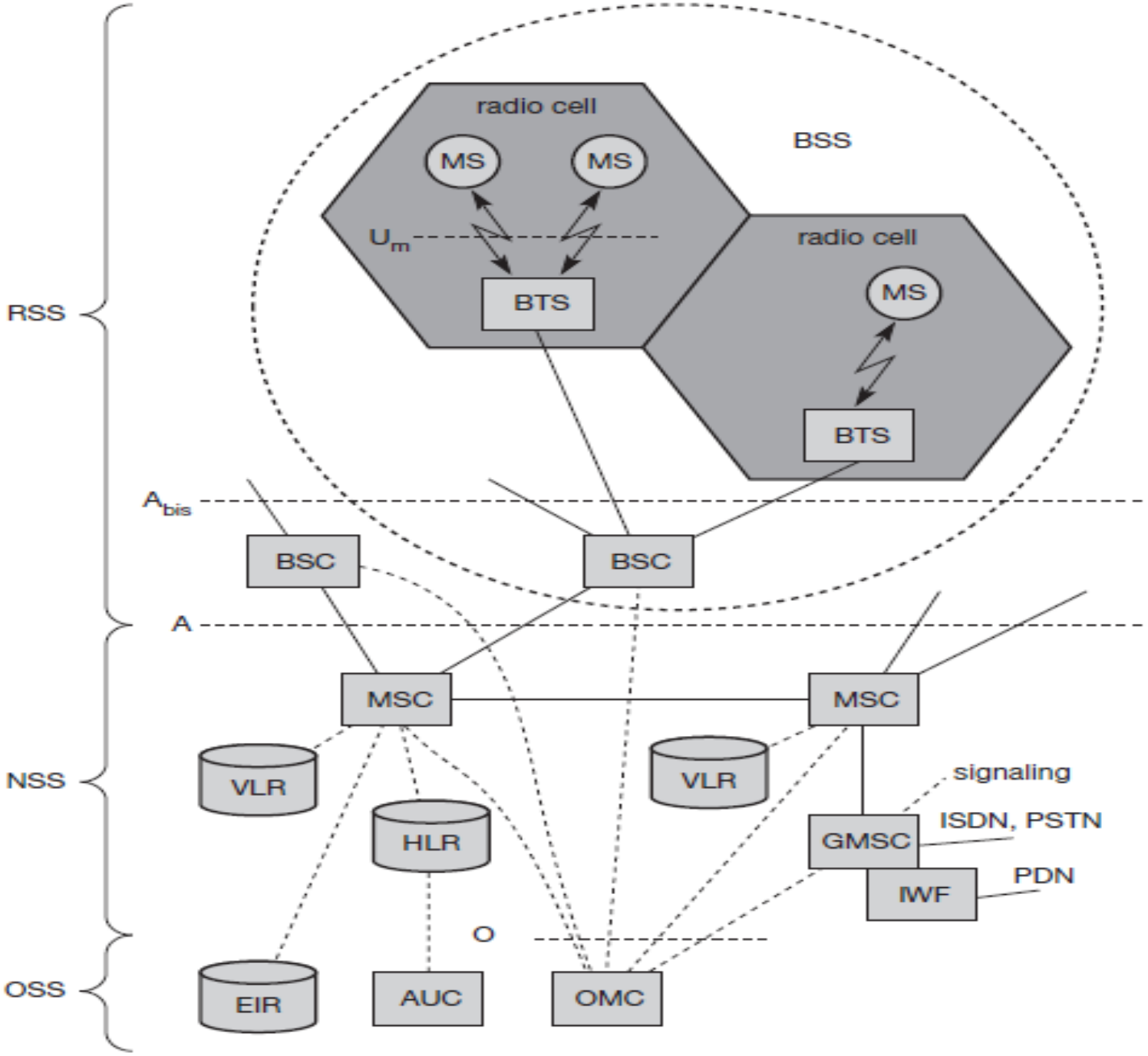
Supplementary Services

- User Identification (Caller ID)
- Call Redirection (Call Forward)
- Closed User Group - For commercial organizations.
- Multi-party communication (Call Conferencing)

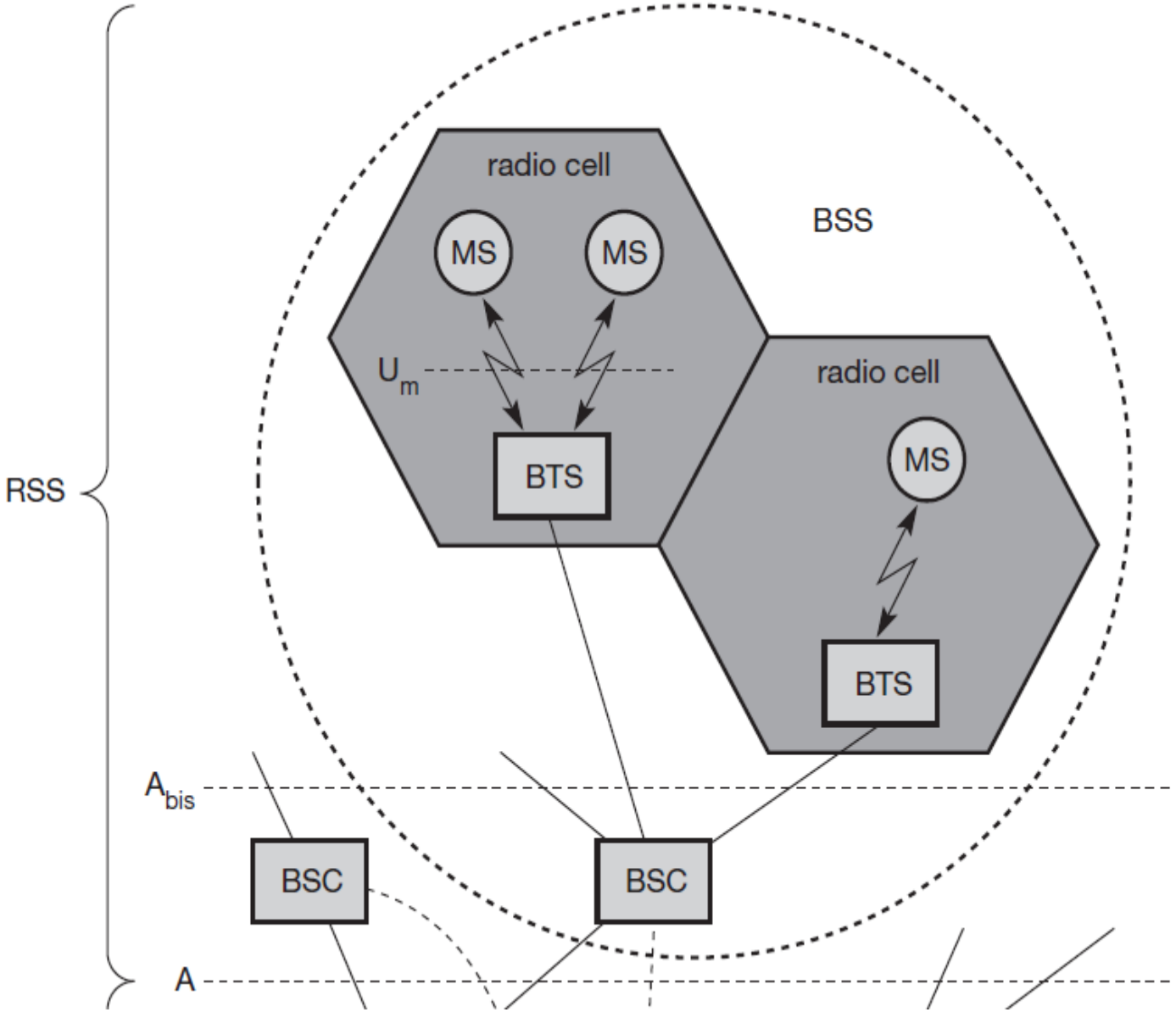
Architecture of GSM System

- A GSM System consists of 3 subsystems:

1. Radio Sub System (RSS)
2. Network and Switching Subsystem (NSS)
3. Operation Sub System (OSS)


radio cell
MS
MS
BSS
U_m
radio cell
BTS
MS
BTS
RSS
A_{bis}
BSC
BSC
A
MSC
MSC
NSS
VLR
VLR
signaling
HLR
ISDN, PSTN
GMSC
PDN
IWF
O
OSS
EIR
AUC
OMC

Radio Sub System (RSS)



RSS

Components

- **Base Station Subsystem (BSS)**

  It consists of MS, BTS and BSC.

- **Mobile Station (MS)**

➢ Consists of independent hardware, software and SIM.

➢ It can be identified by IMEI number.

➢ SIM consist of PIN, PUK, IMSI, Authentication key K1.

➢ MS stores dynamic information such as cipher key, TMSI and LAI (Location Area Identification).

RSS

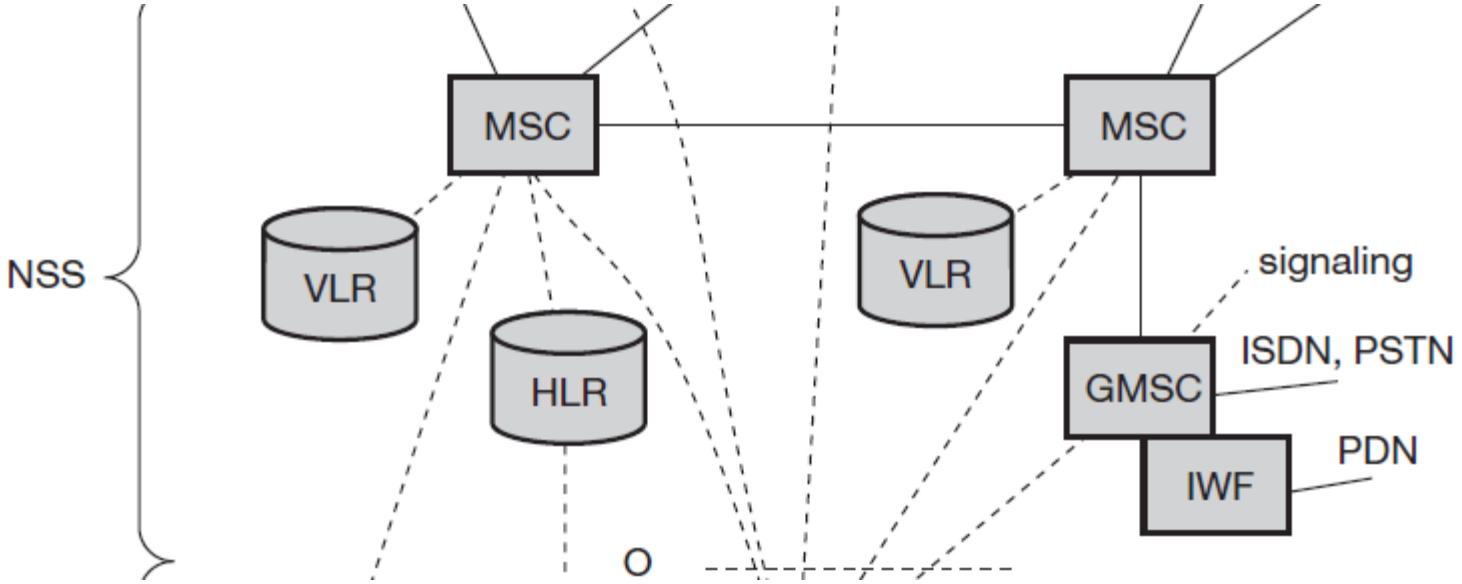
Components

- **Base Transceiver System (BTS)**
  - Sectorized antenna.
- **Base Station Controller (BSC)**
  - It is used to manage BTSs and control whole BSS.

Interfaces

Interface	Connects	Description
Um	MS and BTS	Radio Interface
A - bis	BTS and BSC	Open interface (16 kbps)
A	BSC and MSC	Open interface (64 kbps)

Network and Switching Subsystem (NSS)



- **Components**

MSC – Mobile Service Switching Center

IWF – Internetworking Functions

PSPDN – Packet Switched Public Data Net

CSPDN – Circuit Switched Public Data Net

PSTN – Public Switched Telephone Network

ISDN – Integrated Service Digital Network

- **Databases**

HLR

(Home Location Register)

VLR

(Visitor Location Register)

NSS

- **Mobile Service-Switching Center (MSC)**
  - Performs switching functions
  - Additional functions for mobility support
  - Management of network resources
  - Performs Internetworking functions via Gateway – MSC.
  - It integrates several databases.

Functions of MSC

1. Specific functions for paging and call forwarding
2. Termination of Standard signaling system number 7 (SS7)

   [number portability, free calls, call forwarding]

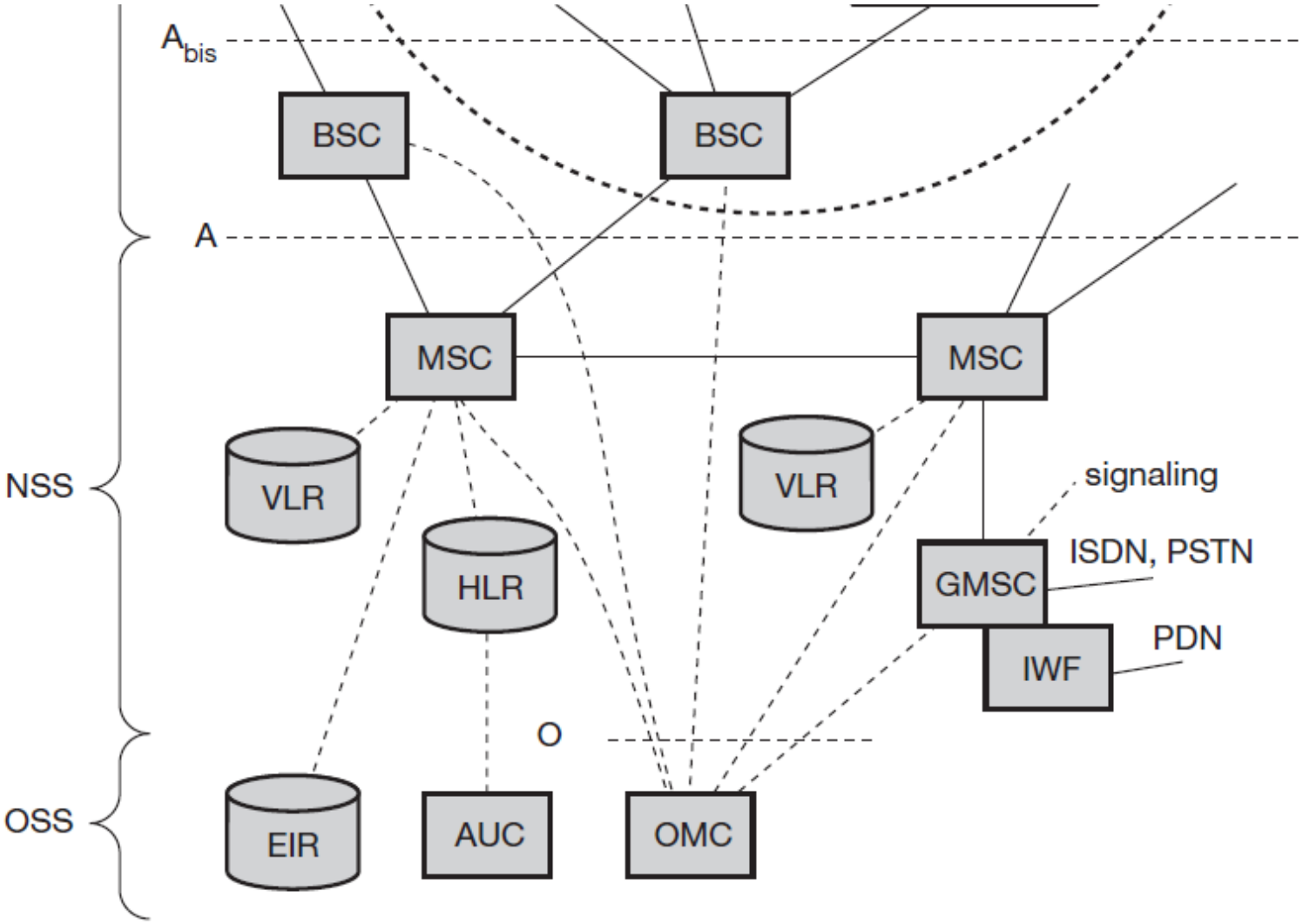
1. Location registration
2. Provision of new services (fax, data calls)
3. SMS support
4. Generation of accounting and billing information

NSS

- **Home Location Register (HLR)**
  - This database stores all user specific information
  - IMSI, LA (Location Area), MSRN
- **Visitor Location Register (VLR)**
  - Stores dynamic information needed for MS users.
  - If new MS comes into LA, the VLR copies all relevant user specific information from HLR.

- GMSC connected to fixed PSTN/ISDN.
- Using IWF, MSC can connected to PDN.

Operating Sub System (OSS)



OSS

Components

- **Operation and Maintenance Center**
  - Uses Telecommunication Management Network (TMN) and performs the functions like
    - ✓Traffic monitoring
    - ✓Status report of Network entities.

- **Authentication Center**
  - used to protect user identity and data transmission.
  - Contains algorithms, keys for encryption needed in HLR.

- **Equipment Identity Register**
  - Stores all device specific information such as IMEI.

Localization and Calling

Mobile Station International ISDN Number (MSISDN)

- Only important number for GSM in phone number of user.
- It consists of
  1. Country Code (CC)
  2. National Destination Code (NDC) – Service provider
  3. Subscriber Number (SN)

Localization and Calling

International Mobile Subscriber Identity (IMSI)

- Internal unique identification of subscriber.
- Consists of CC, NC, MSIN

Temporary Mobile Subscriber Identity (TMSI)

- Used to hide IMSI
- Local subscriber identification in roaming.
- Selected by current VLR and valid temporarily.

Mobile Station Roaming Number (MSRN)

- Another temporary address that hides mobile identity and location.
- Consists: Visitor Country Code(VCC) &
  Visitor National Destination Code (VNDC)

Mobile Terminated Call

1: calling a GSM subscriber

2: forwarding call to GMSC

3: signal call setup to HLR

4, 5: request MSRN from VLR

6: forward responsible MSC to GMSC

7: forward call to current MSC

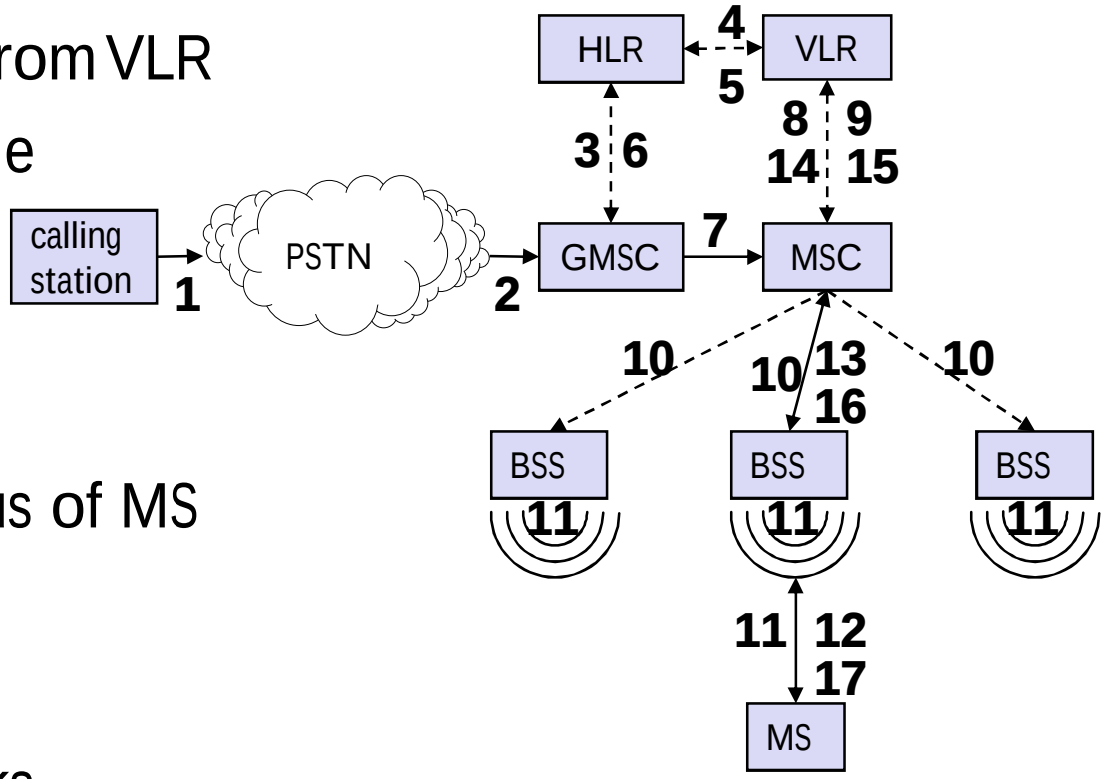
8, 9: get current status of MS

10, 11: paging of MS

12, 13: MS answers

14, 15: security checks

16, 17: set up connection



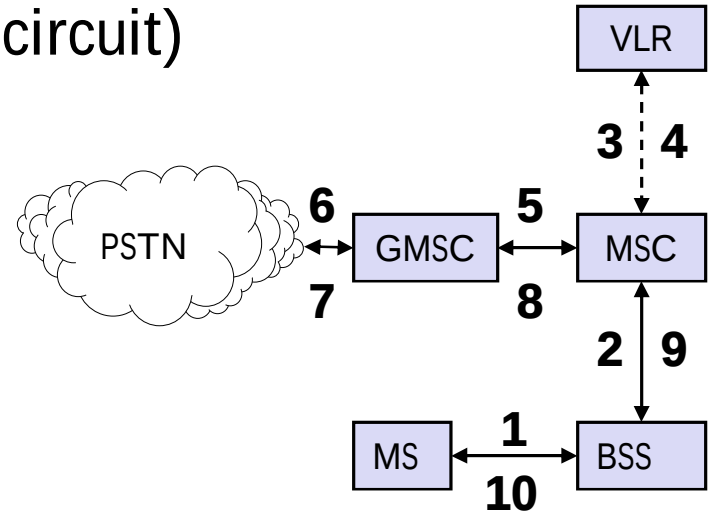
Mobile Originated Call

1, 2: connection request

3, 4: security check

5-8: check resources (free circuit)

9-10: set up call



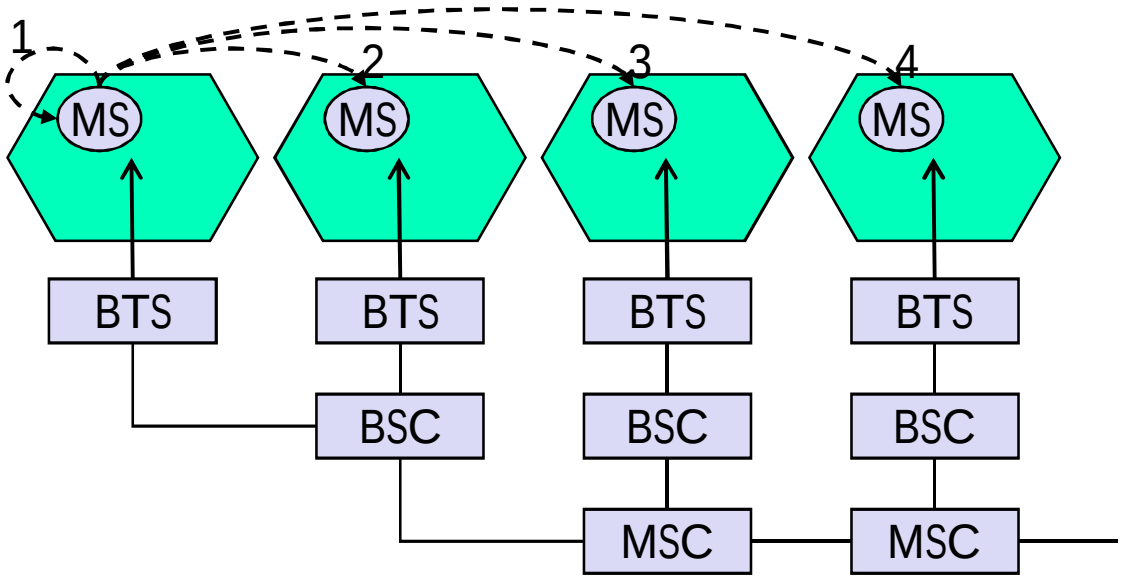
Handover

- As single cell can not cover all area, it has to handover the call.
- But this handover should not cause cut off or call drop.

- Reasons: why to perform handover?

1. Inverse square law.
2. Load balancing

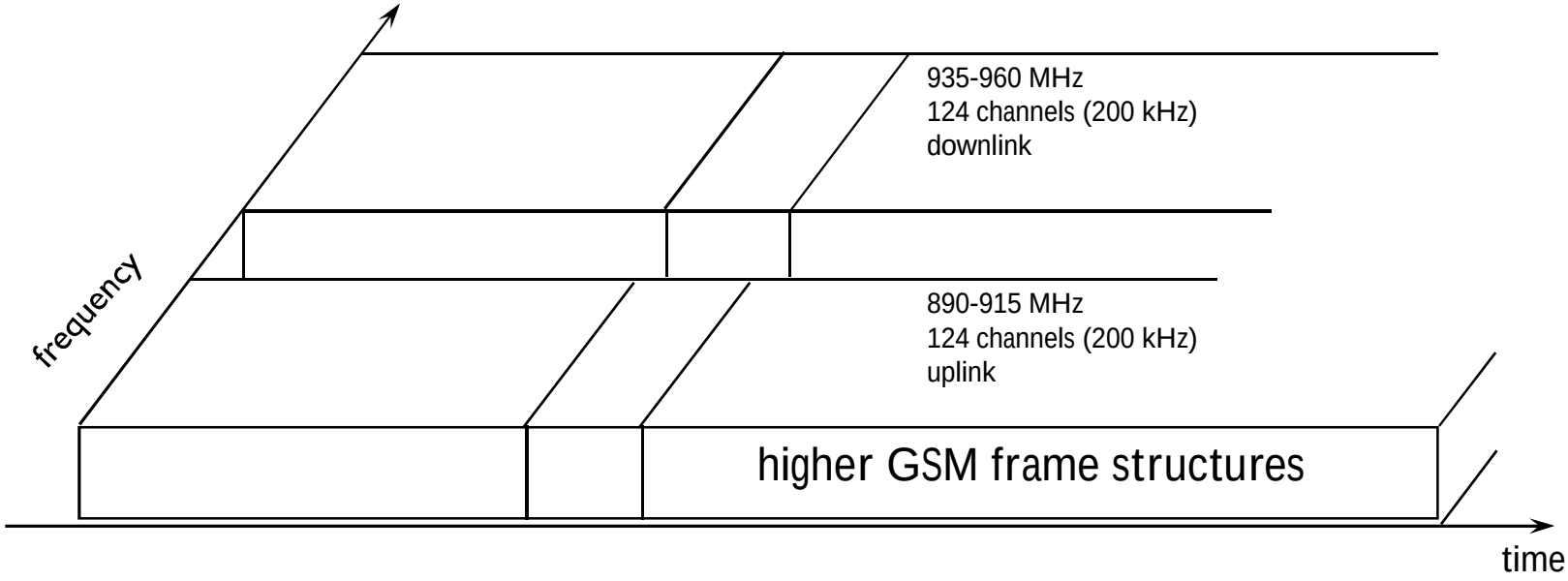
Handover



- Intra cell handover – within same cell
- Inter-cell, Intra-BSC handover – different cells within same BSC
- Inter-BSC, Intra-MSC handover – different BSC within same MSC
- Inter MSC handover – Different MSC

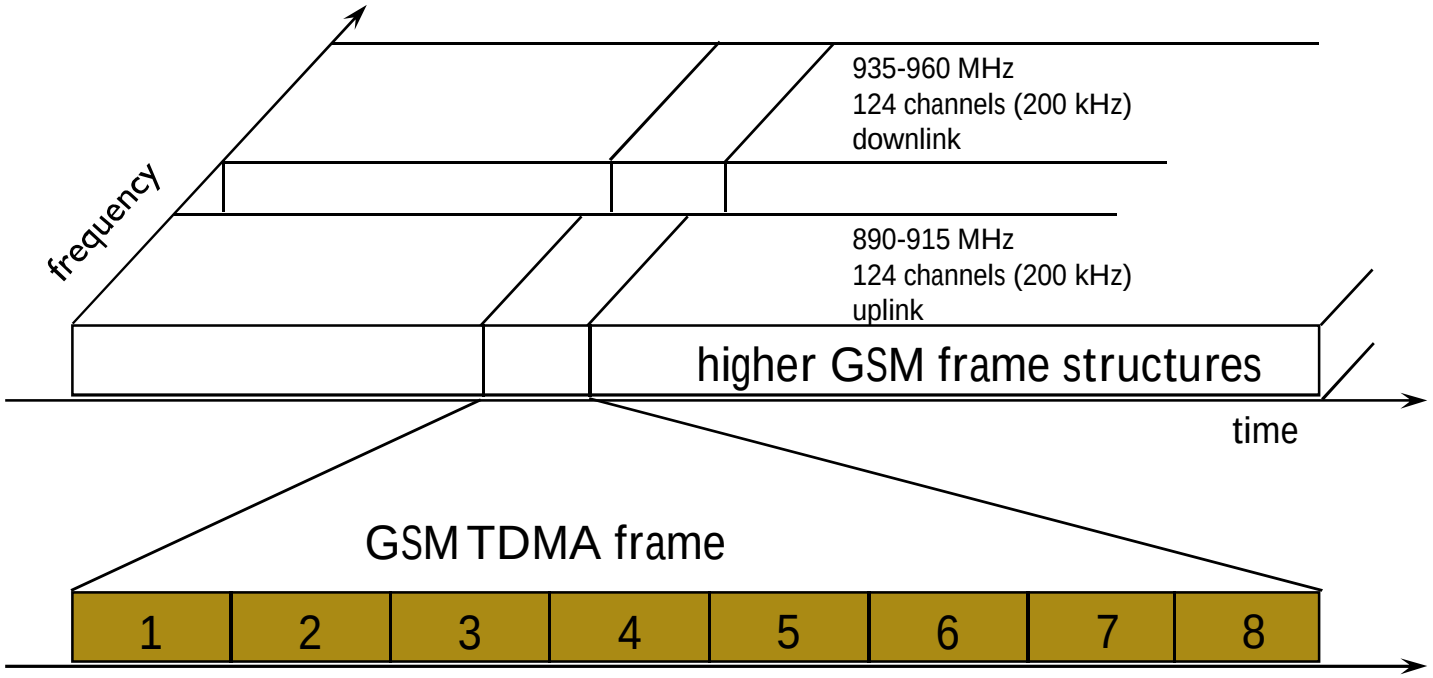
Radio Interface

- Most important interface → Um.
- GSM implements SDMA using cells with BTS and assign MS to BTS.
- Medium access control mechanism combines FDMA & TDMA together.
- In GSM-900, 124 channels each with 200KHz wide for uplinks as well as downlink.

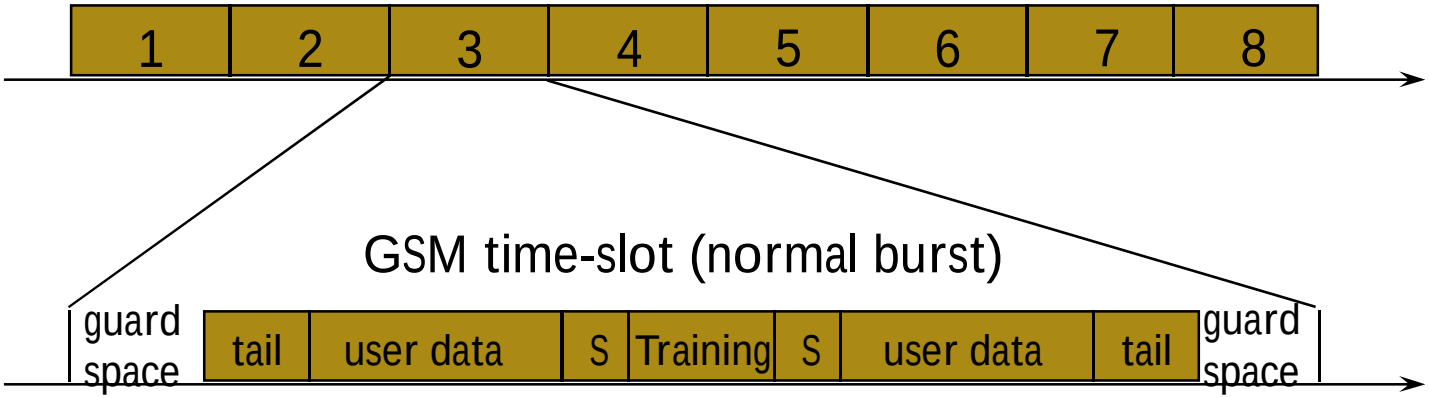


Radio Interface

- Each of 248 channel is additionally separated in time via TDMA frame.
- This frame is again subdivided into 8 time slots



Radio Interface



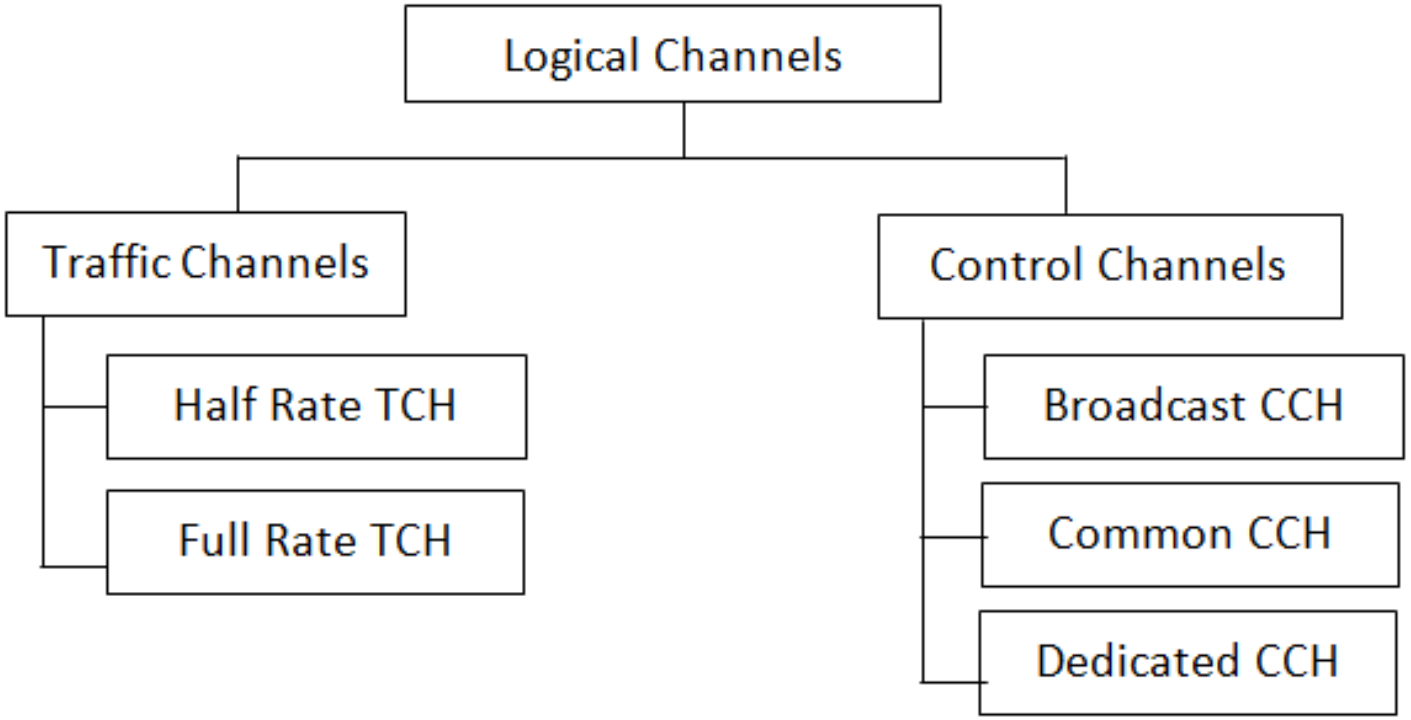
- *Data transmission in small portion is called burst*.
- Normal burst used for data transmission within time slot.
- **Tail** used for synchronous transmission.
- **Training sequence** is used to adapt receiver's parameter.
- **Flag S** is used to indicate whether data filed contains user data or network data.

Radio Interface

- Other burst for data transmission are:

1. **Frequency Correction** – allows MS to correct local oscillator to avoid neighboring channels.
2. **Synchronization Burst** – Synchronizes MS and BTS.
3. **Access Burst** – For initial connection set up between MS and BTS.
4. **Dummy Burst** – used if no data available.

Logical Channels



Traffic Channels (TCH)

- Full Rate TCH (TCH/F) – data rate 22.8 kbps
- Half Rate TCH (TCH/H) – data rate 11.4 kbps

- TCH/FS (Full rate Speech) – used for error correction
  - ✓ Full Rate (FR) – 13 bps
  - ✓ Half Rate (HR) – 5.6 bps
  - ✓ Enhanced Full Rate (EFR) – better than FR

- **Tandem Free Operations (TFO)** used to **avoid** the traditional double speech encoding / decoding in MS to MS call configurations.

Control Channels (CCH)

- Control Channel are used to control medium access, allocation of traffic channels and mobility management.

A) Broadcast Control Channel (BCCH)
B) Common Control Channel (CCCH)
C) Dedicated Control Channel (DCCH)

Broadcast Control Channel (BCCH)

- BTS uses this channel to send information to all MSs within a cell

1. Frequency Correction Channel (FCH)

- BTS send frequency correction information via this channel.

2. Synchronization Channel (SCH)

- BTS send synchronization information via this channel.

Common Control Channel (CCCH)

- All information regarding **connection set up between MS and BTS** is exchanged via CCCH.

1. Paging Channel (PCH) – BTS uses it to page MS.
2. Random Access Channel (RACH) – MS sends data to BTS
3. Access Grant Channel (AGCH) – BTS uses it to signal MS that it can use connection set up.

Dedicated Control Channel (DCCH)

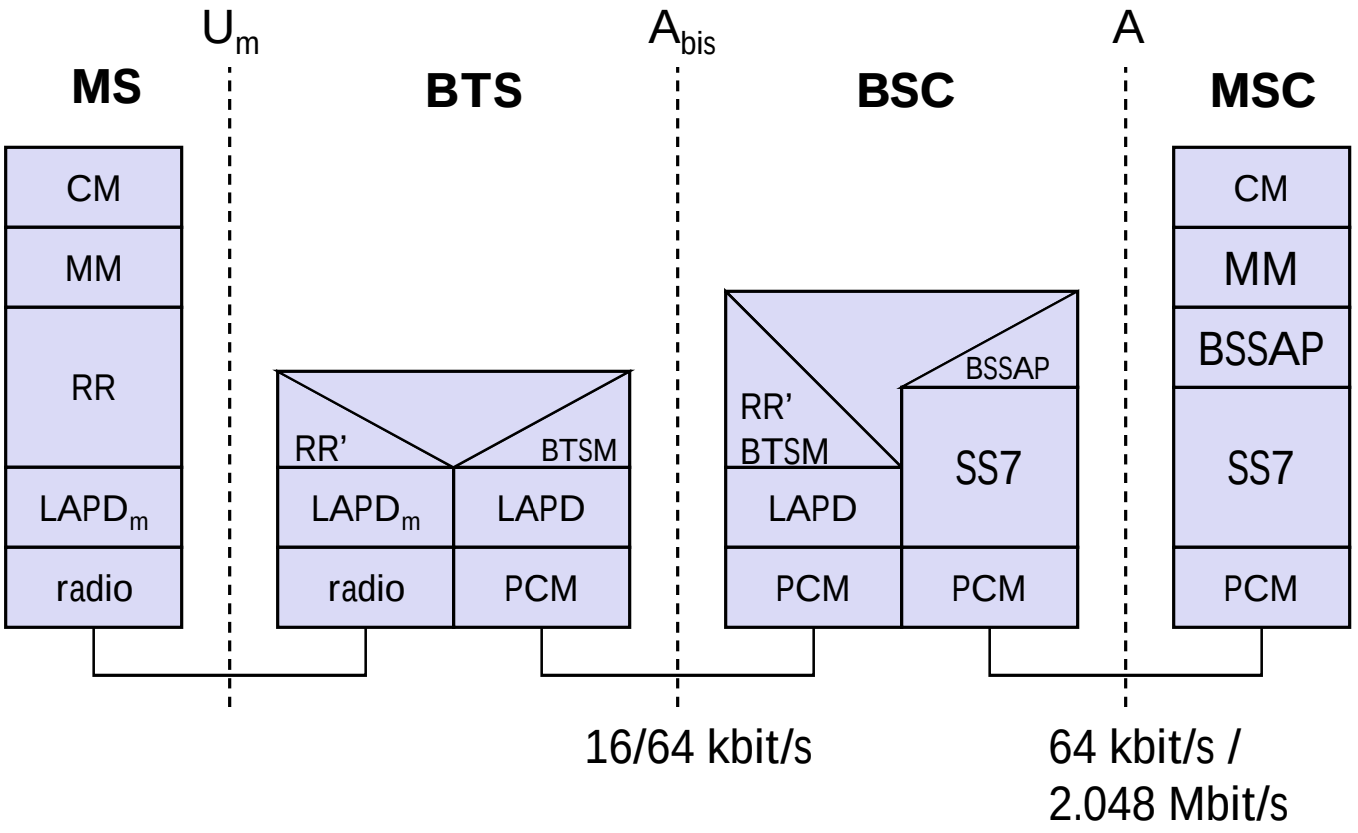
- These are the bidirectional channels that BTS uses.

1. Standalone DCCH (SDCCH) – low data rate signaling if MS has not established connection with BTS.

2. Slow Associated DCCH (SACCH) – used to exchange system information such as signal power & channel quality.

3. Fast Associated DCCH (FACCH) – used for handover where MS and BTS exchange large data.

GSM Protocol Architecture



GSM Protocol Architecture

- CM – Call Management
- MM – Mobility Management
- RR – Radio Resource Management
- LAPD – Link Access Protocol for D-Channel
- PCM – Pulse Code Modulation
- BTSM – BTS Management
- SS7 – Signaling System Number 7
- BSSAP – BSS Application Part

GSM Protocol Architecture

Layer 1 (Physical Layer)

- Handles all radio specific functions →
  - Multiplexing
  - Synchronization
  - Digital Modulation
  - Encryption
  - Channel Quality measurement
  - Error Detection / Correction
- It contains special voice function, Voice Activity Detection
- Protocols – Radio, PCM

GSM Protocol Architecture

Layer 2

- Protocols – $LAPD_m$, SS7
- $LAPD_m$ -[Link Access Procedure for D-Channel]
- It is defined is radio interface U_m
- D-channel – ISDN channel in which control and signaling information is carried.
- Signaling System 7 – used to exchange the information in PSTN channel between MSC & BSC

GSM Protocol Architecture

Layer 3

- Protocols – RR, BTSM
- RR [Radio Resource Management] – inside BTS
- BTSM [BTS Management] - Functions of RR are supported by BSC via this BTSM.

GSM Protocol Architecture

Layer 4 & 5

- Protocols – MM, CM
- MM [Mobility Management] – contains functions like –
  - Registration
  - Authentication
  - Identification
- CM [Call Management] –
  - Call Control
  - SMS & MMS
  - Supplementary Services

GSM Protocol Architecture

Layer 4 & 5

- Protocols – MM, CM
- MM [Mobility Management] – contains functions like –
  - Registration
  - Authentication
  - Identification
- CM [Call Management] –
  - Call Control
  - SMS & MMS
  - Supplementary Services

GSM Security

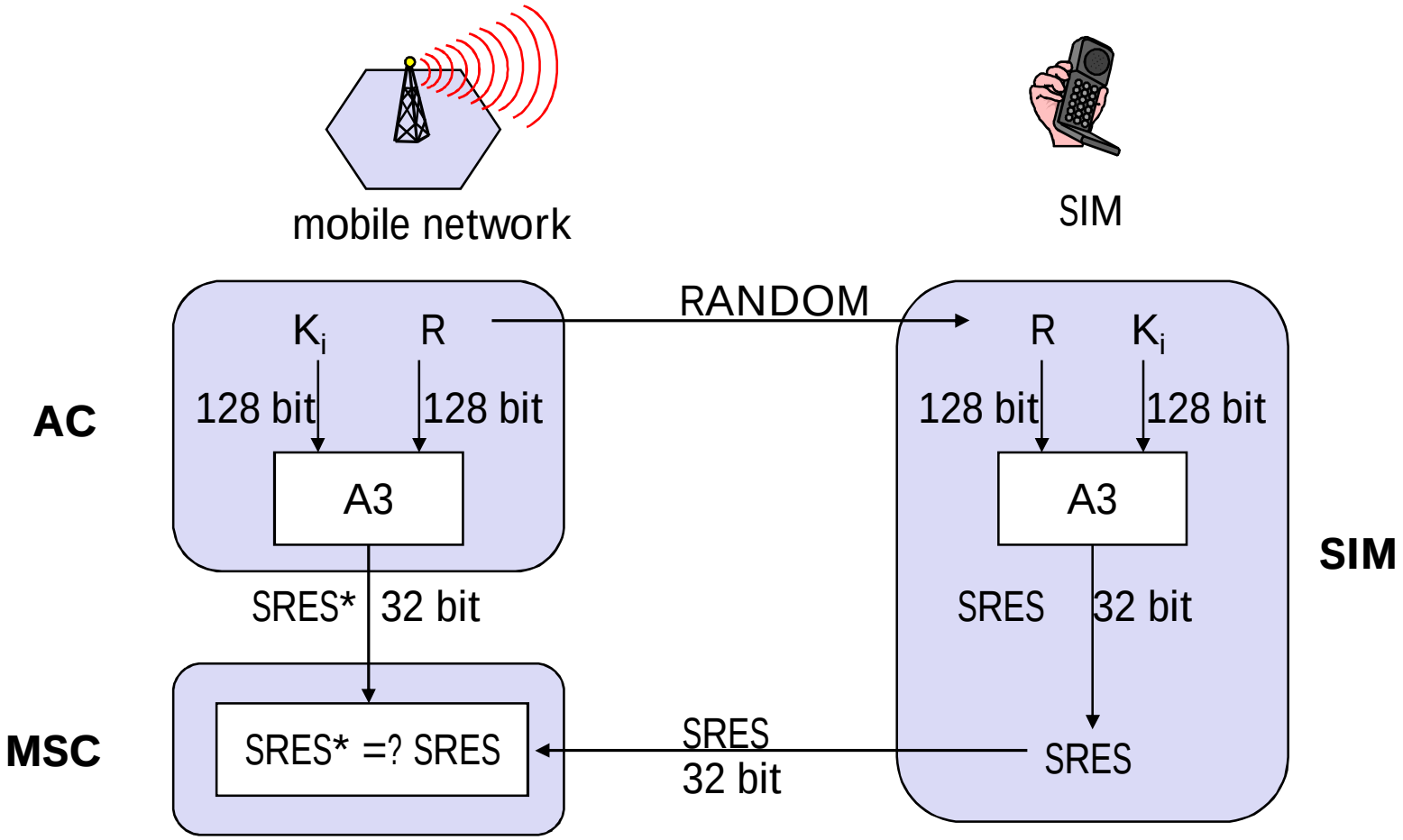
- access control/authentication
  - user ⇔ SIM (Subscriber Identity Module): secret PIN (personal identification number)
  - SIM ⇔ network: challenge response method
- confidentiality
  - voice and signaling encrypted on the wireless link (after successful authentication)
- anonymity
  - temporary identity TMSI (Temporary Mobile Subscriber Identity)
  - newly assigned at each new location update (LUP)
  - encrypted transmission

GSM Security

3 algorithms specified in GSM

- A3 for authentication (“secret”, open interface)
- A5 for encryption (standardized)
- A8 for key generation (“secret”, open interface)

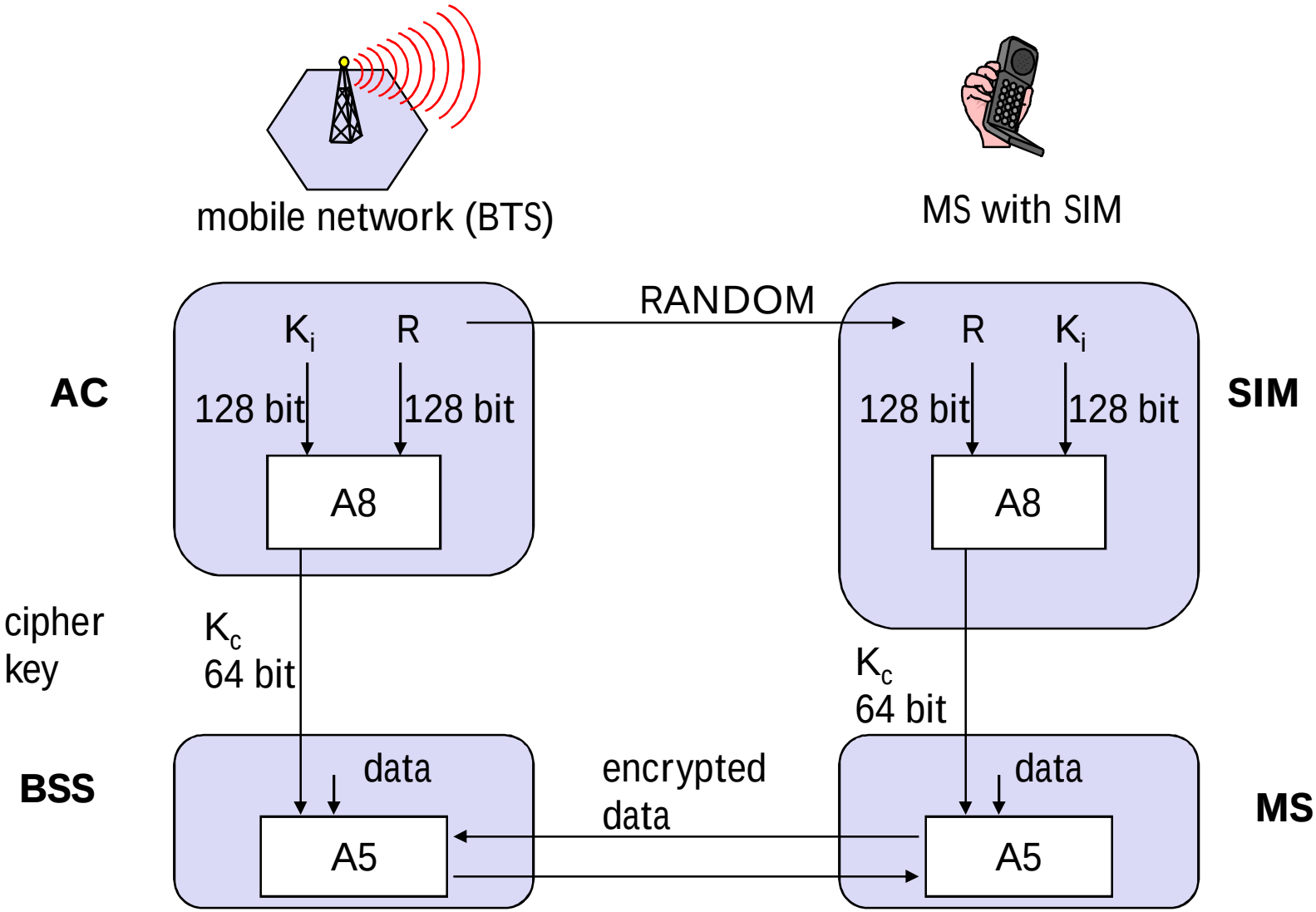
Authentication



K_i: individual subscriber authentication key

SRES: signed response

Encryption


mobile network (BTS)
MS with SIM
RANDOM
AC
SIM
K_i
R
128 bit
128 bit
A8
cipher key
K_c
64 bit
BSS
data
A5
encrypted data
MS