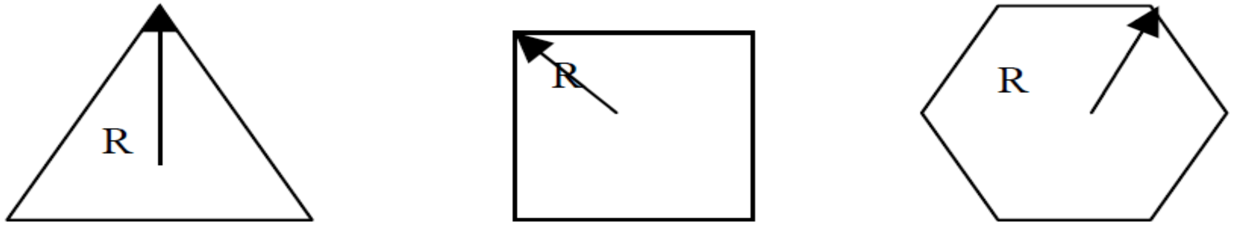
MOBILE TELECOMMUNICATION SYSTEM

Dr. A. Beulah

AP/CSE

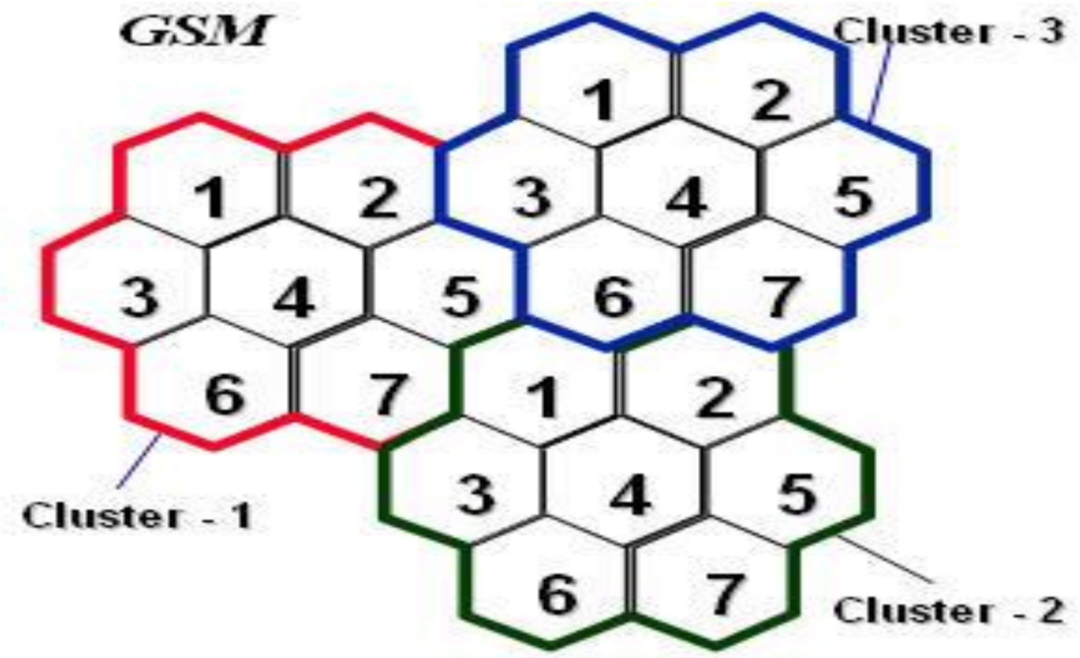
Cell Structure

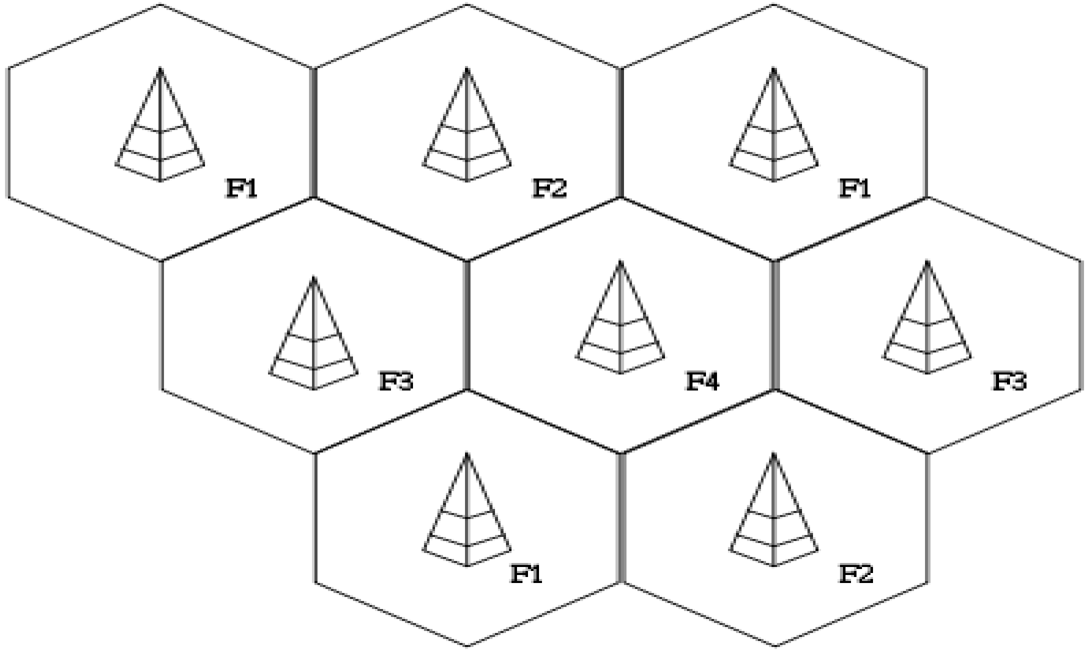
- The actual radio coverage of a cell is known as the cell footprint.
  - It has the most sides that can fit together without gaps.
  - The frequency reuse become possible using this shape.
  - The radiation pattern of the antennas used is 60 degree which means 6 are required for the full 360 degrees coverage which is the same no. of sides the hexagon consists.
- http://cdn.intechweb.org/pdfs/14752.pdf



$$A_{tri} = 1.3R^2 \qquad A_{sq} = 2.0R^2 \qquad A_{hex} = 2.6R^2$$

Frequency Reuse

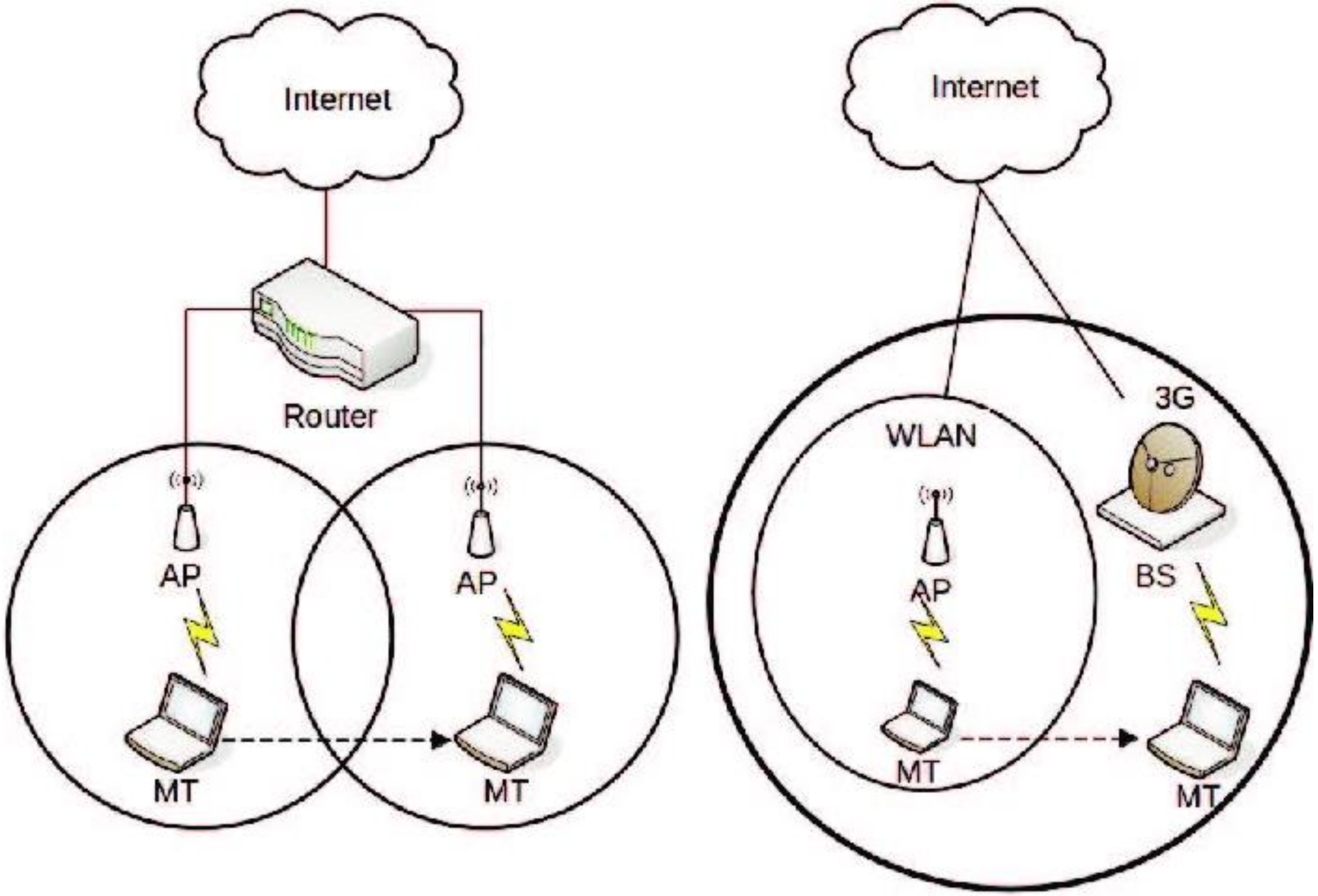




Comparison

Generation	Evolution	Deployment	Speed	Standard	Technology	Handoff	Features
1G	Analog cellular technology	1979	2.4 kbps	AMPS, NMT, TACS	FDMA	Horizontal	Voice calls
2G	Digital cellular technology	1992	64 kbps	GSM, GPRS	TDMA/CDMA	Horizontal	Voice calls, SMS
3G	Mobile broadband technology	2001	2 Mbps	UMTS, CDMA2000	WCDMA/CDMA 2000	Horizontal	Mobile internet, video calls
4G	Ultra-mobile broadband technology	2009	100 Mbps	LTE, WiMAX	OFDMA/MIMO	Horizontal and Vertical	Mobile broadband, HD video streaming, VoIP
5G	Next-generation mobile broadband technology	2019	10 Gbps	5G NR	OFDMA/MIMO/ Massive MIMO	Horizontal and Vertical	Mobile broadband, HD video streaming, VoIP, AR/VR, IoT
6G	Future-generation mobile broadband technology	2030	1 Tbps				Mobile broadband, HD video streaming, VoIP, AR/VR, IoT, AI, Integrate 5G with satellite network for global coverage Ultra fast Internet access Smart home/cities
7G	Terahertz mobile broadband technology	2040	10 Tbps				Mobile broadband, HD video streaming, VoIP, AR/VR, IoT, AI, autonomous driving, Space roaming World completely wireless

Horizontal and vertical



Future 6G, 7G

- 6G
  - Integrate 5G with satellite network for global coverage
  - Ultra fast Internet access
  - Smart home/cities

- 7G
  - Space roaming
  - World completely wireless

Key Points

- PSTN - public switched telephone network
- MTS -Mobile Telephone Systems
- AMTS -Advance Mobile Telephone Systems
- IMTS- Improved Mobile Telephone Systems
- Horizontal handoff
  - between two same wireless mobile network technologies.
- Vertical handoff
  - between two different wireless mobile network technologies.

Key Points

- SMS-Short Message Service
- MMS-Multimedia Messaging Service
- GSM -Global System for Mobile communication
- GPRS -General Packet Radio Service
- EDGE -Enhanced Data for Global Evolution
- UMTS -Universal Mobile Telecommunications Service
- HSDPA -High-Speed Downlink Packet Access
- HSUPA -High-Speed Uplink Packet Access
- LTE- Long Term Evolution

Summary

- Cellular networks
- Comparison of 1G – 5G

Test Your Knowledge?

- Why the cell structure is preferred to be hexagonal shape?
- ------- uses the cellular network to enable high speed internet connections ti devuces wutg built-in compatible technology such as smart phones

a) Cellular radio b) bluetooth c)wi-fi

References

Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.

Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS (GSM)

Dr. A. Beulah

AP/CSE

Introduction

- The primary goal of GSM is to provide a mobile phone system that allows users to roam throughout the environment and provides voice services.
- GSM → 2G system.
- GSM operates in 900 MHz or in 1800 MHz.
- Some countries (USA and Canada)operates in 850 MHz and 1900 MHz.
- Rarely used frequency bands 400MHz and 450 MHz (Scandinavia)
- 900MHz → Uplink(890-915MHz), Downlink(935-960MHz)

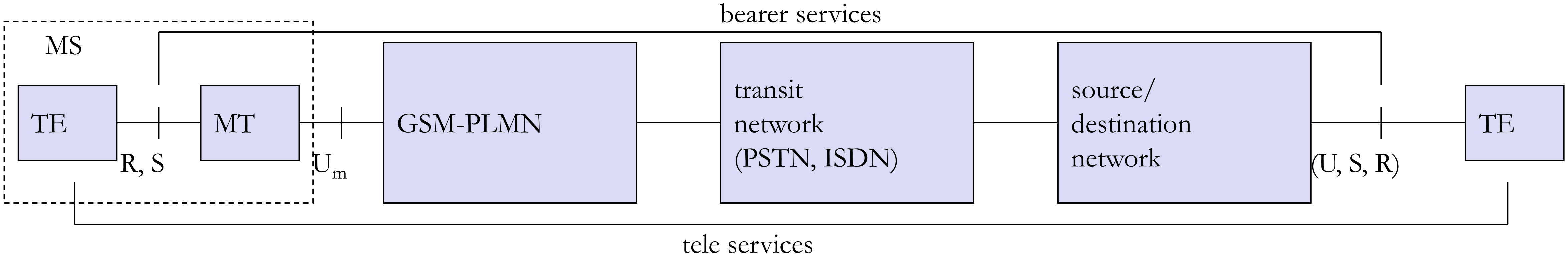
GSM Frequency Bands

Type	Channels	Uplink [MHz]	Downlink [MHz]
GSM 850	128-251	824-849	869-894
GSM 900 classical extended	0-124, 955-1023 124 channels +49 channels	876-915 890-915 880-915	921-960 935-960 925-960
GSM 1800	512-885	1710-1785	1805-1880
GSM 1900	512-810	1850-1910	1930-1990
GSM-R exclusive	955-1024, 0-124 69 channels	876-915 876-880	921-960 921-925

GSM SERVICES

GSM Services

- Three service domains
  - Bearer Services
  - Teleservices
  - Supplementary Services



Bearer Services

- Send/Receive data to/from remote phones/ computers
- Therefore it is known as Data services
- Provides transparent transmission between GSM and other Networks like PSTN, ISDN etc
- PSTN (public switched telephone network)
- ISDN(Integrated Services Digital Network)
- Bearer services are implemented on lower 3 layers of OSI/ISO
- Data rate 9.6 kbps

Bearer Services

- Synchronous and asynchronous modes of transmission
- Transparent Bearer Service
  - Use the functions of Physical Layer to transmit data.
  - Forward Error Correction (FEC) is used to increase transmission quality.
  - FEC → Codes redundancy into the data stream and helps to reconstruct the original data in case of transmission errors
  - Data Rates → 2.4, 4.8 or 9.6 kbps
- Non-Transparent Bearer Service
  - Use protocols of layers 2 and 3 to implement error correction and Flow control
  - Use the transparent bearer services, in addition to Radio Link Protocol (RLP).
  - This comprises mechanism of HDLC
  - Data Rates → 1.2, 2.4, 4.8 or 9.6 kbps

Teleservices

- GSM mainly focuses on voice oriented Tele services through mobile phones.
- All these basic services have to obey cellular functions, security measurements etc.
- Offered services
  - Mobile Telephony

    Primary goal of GSM was to enable mobile telephony offering the traditional bandwidth of 3.1 kHz
  - Emergency number

    Common number throughout Europe (112); mandatory for all service providers; free of charge; connection with the highest priority (preemption of other connections possible)

    Well known emergency number in the world today alongside **911** and **999**

    India police**100 , Medical 102**,**1298**,**108**,**112** Fire**101** Emergency management 2611

Teleservices

- Additional services
  - Non-Voice-Teleservices
    - Voice mailbox (implemented in the fixed network supporting the mobile terminals)
    - Short Message Service (SMS)

      Alphanumeric data transmission to/from the mobile terminal (160 characters) using the signaling channel, thus allowing simultaneous use of basic services and SMS
    - Enhanced Message Service (EMS)

      Offers a larger text message (760 characters)
    - Multimedia Message Service (MMS)

      Transmission of large pictures, short video clips etc.

Supplementary services

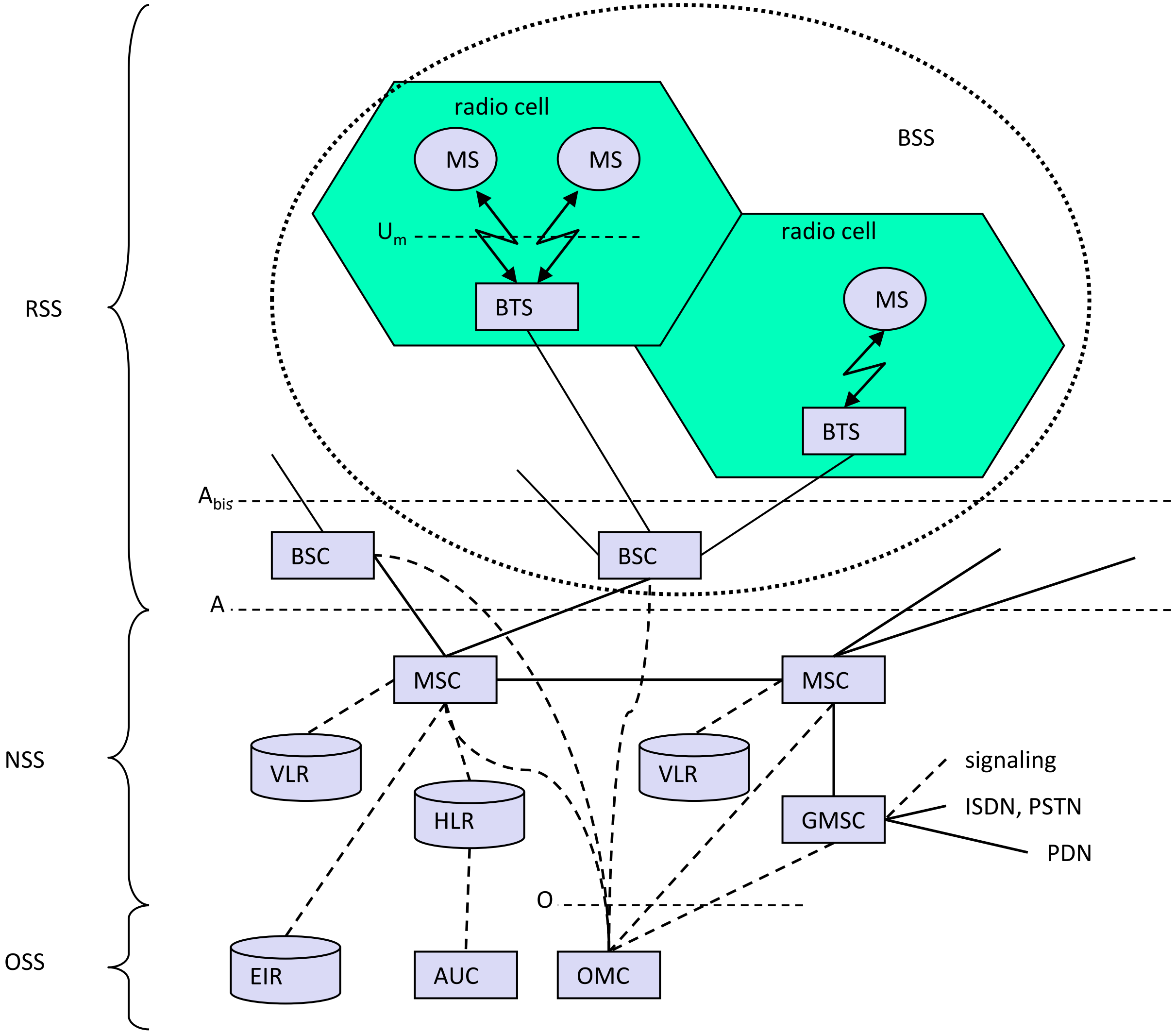
- GSM offers Supplementary services
- May differ between different service providers, countries and protocol versions
- Important services
  - User Identification
  - Call redirection
  - Forwarding of ongoing calls
  - Closed user group
  - Multiparty communication(Conferencing with up to 7 participants)

GSM ARCHITECTURE

System Architecture of GSM

- GSM consists of 3 Subsystems
  - RSS (Radio SubSystem):
    - Covers all radio aspects
  - NSS (Network and Switching Subsystem):
    - Call forwarding, handover, switching
  - OSS (Operation SubSystem):
    - Management of the network

GSM: Elements and Interfaces



- *BSS* (Base Station Subsystem)
- *BTS* (Base Transceiver Station): sender and receiver
- *BSC* (Base Station Controller): controlling several transceivers
- MSC (Mobile Station Controller)
- HLR (Home Location Register)
- VLR (Visitor Location Register)
- GMSC (Gateway Mobile Station Controller)
- EIR (Equipment Identity Register)
- AuC (Authentication Centre)
- OMC (Operation and Maintenance Centre)
- Interfaces
  - Um : radio interface
  - Abis : standardized, open interface with 16 kbps user channels
  - A: standardized, open interface with 64 kbps user channels

Radio SubSystem

- Components
  - MS (Mobile Station)
  - BSS (Base Station Subsystem):
  - BTS (Base Transceiver Station)
  - BSC (Base Station Controller)

Mobile Station

- A mobile station (MS) has different types of interfaces
  - Display, loudspeaker, microphone and programmable soft keys
  - Connection with computer modems(USB), Bluetooth.
- Many vendor specific functions and components such as cameras, fingerprint sensors, calendars, address books, games, and Internet browsers.

Mobile Station

- SIM (Subscriber Identity Module):
  - Personalization of the mobile terminal, stores user parameters
  - Stores all user specific data that is relevant to GSM(protected memory, flash memory)
  - Without a SIM only emergency calls are possible.
  - Contains
    - PIN (Personal Identity Number)
      - To unlock MS. Using wrong PIN 3 times will lock the SIM.
    - PUK (PIN unblocking key)
    - Authentication key Ki
    - International Mobile Subscriber Identity (IMSI)

Mobile Station

- International Mobile Equipment Identity (IMEI)
  - Device specific mechanisms Ex. For Theft protection use the device specific IMEI
  - It is usually found printed inside the battery compartment of the phone.
  - It can also be displayed on the screen of the phone by entering *#06# into the keypad on most phones.
- International Mobile Subscriber Identity (IMSI)
  - is a unique identification associated with all GSM network mobile phone users. It is stored as a 64 bit field in the SIM inside the phone and is sent by the phone to the network
  - An IMSI is usually presented as a 15 digit long number, but can be shorter .

Base Station Subsystem (BSS)

- Each BSS is controlled by a BSC (Base Station Controller)
- Functions of BSS
  - Maintaining Radio connection to MS
  - Coding/ Decoding of voice
  - Rate adaptation from /to the wireless network part

Base Transceiver Station

- Comprises of
  - Radio components including sender, receiver, antenna
- BTS connected to MS via U_m interface
- BTS connected to BSC via A_{bis}
- U_m interface Contains all the mechanisms necessary for wireless transmission (TDMA, FDMA)
- A GSM cell can measure between 100m to 35km depending on the environment (buildings, open source, mountains etc)

Base Station Controller

- Manages several BTSs.
- Handles
  - Switching between BTSs
  - Controlling BTSs
  - Managing of network resources
  - Multiplexes the radio signals and transmit to MSC

Network and Switching Subsystem

- NSS is the main component of the public mobile network GSM
  - switching, mobility management, interconnection to other networks, system control
- Components
  - MSC (Mobile Station Controller)
  - HLR (Home Location Register)
  - VLR (Visitor Location Register)
  - GMSC (Gateway Mobile Station Controller)

Mobile Services Switching Center

- High performance digital ISDN switches
- Setup connections to other MSCs and to the BSCs via the A interface.
- Forms the backbone of the GSM network.
  - Switching functions
  - Connection Setup
  - Connection Release
  - Call Handoff
  - C all forwarding
  - Conference calls
- GMSC → Gateway MSC

Home Location Register

- Central master database
- Comprise static information such as MSISDN and IMSI
- MSISDN
  - Mobile subscriber ISDN number(Phone number)
  - Services → Call forwarding, Roaming, GPRS etc.
  - The MSISDN together with IMSI are two important numbers used for identifying a mobile subscriber.
  - The latter identifies the SIM, i.e. the card inserted in to the mobile phone, while the former is used for routing calls to the subscriber.
- Contains Dynamic information such as LA ie current Location area and MSRN (Mobile subscriber Roaming Number)
- When MS leaves current LA, the information in the HLR is updated.
- HLRs can manage data for several million customers.

Visitor Location Register

- Dynamic database which stores information needed for the MS in the current LA. Such as IMSI, MSISDN, HLR address.
- When a new MS comes into an LA the VLR is responsible for copying all information for this user form HLR.
- This hierarchy avoids frequent HLR updates.

Operation SubSystem

- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems
- Authentication Center (AUC)
  - Protects intruders targeting the air interface.
  - AUC stores information concerned with security features such as user authentication and encryption.
- Equipment Identity Register (EIR)
  - Registers GSM mobile stations and user rights
  - Stolen or malfunctioning mobile stations can be locked and sometimes even localized
- Operation and Maintenance Center (OMC)
  - Different control capabilities for the radio subsystem and the network subsystem
  - Traffic monitoring, status reports of network entities,, subscriber management, security management, accounting, billing

GSM SECURITY

Security

- GSM offers security services with the help of Confidential information stored in
  - The AuC
  - The individual SIM
- AuC contains
  - The algorithms for authentication and generates the values needed for user authentication
  - The keys for encryption
- SIM stores
  - Personal data
  - Secret data.
  - These are protected with the help of PIN

Security Services

- Access control and Authentication
  - Authentication of a valid user for the SIM.
  - The user needs a secret PIN to access the SIM
  - Subscriber Authentication has to be done.
- Confidentiality
  - User data is encrypted
  - After authentication, BTS and MS apply encryption to voice, data, and Signal.
  - Confidentiality exists only between MS and BTS.
- Anonymity
  - User identifiers are not used over the air.
  - TMSI (newly assigned by the VLR) is transmitted after each location update
  - VLR can change the TMSI at any time.

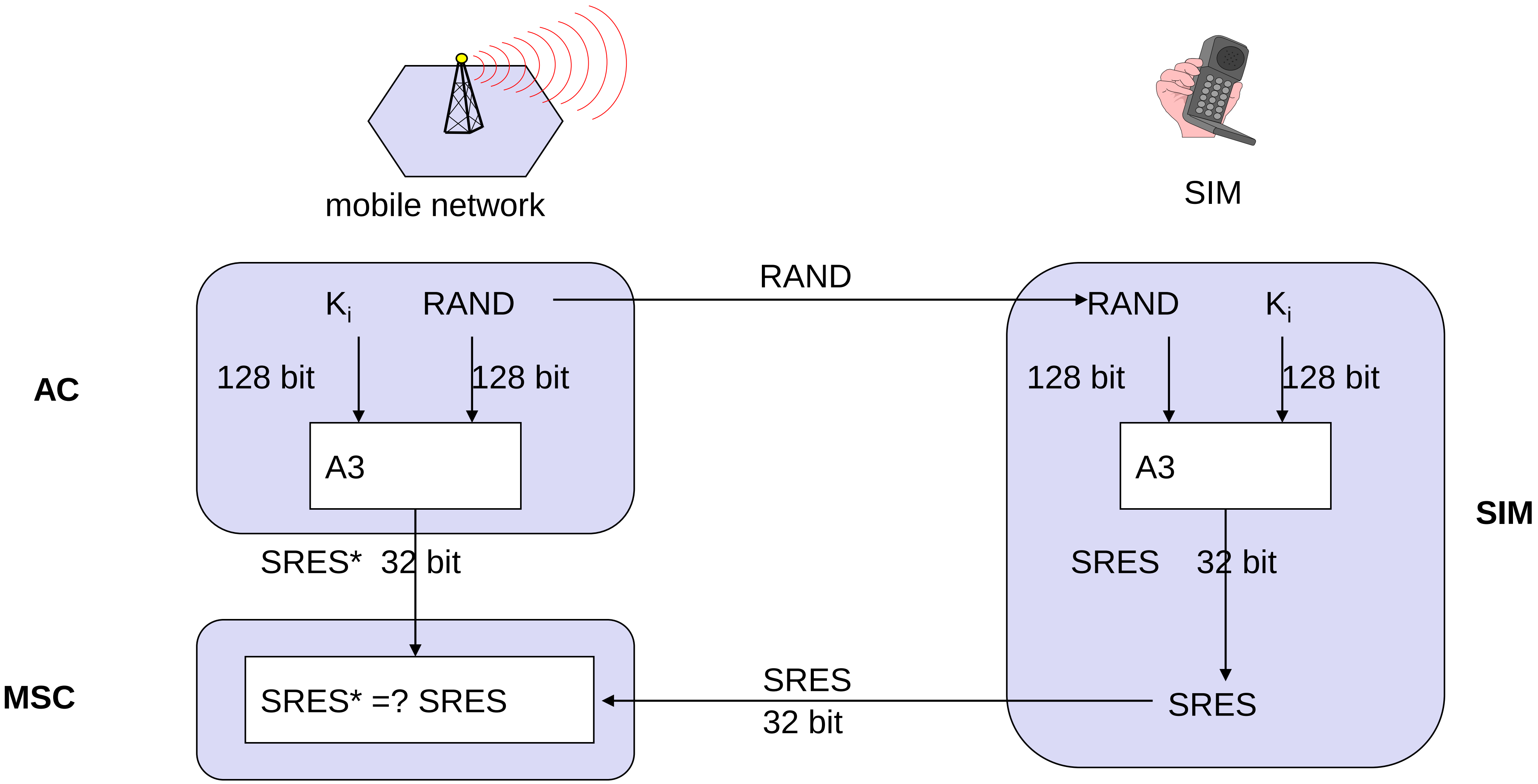
Security Services

- 3 Algorithms
- Algorithm A3 is used for authentication
- Algorithm A5 for Encryption
- Algorithm A8 for the generation of a Cipher Key.

Authentication

- The user should be authenticated, before using any service from the network.
- Authentication is based on SIM
- SIM contains
  - Authentication key K_i
  - User Identification IMSI
  - Algorithm A3 → algorithm used for authentication.
- Authentication uses a challenge-response method.

Authentication

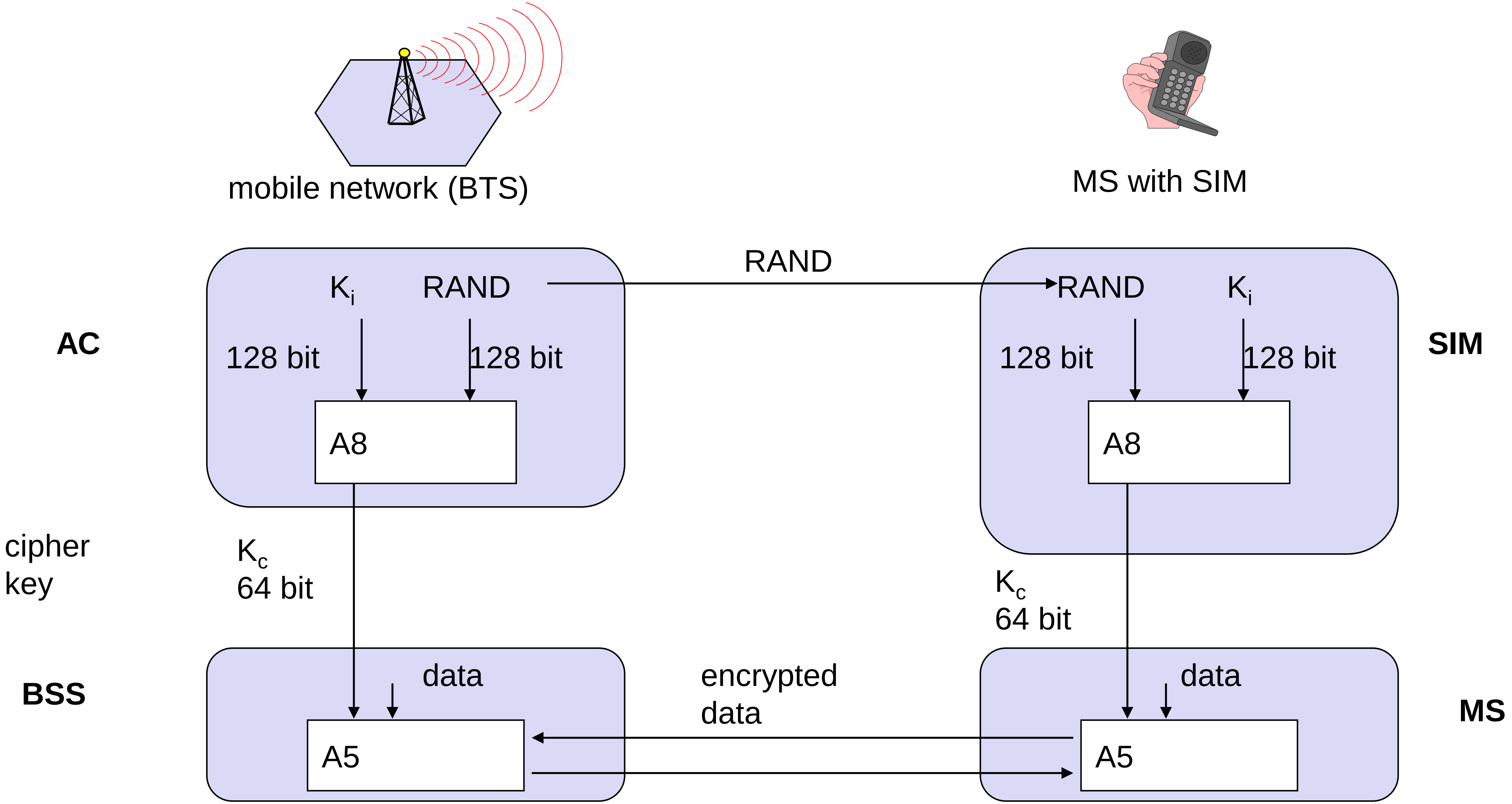


K_i: individual subscriber authentication key SRES: signed response

Encryption

- User data are encrypted
- MS and BTS uses k_c (cipher key) for encryption
- K_c is generated using the authentication key k_i and a random value by applying the algorithm A8

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
BSS
data
A5
encrypted data
data
A5
MS

Summary

- GSM Services
  - Bearer service
  - Teleservice
  - Supplementary service
- GSM Architecture
  - RSS
  - NSS
  - OSS
- GSM Security

Test your understanding

- Identify the main reason as to why a mobile handset is compact and lightweight and yet provides a large number of features such as roaming, camera, audio and video play, record internet etc., while traditional landline phone handsets are bulky and provide only limited features.

References

Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.

Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.

RADIO INTERFACE

Dr. A. Beulah

AP/CSE

Frequency Allocation

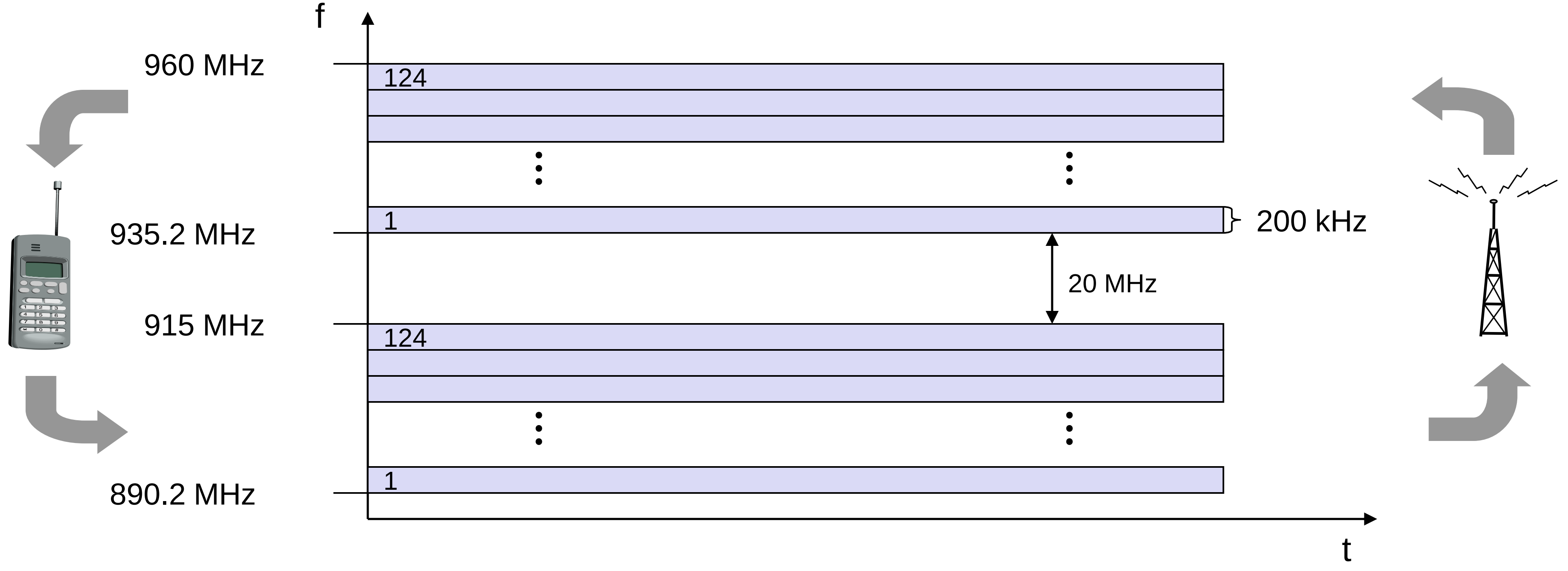
- Important interface in GSM is U_m interface.
- GSM implements SDMA using cells with BTS and assign an MS to BTS
- FDD- Frequency Division Duplex
  - The transmitter and Receiver operates at different Frequencies
- In GSM FDD is used to separate downlink and uplink.
- Media access combines TDMA and FDMA

Frequency Allocation

- GSM 900 →124 channels each 200kHz used for FDMA (total 248 uplink, downlink)
  - Channels 1 and 124 are not used for transmission, due to technical reasons.
  - 32 Channels → are reserved for organizational data.
  - Remaining 90 channels → are used for customers
- GSM 1800 → 374 channels

Frequency Allocation

- GSM 900 MHz



Frequency Allocation

Uplink Frequency (For Transmission)

- From mobile station to base station or from ground control to satellite
- All uplinks use the band between 890.2 and 915

Downlink Frequency (Receiving information)

- From base station to mobile station or from satellite to ground control
- All downlinks use 935.2 to 960 MHz

Frequency Allocation

- Media access Technique used in GSM is TDMA and FDMA.
- Using FDMA
  - A frequency is assigned to each user.
  - For large number of users in a FDMA system, the number of required frequencies is large.
  - Scalability Problem → The limited available frequency and the fact that a user will not free its assigned frequency until the user does not need it anymore.
- Using TDMA
  - Allows several users to share the same channel.
  - Each subscriber multiplexes the shared channel, scheduling their frame for transmission.
- Usually TDMA is used with an FDMA structure.

Frequency Allocation

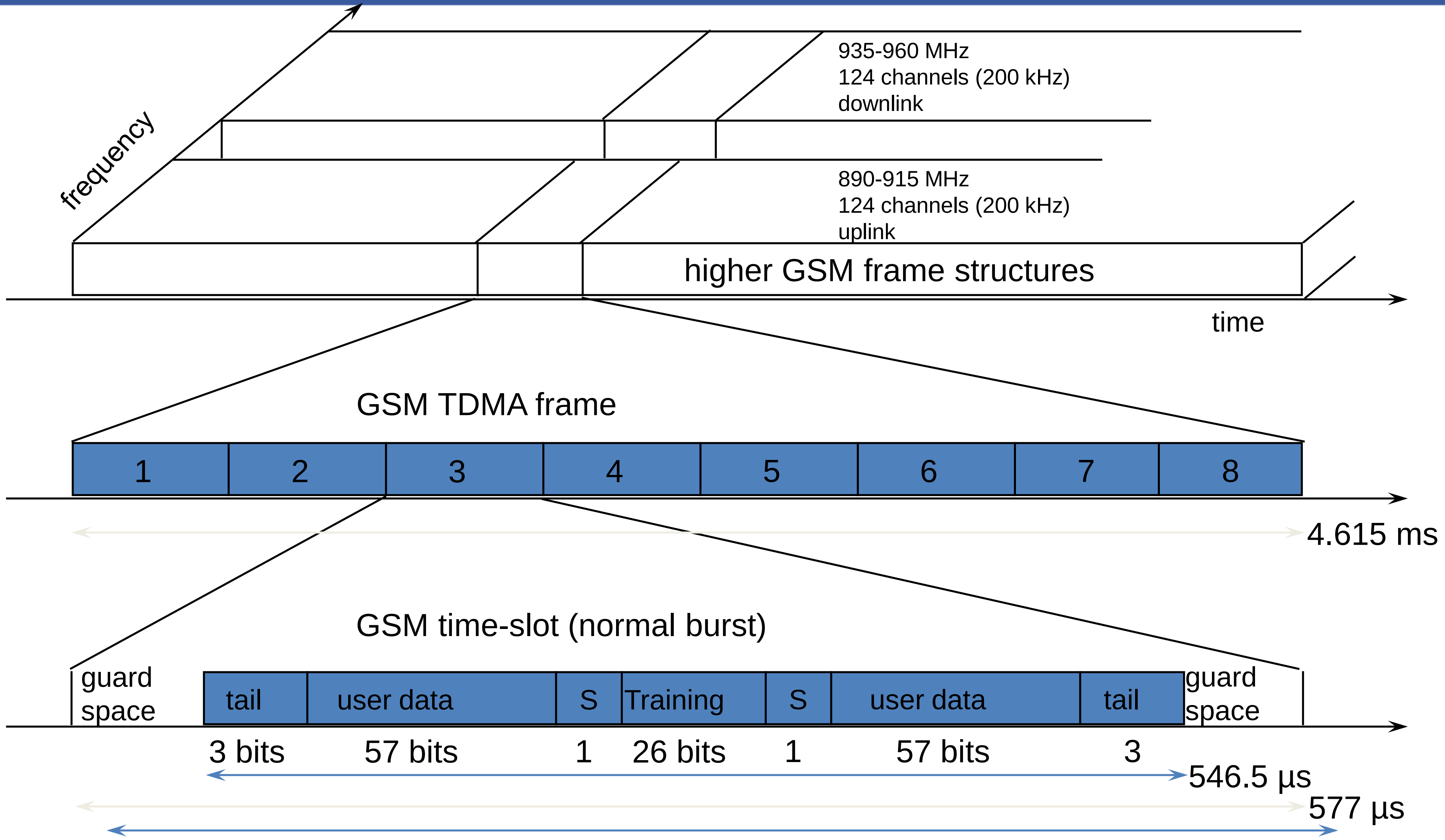
Allocation of uplink and downlink Frequency

- According to FDMA, the base station, allocates a certain frequency for up and downlink to establish a with a mobile phone
- Up and downlink have a fixed relation
- If the uplink frequency is fu= 890 MHz + n·0.2 MHz, the downlink frequency is fd= fu+ 45 MHz, i.e., fd= 935 MHz + n·0.2 MHz for a certain channel n.
- The base station selects the channel. Each channel (uplink and downlink) has a bandwidth of 200 kHz
- This illustrates the use of FDM for multiple access (124 channels per direction are available at 900 MHz) and duplex according to a predetermined scheme.

Frequency Allocation

- Each of 248 channels is additionally separated in time via GSM TDMA Frame
  - ie 200kHz carrier is subdivided into frames that are repeated continuously.

GSM FDMA -TDMA



GSM FDMA -TDMA

- A 25 MHz frequency band is divided, using a FDMA scheme, into 124 carrier frequencies with a 200khz spacing.
  - 915 -890 (25)
  - 960 -935 (25)
  - 25000/200 = 125 channels
- A 25 Mhz frequency band can provide 125 carrier frequencies
- The *first* carrier frequency is used as a *guard-band* between GSM and other services working on lower freq.

- Each frequency is time-divided using a TDMA scheme.
- This scheme splits a 200kHz channel, into 8 *bursts.*(GSM Time Slots) . Data is transmitted in form of Bursts.
- A burst is the unit of time in a TDMA system, and it lasts approximately 0.577ms or 577µs
- Remaining 30 µs gaurd band
- Thus a TDMA lasts *4.615ms*. Each burst is assigned to a *single* user.

GSM FDMA -TDMA

- A normal burst is only 546.5 µs long.
- Each burst contains 148 bits.
- Remaining 30.5µs is used as guard space to avoid overlapping with other burst.
- Within 577µs 156.25 bits can be allotted.
- Therfore
  - Each TDM channel has a data rate of 33.8kbps
  - Each Radio carrier frequency transmits 270kbps over U_m interface

Burst structure

- The *tail bits* (T) are a group of 3 bits set to zero and placed at the *beginning* and the *end* of a burst. Used to enhance the receiver performance.
- The *training sequence* has a length of *26 bits*. It synchronizes the receiver to the current path propagation characteristics and select strongest signal in the multipath propagation.
- The coded data bits corresponds to two groups, of *57 bits* each, containing signaling or user data.
- The stealing flags (S) indicate, to the receiver, whether the data bits are data or signaling traffic.
- The *guard period* (GP), with a length of *8.25 bits*, is used to avoid a possible overlap of two mobiles.

Burst structure

Different types of bursts can be distinguished in GSM:

- Frequency-correction
  - Allows MS to correct local oscillator to avoid interference with neighboring channels.
- Synchronization
  - It has the same length as the normal one but a different structure.
  - Synchronizes MS with BTS
- Random access
  - shorter than the normal burst.
- Normal Burst
  - burst used to carry speech or data information.
  - It lasts approximately 0.577 ms and has a length of 156.25 bits.
- Dummy Burst
  - If no data is available for a slot dummy burst is used.

Logical Channel

- In GSM Channels are separated into Physical and Logical Channel
- The Physical channels are determined by the timeslot (8*124 physical channels)
- A physical channel consists of a slot, repeated every 4.615 ms.

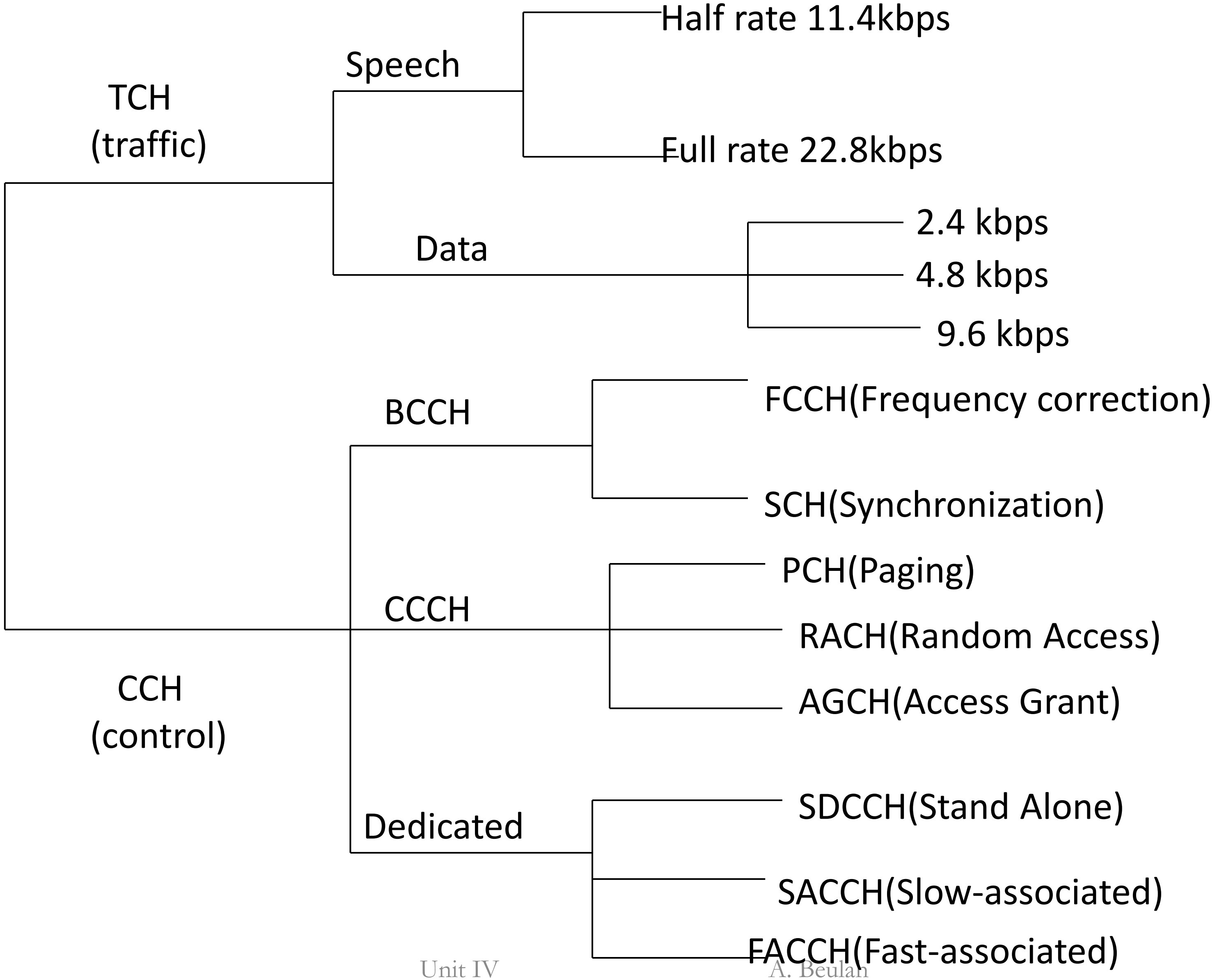
Logical Channel

- The logical channels are determined by the information carried within the physical channel.
- Example: A logical channel C1 that only takes up every fourth slot and another logical channel C2 that uses every other slot.
- Both logical channels could use the same physical channel with the pattern $C_1C_2xC_2C_1C_2xC_2C_1$ etc.

Logical Channel

- A logical channel is defined by its frequency and the position of its corresponding burst within a TDMA frame.
- In GSM there are two types of Logical channels:
  - Traffic channels (TCH)used for speech and data.
  - Control channels (CCH) used for network management messages and channel maintenance tasks.

Channel Structure



Traffic channels (TCH)

- Used for user data (Ex: speech and fax)
- 2 Categories
  - Full Rate TCH → TCH/F
  - Half Rate TCH → TCH/H

Full-rate traffic channels (TCH/F)

- Data rate of 22.8 Kbps, with a useable rate of 9.6 Kbps for data (or approximately 13 Kbps for speech).
- 13 kbit/s were required for speech, whereas the remaining capacity of the TCH/F (22.8 kbit/s) was used for error correction (TCH/FS).
- A newer codec, enhanced full rate (EFR), provides better voice quality than FR as long as the transmission error rate is low. The generated data rate is only 12.2 kbit/s.
- Data transmission in GSM is possible at many different data rates,
  - e.g., TCH/F4.8 for 4.8 kbit/s, TCH/F9.6 for 9.6 kbit/s, and, as a newer specification, TCH/F14.4 for 14.4 kbit/s.
  - These logical channels differ in terms of their coding schemes and error correction capabilities.

Half-rate traffic channels (TCH/H)

- Data rate of 11.4 Kbps, with a useable rate of 4.8 Kbps for data
- Improved codes allow for better voice coding and can use a TCH/H.
- However, speech quality decreases with the use of TCH/HS(half rate speech) and many providers try to avoid using them.
- **The standard codecs for voice are called full rate (FR, 13 kbit/s) and half rate (HR, 5.6 kbit/s).**

Control Channels

- Control Channels are used to
  - Control media access
  - Allocation of Traffic channels
  - Mobility Management
- Types of Control Channels
  - Broadcast Control Channel (BCCH)
  - Common Control Channels (CCCH)
  - Dedicated Control Channels (DCCH)

Broadcast Control Channel (BCCH)

- Unidirectional Channel
- **BTS uses this channel to signal information to all MSs within a cell.**
- Information Transmitted are
  - Cell Identifier
  - Options available within the cell (Frequency hopping)
  - Frequencies available inside and in neighboring cells.
- Frequency Correction Channel(FCCH)
  - BTS sends information for frequency correction via FCCH.
- Synchronization Channel (SCH)
  - BTS sends time synchronization through SCH.
- FCCH & SCH are sub channels of BCCH

Common Control Channels (CCCH)

- Bidirectional Channel.
- **All information regarding connection setup between MS and BTS is exchanged via the CCCH**
- Helps to establish the calls from the mobile station or the network.
- Paging Channel (PCH)
  - BTS uses PCH to alert the MS of an incoming call. (paging)
- Random Access Channel (RACH)
  - If MS wants to setup a call, it uses the RACH to send data to the BTS.
  - Uses multiple access as slotted ALOHA.
- Access Grant Channel (AGCH)
  - BTS uses AGCH to signal an MS that it can use a TCH (traffic channel) or SDCCH (standalone DCCH) for further connection setup

Dedicated Control Channels(DCCH)

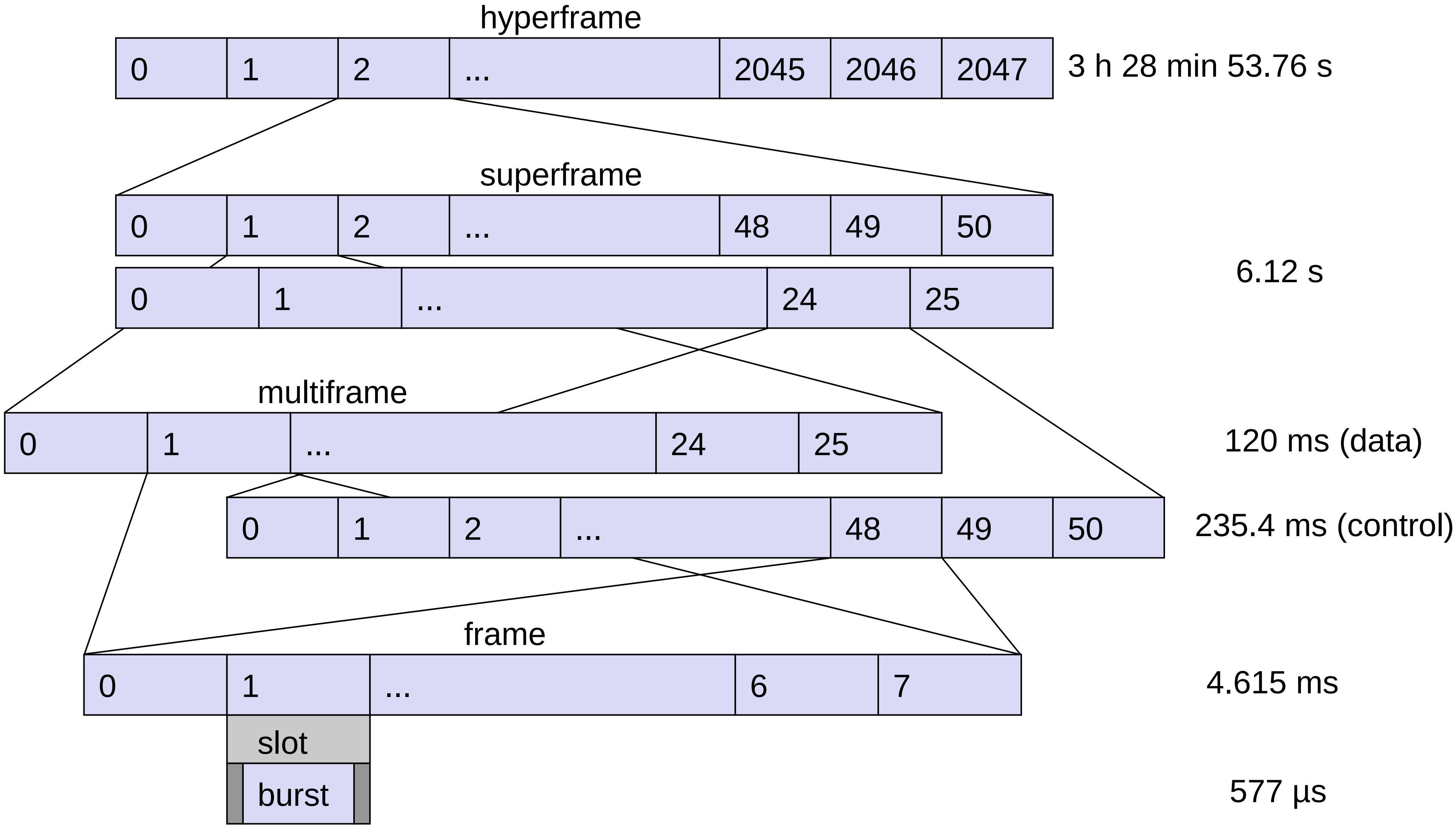
- Bidirectional Channel.
- **Used for message exchange between several mobiles or a mobile and the network.**
- Standalone Dedicated Control Channel (SDCCH):
  - MS uses SDCCH to exchange signaling in the downlink and uplink.
- Slow Associated Control Channel (SACCH):
  - Used for channel maintenance and control.(used to exchange system information, such as the channel quality and signal power level)
- Fast Associated Control Channels (FACCH)
  - Replace all or part of a traffic channel when urgent signaling must be transmitted.
- The FACCH channels carry the same signaling as SDCCH channels.

Logical Channels

- However, these channels cannot use time slots arbitrarily
  - GSM specifies a very elaborate multiplexing scheme that integrates several hierarchies of frames.
- If a simple TCH/F is used for user data transmission, each TCH/F will have an associated SACCH for slow signaling.
- If fast signaling is required, the FACCH uses the time slots for the TCH/F.
- A typical usage pattern of a physical channel for data transmission now looks like this (with T indicating the user traffic in the TCH/F and S indicating the signalling traffic in the SACCH):

  TTTTTTTTTTTTSTTTTTTTTTTTx
  TTTTTTTTTTTTSTTTTTTTTTTTx

GSM Frame Hierarchy



GSM Frame Hierarchy

- Multiframe
  - 26 slots
  - 12 slots with user data followed by a signaling slot, again 12 slots with user data then an unused slot.
  - 24 out of 26 physical slots are used.
  - This periodic pattern of 26 slots of frames is called as Traffic multiframe.

GSM Frame Hierarchy

Superframe

- 51 multiframes with 26 frames.

Hyperframe

- 2048 superframes constitute a hyperframe

Test your Knowledge

- What multiplexing schemes are used in GSM and for what purpose? Think of other layers apart from the physical layer.

Summary

- Radio Interface
  - Physical Channel
  - Logical Channel

References

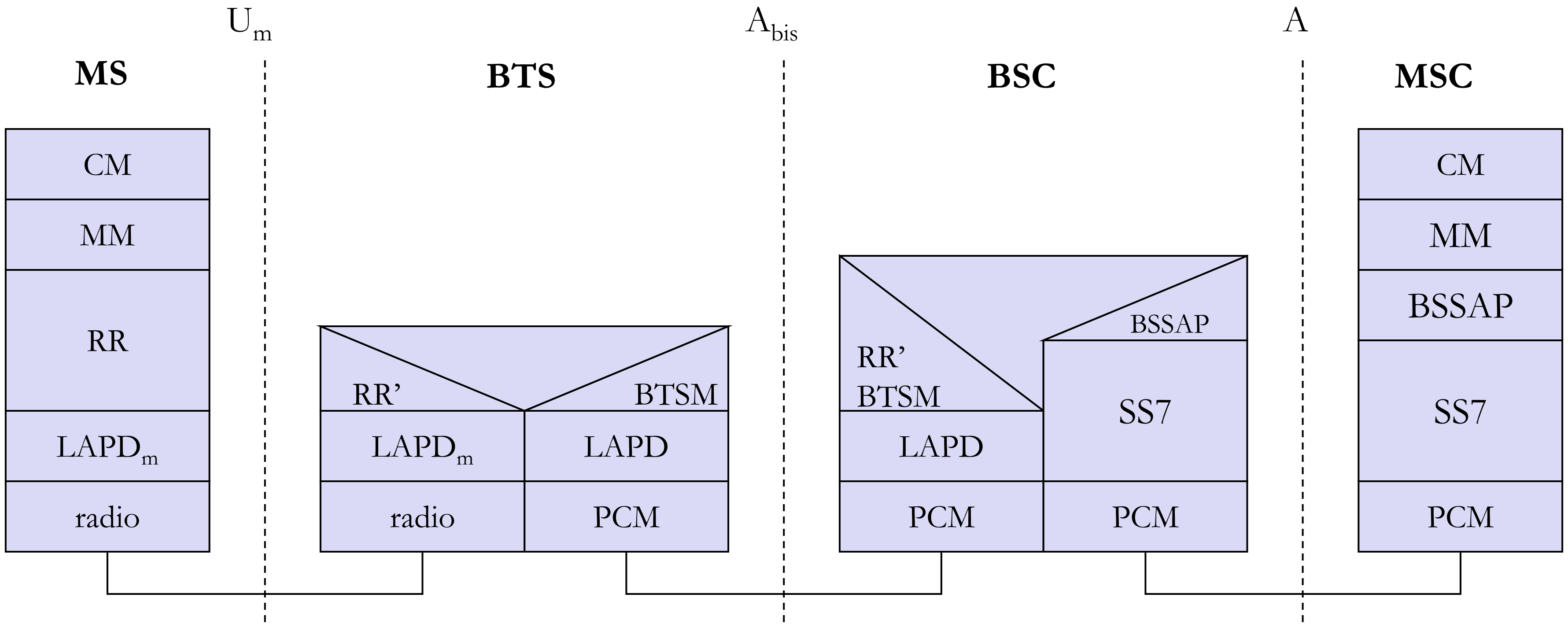
Behrouz A. Forouzan, Data Communications and Networking, Fifth Edition TMH, 2013.

PROTOCOLS

Dr. A. Beulah

AP/CSE

GSM protocol layers for signaling



16/64 kbit/s

64 kbit/s /
2.048 Mbit/s

Layer 1

- Um interface is the only air interface.
- **Layer 1**
  - the physical layer, handles all radio-specific functions.
    - creation of bursts according to the five different formats,
    - Multiplexing of bursts into a TDMA frame,
    - synchronization with the BTS,
    - Detection of idle channels,
    - measurement of the channel quality on the downlink.
  - The physical layer at Um uses GMSK for digital modulation and performs encryption/decryption of data,
    - **encryption is not performed end-to-end,** but only between MS and BSS over the air interface.

Layer 1

- Synchronization with the BTS
  - includes the correction of the individual path delay between an MS and the BTS.
  - All MSs within a cell use the same BTS and thus must be synchronized to this BTS.
  - The BTS generates the time-structure of frames, slots etc.
  - Different round trip times (RTT) is the disadvantage
    - An MS close to the BTS has a very short RTT, whereas an MS 35 km away already exhibits an RTT of around 0.23 ms.
    - If the MS far away used the slot structure without correction, large guard spaces would be required, as 0.23 ms for each slot.
    - Therefore, the BTS sends the current RTT to the MS, which then adjusts its access time so that all bursts reach the BTS within their limits.
    - This mechanism reduces the guard space to only 30.5 μs

Layer 1

- **Channel coding and error detection/correction**
  - Channel coding makes extensive use of different **forward error correction (FEC) schemes.**
  - FEC adds redundancy to user data, allowing for the detection and correction of selected errors.
  - Advantage of an FEC scheme depends on the amount of redundancy, coding algorithm and further interleaving of data to minimize the effects of burst errors.
  - The FEC is also the reason why error detection and correction occurs in layer one and not in layer two as in the ISO/OSI reference model.
  - The GSM physical layer tries to correct errors, but it does not deliver erroneous data to the higher layer.

Layer 2

- Link Access Protocol in the D channel (**LAPDm)**
  - Signaling between entities in a GSM network requires higher
  - LAPDm is a lightweight LAPD because it does not need synchronization flags or check summing for error detection.
  - LAPDm offers reliable data transfer over connections, re-sequencing of data frames, and flow control
  - As there is no buffering between layer one and two, LAPDm has to obey the frame structures, recurrence patterns etc. defined for the Um interface.
  - Further services provided by LAPDm include segmentation and reassembly of data and acknowledged/unacknowledged data transfer.

Layer 3

- **Radio resource management (RR)**
  - Only a part of this layer, **RR', is implemented in the BTS, the remainder is situated in the BSC**.
  - The functions of RR' are supported by the BSC via the **BTS management (BTSM).**
  - The main tasks of RR are **setup, maintenance, and** release of radio channels.
  - RR also directly accesses the physical layer for radio information and offers a reliable connection to the next higher layer.

Layer 4

- **Mobility management (MM)**
  - registration,
  - authentication,
  - Identification,
  - location updating,
  - the provision of a temporary mobile subscriber identity (TMSI) that replaces the international mobile subscriber identity (IMSI) and which hides the real identity of an MS user over the air interface.
- While the IMSI identifies a user, the TMSI is valid only in the current location area of a VLR.
- MM offers a reliable connection to the next higher layer.

Layer 5

- **Call management (CM)**
  - call control (CC),
    - CC provides a point-to-point connection between two terminals and is used by higher layers for call establishment, call clearing and change of call parameters.
  - short message service (SMS)
    - SMS allows for message transfer using the control channels SDCCH and SACCH
  - supplementary service (SS).

Pulse code modulation (PCM)

- **PCM systems** offer transparent 64 kbit/s channels, GSM also allows for the submultiplexing of four 16 kbit/s channels into a single 64 kbit/s channel (16 kbit/s are enough for user data from an MS).

Signaling system No. 7 (SS7)

- Signaling system No. 7 (SS7) is used for signaling between an MSC and a BSC.
- This protocol also transfers all management information between MSCs, HLR, VLRs, AuC, EIR, and OMC.
- An MSC can also control a BSS via a BSS application part (BSSAP).

Test your Knowledge

- How is synchronization achieved in GSM? Who is responsible for synchronization and why is it so important?

Summary

- Protocol stack
  - Different layers between entities in GSM

References

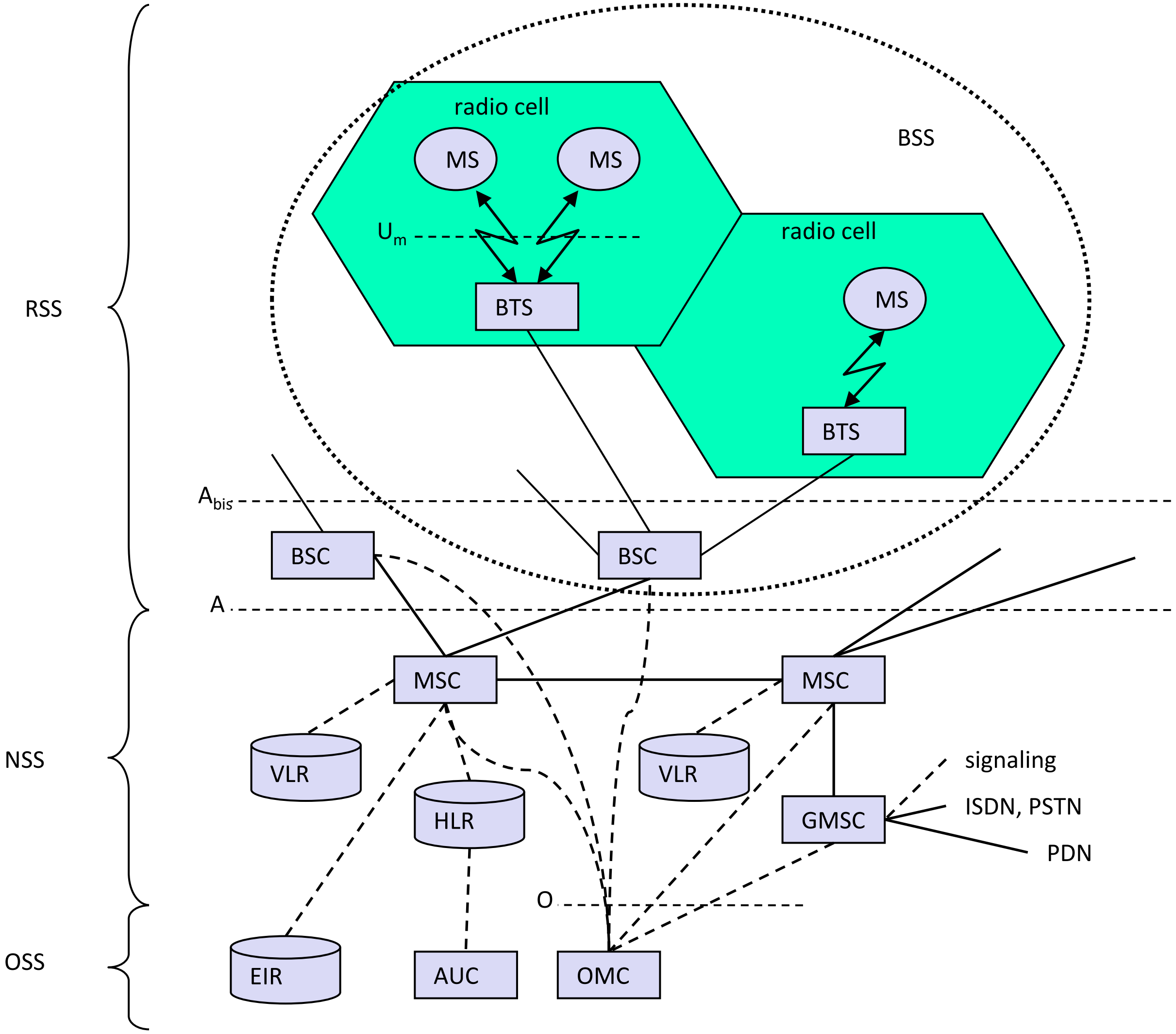
Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.

LOCALIZATION AND CALLING

Dr. A. Beulah

AP/CSE

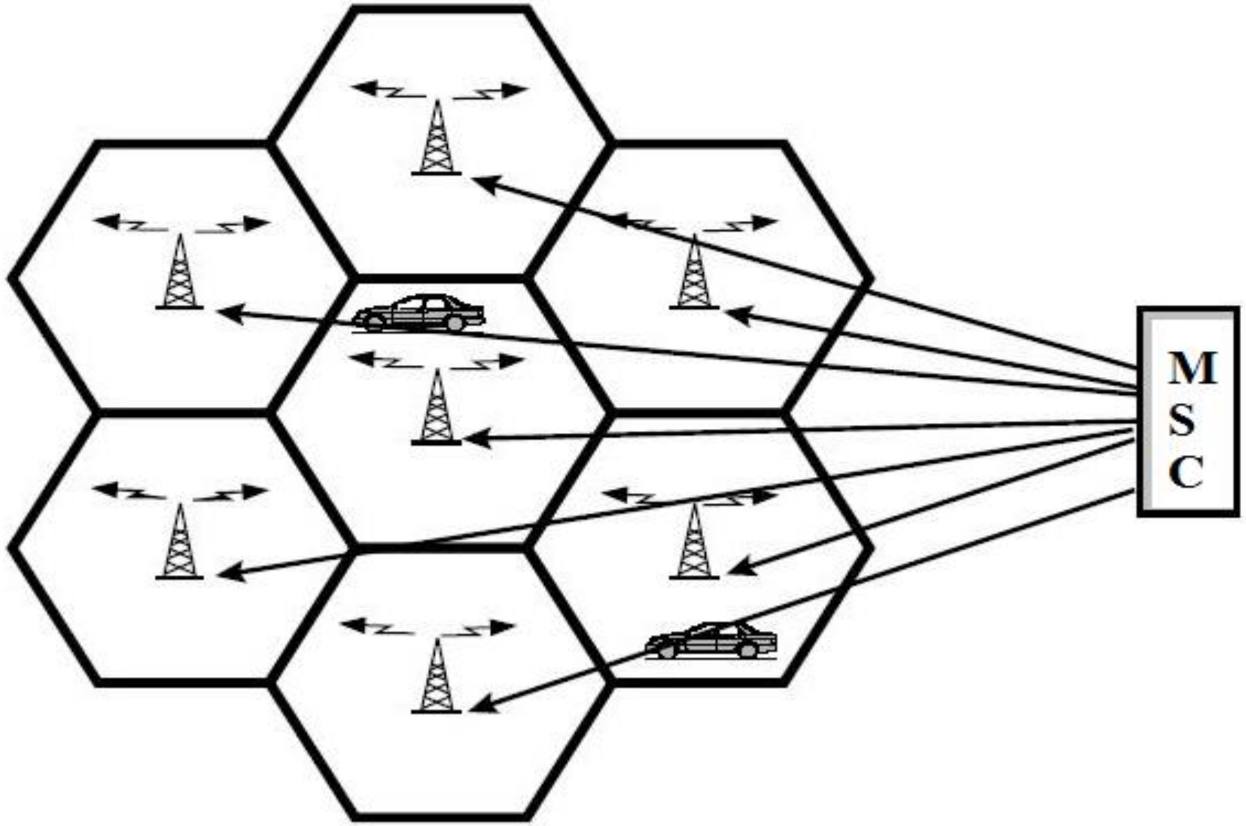
GSM Architecture: Recall



- *BSS* (Base Station Subsystem)
- *BTS* (Base Transceiver Station): sender and receiver
- *BSC* (Base Station Controller): controlling several transceivers
- MSC (Mobile Station Controller)
- HLR (Home Location Register)
- VLR (Visitor Location Register)
- GMSC (Gateway Mobile Station Controller)
- EIR (Equipment Identity Register)
- AuC (Authentication Centre)
- OMC (Operation and Maintenance Centre)
- Interfaces
  - Um : radio interface
  - Abis : standardized, open interface with 16 kbps user channels
  - A: standardized, open interface with 64 kbps user channels

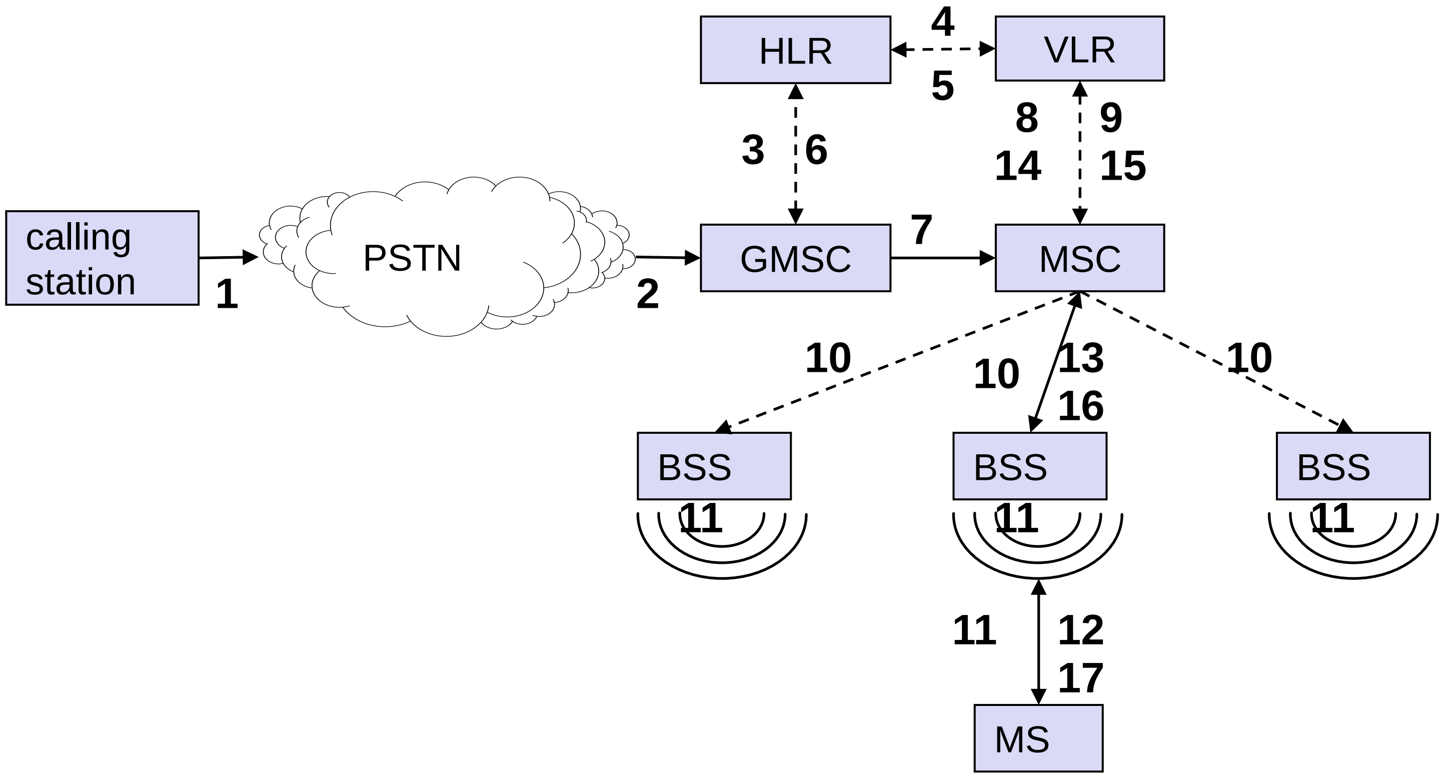
Types of Calls

- 2 types of calls
  - Mobile Terminated Call (MTC)
  - Mobile Originated Call (MOC)
- Paging
  - Broadcasting a message in a cell or group of cells to get a response from the MS for which a call or message is incoming.



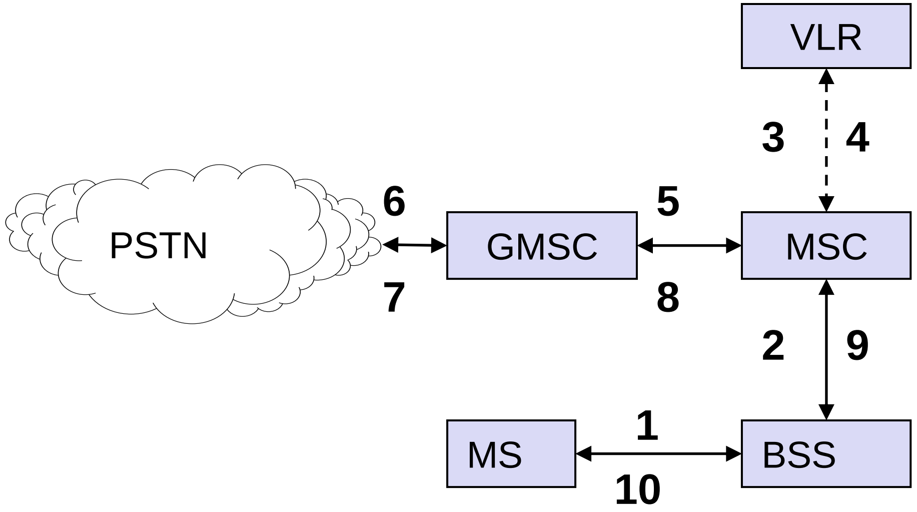
Mobile Terminated Call

- 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
- 9-10: set up call



HANDOVER

Dr. A. Beulah

AP/CSE

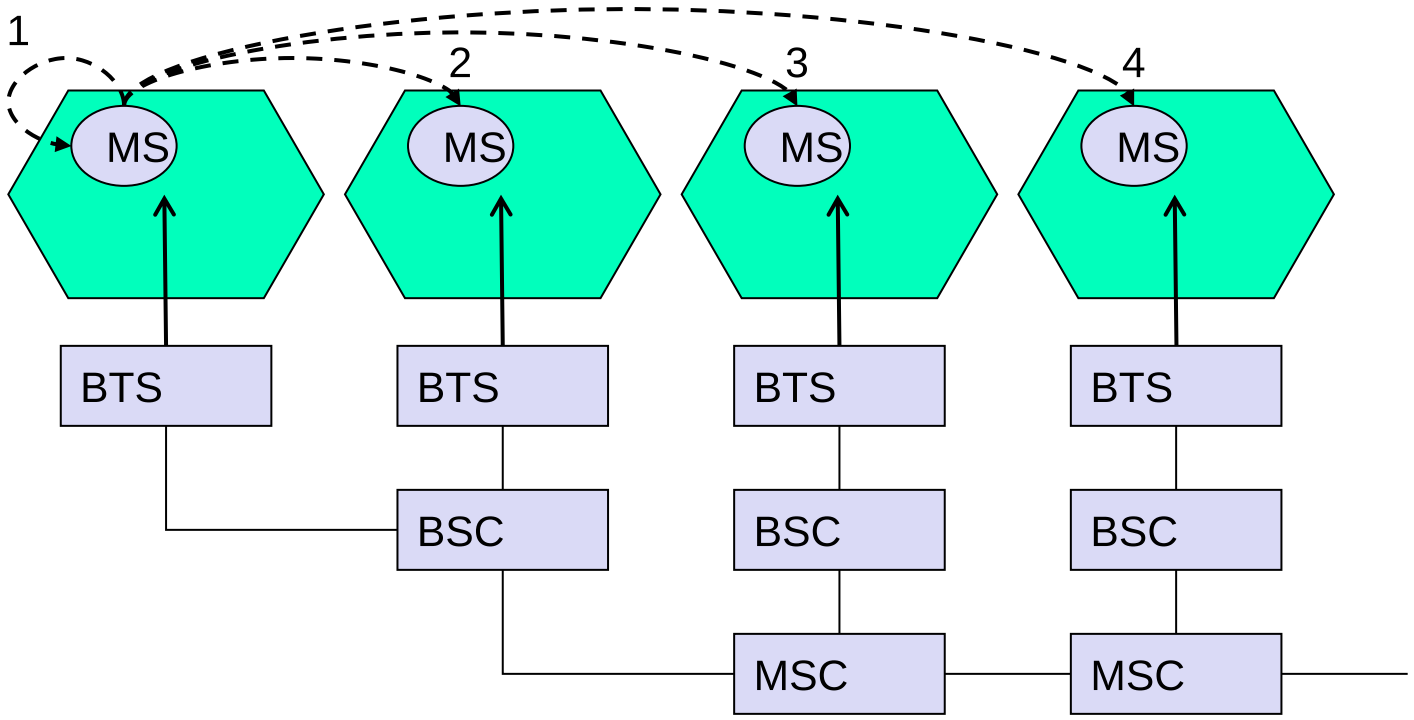
Introduction

- Single cell do not cover the whole service area.
- Therefore handover procedure is required in GSM
- More handover for ongoing call are needed when the cell size is small and the movement of the mobile station is fast (Upto 250 km/h)
- A handover should not cause a cut-off or call drop.
- Maximum handover duration is about 60ms.

Basic Reasons for handover

1. The mobile station moves out of the range of a BTS.
    - The signal strength decreased continuously until it falls below the minimum requirement.
    - The error rate is high due to interference. (BTS may be too high max 35km)
2. MSC or BSC may decide that the traffic in one cell is too high and shift some MS to other cells with a lower load ie load balancing

Types of Handover



Types of Handover

- Intra cell handover
  - Within a cell.
  - Narrow band interference could make transmission with error at a certain frequency
  - BSC then decides to change the carrier frequency
- Inter cell, Intra BSC handover
  - Mobile station moves from one cell to another, but stays within the control of the same BSC.
  - BSC performs a handover, assigns a new channel in the new cell and releases the old one.

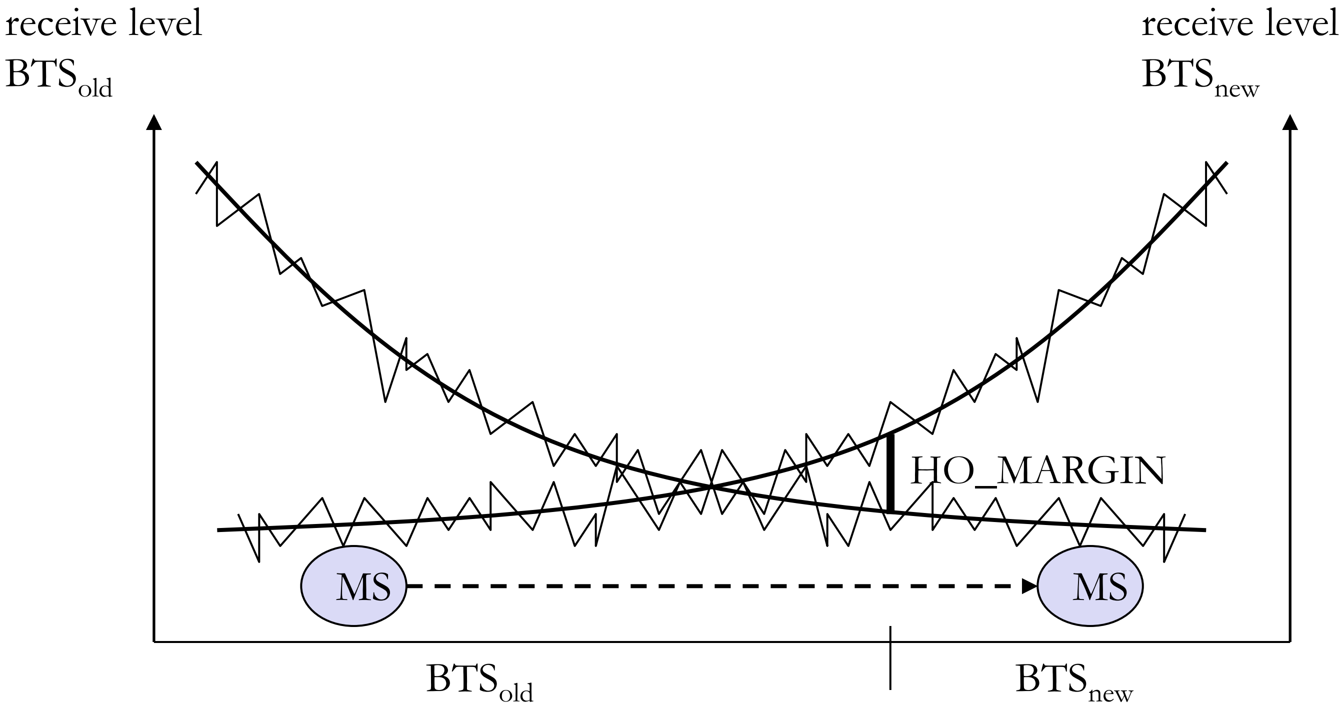
Types of Handover

- Inter BSC, Intra MSC handover
  - BSC controls only limited number of cells.
  - GSM has to perform handovers between cells controlled by different BSCs.
  - This handover is then controlled by MSC.
- Inter MSC handover
  - A handover could be required between two cells belonging to different MSCs.
  - Both MSCs perform the handover together.

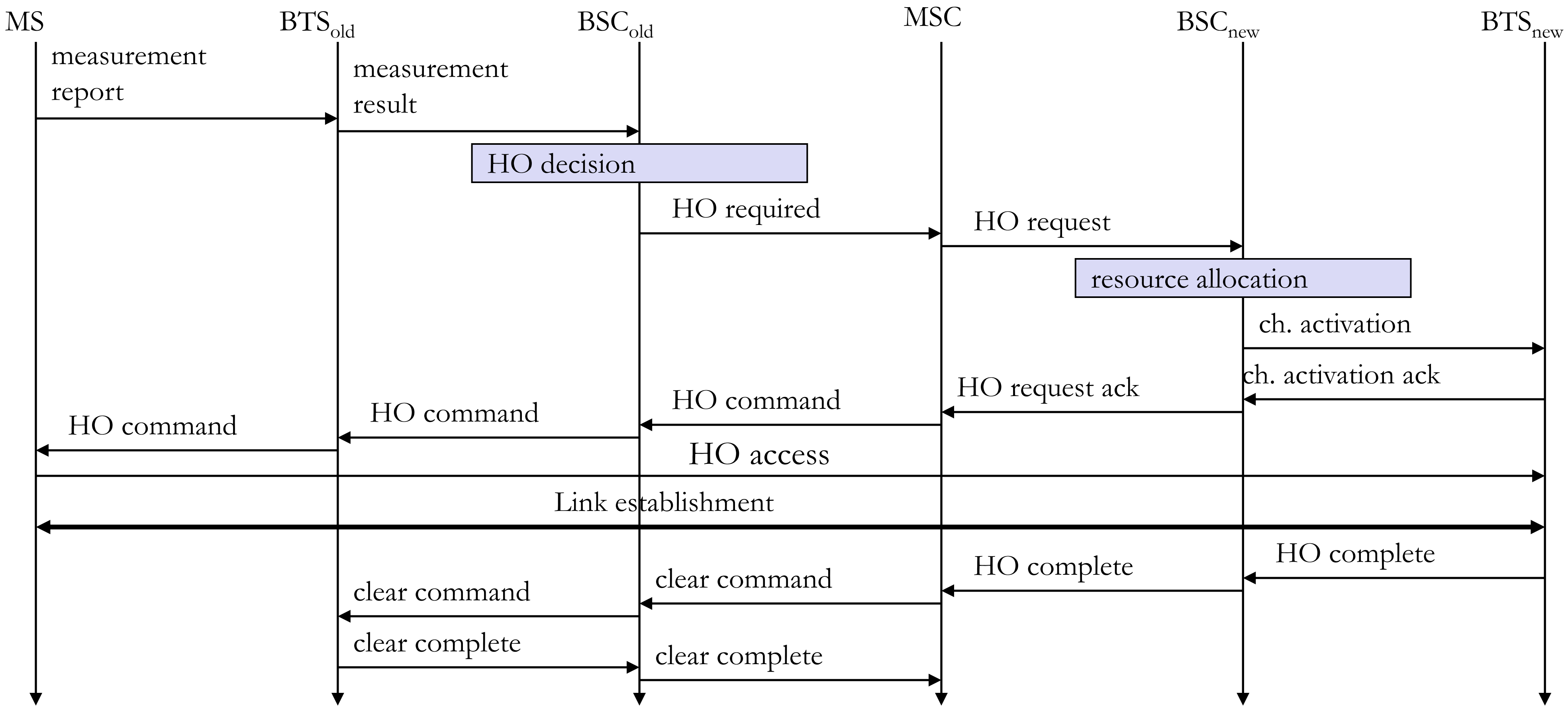
Handover Decision

- To identify a weak link
  - MS and BTS perform periodic measurements of the downlink and uplink quality respectively.
  - For every half second MS sent information about the quality of the current link used for transmission and the quality of certain channels in neighboring cells.
- Handover value does not depends on the actual value, but it depends on the average value.

Handover Decision



Intra MSC Handover



Summary

- Localization
    - Paging
- Calling
    - Mobile Terminated Call
    - Mobile Originated Call
- Handover
    - Different types
    - Handover margin
    - Handover Decision

Test your understanding

- How a call connection is established between 2 mobile phones.

References

Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.

GSM SECURITY

Dr. A. Beulah

AP/CSE

Security

- GSM offers security services with the help of Confidential information stored in
  - The AuC
  - The individual SIM
- AuC contains
  - The algorithms for authentication and generates the values needed for user authentication
  - The keys for encryption
- SIM stores
  - Personal data
  - Secret data.
  - These are protected with the help of PIN

Security Services

- Access control and Authentication
  - Authentication of a valid user for the SIM.
  - The user needs a secret PIN to access the SIM
  - Subscriber Authentication has to be done.
- Confidentiality
  - User data is encrypted
  - After authentication, BTS and MS apply encryption to voice, data, and Signal.
  - Confidentiality exists only between MS and BTS.
- Anonymity
  - User identifiers are not used over the air.
  - TMSI (newly assigned by the VLR) is transmitted after each location update
  - VLR can change the TMSI at any time.

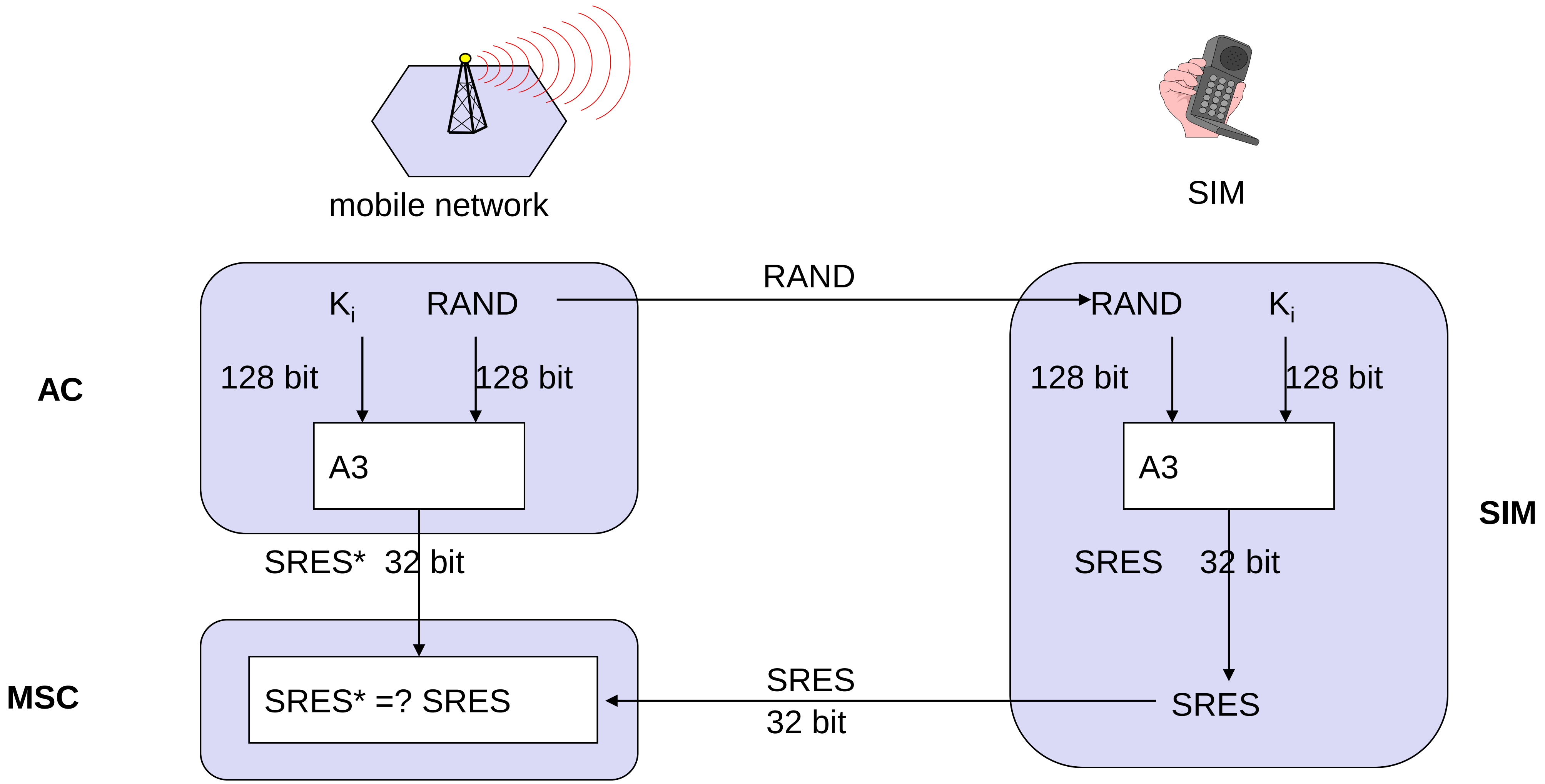
Security Services

- 3 Algorithms
- Algorithm A3 is used for authentication
- Algorithm A5 for Encryption
- Algorithm A8 for the generation of a Cipher Key.

Authentication

- The user should be authenticated, before using any service from the network.
- Authentication is based on SIM
- SIM contains
  - Authentication key K_i
  - User Identification IMSI
  - Algorithm A3 → algorithm used for authentication.
- Authentication uses a challenge-response method.

Authentication



mobile network

SIM

AC

K_i RAND

128 bit 128 bit

A3

SRES* 32 bit

RAND

RAND K_i

128 bit 128 bit

A3

SRES 32 bit

SIM

MSC

SRES* =? SRES

SRES

32 bit

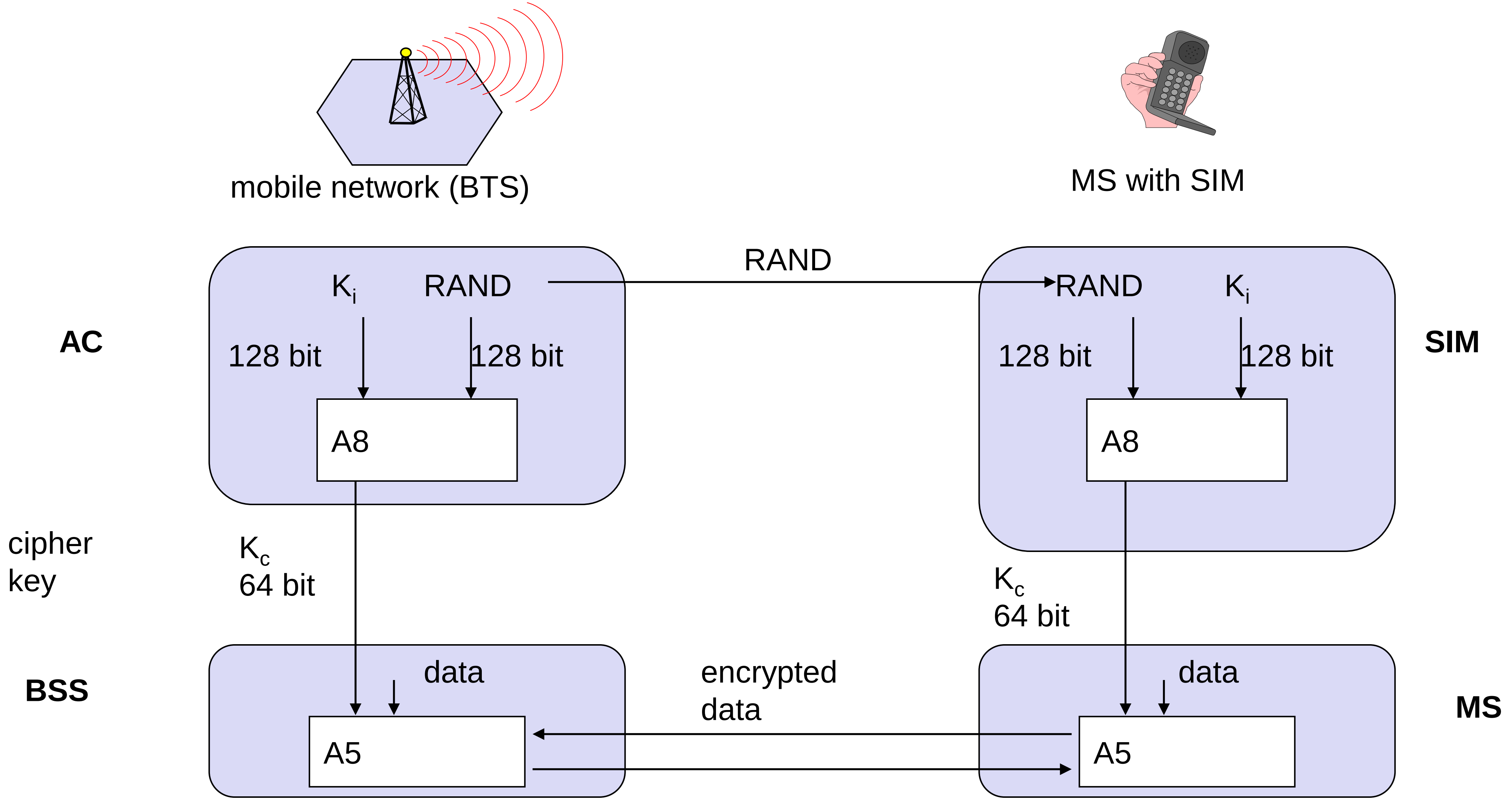
SRES

K_i: individual subscriber authentication key SRES: signed response

Encryption

- User data are encrypted
- MS and BTS uses k_c (cipher key) for encryption
- K_c is generated using the authentication key k_i and a random value by applying the algorithm A8

Encryption


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

Summary

- GSM Services
  - Bearer service
  - Teleservice
  - Supplementary service
- GSM Architecture
  - RSS
  - NSS
  - OSS
- GSM Security

Test your understanding

- Identify the main reason as to why a mobile handset is compact and lightweight and yet provides a large number of features such as roaming, camera, audio and video play, record internet etc., while traditional landline phone handsets are bulky and provide only limited features.

References

Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.

Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.

GENERAL PACKET RADIO SERVICE (GPRS)

Dr. A. Beulah

AP/CSE

What is GPRS?

- A new bearer service for GSM that greatly improves and simplifies wireless access to external Packet Data Networks(PDN), e.g to the internet.
- General Packet Radio Service
  - General → not restricted to GSM use
  - Packet Radio → enables packet mode communication over air ie. packet switching
  - Service, not System → existing BSS (partially also NSS) infrastructure is used

What is GPRS?

- Billing
  - GSM→ Based on time duration of connection
  - GPRS → Based on amount of transmitted data rather duration of connection
- GPRS allows broadcast, multicast, and unicast.
- In GPRS no connection has to setup prior to data transfer.
- GPRS needs additional network elements ie. The hardware and the software.
- Requires many new network elements into NSS
- Provides connections to external packet data networks (Internet, X.25)

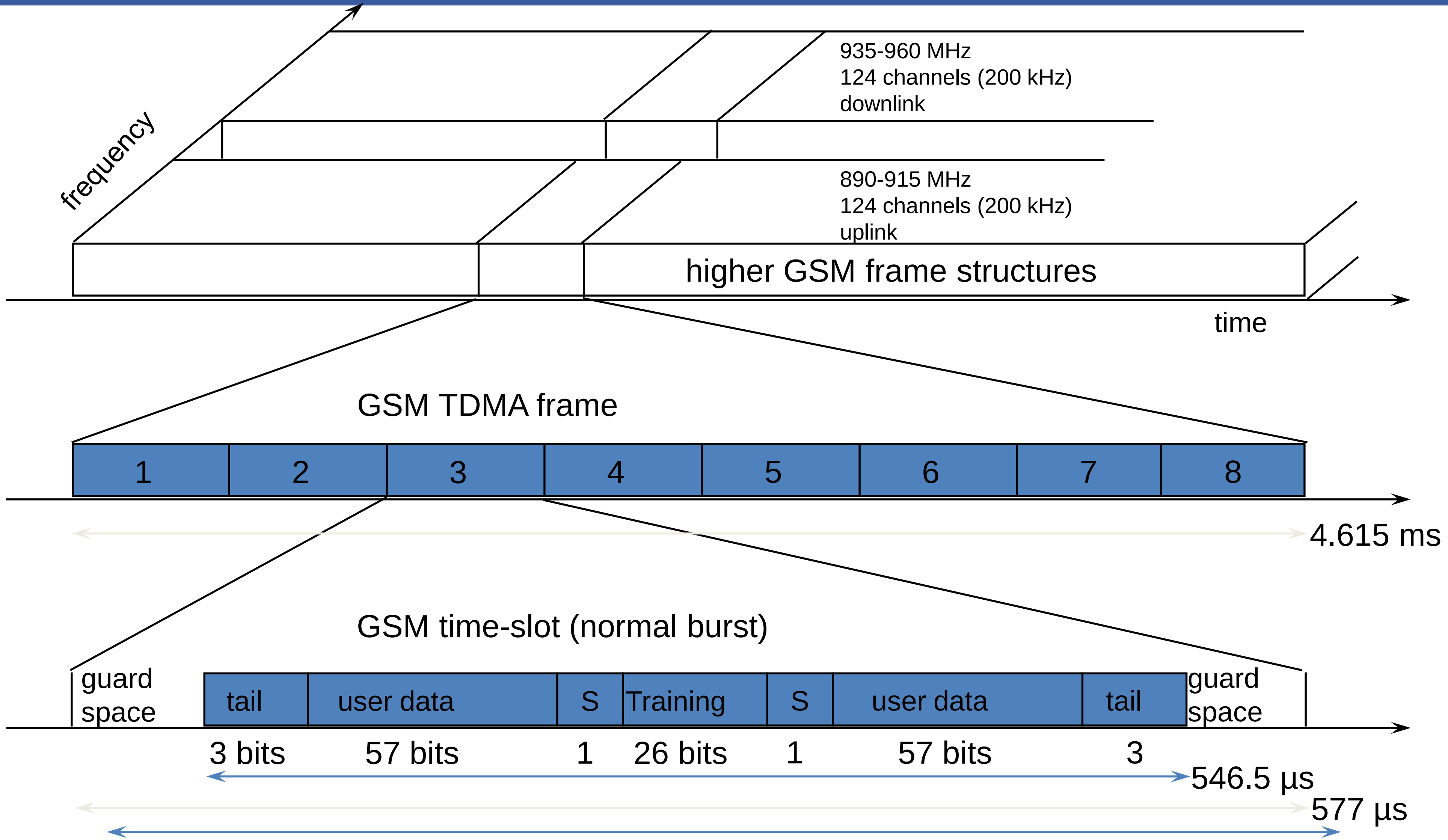
What is GPRS?

- Main benefits
  - Resources are reserved only when needed and charged accordingly
  - Connection setup times are reduced
  - Enables new service opportunities
- Advantage: More flexible
- Disadvantage: More investment needed (new hardware and software)

GPRS Time Slots

- GSM allocates time slots between 1 and 8 within a TDMA frame for a GPRS.
- Time slots are not allocated in a fixed, predetermined manner but on demand.
- All time slots can be shared by the active users..
- Uplink and downlink are allocated separately.
- Data transfer rate is upto 170kbps
- Operators usually reserve atleast a time slot per cell to guarantee a minimum data rate.
- Channel characteristics and the type of channel and does not limit the maximum data rate.
- All GPRS services can be used in parallel to conventional services.

GSM Time slot



GPRS user data rates in kbps

Coding scheme	**1 slot**	**2 slots**	**3 slots**	**4 slots**	**5 slots**	**6 slots**	**7 slots**	**8 slots**
CS-1	9.05	18.1	27.15	36.2	45.25	54.3	63.35	72.4
CS-2	13.4	26.8	40.2	53.6	67	80.4	93.8	107.2
CS-3	15.6	31.2	46.8	62.4	78	93.6	109.2	124.8
CS-4	21.4	42.8	64.2	85.6	107	128.4	149.8	171.2

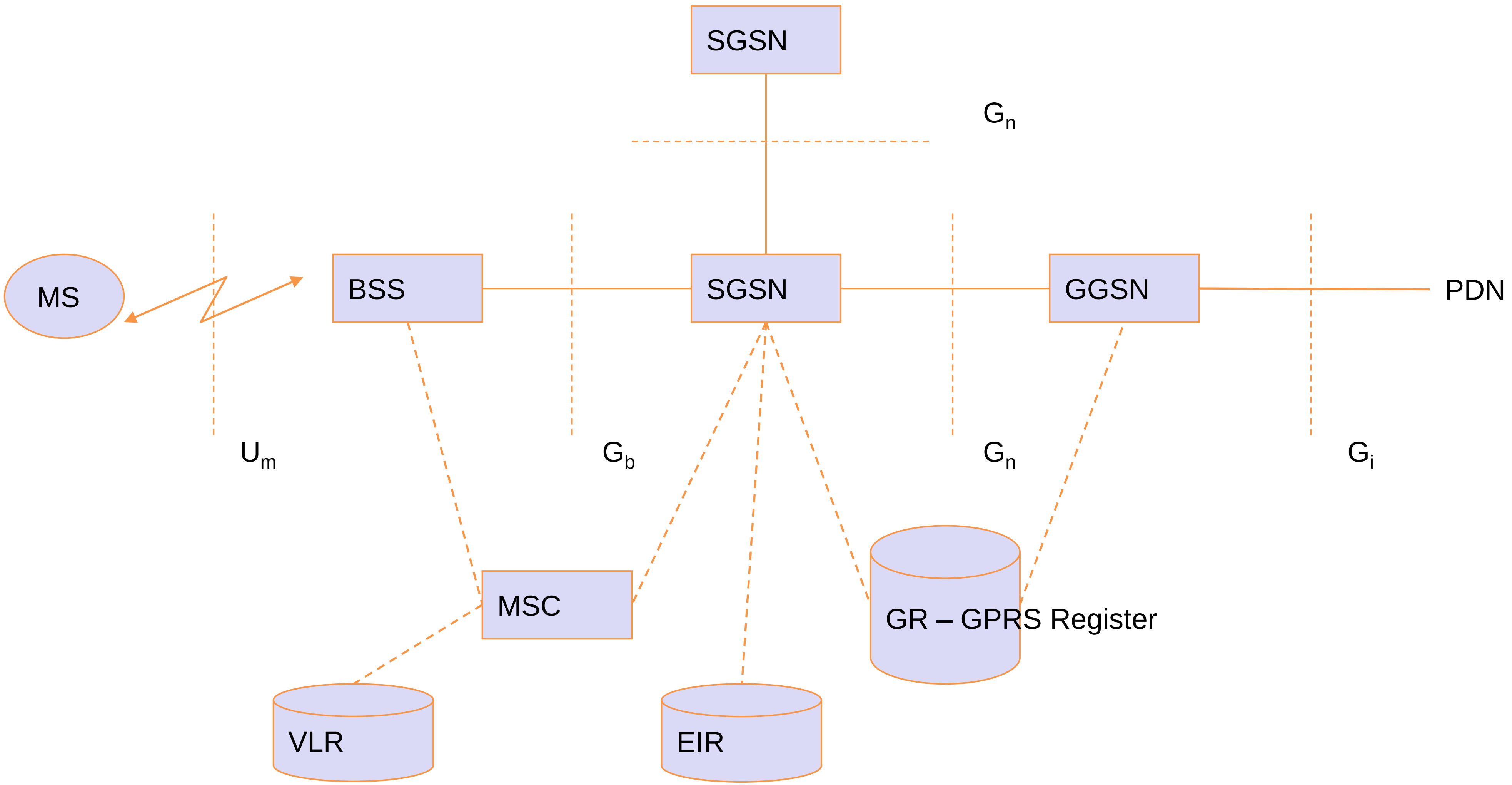
Examples for GPRS device classes

Class	Receiving slots	Sending slots	Maximum number of slots
1	1	1	2
2	2	1	3
3	2	2	3
5	2	2	4
8	4	1	5
10	4	2	5
12	4	4	5

GPRS Services

- Point-to-Point Service
  - Between 2 users.
  - Connection less or Connection oriented
  - Toll road system, UIC train control system
- Point-to-Multipoint Service
  - Multicast, Broadcast
  - Weather info, road traffic info, news, fleet management

GPRS Architecture



GPRS Architecture

GSM Network Element	**Modification or Upgrade Required for GPRS.**
Mobile Station (MS)	New Mobile Station is required to access GPRS services. These new terminals will be **backward compatible with GSM for voice calls**.
BTS	A **software upgrade** is required in the existing base transceiver site.
BSC	The base station controller (BSC) requires a **software upgrade** and the installation of new hardware called the **packet control unit (PCU).** The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
GPRS Support Nodes (GSN)	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).
Databases (HLR,VLR etc)	All the databases involved in the network will require **software upgrades** to handle the new call models and functions introduced by GPRS.

Interfaces

- Gb
  - Interface between the BSS and the SGSN the transmission protocol could be Frame Relay or IP.
- Gn
  - IP Based interface between SGSN and other SGSNs and (internal) GGSNs
- Gi
  - IP based interface between the GGSN and a public data network (PDN) either directly to the Internet or through a WAP gateway

GPRS Mobile Stations

- Mobile Station with GPRS services is needed. Because old GSM phones do not handle the enhanced air interface or packet data.
- A variety of MS can exist, including a high-speed version of current phones to support high-speed data access
- These mobile stations are backward compatible for making voice calls using GSM.

GPRS BSS

- The BTS requires a software upgrade but typically does not require hardware enhancements.
- Each BSC requires the installation of one or more **Packet Control Units (PCUs)** and a software upgrade.
- The PCU provides a physical and logical data interface to the base station subsystem (BSS) for packet data traffic.
- When either voice or data traffic is originated at the Mobile Station, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call.
- However, at the output of the BSC, the traffic is separated; voice is sent to the mobile switching center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

GPRS Support Nodes

- Following two new components, called GPRS support nodes (GSNs), are added:
  - Gateway GPRS support node (GGSN)
  - Serving GPRS support node (SGSN)

Gateway GPRS Support Node

- The Gateway GPRS Support Node acts as an interface and a router to external networks.
- The GGSN contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node.
- The GGSN can act as a packet filter for incoming traffic.

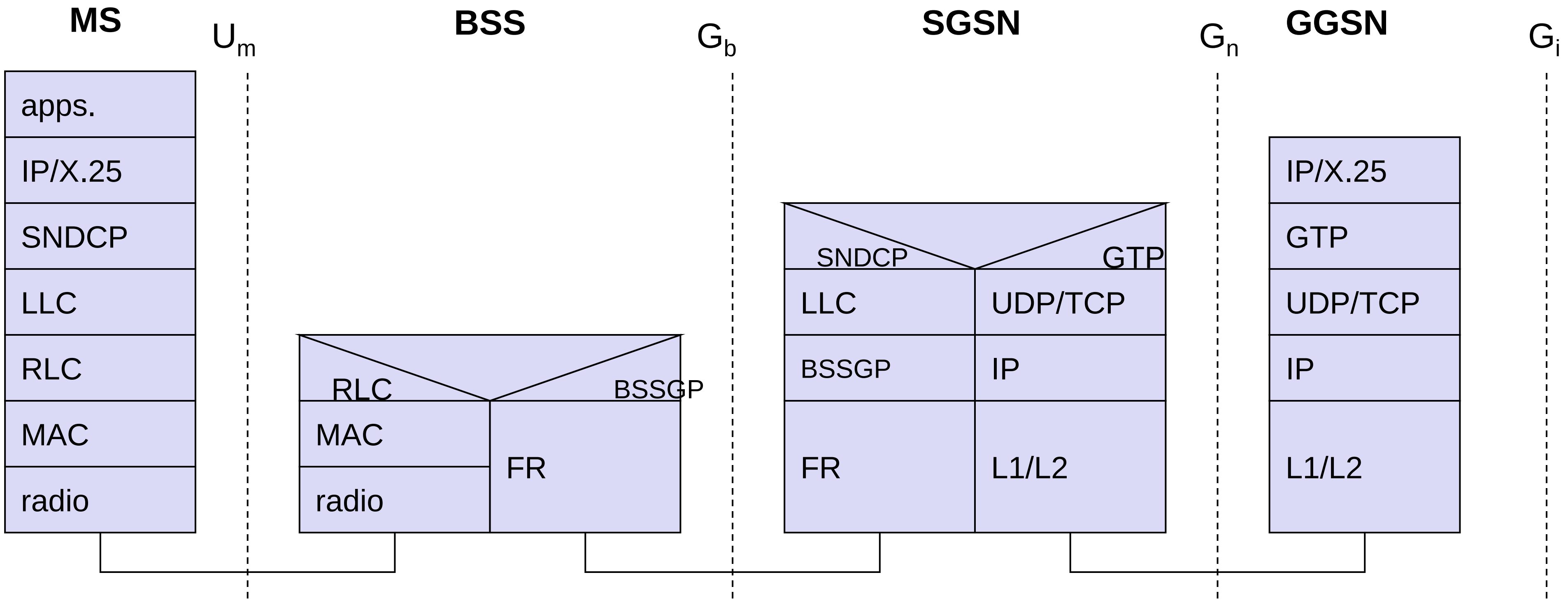
Serving GPRS Support Node

- The Serving GPRS Support Node is responsible for
  - authentication of GPRS mobiles,
  - registration of mobiles in the network,
  - mobility management, and
  - collecting information for charging for the use of the air interface.

Internal Backbone

- The internal backbone is an IP based network used to carry packets between different GSNs.
- Tunneling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network.
- Signaling from a GSN to a MSC, HLR or EIR is done using SS7

GPRS protocol architecture



GPRS protocol architecture

- **GPRS Tunnellling Protocol (GTP)**
  - All data within the GPRS backbone, i.e., between the GSNs, is transferred using GTP
  - GTP use two different transport protocols:
    - The reliable **TCP (needed for reliable transfer of X.25 packets)**
    - The non-reliable **UDP (used for IP packets).**
- The network protocol for the GPRS backbone is **IP (using any lower layers)**
- X.25 → Packet switched n/w for WAN
- Framerelay → Physical and Datalink layers for WAN

GPRS protocol architecture

- **Subnetwork dependent convergence protocol (SNDCP)**
  - To adapt to the different characteristics of the underlying networks, **SNDCP** is used between an SGSN and the MS
- On top of SNDCP and GTP, user packet data is tunnelled from the MS to the GGSN and vice versa.
- **Logical Link control (LLC)**
  - To achieve a high reliability of packet transfer between SGSN and MS
  - Comprises ARQ and FEC mechanisms for PTP (and later PTM) services

GPRS protocol architecture

- **Base station subsystem GPRS protocol (BSSGP)**
  - Conveys **routing and QoS-related information** between the BSS and SGSN.
  - BSSGP does not perform error correction and works on top of a frame relay (FR) network
- **Radio link protocol (RLC)**
  - to transfer data over the U_m interface.

Quality of Service

- Service Precedence:
  - The service precedence is the priority of a service in relation to another service.
  - There exist three levels of priority: high, normal, and low.
- Reliability:
  - The reliability indicates the transmission characteristics required by an application.
  - Three reliability classes are defined, which guarantee certain maximum values for the probability of loss, duplication, mis-sequencing, and corruption of packets.

Quality of Service

- Delay
  - The delay is defined as the end-to end transfer time between two communicating mobile stations or between a mobile station and the Gi interface to an external packet data network.
  - This includes all delays within the GPRS network, e.g., the delay for request and assignment of radio resources and the transit delay in the GPRS backbone network.
  - Transfer delays outside the GPRS network, e.g., in external transit networks, are not taken into account.

Quality of Service

- Throughput
  - The throughput specifies the maximum/peak bit rate and the mean bit rate.
- Using these QoS classes, QoS profiles can be negotiated between the mobile user and the network for each session, depending on the QoS demand and the current available resources.
- The billing of the service is then based on the transmitted data volume, the type of service, and the chosen QoS profile.

Summary

- Why GPRS?
- GPRS Architecture
- GPRS Quality of Service

Test your Knowledge

- Mention the advantages of GPRS over GSM.
- Without GPRS whether packet data can be transmitted over GSM???

References

Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.

UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM (UMTS)

Dr. A. Beulah

AP/CSE

Evolution : From 2G to 3G

- Services must be independent from radio access technology and is not limited by the network infrastructure.
- Support of multimedia and all of its components.
- Increased data rate.
- Convergence of existing networks.
- Video Telephony.
- MP3 downloads.
- Potential good applications like TV on a mobile phone.
- However, to convert to UMTS, the network needs to be reengineered from the ground up.
  - Actually uses the lower 3 layers of the OSI model.

Evolution : From 2G to 3G

- GPRS – General Packet Radio Services
  - 2.5G protocol
  - Involved only software changes to the GSM network.
  - Used under utilized TDMA channels more effectively.
  - Increased data rates to a max of 170 Kbps.
- EDGE – Enhanced Data rates for GSM Evolution.
  - 2.75G protocol.
  - Required minimal hardware changes
  - Added a new encoding scheme that allowed for more bits to be added into each time slice.
  - Data can now be passed optimally at 384 Kbps.
- Both of these use TDMA over GSM

UMTS

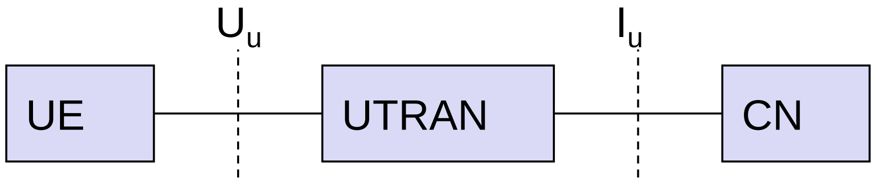
- 3G Standard for Cellular Communication
- Uses W-CDMA (Wideband CDMA)
  - 5 MHz of bandwidth for each channel.
  - Several thousand users can be supported on each cell site.
- Offers 11 Mbps download speeds in theory.
  - Uplink speeds are much slower
  - Most users are finding download throughput of about 384 Kbps.
    - However, this is still much faster than the 14.4 Kbps optimally that GSM offered.

UMTS - Standards

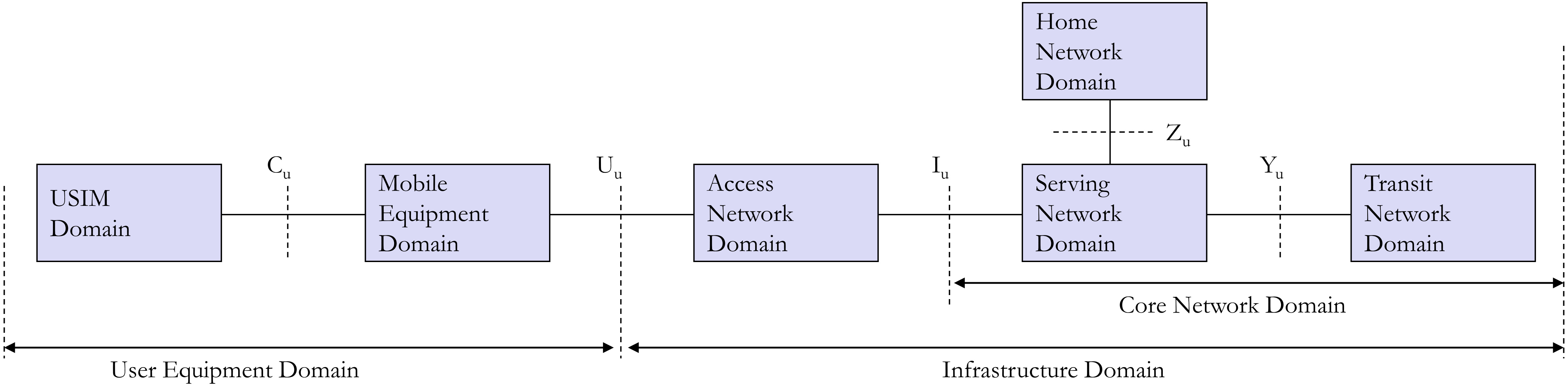
- The 3G standard was written by the International Telecommunication Union (ITU)
  - The standard is referred as IMT-2000 (International Mobile Telecommunications for the year 2000)
- The key to the standards is the available data over the air interface
  - 2 Mbps in fixed or in-building environments
  - 384 kbps in pedestrian or urban environments
  - 144 kbps in wide area mobile environments
  - Variable data rates in large geographic area systems (satellite)

UMTS Architecture

- UE (User Equipment)
- UTRAN (UMTS Terrestrial Radio Access Network)
  - Cell level mobility
  - Radio Network Subsystem (RNS)
  - Encapsulation of all radio specific tasks
- CN (Core Network)
  - Inter system handover
  - Location management if there is no dedicated connection between UE and UTRAN



UMTS Domains and Interfaces



- User Equipment Domain
  - Assigned to a single user in order to access UMTS services
- Infrastructure Domain
  - Shared among all users
  - Offers UMTS services to all accepted users

UMTS Domains and Interfaces

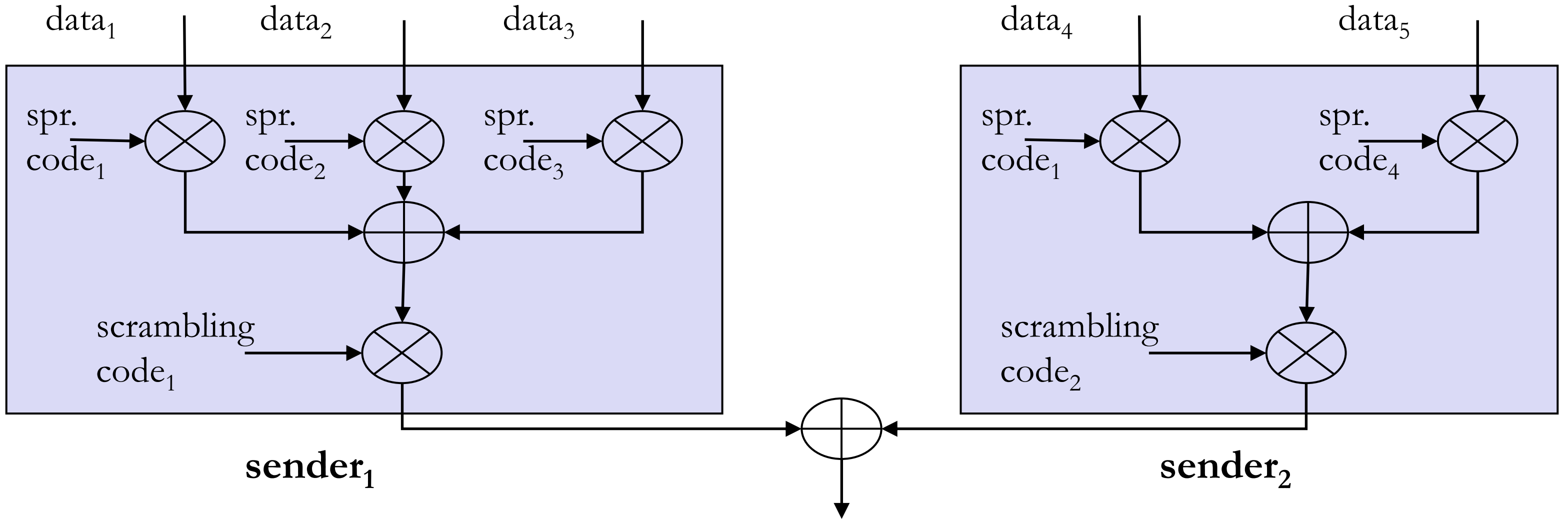
- Universal Subscriber Identity Module (USIM)
  - Functions for encryption and authentication of users
  - Located on a SIM inserted into a mobile device
- Mobile Equipment Domain
  - Functions for radio transmission
  - User interface for establishing/maintaining end-to-end connections
- Access Network Domain
  - Access network dependent functions
- Core Network Domain
  - Access network independent functions
  - Serving Network Domain
    - Network currently responsible for communication
  - Home Network Domain
    - Location and access network independent functions

UMTS Radio Interface

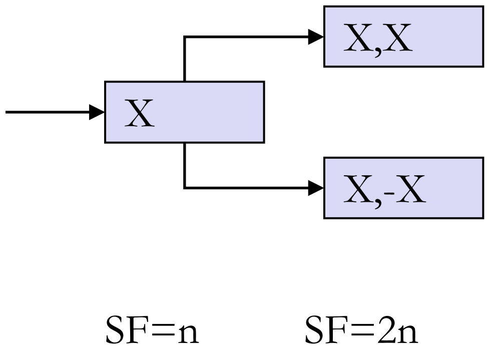
- Spreading and scrambling of user data
- OVSF coding (orthogonal variable spreading factor)
- UMTS FDD frame structure (WCDMA)
- UMTS TDD Frame Structure

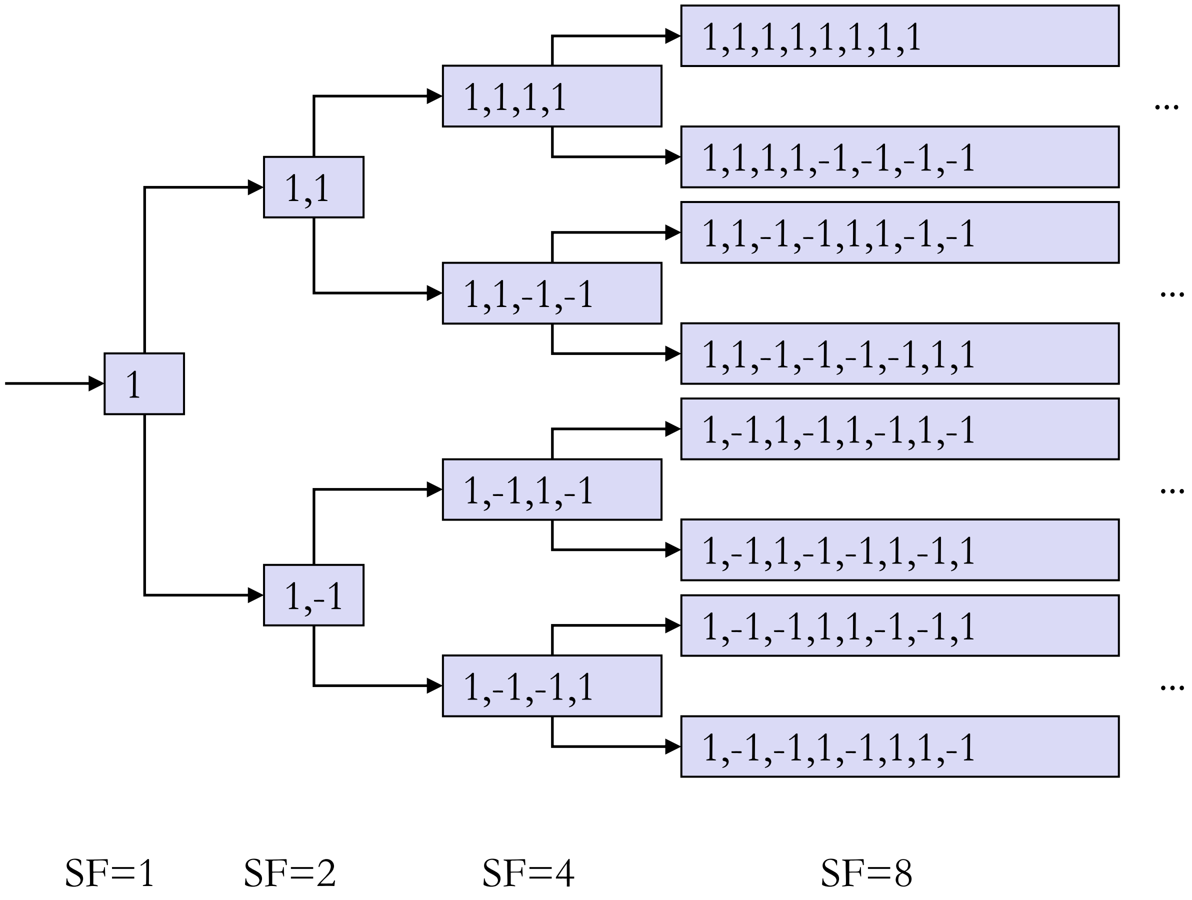
Spreading and scrambling of user data

- Constant chipping rate of 3.84 Mchip/s
- Different user data rates supported via different spreading factors
  - higher data rate: less chips per bit and vice versa
- User separation via unique, quasi orthogonal scrambling codes
  - users are not separated via orthogonal spreading codes
  - much simpler management of codes: each station can use the same orthogonal spreading codes
  - precise synchronization not necessary as the scrambling codes stay quasi-orthogonal

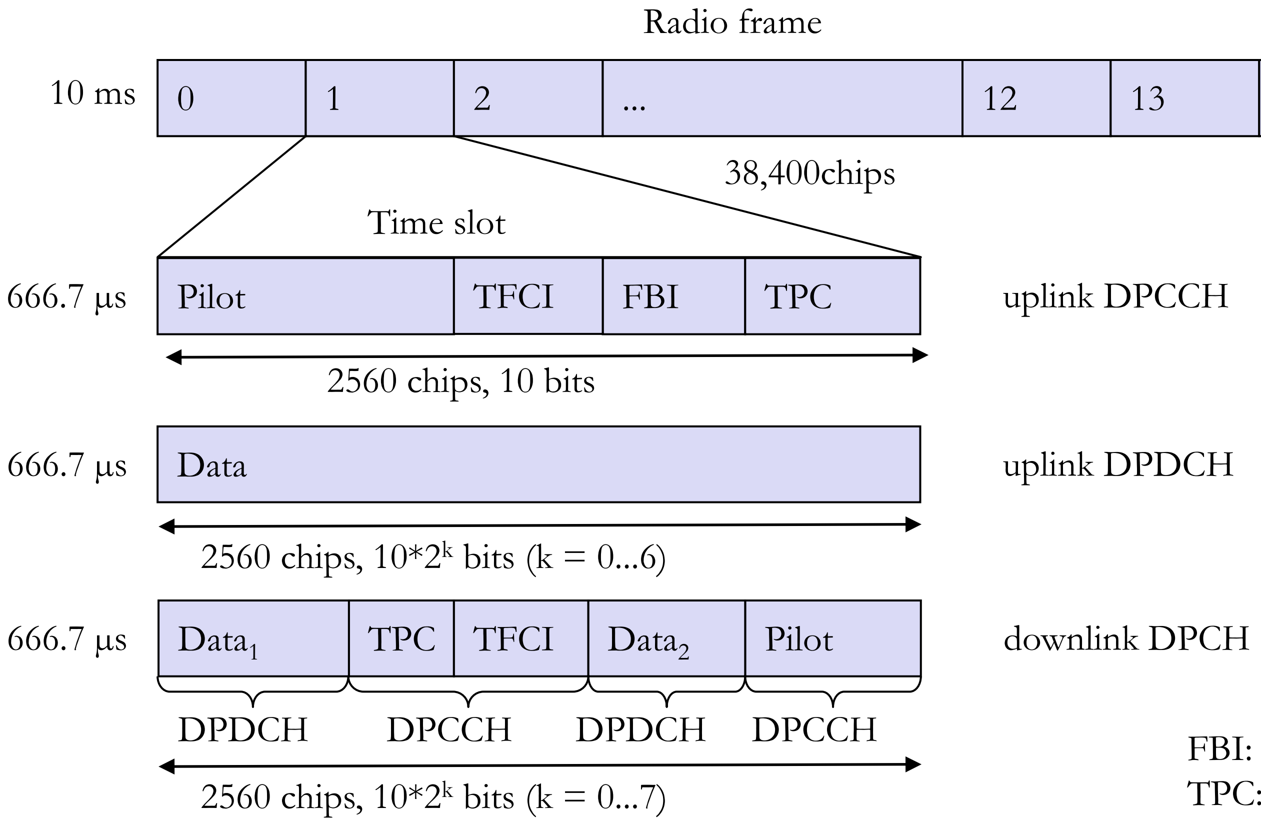


OVSF coding


X
X,X
X,-X
SF=n
SF=2n


1
1,1
1,-1
1,1,1,1
1,1,-1,-1
1,-1,1,-1
1,-1,-1,1
1,1,1,1,1,1,1,1
1,1,1,1,-1,-1,-1,-1
1,1,-1,-1,1,1,-1,-1
1,1,-1,-1,-1,-1,1,1
1,-1,1,-1,1,-1,1,-1
1,-1,1,-1,-1,1,-1,1
1,-1,-1,1,1,-1,-1,1
1,-1,-1,1,-1,1,1,-1
...
...
...
...
SF=1
SF=2
SF=4
SF=8

UMTS FDD Frame Structure (W-CDMA)



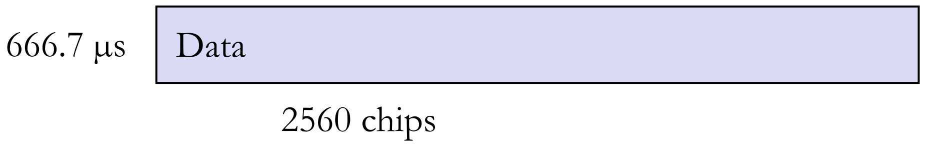
W-CDMA

- 1920-1980 MHz uplink
- 2110-2170 MHz downlink
- chipping rate: 3.840 Mchip/s
- soft handover
- QPSK
- spreading factor: UL: 4-256; DL:4-512

FBI: Feedback Information
TPC: Transmit Power Control
TFCI: Transport Format Combination Indicator
DPCCH: Dedicated Physical Control Channel
DPDCH: Dedicated Physical Data Channel
DPCH: Dedicated Physical Channel

Dedicated Physical Data Channel

- Offered Data Rates
  - 960 kbps, 480, 240, 120, 60, 30, and 15 kbps (spreading factor 256).
- 960 kbps
  - spreading factor 4,
  - 640 bits per slot,
  - 15 slots per frame,
  - 100 frames



666.7 µs

Data

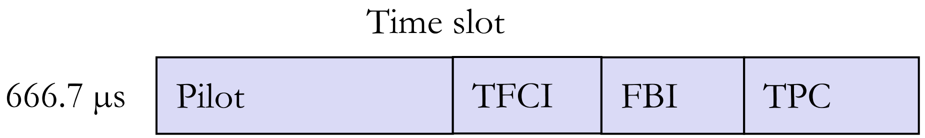
2560 chips

Typical UTRA-FDD uplink data rates

User data rate [kbit/s]	12.2 (voice)	64	144	384
DPDCH [kbit/s]	60	240	480	960
DPCCH [kbit/s]	15	15	15	15
Spreading	64	16	8	4

Dedicated Physical Control Channel

- Constant spreading factor 256
- Pilot is used for channel estimation.
- Transport Format Combination Identifier (TFCI) specifies the channels transported within the DPDCHs.
- Feedback Information Field (FBI) supports soft handover.
- Transmit Power Control (TPC) is used for controlling the transmission power of a sender



Time slot

666.7 µs

Pilot

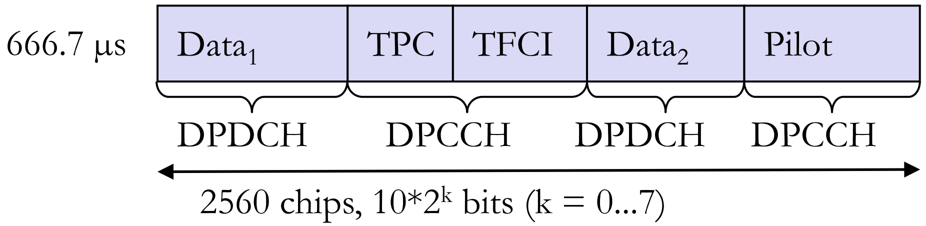
TFCI

FBI

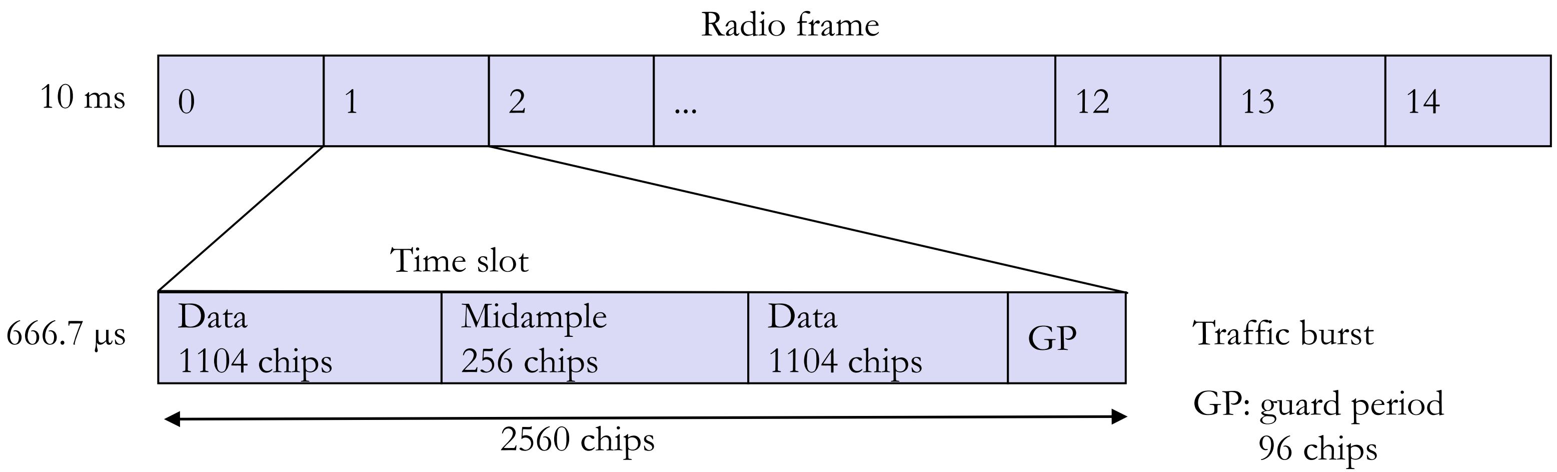
TPC

Dedicated Physical Channel

- Spreading factors between 4 and 512 are available
- data rates for data channels (DPDCH) within a DPCH are
  - 6 kbit/s (SF=512),
  - 24 kbit/s
  - 51 kbit/s
  - 90 kbit/s
  - 210,
  - 432,
  - 912,
  - 1,872 kbit/s (SF=4)



UMTS TDD Frame Structure



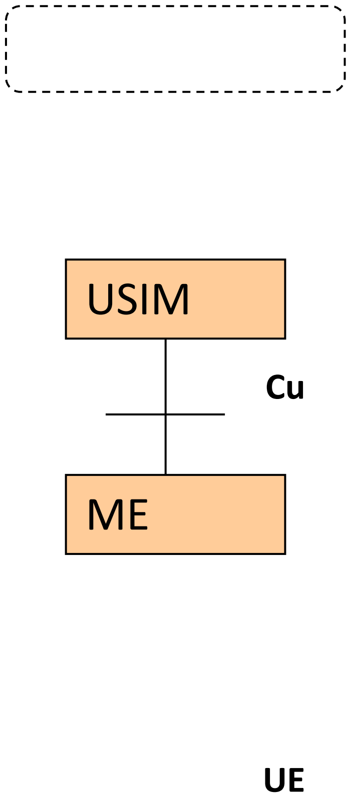
Traffic burst

GP: guard period
96 chips

TD-CDMA

- 2560 chips per slot
- spreading factor: 1-16
- symmetric or asymmetric slot assignment to UL/DL (min. 1 per direction)

User Equipment Architecture



- User Equipment → any UMTS enabled mobile device
- User Equipment Domain handles the access of the user onto the UMTS services
- USIM – User Services Identity Module
  - Extended SIM functionality
  - Functions for user identification, authentication and encryption
  - Integrated into SIM card (of the established format)
  - Most recent Mobile Equipment can handle both SIM and USIM
- Mobile Equipment Domain responsible for air interface
  - User interface for end-to-end connections

UE – User Equipment

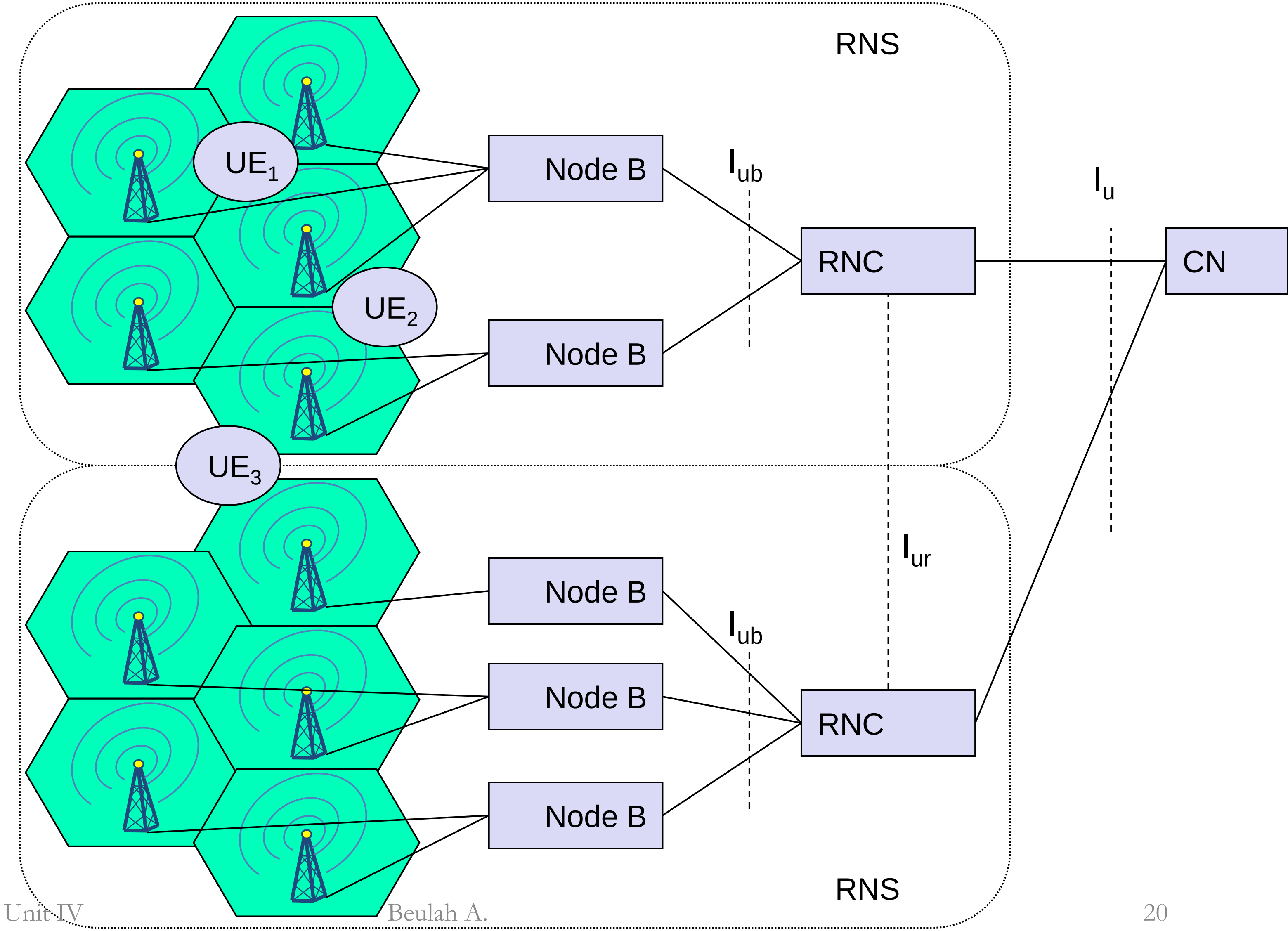
- The UE is the counterpart of several nodes of the architecture.
- As the counterpart of a node B, the UE performs
  - Signal quality measurements, inner loop power control, spreading and modulation, and rate matching.
- As a counterpart of the RNC, the UE
  - Has to cooperate during handover and cell selection, performs encryption and decryption, and participates in the radio resource allocation process.
- As a counterpart of the CN, the UE
  - Has to implement mobility management functions, performs bearer negotiation, or requests certain services from the network.

UTRAN Architecture

RNC: Radio Network Controller

RNS: Radio Network Subsystem

- UTRAN comprises several RNSs
- Node B can support FDD or TDD or both
- RNC is responsible for handover decisions requiring signaling to the UE
- Cell offers FDD or TDD



Radio Network Controller

- Call admission control
  - The RNC calculates the traffic within each cell and decides, if additional transmissions are acceptable or not
- Congestion control
  - The RNC allocates bandwidth to each station in a cyclic fashion and must consider the QoS requirements
- Encryption/Decryption
  - The RNC encrypts all data arriving from the fixed network before transmission over the wireless link (and vice versa)
- ATM switching and multiplexing, protocol conversion
  - The connections between RNCs, node Bs, and the CN are based on ATM. An RNC has to switch the connections to multiplex different data streams.
- Radio bearer setup and release
  - An RNC has to set-up, maintain, and release a logical data connection to a UE

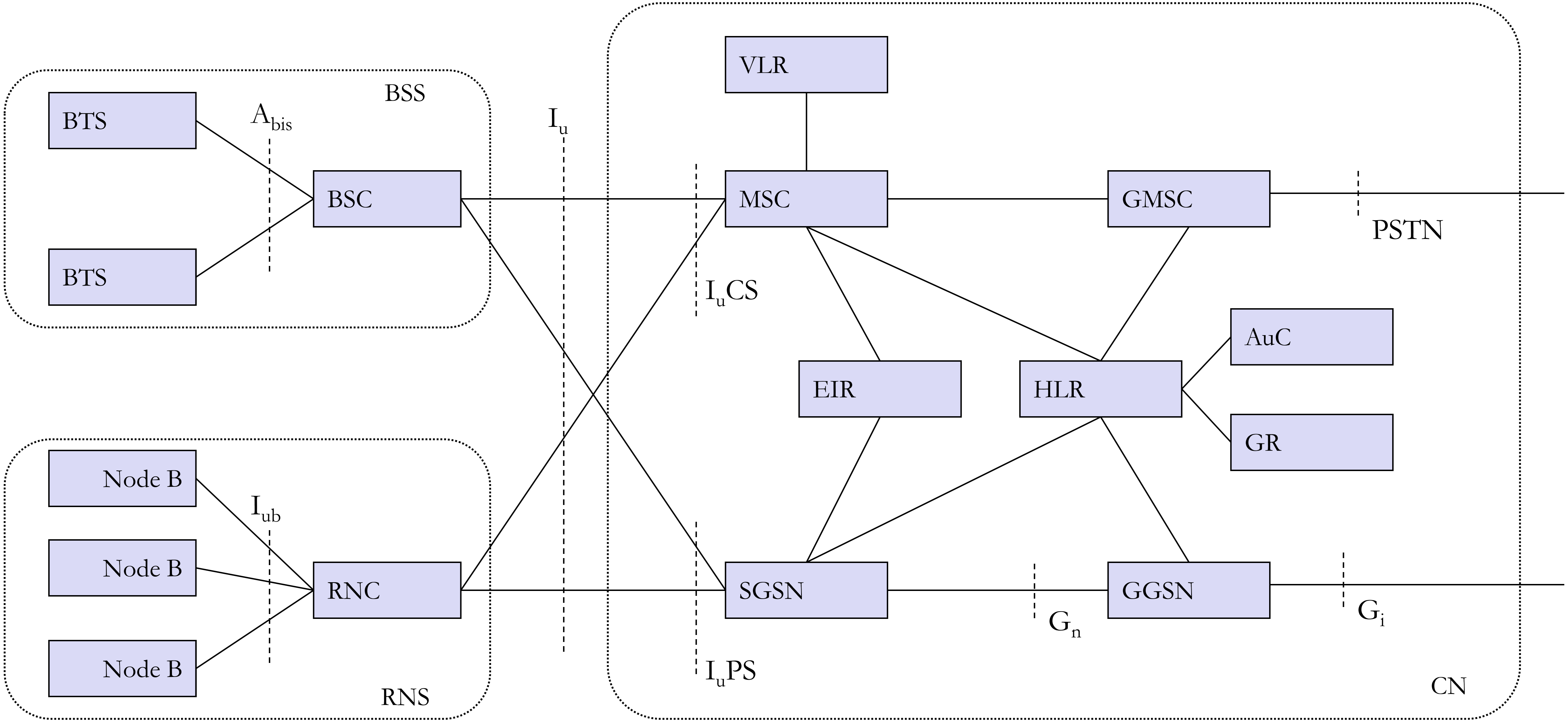
Radio Network Controller

- Code allocation
  - The CDMA codes used by a UE are selected by the RNC
- Power control
  - The RNC only performs a relatively loose power control (the outer loop).
  - This outer loop of power control helps to minimize interference between neighbouring cells or controls the size of a cell
- Handover control and RNS relocation
  - Depending on the signal strengths received by UEs and node Bs, an RNC can decide if another cell would be better suited for a certain connection
- Management
  - The network operator needs a lot of information regarding the current load, current traffic, error states etc. to manage its network

Node B

- Node B connects to one or more antennas creating one or more cells.
- The cells can either use FDD or TDD or both
- An important task of a node B is the inner loop power control to mitigate near-far effects.
- Node B also measures connection qualities and signal strengths
- Node B can even support a special case of handover, a so-called softer handover which takes place between different antennas of the same node B

Core Network Architecture



Core Network Architecture

- The Core Network (CN) and thus the Interface I_u, too, are separated into two logical domains:
- Circuit Switched Domain (CSD)
  - Circuit switched service incl. signaling
  - Resource reservation at connection setup
  - GSM components (MSC, GMSC, VLR)
  - I_uCS
  - Mobile Switching Centre (MSC)
    - Switching CS transactions
  - Visitor Location Register (VLR)
    - Holds a copy of the visiting user's service profile, and the precise info of the UE's location
  - Gateway MSC (GMSC)
    - The switch that connects to external networks
  - Home Location Register (HLR)
    - Stores master copies of users service profiles
    - Stores UE location on the level of MSC/VLR/SGSN
- Packet Switched Domain (PSD)
  - GPRS components (SGSN, GGSN)
  - I_uPS
  - Serving GPRS Support Node (SGSN) (Similar function as MSC/VLR)
  - Gateway GPRS Support Node (GGSN) (Similar function as GMSC)

UMTS Handover

- Hard Handover
- Soft Handover
- Softer Handover

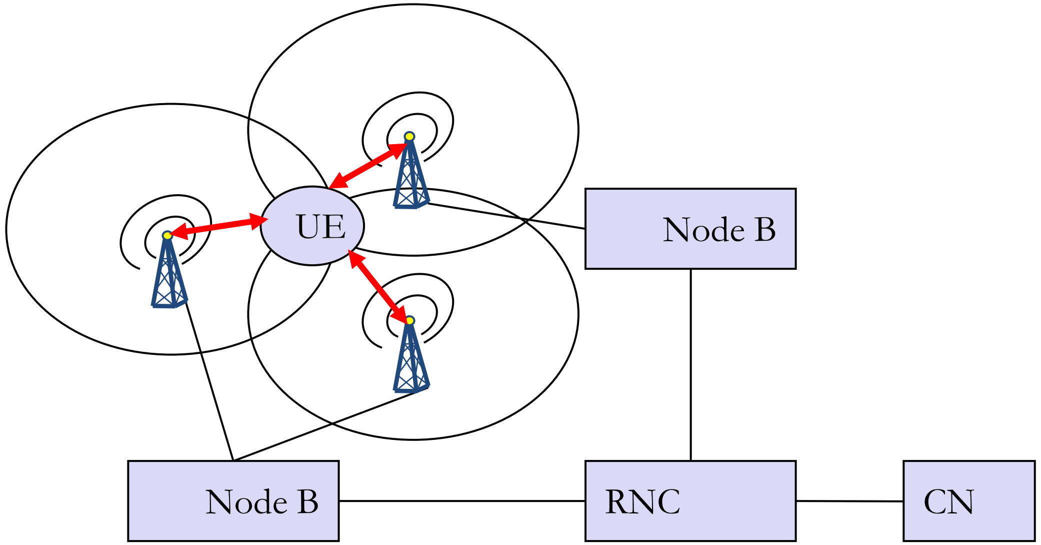
Hard Handover

- All the old radio links in the UE are removed before the new radio links are established.
- Inter Frequency Handover
  - Changing the carrier frequency, is a hard handover
  - Receiving data at different frequencies at the same time requires a more complex receiver
- Inter System Handovers
  - Handovers to and from GSM or other IMT-2000 systems

Soft Handover

- Soft handover means that the radio links are added and removed in a way that the UE always keeps at least one radio link to the UTRAN
- Soft handovers are well known from traditional CDMA networks as they use macro diversity, a basic property of
- CDMA

Support of Mobility: Macro Diversity

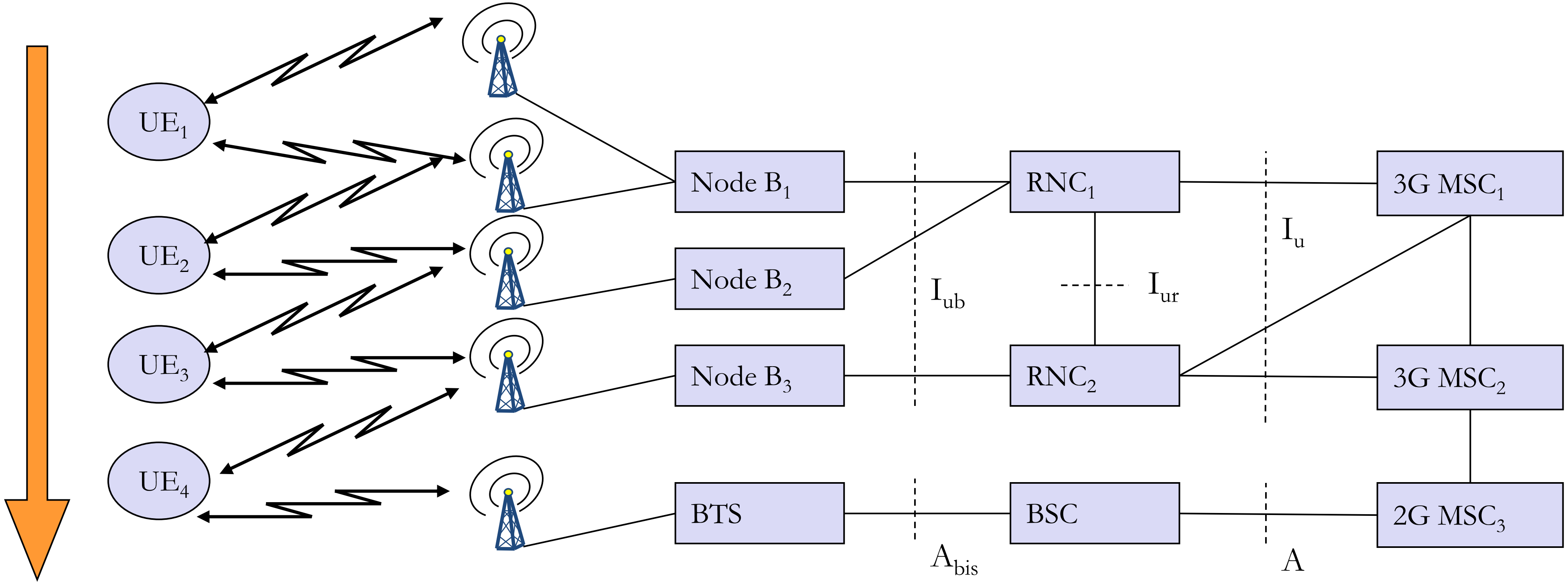


- UE can receive signals from up to three different antennas, which may belong to different node Bs.
- Downlink
  - The RNC splits the data stream and forwards it to the node Bs.
  - The UE combines the received data again.
- Uplink
  - UE simply sends its data which is then received by all node Bs involved.
  - The RNC combines the data streams received from the node Bs.
- The fact that a UE receives data from different antennas at the same time makes a handover soft.
- Moving from one cell to another is a smooth

Softer Handover

- Softer handover is a special case of soft handover where the radio links that are added and removed belong to the same Node B

Handover Types in UMTS



Handover Types in UMTS

- Intra-node B, intra-RNC
  - UE1 moves from one antenna of node B1 to another antenna. This type of handover is called softer handover.
  - In this case node B1 performs combining and splitting of the data streams.
- Inter-node B, intra-RNC:
  - UE2 moves from node B1 to node B2.
  - In this case RNC1 supports the soft handover by combining and splitting data.
- Inter-RNC
  - When UE3 moves from node B2 to node B3 two different types of handover can take place.
  - internal inter-RNC handover and external inter-RNC handover.
- Inter-MSC
  - MSC2 takes over and performs a hard handover of the connection.
- Inter-system
  - UE4 moves from a 3G UMTS network into a 2G GSM network.
  - This is hard handover.

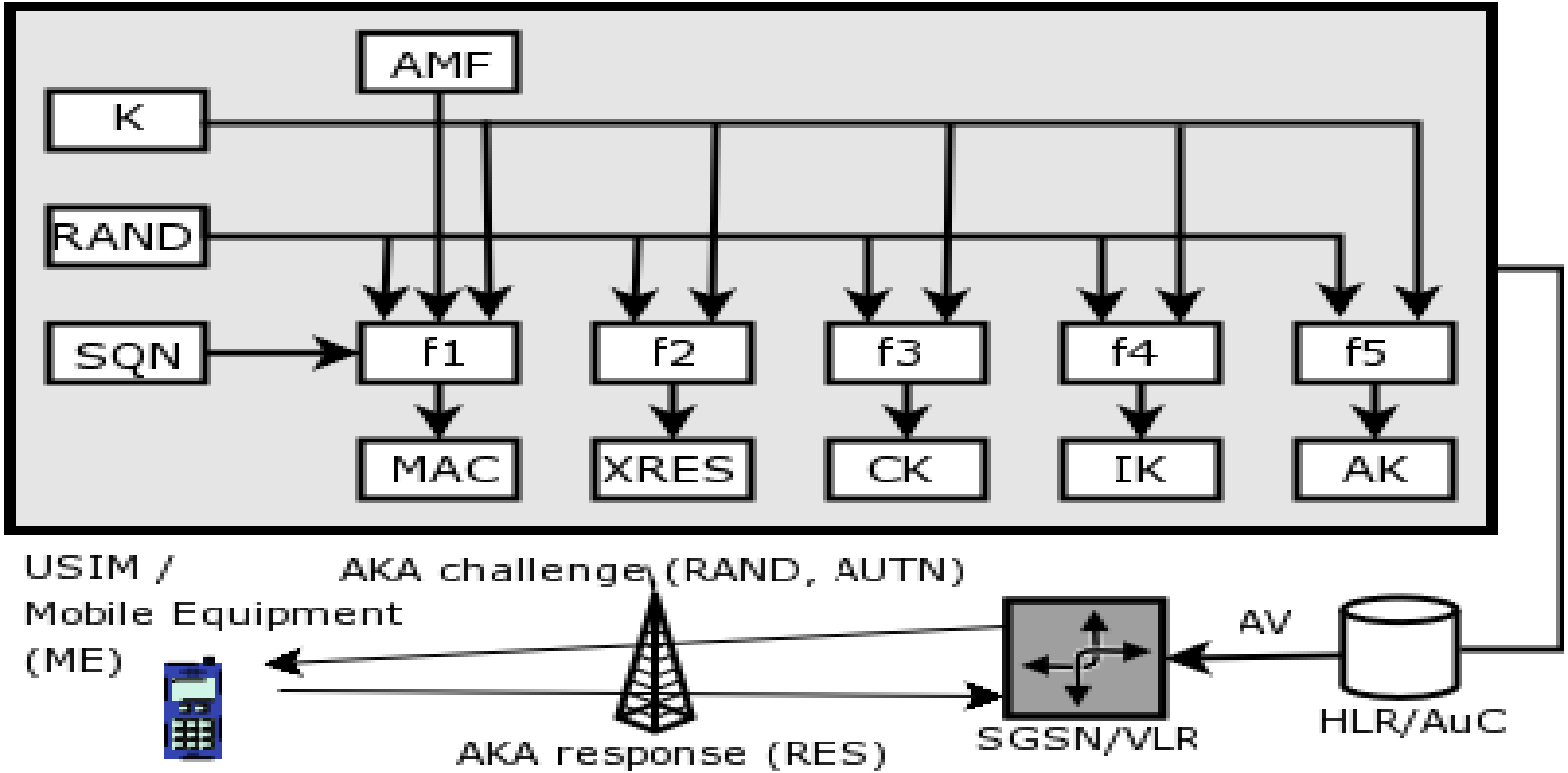
QoS Classes

Traffic class	Conversational class	Streaming class	Interactive class	Background
Fundamental characteristics	Preserve time relation between information entities of the stream Conversational pattern (stringent and low delay)	Preserve time relation between information entities of the stream	Request response pattern Preserve data integrity	Destination is not expecting the data within a certain time Preserve data integrity
Example of the application	Voice, videotelephony, video games	Streaming multimedia	Web browsing, network games	Background download of emails

Security and Authentication

- Security in GSM is weak by our todays standards, mostly broken and only one way (client-to-network auth)
- Authentication in UMTS
  - Basis is a common secret key K, which is only known by the USIM (User Services Identity Module) in the UE and by the HLR/AuC of the provider
  - The VLR or SGSN which should authenticate the user requests from the HLR/AuC 1..n AV(Auth Vectors)
  - Each AV is a 5-tupel consisting of
    - RAND (random challenge) and XRES (expected response) for the user authentication
    - CK (cipher key) for protection of confidentiality, IK (integrity key) for protection of integrity, AUTN (auth token) for network authentication

Security and Authentication



Security and Authentication

  - RAND and AUTN are sent to the UE/USIM, which checks AUTN and computes the response RES to the challenge RAND
  - RES is sent to the VLR/SGSN which compares it to XRES
- Integrity and confidentiality
  - By request of MSC/VLR or SGSN the communication can be encrypted with CK or IK between UE and RNC
  - Encryption takes place on the RLC layer and prevents forgery of data and encryption

Summary

- From 2G to 3G
- Architecture of UMTS
  - UE
  - UTRAN
  - CN
- UMTS Handover
- UMTS Security

Test your understanding

- Any idea about Virtual Home Environment (VHE)??

- What type of handover will happen when a mobile handset switch between 2G and 3G?

References

Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.

Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.