بسم الله الرحمن الرحيم

Mobile Networking

Mohammad Hossein Manshaei

manshaei@gmail.com

1393

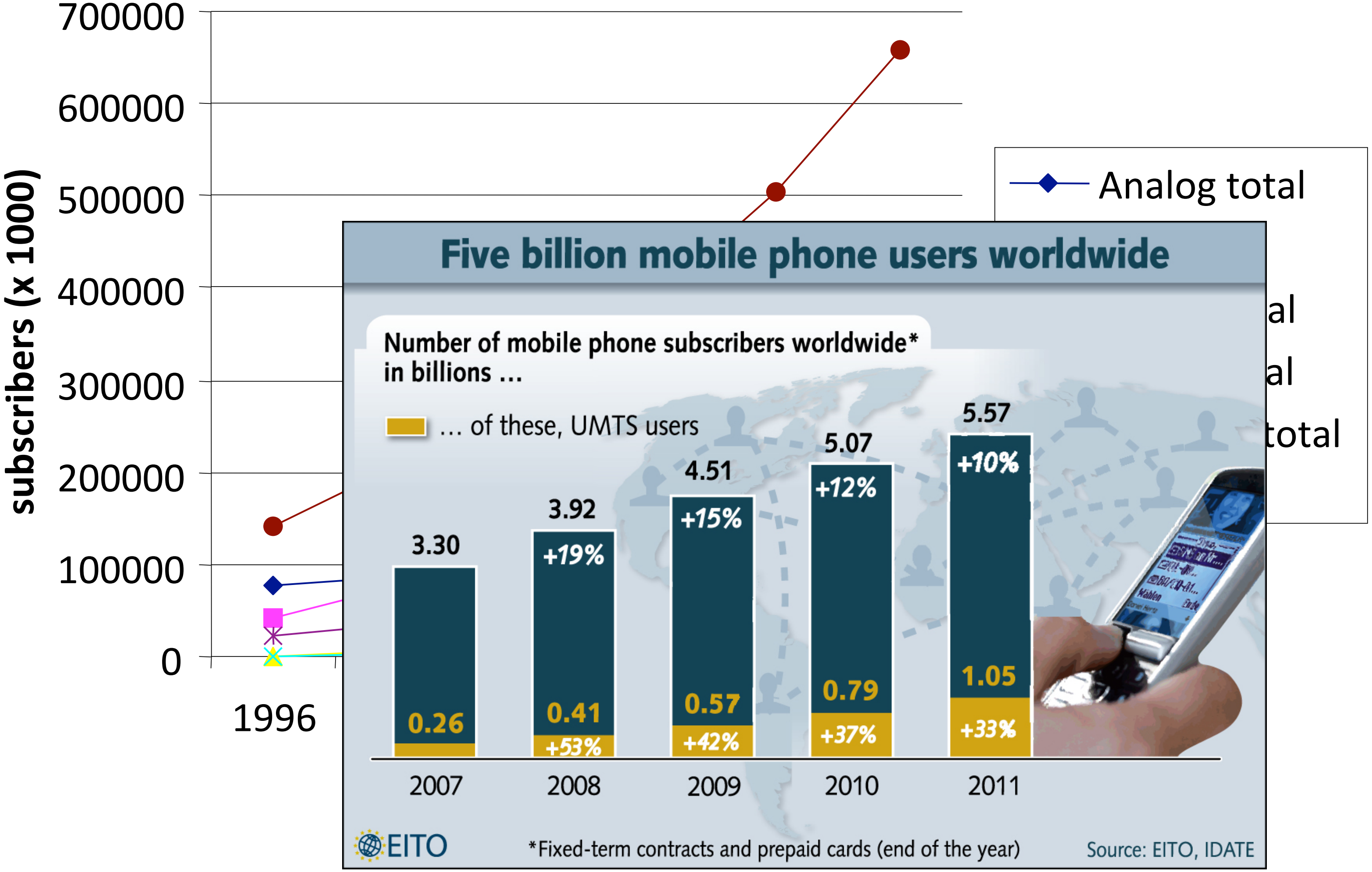
GSM

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Content

- GSM Architecture
- Frequency Band and Channels
- Frames in GSM
- Interfaces, Planes, and Layers of GSM
- Handoff
- Short Message Service (SMS)

Mobile Phone Subscribers Worldwide



*Fixed-term contracts and prepaid cards (end of the year)

Source: EITO, IDATE

GSM: Overview

- **GSM**
  - **formerly:** Groupe Spéciale Mobile (founded 1982)
  - **now:** Global System for Mobile Communication
  - Pan-European standard (ETSI, European Telecommunications Standardisation Institute)
  - Simultaneous introduction of essential digital cellular services in three phases (1991, 1994, 1996) by the European telecommunication administrations, seamless roaming within Europe possible
  - Today many providers all over the world use GSM (more than 130 countries in Asia, Africa, Europe, Australia, America)

Performance Characteristics of GSM

- **Communication**
  - mobile, wireless digital communication; support for voice and data services
- **Total mobility**
  - international access, chip-card enables use of access points of different providers
- **Worldwide connectivity**
  - one number, the network handles localization
- **High capacity**
  - better frequency efficiency, smaller cells, more customers per cell
- **High transmission quality**
  - high audio quality
  - uninterrupted phone calls at higher speeds (e.g., from cars, trains) – better handoffs and
- **Security functions**
  - access control, authentication via chip-card and PIN

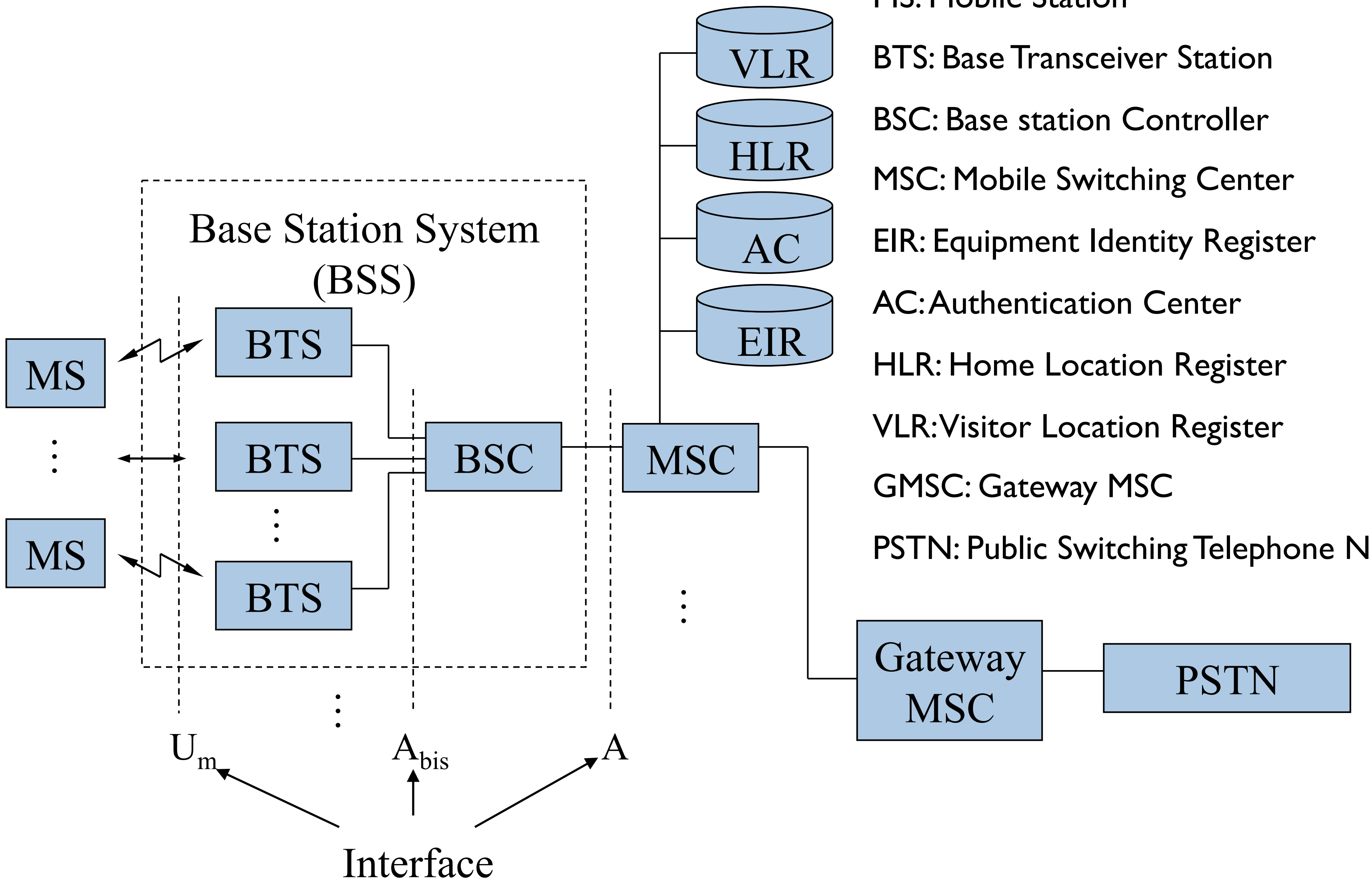
Disadvantages of GSM

- **There is no perfect system!!**
  - no end-to-end encryption of user data
  - no full ISDN bandwidth of 64 kbit/s to the user, no transparent B-channel

  - **abuse of private data possible**
    - roaming profiles accessible

  - **high complexity of the system**
  - **several incompatibilities within the GSM standards**

GSM Infrastructure



MS: Mobile Station

BTS: Base Transceiver Station

BSC: Base station Controller

MSC: Mobile Switching Center

EIR: Equipment Identity Register

AC: Authentication Center

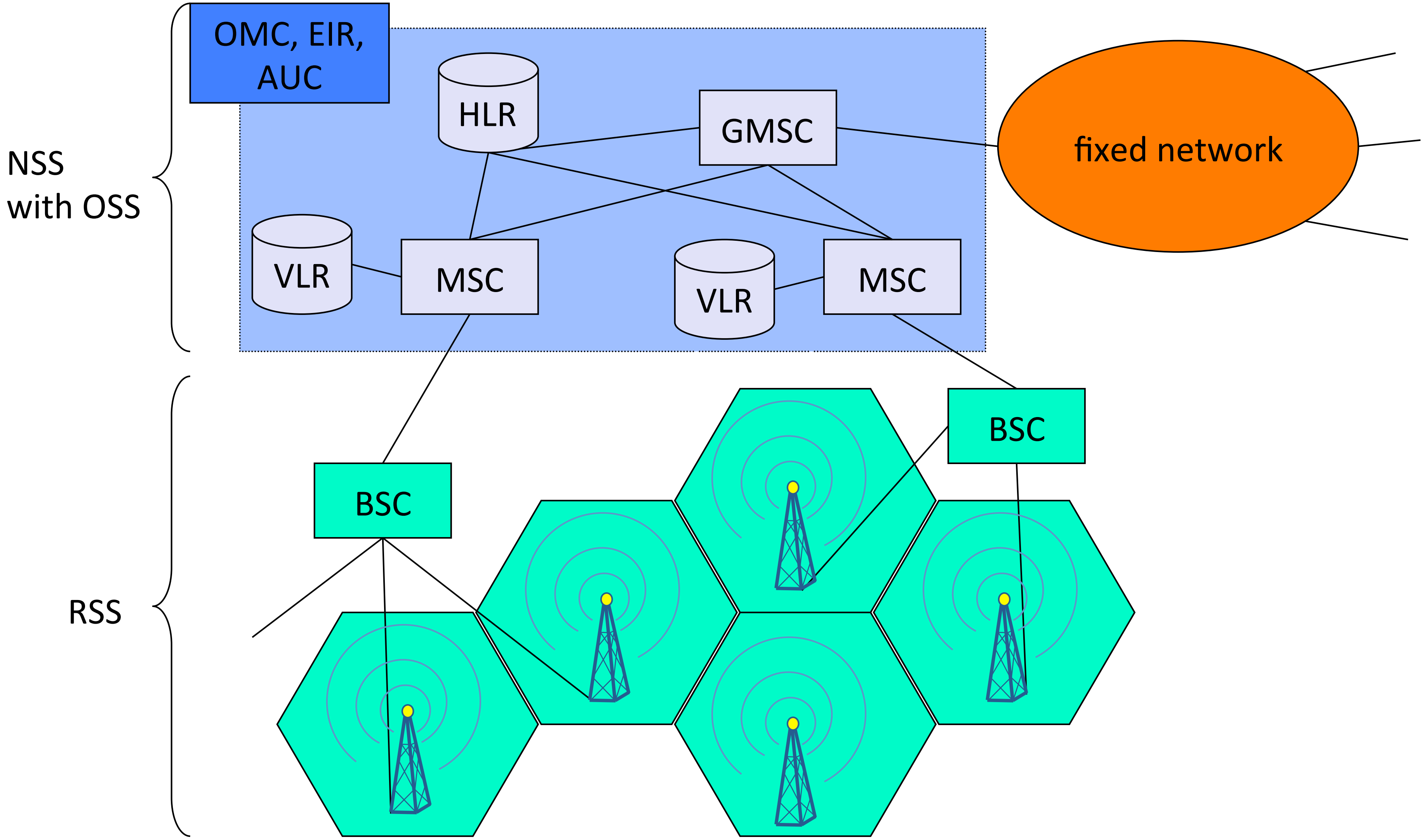
HLR: Home Location Register

VLR: Visitor Location Register

GMSC: Gateway MSC

PSTN: Public Switching Telephone Network

GSM: Overview



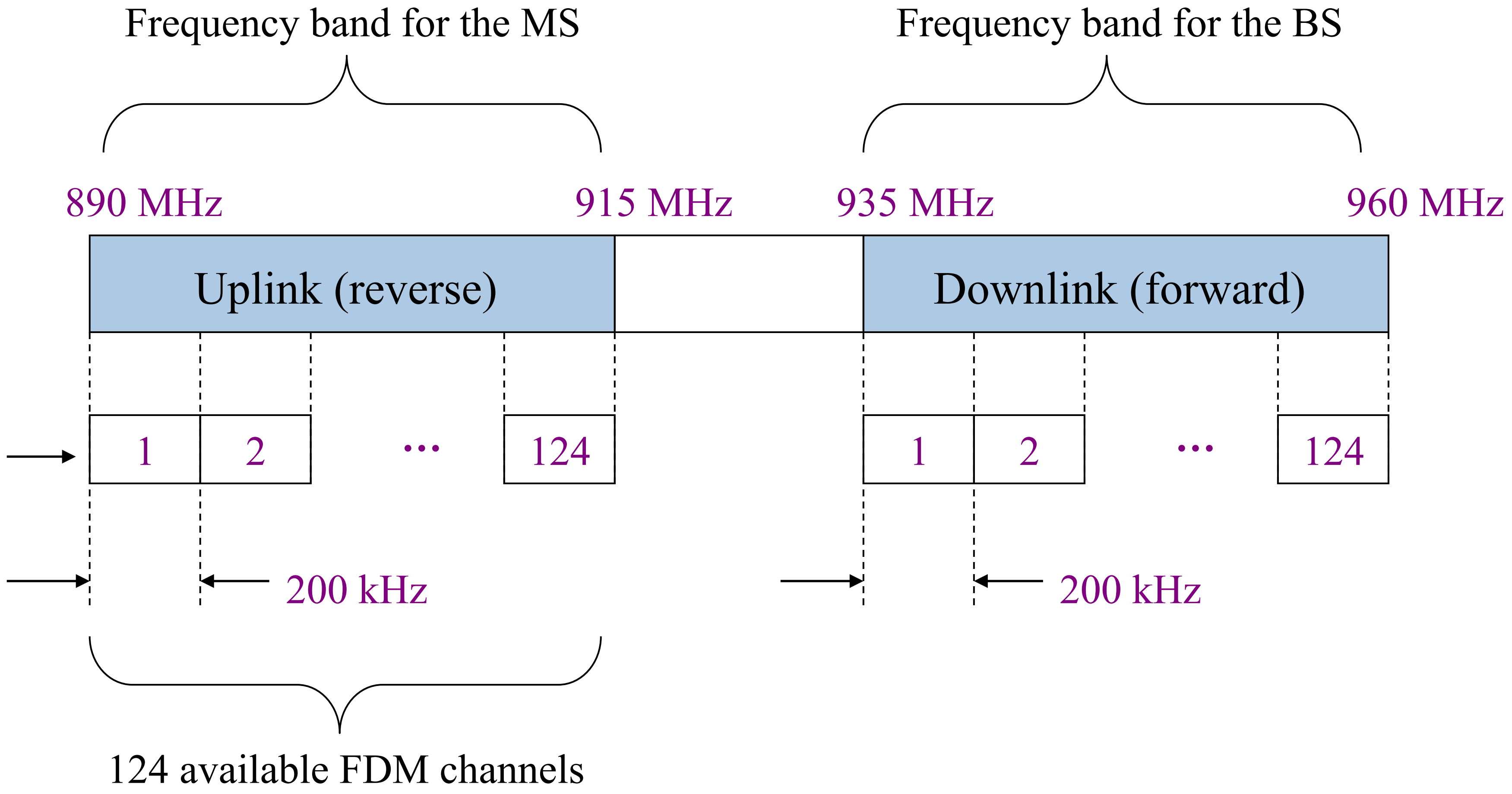
Functionalities of Constituents of GSM

- **Base Station Controller (BSC):** looks over a certain number of BTS to ensure proper operation, takes care of Handoff between BTSs.
- **Mobile Switching Center (MSC):** Mainly performs the switching by controlling calls to and from other telephone/ data systems. Also, performs functions such as network interfacing, common channel signaling, etc.
- **Authentication Center (AC):** AC unit provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call
- **Equipment Identity Register (EIR)**: EIR is a database that contains information about the identity of mobile equipment that prevents calls from stolen, unauthorized, or defective MSs.

Content

- GSM Architecture
- Frequency Band and Channels
- Frames in GSM
- Interfaces, Planes, and Layers of GSM
- Handoff
- Short Message Service (SMS)

Frequency Band Used by GSM



Channels in GSM

Group		Channel	Direction
Control Channel	**BCCH** **(Broadcast control channel)**	BCCH (Broadcast control channel)	BS → MS
		FCCH (Frequency correction channel)	BS → MS
		SCH (Synchronization channel)	BS → MS
	CCCH **(Common control channel)**	PCH (Paging channel)	BS → MS
		RACH (Random access channel)	BS ← MS
		AGCH (Access grand channel)	BS → MS
	DCCH **(Dedicated control channel)**	SDCCH (Stand-alone dedicated control channel)	BS ←→ MS
		SACCH (Slow associated control channel)	BS ←→ MS
		FACCH (Fast associated control channel)	BS ←→ MS
Traffic Channel	**TCH** **(Traffic Channel)**	TCH/f (Full-rate traffic channel)	BS ←→ MS
		TCH/s (Half-rate traffic channel)	BS ←→ MS

Control Channels of GSM

Control Channels used to Broadcast Information to all MSs.

- **Broadcast Control Channel (BCCH):** Used to transmit the system parameters like the frequency of operation in the cell, operator identifiers, etc.,
- **Frequency Correction Channel (FCCH):** Used for transmission of frequency references and frequency correction bursts
- **Synchronization Channel (SCH):** Used to provide the synchronization training sequences burst of 64 bits length to the MSs.

Control Channels used to establish link between MS and BS

- **Random Access Channel (RACH):** Used by the MS to transmit information regarding the requested dedicated channel from GSM.
- **Paging Channel:** Used by the BS to communicate with individual MS in the cell.
- **Access Grant Channel:** Used by the BS to send information about timing and synchronization.

Control Channels of GSM

Dedicated Control Channels used to serve for any control information transmission during the actual communication

- **Slow Associated Control Channel (SACCH):** Allocated along with a user channel, for transmission of control information during the actual transmission.

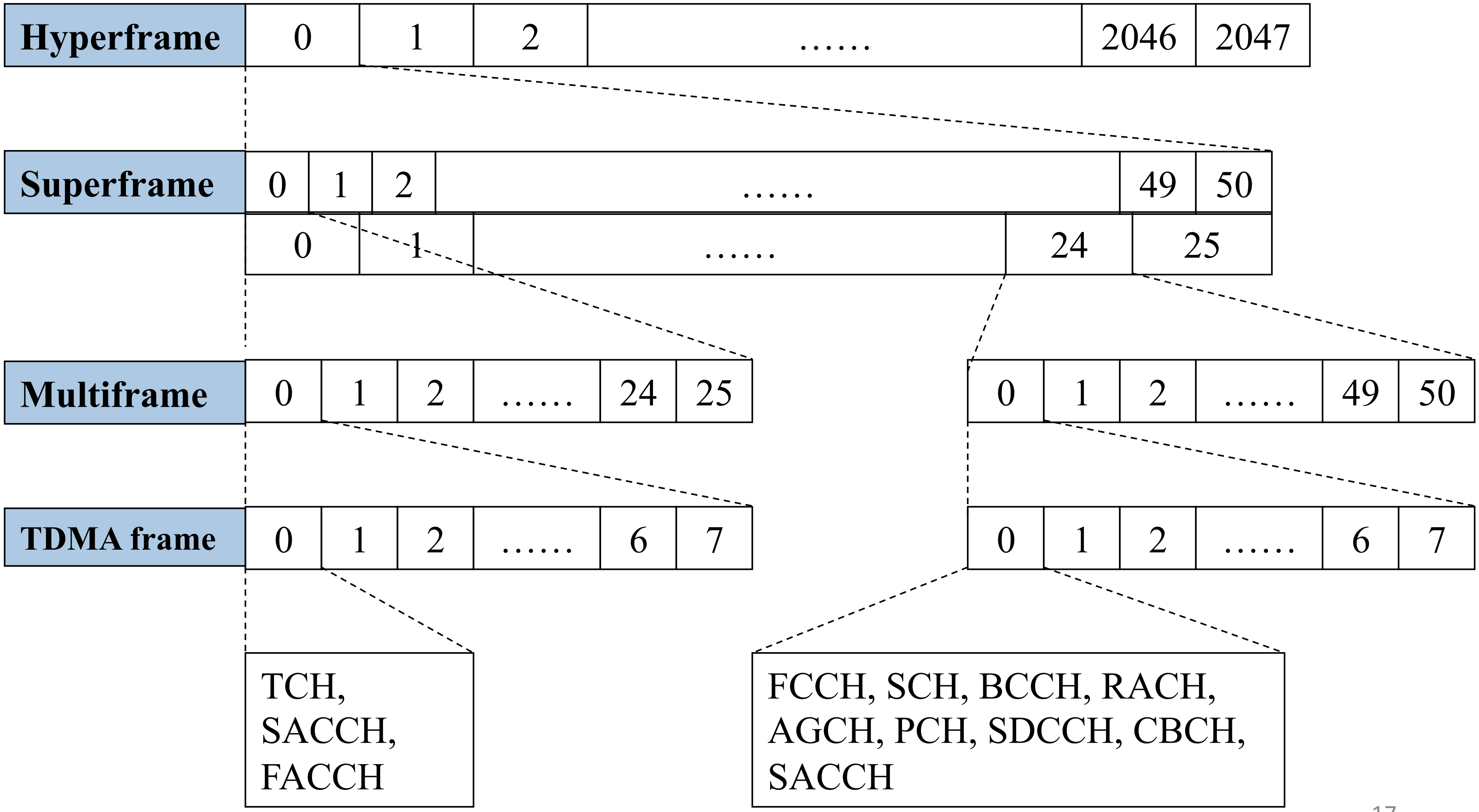
- **Stand-alone dedicated Control Channel:** Allocated with SACCH, used for transfer of signaling information between the BS and the MS.
-
- **Fast Associated Control Channel (FACCH):** Not a dedicated channel but carries the same information as SDCCH. But, it is a part of Traffic channel while SDCCH is a part of control channel

Content

- GSM Architecture
- Frequency Band and Channels
- Frames in GSM
- Interfaces, Planes, and Layers of GSM
- Handoff
- Short Message Service (SMS)

Frames in GSM

1 hyperframe = 2048 superframes = 2715684 TDMA frames (3 hr, 28 min, 53 s, 750 ms



Hyperframe 0 1 2 …… 2046 2047

Superframe 0 1 2 …… 49 50

0 1 …… 24 25

Multiframe 0 1 2 …… 24 25

0 1 2 …… 49 50

TDMA frame 0 1 2 …… 6 7

0 1 2 …… 6 7

TCH, SACCH, FACCH

FCCH, SCH, BCCH, RACH, AGCH, PCH, SDCCH, CBCH, SACCH

International Mobile Subscriber Identity (IMSI)

- Each mobile unit is identified uniquely with a set of values. These values are used to identify the country in which the mobile system resides, the mobile network, and the mobile subscriber.
- The remainder of the IMSI is made up of the mobile subscriber identification code (MSIC), which is the customer identification number.
- The IMSI is also used for an MSC/VLR to find out the subscriber's home PLMN (Public land mobile network).
- The IMSI is stored on the subscriber identity module (SIM), which is located in the subscriber's mobile unit.

Format of IMSI

15 digits or less

3 digits	2 digits	Up to 9 digits
Mobile country code (MCC)	Mobile network code (MNC)	Mobile subscriber identification code (MSIC)

Example:

MCC = 05 → Australia; MCC = 234 → UK

MNC = 01 → Telecom Australia; MNC = 234 → UK Vodafone

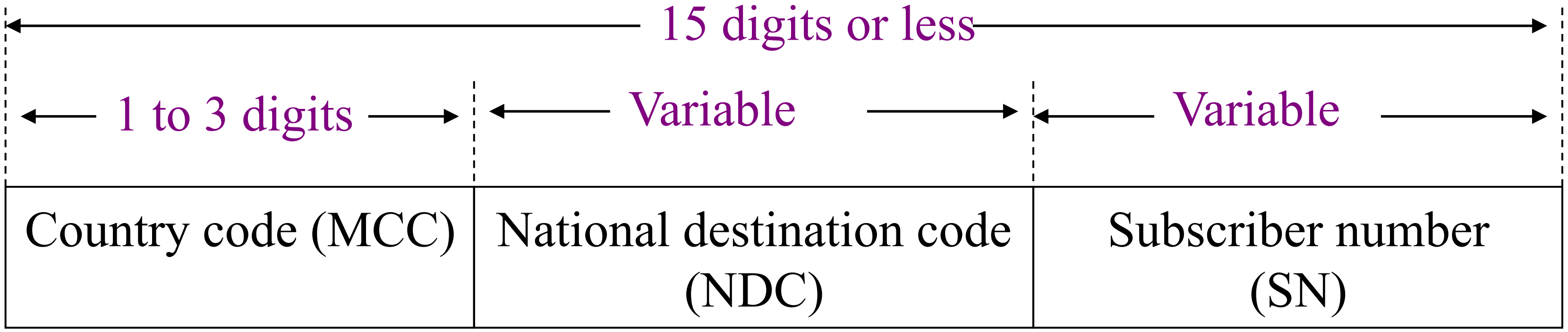
Subscriber Identity Module (SIM)

- SIM contains subscriber-specific information such as:
  - – Phone numbers,
  - – Personal identification number (PIN),
  - – Security/Authentication parameters.
- SIM can also be used to store short message.
- SIM can be a small plug-in module that is placed (somewhat permanently) in the mobile unit
- A modular portable SIM allows a user to use different terminal sets.
- SIM supports roaming.

Mobile System ISDN (MSISDN)

- MSISDN is the number that the calling party dials in order to reach the subscriber.
- It is used by the land network to route calls toward an appropriate MSC

The format of MSISDN

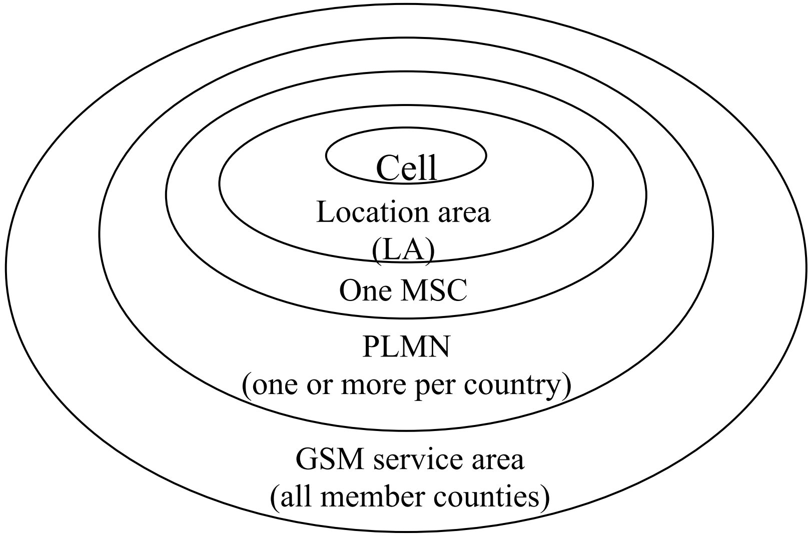


15 digits or less

1 to 3 digits	Variable	Variable
Country code (MCC)	National destination code (NDC)	Subscriber number (SN)

Location Area Identity (LAI)

- LAI identifies a cell or a group of cells.
- Relation between areas in GSM:


Cell
Location area (LA)
One MSC
PLMN (one or more per country)
GSM service area (all member counties)

PLMN: Public Land Mobile Network

The format of LAI

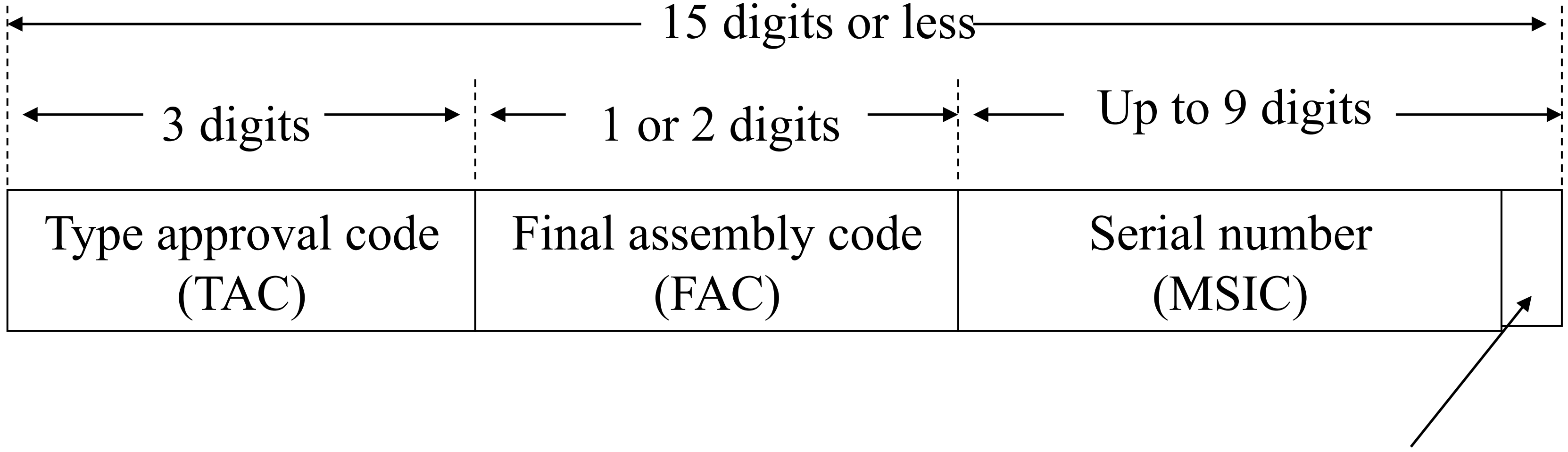
15 digits or less

3 digits	1 or 2 digits	Up to 9 digits
Mobile country code (MCC)	Mobile network code (MNC)	Mobile subscriber identification code (MSIC)

International MS Equipment Identity (IMSEI)

- IMSEI is assigned to each GSM unit at the factory.

The format of IMSEI



15 digits or less

3 digits

1 or 2 digits

Up to 9 digits

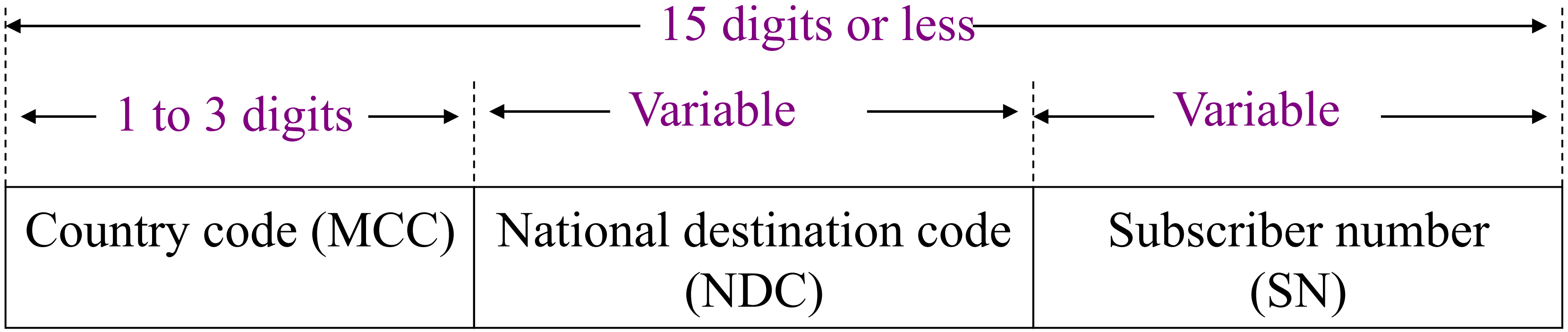
Type approval code (TAC)	Final assembly code (FAC)	Serial number (MSIC)	

Spare 1 digit

Mobile Station Roaming Number (MSRN)

- MSRN is allocated on a temporary basis when the MS roams into another numbering area.
- MSRN is used by the HLR for rerouting call to the MS.

The format of MSRN



15 digits or less		
1 to 3 digits	Variable	Variable
Country code (MCC)	National destination code (NDC)	Subscriber number (SN)

IMSI and TMSI

International Mobile Subscriber Identity (IMSI)

- IMSI is the primary function of subscriber within the mobile network and is permanently assigned to him.

Temporary Mobile Subscriber Identity (TMSI)

- TMSI is an alias, used in place of the IMSI. This value is sent over the air interface in place of the IMSI for purposes of security.

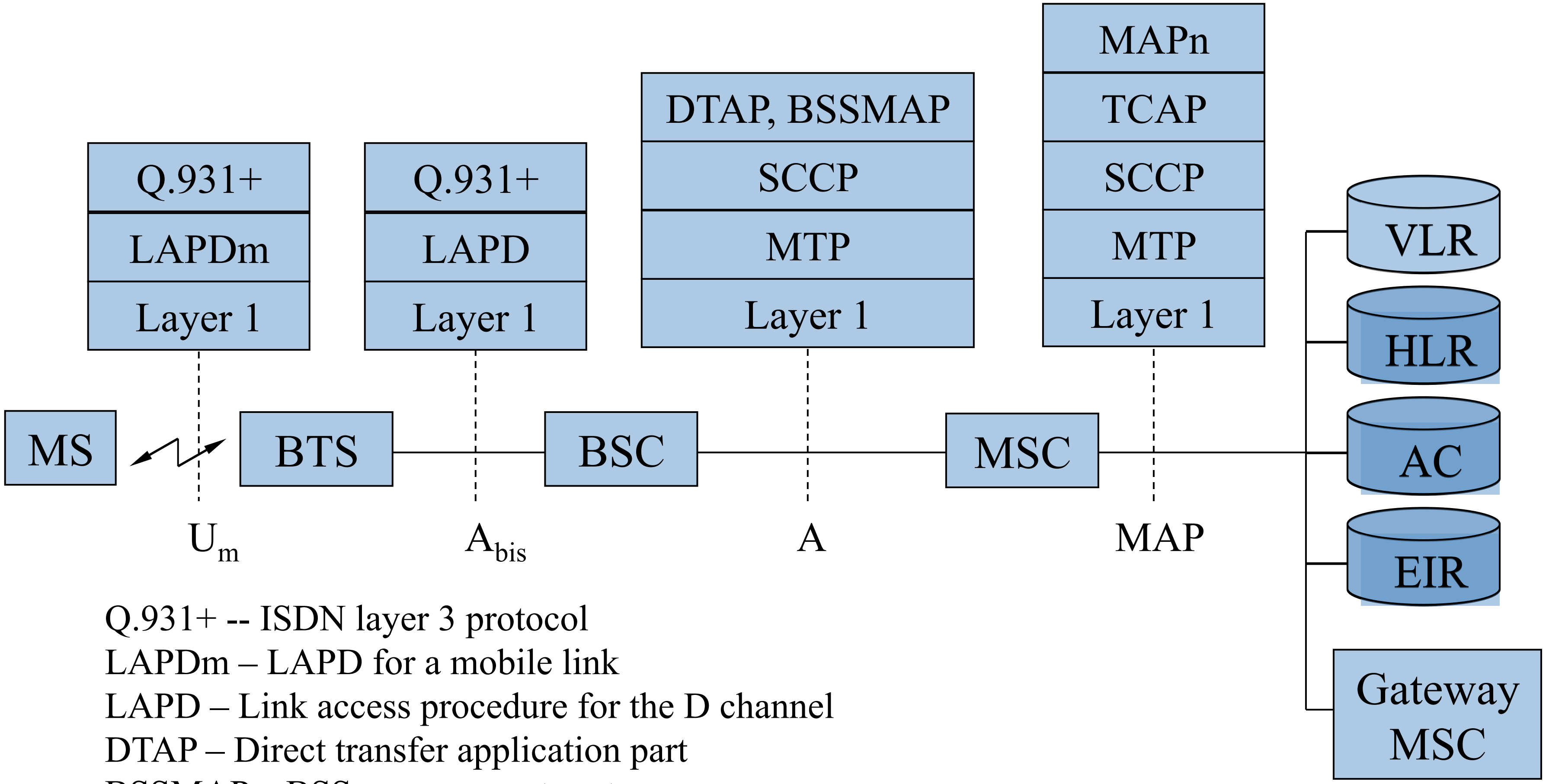
Content

- GSM Architecture
- Frequency Band and Channels
- Frames in GSM
- Interfaces, Planes, and Layers of GSM
- Handoff
- Short Message Service (SMS)

Interfaces of GSM

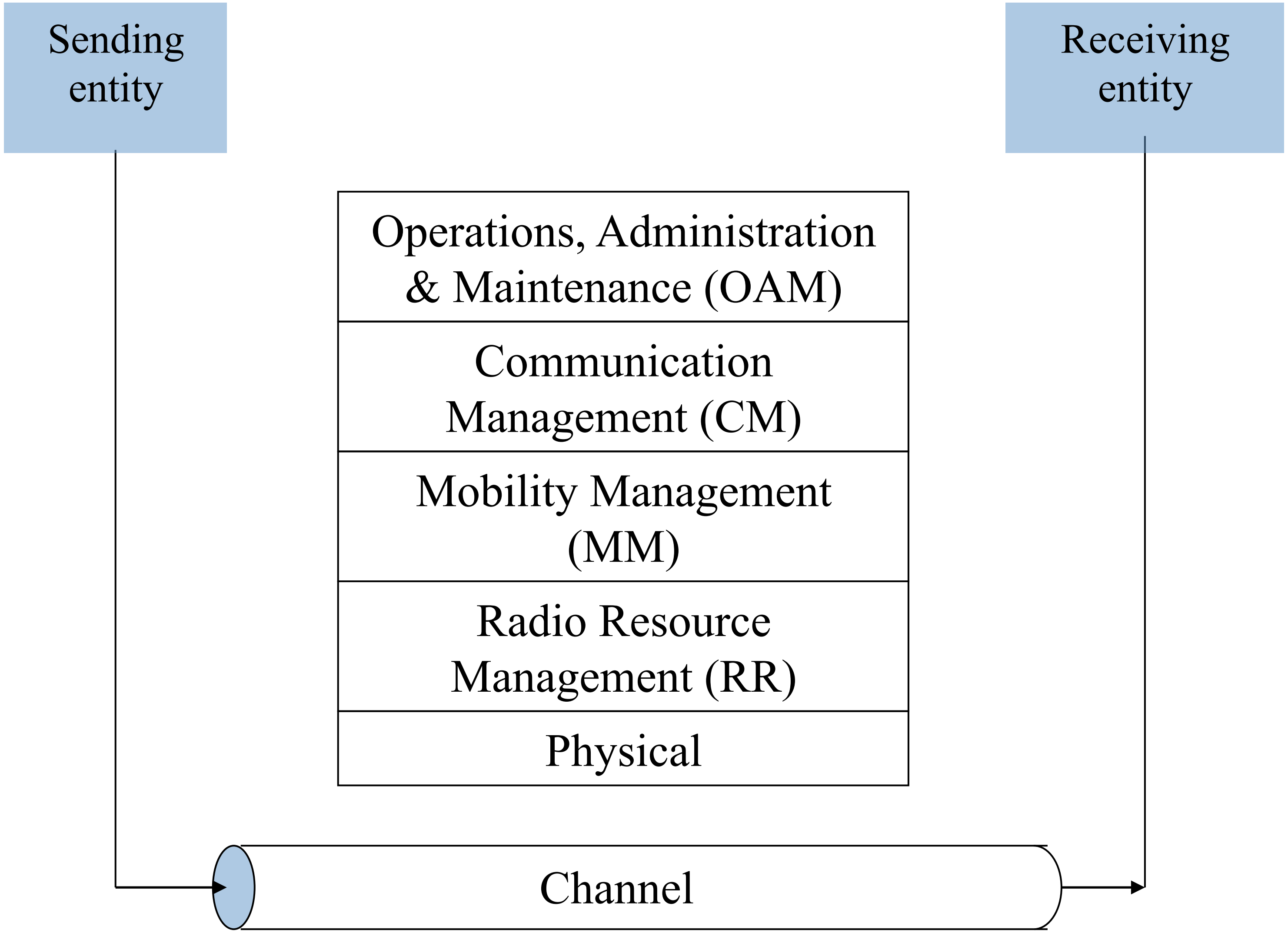
Interface Designation		Between
U_m		MS – BTS
A_{bis}		BTS – BSC
A		BSC – MSC
MAPn	**B**	MSC – VLR
	C	MSC – HLR
	D	HLR – VLR
	E	MSC – MSC
	F	MSC – EIR
	G	VLR – VLR

Layers, Planes and Interfaces of GSM



Q.931+ -- ISDN layer 3 protocol
LAPDm – LAPD for a mobile link
LAPD – Link access procedure for the D channel
DTAP – Direct transfer application part
BSSMAP – BSS management part
MTP – Message transfer part SCCP
– Signaling connection control part
TCAP – Transaction capabilities application part

GSM Functional Planes

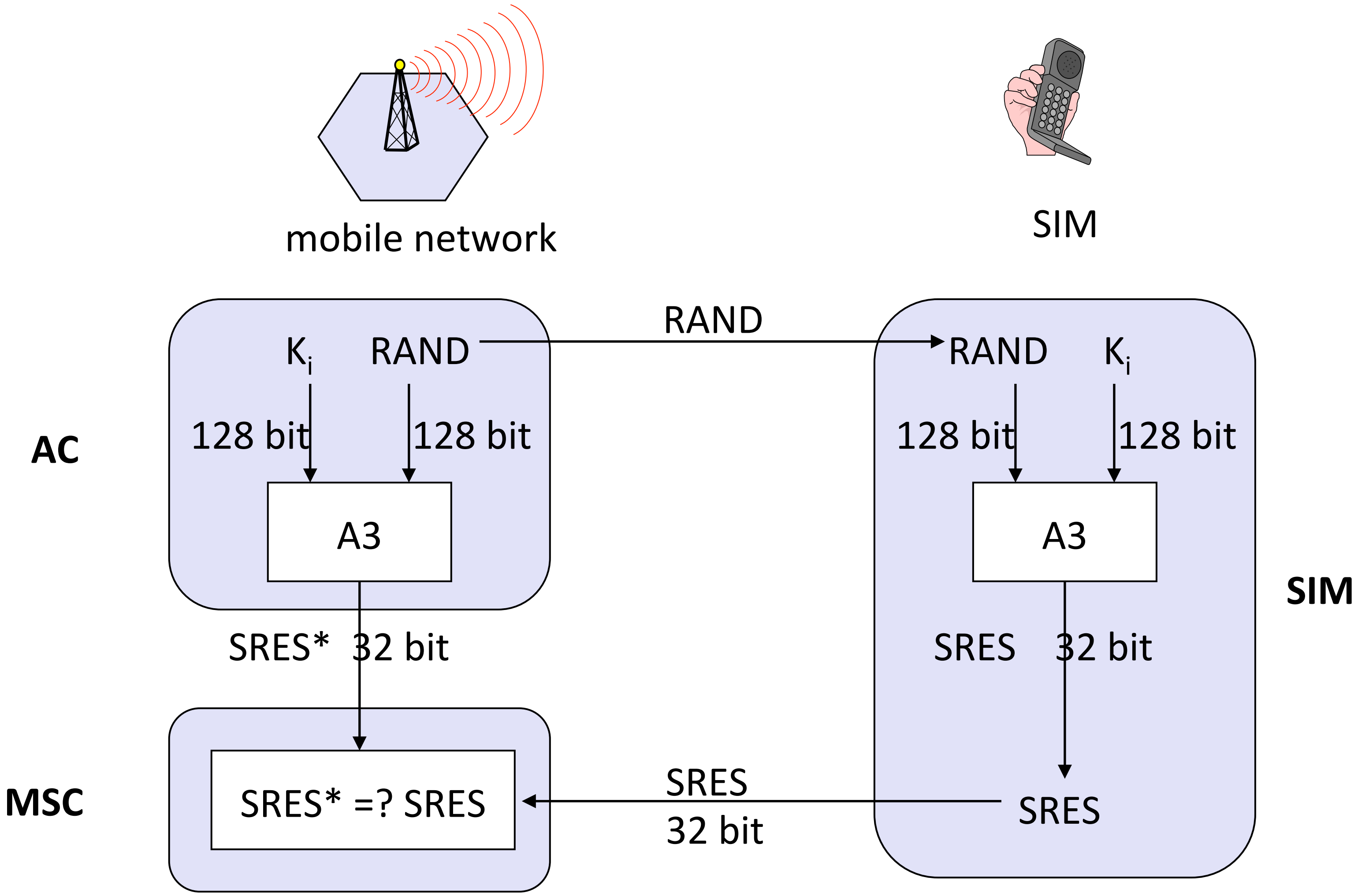

Sending entity
Receiving entity
Operations, Administration & Maintenance (OAM)
Communication Management (CM)
Mobility Management (MM)
Radio Resource Management (RR)
Physical
Channel

Security in GSM

- Security services
  - 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
- 3 algorithms specified in GSM
  - A3 for authentication ("secret", open interface)
  - A5 for encryption (standardized)
  - A8 for key generation ("secret", open interface)

"secret":
- A3 and A8 available via the Internet
- network providers can use stronger mechanisms

GSM - Authentication



mobile network

SIM

AC

K_i 128 bit

RAND 128 bit

A3

SRES* 32 bit

RAND

RAND 128 bit

K_i 128 bit

A3

SRES 32 bit

SIM

MSC

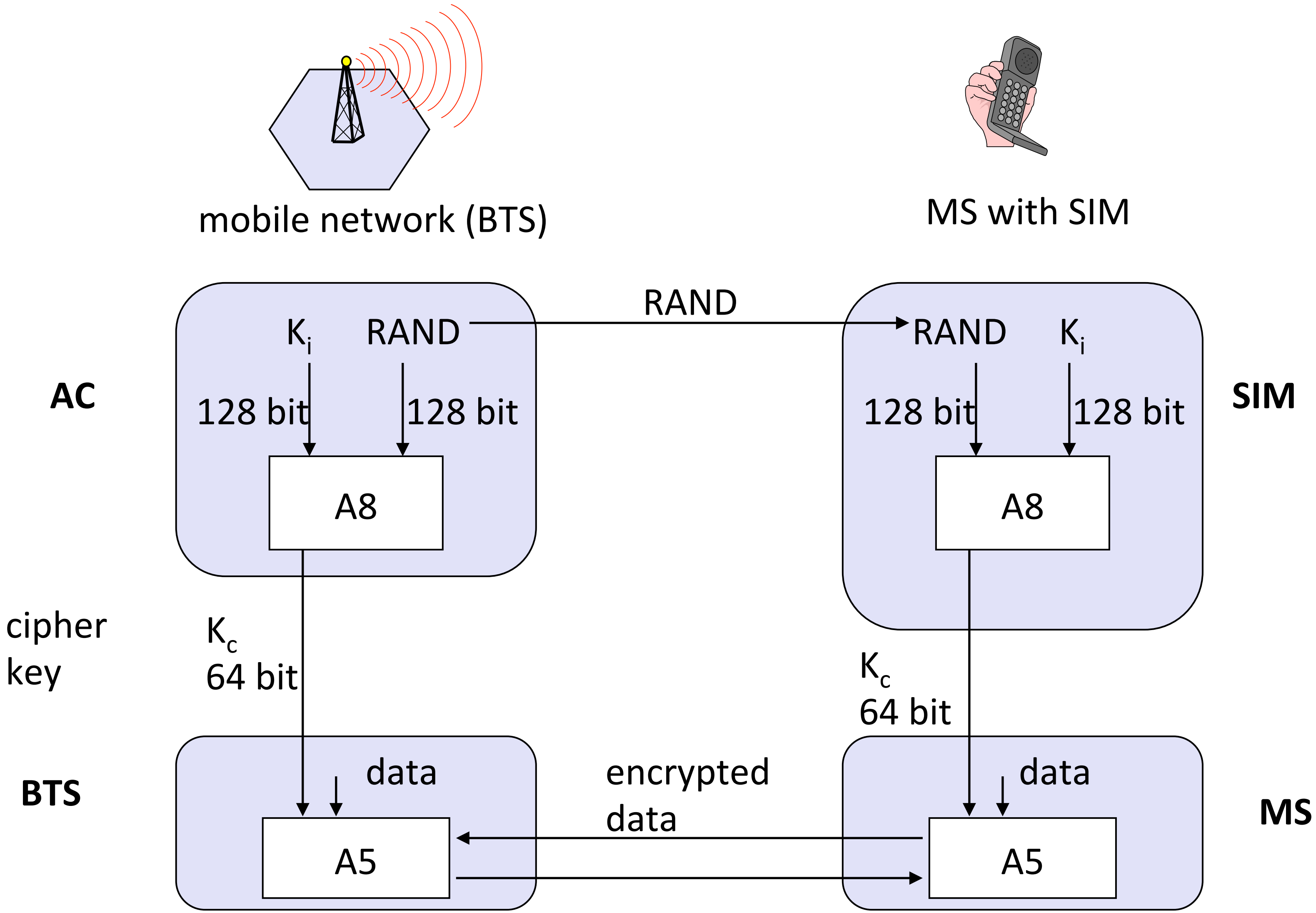
SRES* =? SRES

SRES 32 bit

SRES

K_i: individual subscriber authentication key SRES: signed response

GSM - key generation and encryption



mobile network (BTS)

MS with SIM

AC

K_i

RAND

128 bit

128 bit

A8

RAND

RAND

K_i

128 bit

128 bit

A8

SIM

cipher key

K_c

64 bit

K_c

64 bit

BTS

data

A5

encrypted data

data

A5

MS

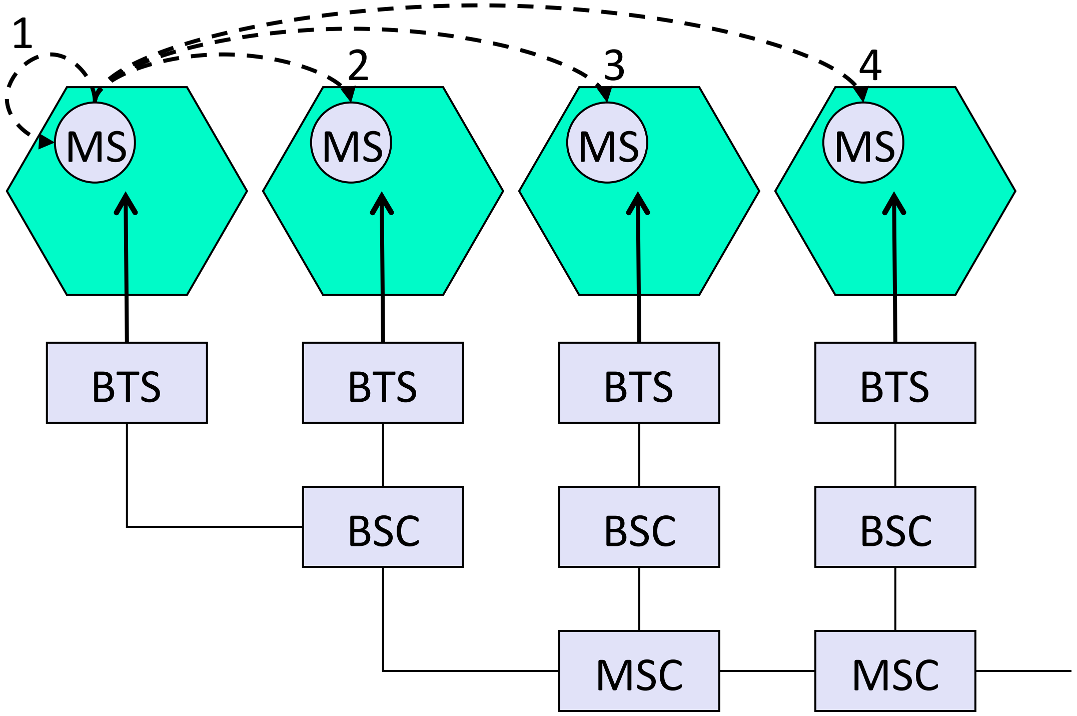
Content

- GSM Architecture
- Frequency Band and Channels
- Frames in GSM
- Interfaces, Planes, and Layers of GSM
- Handoff
- Short Message Service (SMS)

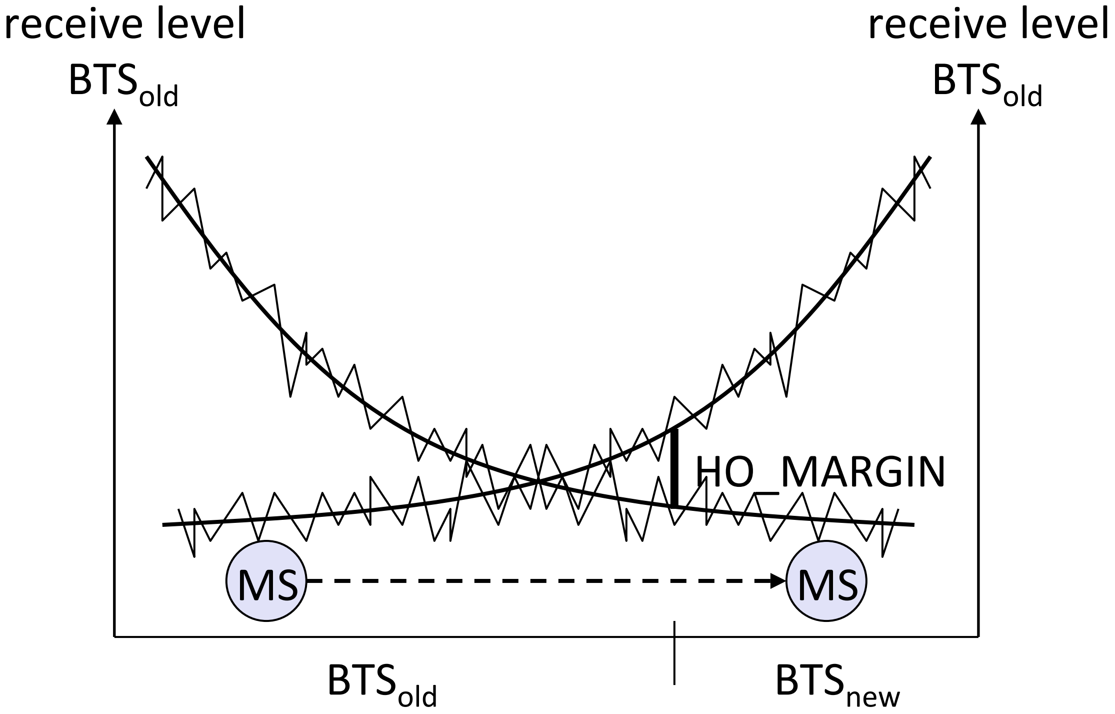
Handover (Handoff)

Handover	Description
Intra-cell / Intra-BTS	The channel for the connection is changed within the cell, e.g., if the channel has a high level of interference. The change can apply to another frequency of the same cell or to another time slot of the same frequency.
Inter-cell / Intra-BSC	In this case there is a change in radio channel between two cells that are served by the same BSC.
Inter-BSC / Intra-MSC	A connection is changed between two cells that are served by different BSCs but operate in the area of the same MSC.
Inter-MSC	A connection is changed between two cells that are in different MSC areas.

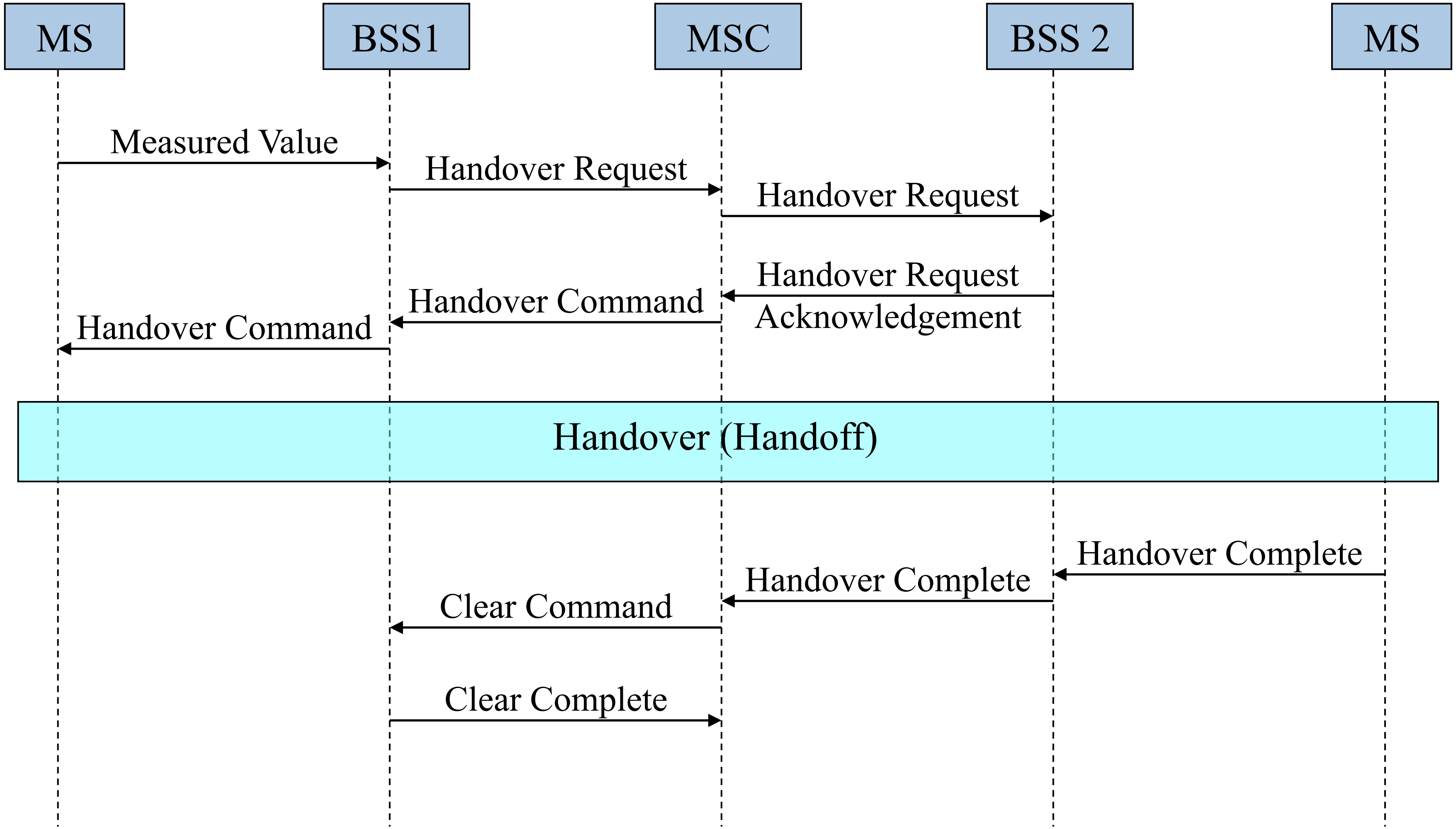
Four Types of Handover



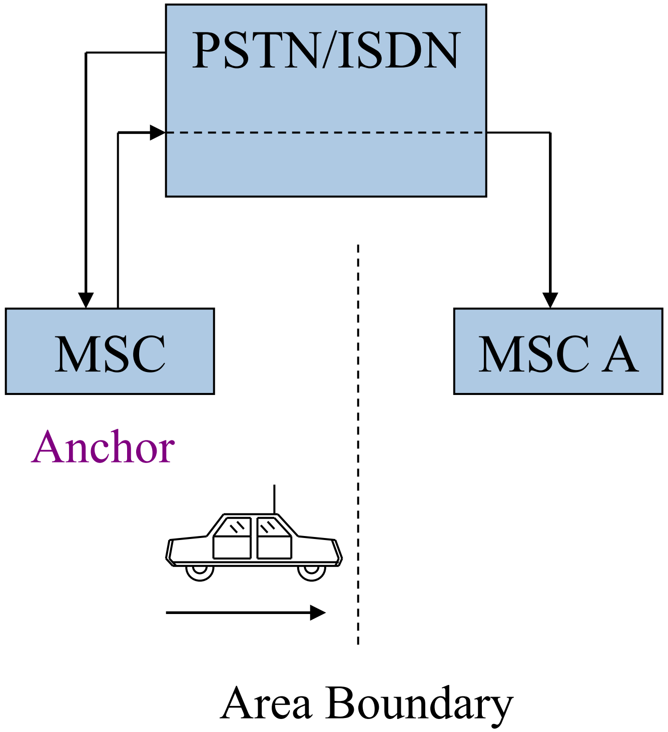
Handover Decision


receive level
BTS_{old}
receive level
BTS_{old}
HO_MARGIN
MS
MS
BTS_{old}
BTS_{new}

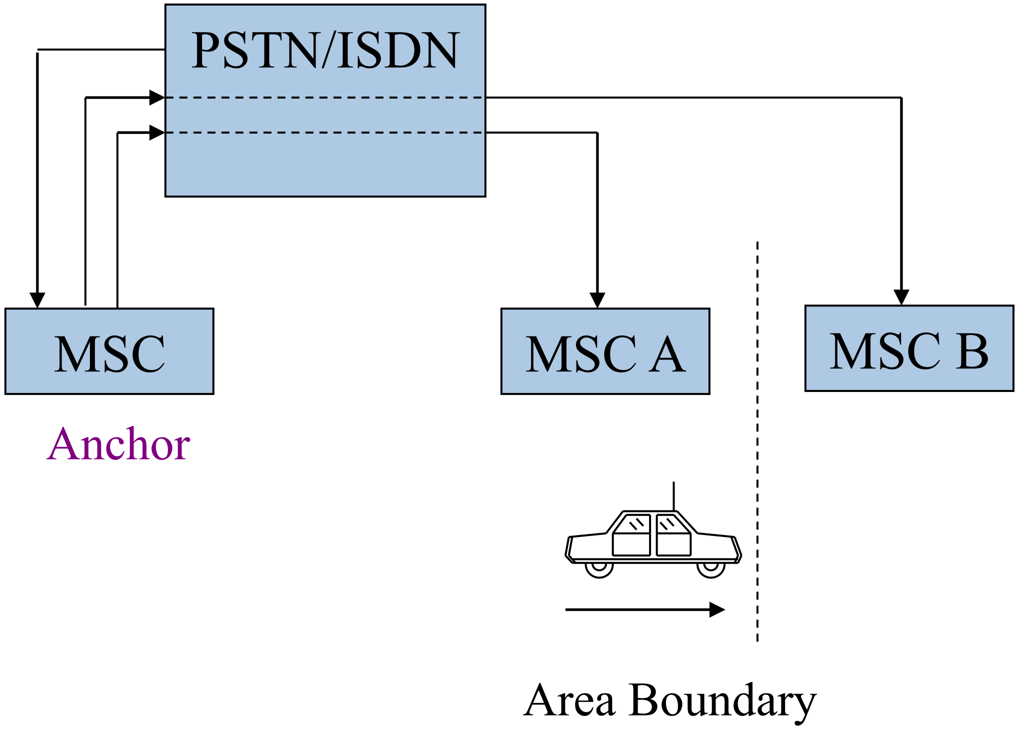
Handover (BSS 1 → BSS 2) Executed with an MSC



Inter-MSC Handover



(a) Basic handover



(b) Subsequent handover

Short Message Service (SMS)

- Ability to send or receive a text message to or from mobile phones
- Using unused bandwidth
- SMS can be sent and received simultaneously with GSM voice, data, and fax calls, because SMS travels over control channels
- Each mobile phone network that supports SMS has one or more messaging centers to handle and manage the short messages