Mobile/Cellular Networks

School of Informatics
Institute for Computing Systems Architecture

Overview

- Mobile phone subscriptions worldwide reached almost 7 billion at the end of 2014 ➔ 96% penetration rate [ITU ICT Facts and Figures, 2014]
  - More than fixed Internet hosts and telephone lines combined
  - In the UK, more than 83 million mobile phone users ➔ 1.3 mobile phones per person!
- Originally intended for mobile voice communication
- But increasingly data oriented to keep up with the demand for mobile Internet use from smartphones, tablets and USB mobile broadband dongles
  - Note that texting (SMS) is also a form of data communication
- Use on the move and everywhere ➔ need blanket wide area coverage, even across country borders
  - Blanket coverage especially crucial to support emergency calls

Overview (Contd.)

- Also known as:
  - Mobile (broadband) networks
  - Mobile cellular networks
  - Public land mobile network (PLMN)

- We will study:
  - Cellular concept
  - Historical evolution of cellular technologies
  - Take a closer look at 2G/3G/4G cellular systems based on 3GPP standards

Cellular Concept
Motivation: Efficient Use of Scarce Spectrum

- Design approach for early mobile radio systems: a single, high-powered transmitter with an antenna mounted on a tall tower to cover a large service area (e.g., city)
- Similar to over-the-air radio and television broadcasting
- Works well from a coverage perspective
- But system capacity (e.g., number of simultaneous mobile users or voice calls supported) limited by available spectrum, which is scarce and tightly regulated
- E.g., Bell mobile system in New York City in the 1970s could only support a max. of 12 simultaneous calls over a thousand square miles area

Cellular Concept

- Replace a high power transmitter with many lower power transmitters, each covering only small portion of the service area called a *cell*
- Channel allocation and *frequency reuse*:
  - Each transmitter (base station) is allocated a portion of the available spectrum, specifically a subset of channels from the total number of channels available
  - Neighbouring base stations assigned different sets of channels to minimize mutual interference
  - Base stations that are further away can reuse the same set of channels, exploiting signal power falloff with distance

Cellular System Capacity

- Let S be the total number of channels available
- Each cell allocated a subset of k $(k < S)$ channels
- If S channels evenly distributed among N neighbouring cells, collectively called a **cluster**:

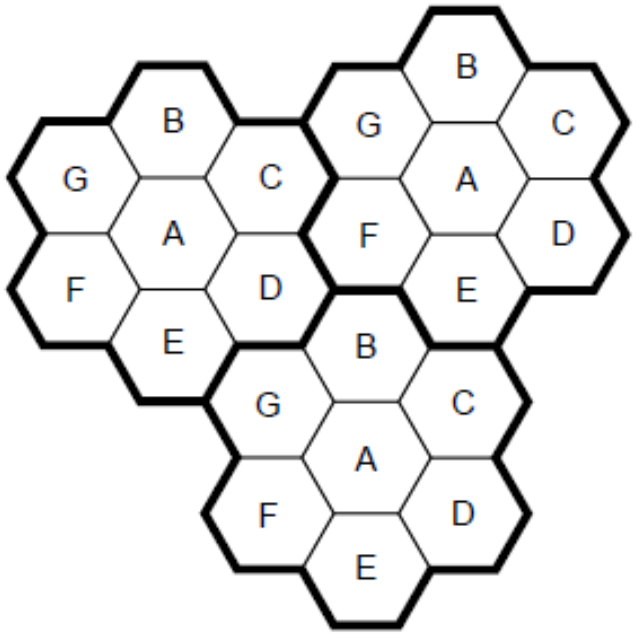
  $S = k \times N$

- **Frequency reuse factor**: N
- If a cluster is replicated M times in the system then system capacity, C, can be measured as:

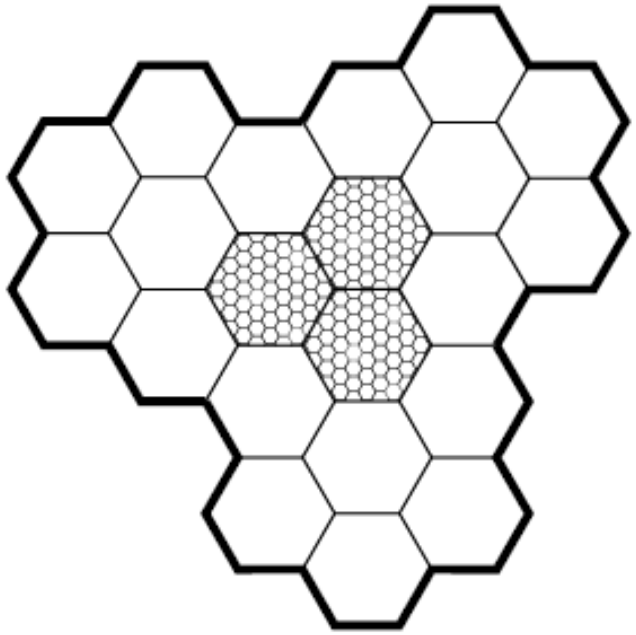
  $C = M \times k \times N = M \times S$

- The parameters M and N allow the system designer control over the system capacity even if available spectrum is fixed and limited
- Increase M to increase C, by:
  - Reducing cell size (e.g., macrocells ➔ microcells)

Illustrating the Impact of Cellular Frequency Reuse and Cell Size on System Capacity

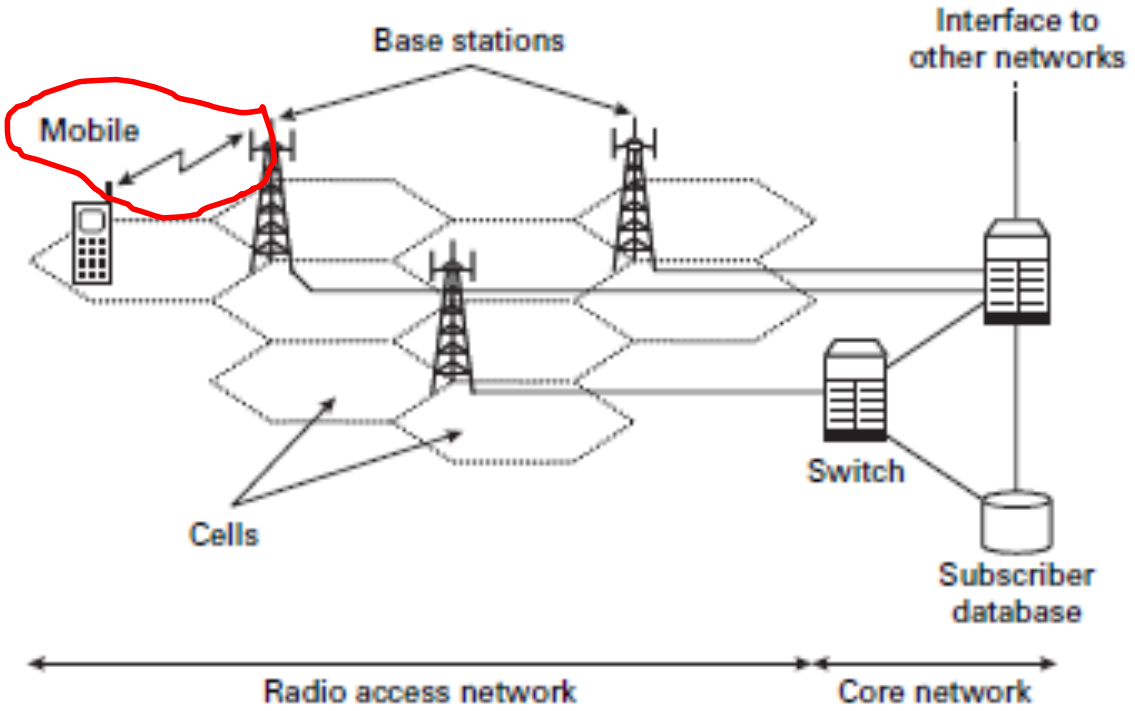


Cellular frequency reuse pattern: cell cluster outlined in **bold** is replicated over the coverage area



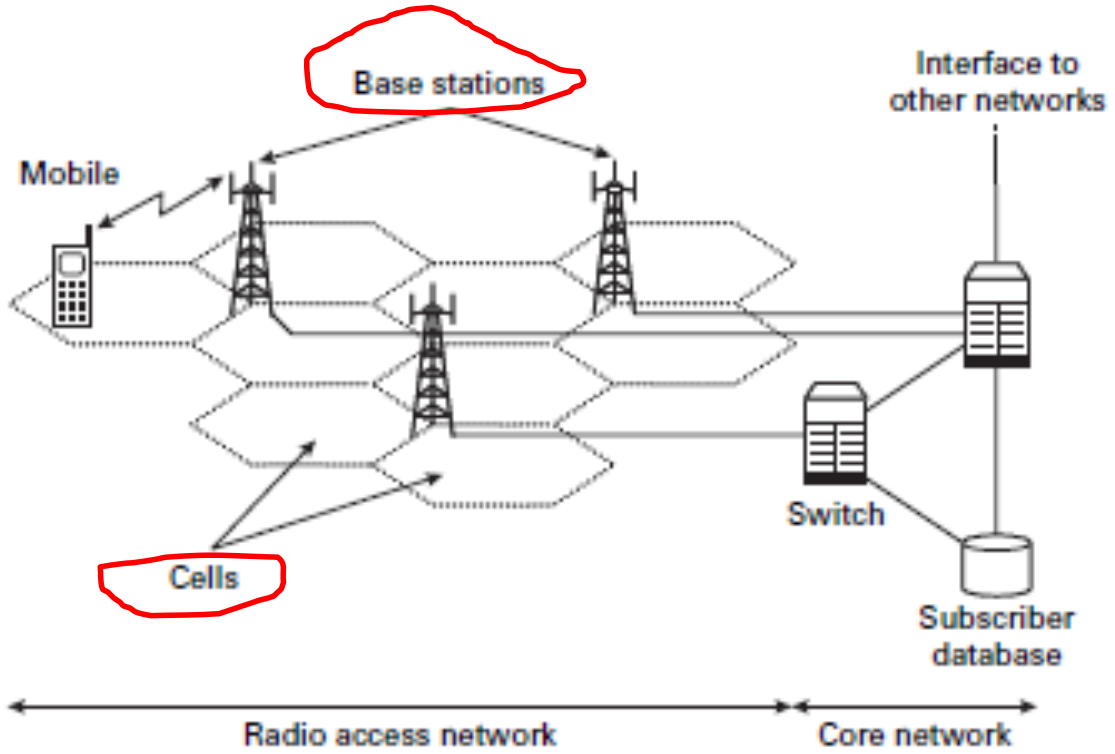
Smaller cells for increased system capacity

A Simplified Cellular Network Architecture & Terminology



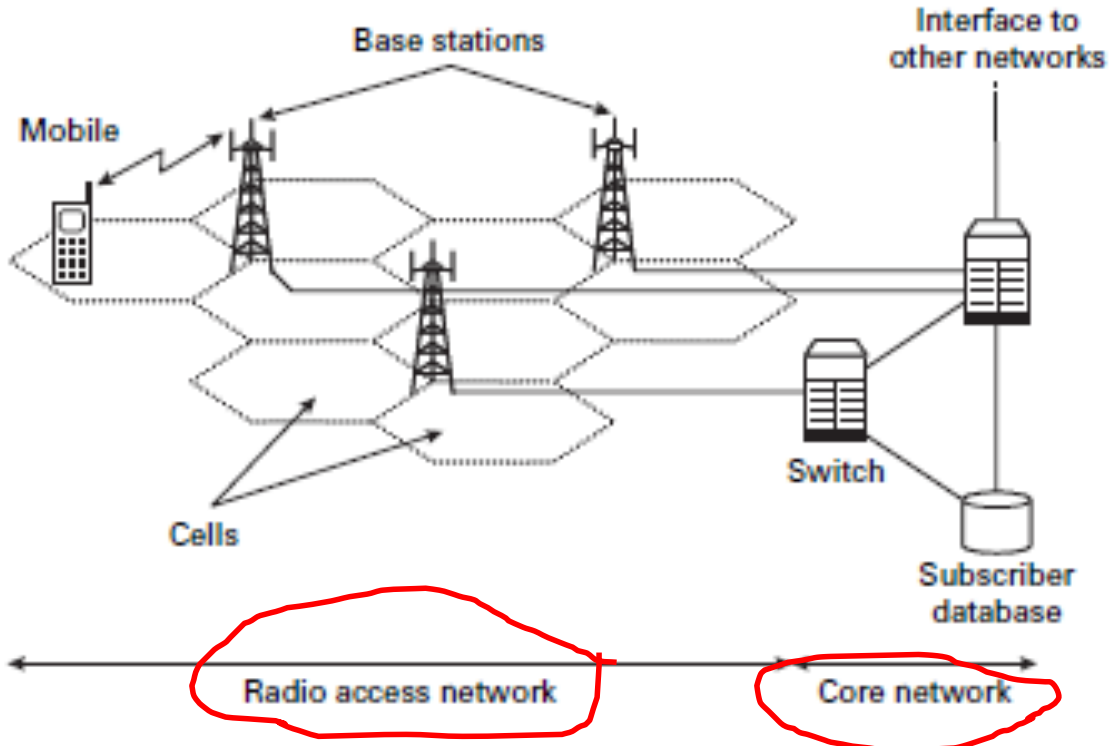
- **Mobile phone** also known as: **mobile**, **cell phone**, **user equipment (UE)** from UMTS (a third-generation cellular technology standard) onwards
- **Air interface** or **radio interface**
  - **Downlink (DL)** or **forward link**: from base station to mobile
  - **Uplink (UL)** or **reverse link**: from mobile to base station

A Simplified Cellular Network Architecture & Terminology



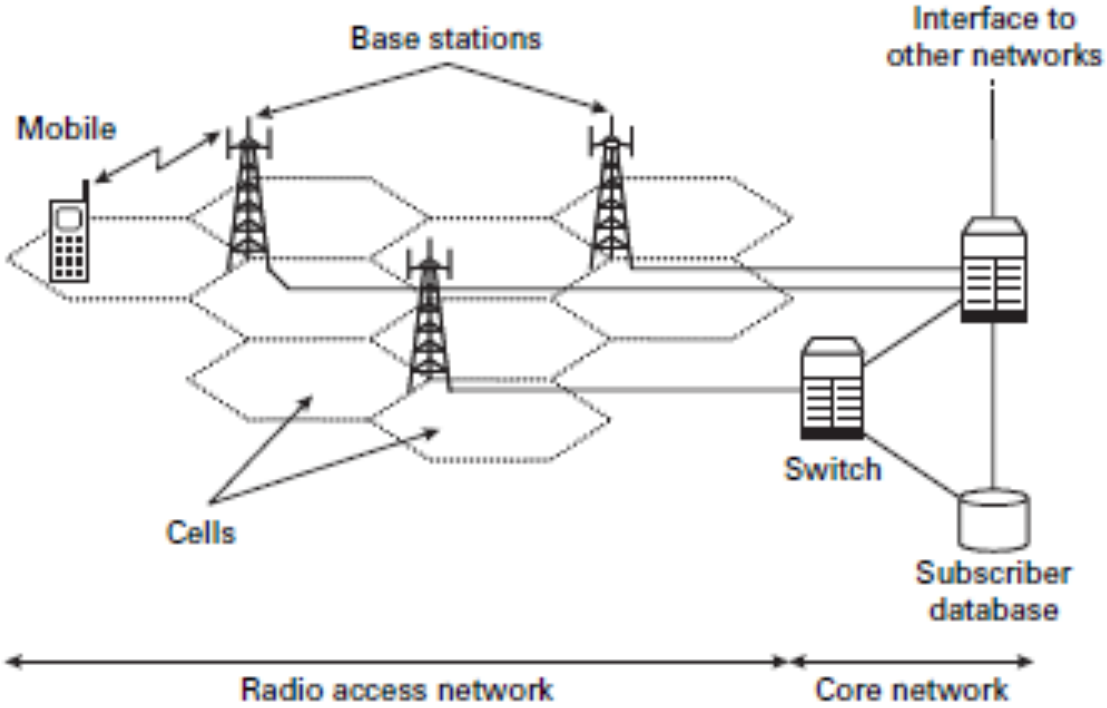
- **Base station**
  - Typically located at corner of a cell and area around it divided into multiple sectors, each served by a different sector antenna
- Cells of different sizes and overlapping cells:
  - **Macrocells** (coverage up to few kms)
  - **Microcells** (up to few hundreds of metres)
  - **Picocells** (up to few tens of metres)
  - **Femtocells** (cover a few metres across such as a home)

A Simplified Cellular Network Architecture & Terminology



- **Radio Access Network (RAN):** the access part of the cellular network that consists of base stations and controllers, and provides connectivity between mobiles and core network
- **Core Network:** interconnects RANs and also connects them to external networks, including telephone network and Internet

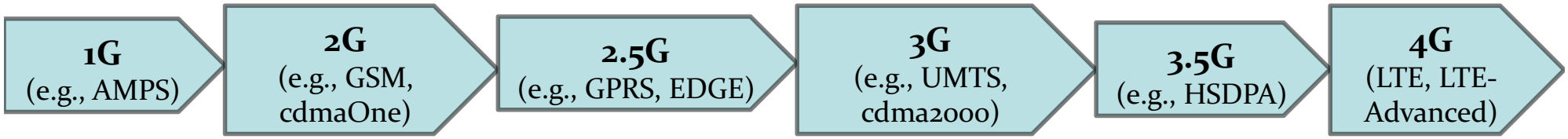
A Simplified Cellular Network Architecture & Terminology



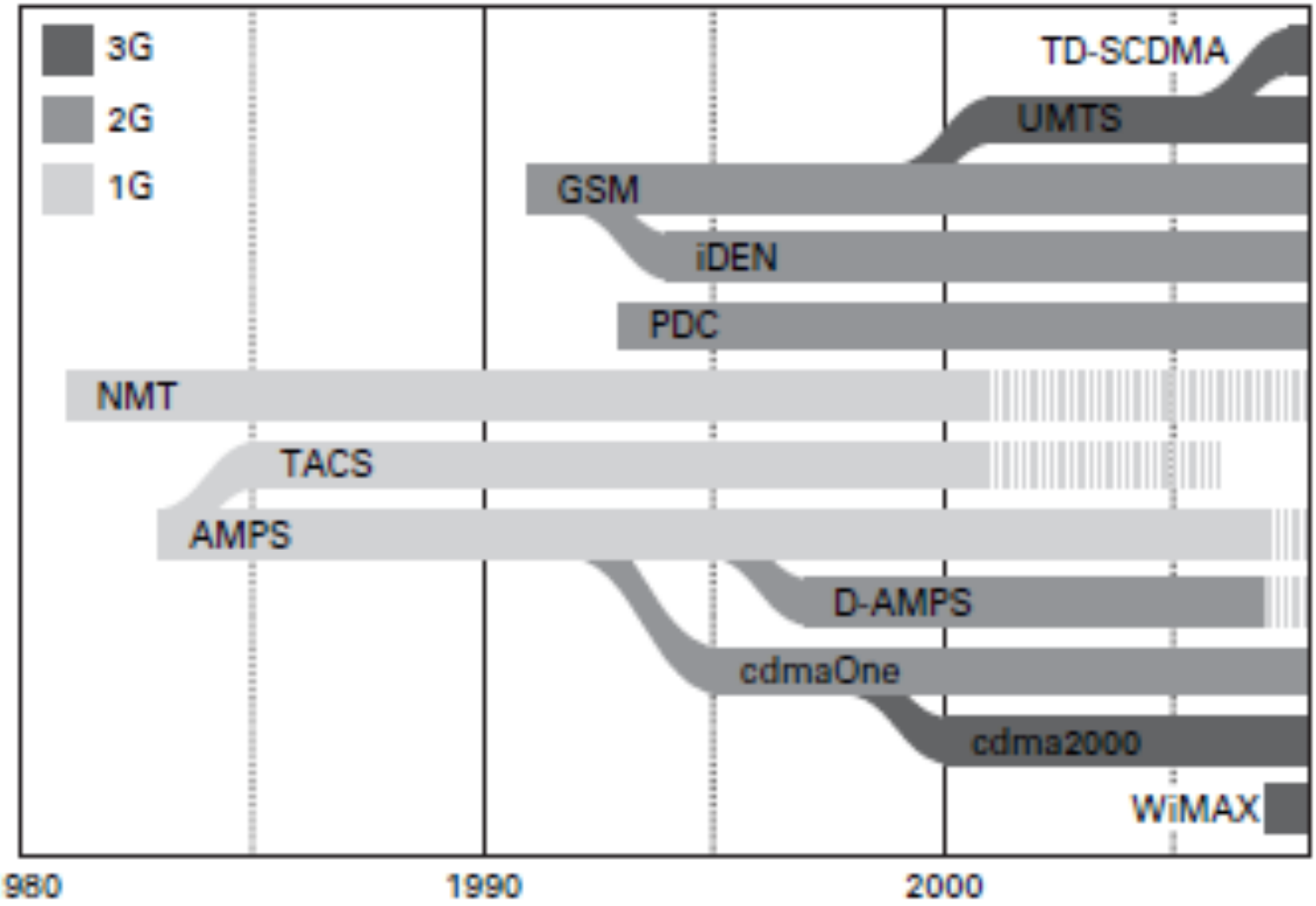
- **Handover/Handoff**: the process of switching connectivity for a mobile from one cell to another (e.g., while moving); can be soft or hard
- **Home network:** the cellular network of a mobile's operator
- **Visited network:** a cellular network different from that of a mobile's operator
- **Roaming:** when a mobile connects via a visited network

Evolution of Cellular Network Technologies/Standards

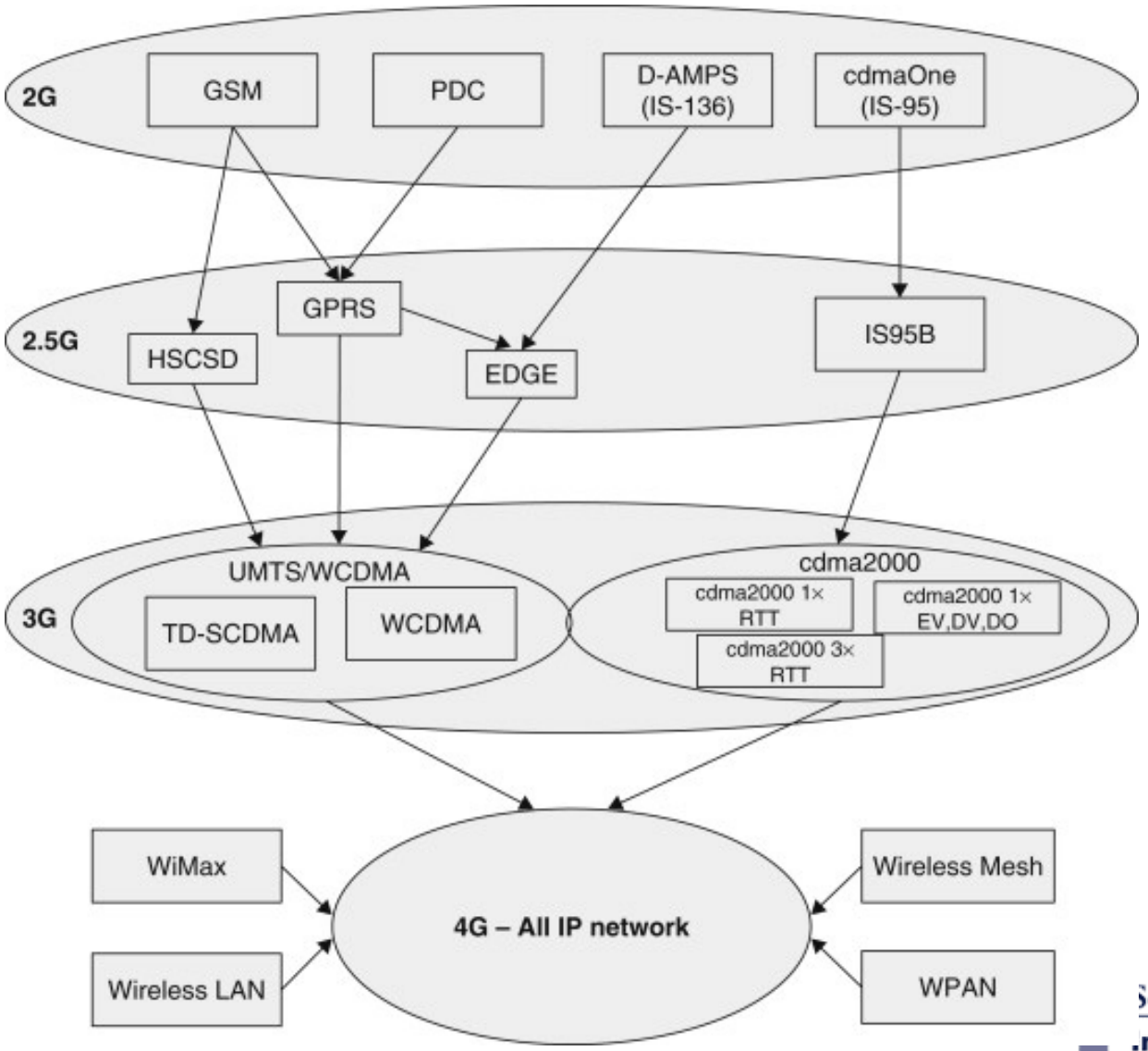
- As different generations: first generation – 1G, second generation – 2G, ..
  - 1G: analogue, voice only, based on FDMA
  - 2G: digital, initially designed for voice but later extended to support data (2.5G)
  - 3G: digital voice and data with greater emphasis on data and higher data rates
  - 4G: same as 3G but focus on even higher data rates + all IP core



Another View of the Technology Evolution



Yet Another View of the Evolution



Our Focus

- Discuss AMPS (1G) as a historical backdrop for modern cellular systems

- Give detailed overview of three key cellular standards that are widely deployed or being deployed:
  - 2G: Global System for Mobile communications (GSM)
  - 3G: Universal Mobile Telecommunications System (UMTS)
  - 4G: Long-Term Evolution (LTE)

Frequency vs. Time Division Duplex

- Modes to ensure uplink and downlink transmissions do not interfere with each other
- Frequency Division Duplex (FDD)
  - Each base station and mobile pair assigned a pair of frequencies for simultaneous uplink and downlink transmissions
  - More common as it is easier to implement
  - Do not require accurate time synchronization
  - Less prone to interference due to frequency separation
- Time Division Duplex (TDD)
  - Both base station and mobile transmit using the same frequency but at different times ➔ more efficient
  - Also more flexible: if more traffic in downlink than uplink then more time for downlink

Advanced Mobile Phone System (AMPS)

- Invented by Bell Labs and first installed in the US in 1982
- Also used elsewhere:
  - in England as TACS
  - in Japan as MCS-L1
- Formally retired in 2008
- First system to (explicitly) implement cellular design and frequency reuse
- Analogue system, designed primarily for mobile voice communication
- Large sized cells (10-20Km across) relative to later digital systems
- But smaller compared to older systems (e.g., IMTS from 1960s)
  - From 1 100Km cell and 1 call per frequency in IMTS to 100 10Km cells and 10-15 simultaneous calls per frequency in distant cells in AMPS
    - At least an order of magnitude improvement in system capacity
    - Lower power requirement ➔ smaller and cheaper transmitters and handsets

AMPS Architecture

- Base station (a dumb radio relay to mobile) at the centre of each cell
- Mobile Telephone Switching Office (MTSO) for several neighbouring base stations
  - Manages channel assignment of base stations
- MTSOs interconnected with each other and to PSTN using a circuit-switched network
- Handoffs triggered and handled solely by system without mobile involvement, take about 300ms

AMPS Channels

- Uses FDMA/FDD
- 832 full-duplex channels, each a pair of 30KHz wide simplex channels
  - Downlink channels in 869-894MHz
  - Uplink channels in 824-849MHz
  - Four categories:
    - **Control channels** (unidirectional from base to mobile) for system management (21 channels set aside globally for use in every cell): information sent in digital form, multiple times with error-correcting code
    - **Access channels** (bidirectional) for call setup and channel assignment
    - **Paging channels** (unidirectional from base to mobile) to alert mobile users about incoming calls
    - **Data channels** (bidirectional) for voice, fax and data (~45 per cell)

AMPS Call Management

- Each mobile phone has:
  - 32-bit serial number
  - 34-bit phone number (10-bits for 3 digit area code and 24 bits for 7-digit subscriber number)
- Power-on and registration procedure:
  - Scans all 21 control channels to find the one with the strongest signal
  - Broadcasts serial and phone numbers
  - Base station on receiving this info informs MTSO
  - MTSO notes mobile's presence and also informs mobile's home MTSO
- During normal/idle operation, each mobile:
  - Re-registers every 15 mins
  - Continuously listens on the paging channel for messages to it

AMPS Call Management (contd.)

- Making a call:
  - Broadcasts its identity and number to be called on access channel, retry if collision
  - Base station on receiving this info informs its MTSO
  - MTSO finds an idle data channel and sent to mobile over the control channel
  - Mobile switches to the given data channel and waits for callee to pick up phone
- Receiving a call:
  - Call directed by system to visiting MTSO in whose coverage area mobile is currently present
  - Visiting MTSO informs mobile of incoming call by broadcasting on the paging channel
  - Mobile responds to visiting MTSO on the access channel
  - Visiting MTSO asks mobile over the control channel to take the call on a specified data channel, which it does

Second Generation (2G) Cellular Wireless Technologies

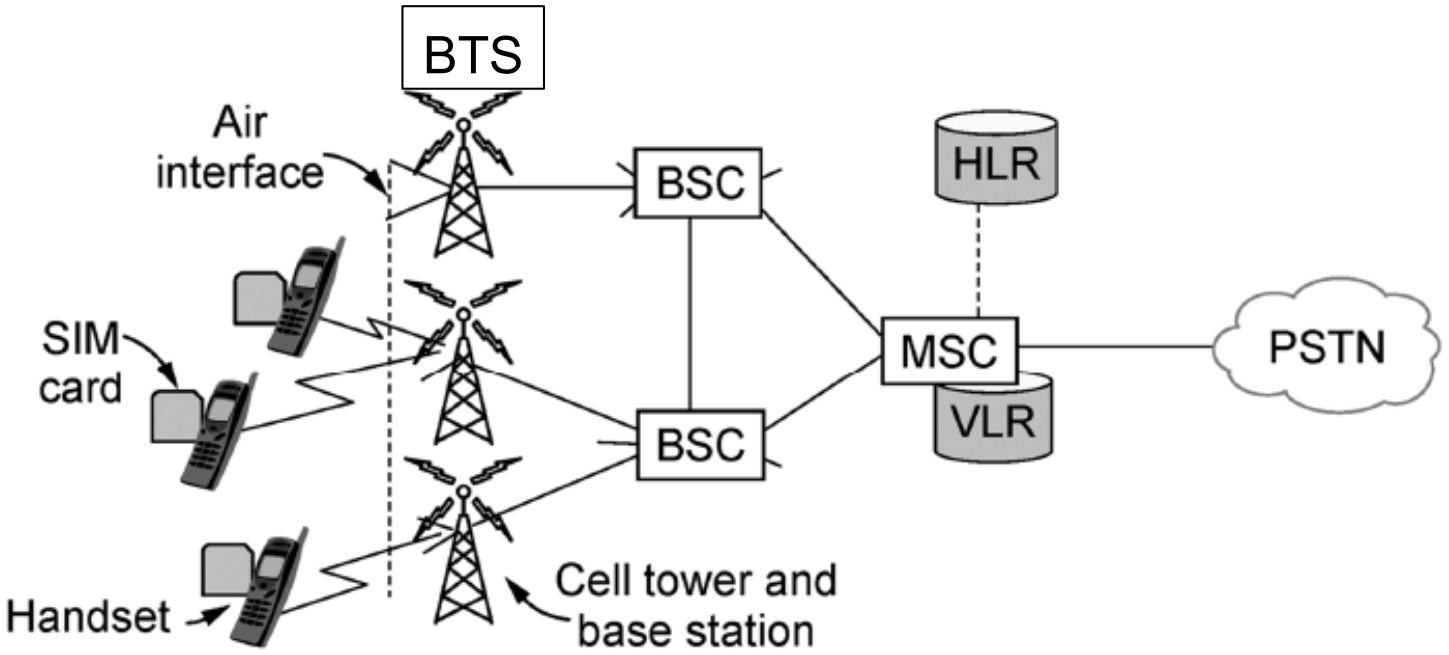
- Major difference from 1G: from analogue to digital
  - Allows compression and encryption ➔ Increased capacity and security
  - Enables inherently digital services (text messaging, email, web access, etc.)
- Sometimes referred to under the name "Personal Communications Services (PCS)"
- Three prominent standards:
  - Digital AMPS (D-AMPS) standardized initially as IS-54 and then as IS-136
    - Originated in US
    - Uses a combination of TDMA and FDMA: TDMA within each full-duplex frequency channel
    - Coexists with AMPS
  - Global System for Mobile Communications (GSM)
    - Originated in Europe, first installed in 1991
    - The dominant 2G technology/standard
    - Like D-AMPS, uses a mix of TDMA and FDMA
  - cdmaOne (IS-95 standard)
    - Based on CDMA

GSM Overview

- Retain several key ideas from 1G systems: cellular design, frequency use and mobility support via handoffs
- But a digital system
- Combined FDM/TDM: 200 KHz channels, each supporting 8 TDM calls
- Besides voice, provides basic data services (e.g., SMS)
- Mobile now split into two parts:
  1. Handset
  2. SIM (Subscriber Identity Module) card
     - *Removable* chip with subscriber and account info
     - Needed to activate handset
     - Contains security keys

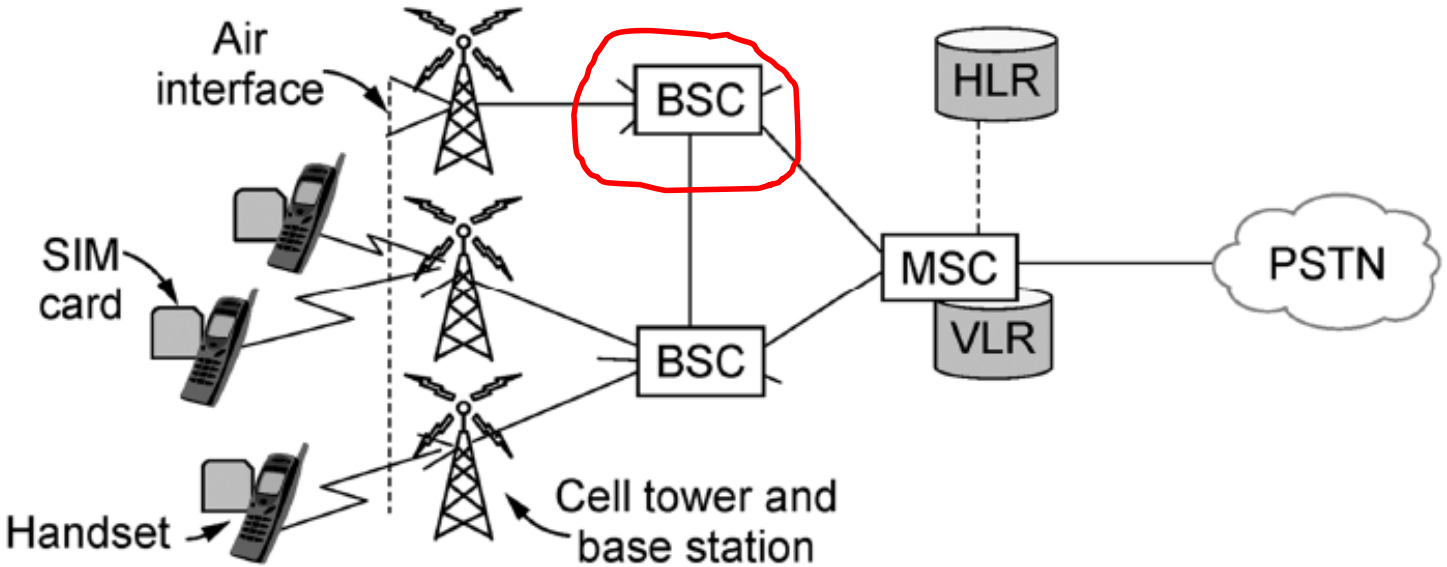
GSM Architecture

- Elements of GSM architecture:
  - Mobile subscribers
  - BTS (base transceiver station)
  - BSC (base station controller)
  - MSC (mobile switching centre)



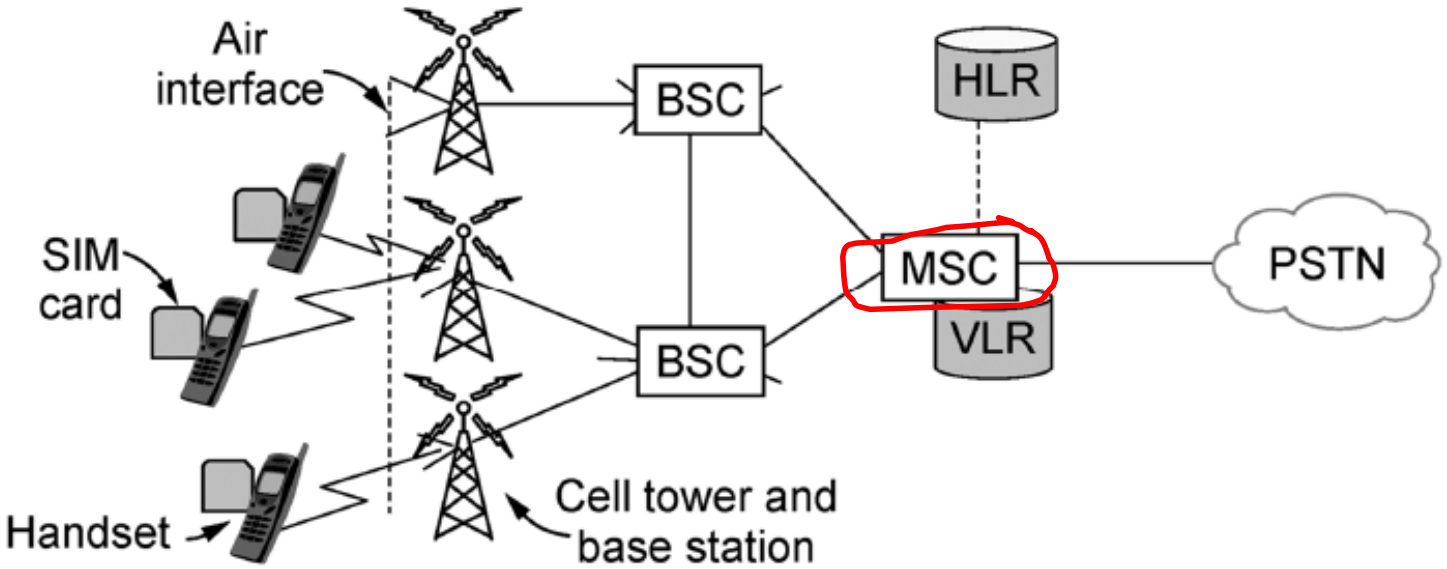
GSM Architecture (contd.)

- Base Station Controller (BSC)
  - Serves several tens of BTSs
  - BSC and BTSs it serves together make up a **BSS (base station system)**
  - Manages radio resources of cells (e.g., allocates BTS radio channels to mobile subscribers)
  - Performs paging (finding the cell where the mobile user is currently present)
  - Controls handoffs among BTSs within the same BSS



GSM Architecture (contd.)

- Mobile Switching Centre (MSC)
  - Plays the key role in user authorization, call establishment/teardown, handoffs and accounting
    - Facilitates handoffs across different BSCs
  - Manages subscriber database and up-to-date location of mobiles via **Home Location Register (HLR)** and **Visitor Location Register (VLR)**
  - Gateway MSC connects to the larger public telephone network (PSTN)
  - One MSC for every 5 BSCs and ~200K subscribers

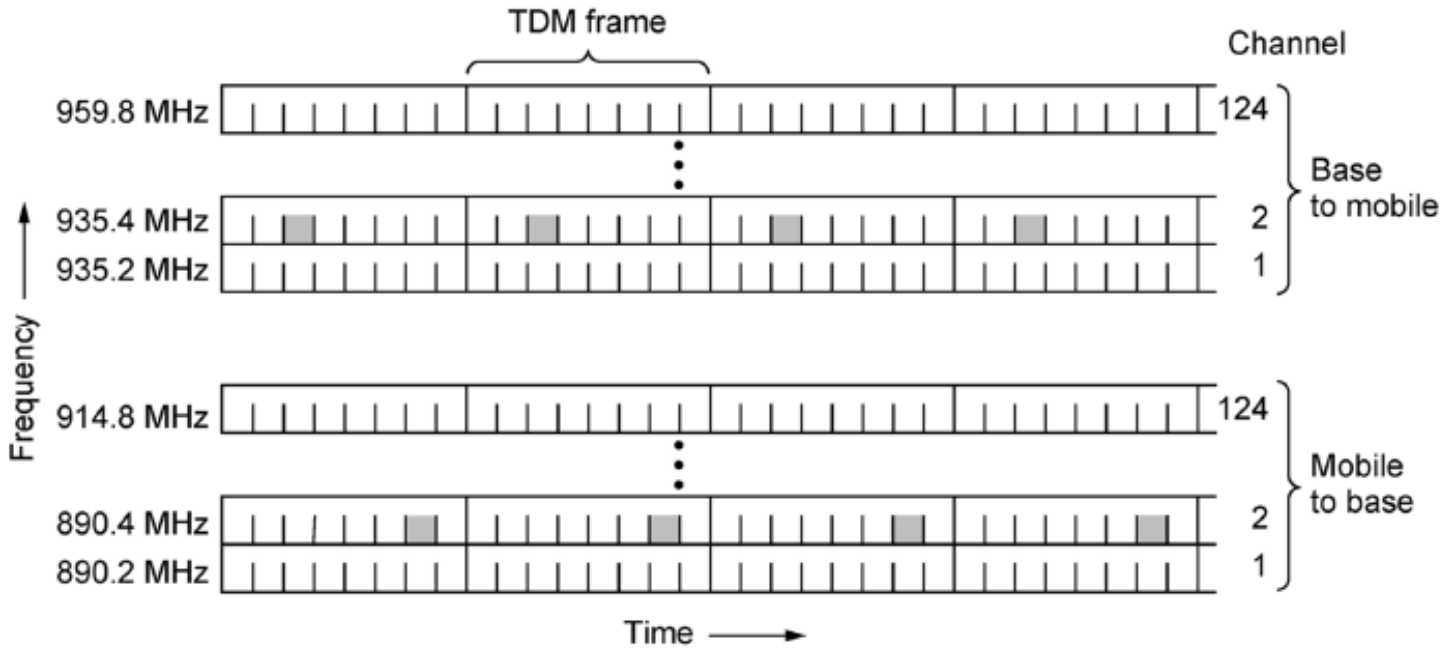


GSM Channels

- Works over several frequency bands (e.g., 900MHz, 1800MHz, 1900MHz) depending on country and operator
- FDD like AMPS
- GSM frequency allocation in UK (http://maps.mobileworldlive.com/network.php?cid=39&cname=United%20Kingdom)
  - In two bands: 900MHz and 1800MHz
    - 900MHz band – downlink: 925-960MHz; uplink: 880-915MHz
    - 1800MHz band – downlink: 1805-1880MHz; uplink: 1710-1785MHz
  - O2/Telefonica: 900MHz and 1800MHz
  - Vodafone: 900MHz and 1800MHz
  - Everything Everywhere (Orange): 1800MHz
  - Everything Everywhere (T-Mobile): 1800MHz
  - PMN, another GSM licensee : 1800MHz
- More spectrum compared to AMPS, used in the form of wider channels to support larger number of users (200KHz vs. 30KHz)

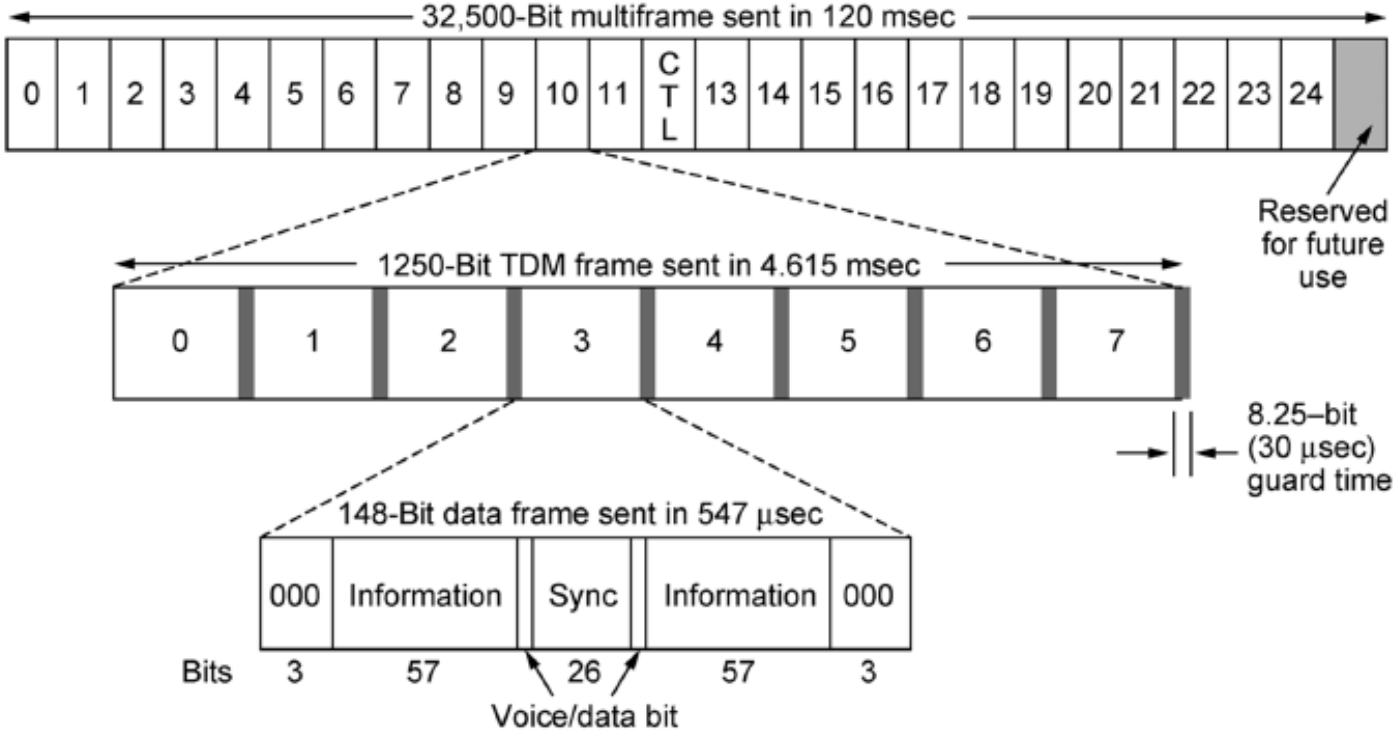
GSM Air Interface

- Each full-duplex channel divided into 8 time slots to accommodate 8 active base-mobile connections (the TDMA part)
  - GSM radios half-duplex, so different slots used for downlink and uplink part of the connection



School of Informatics
Institute for Computing Systems Architecture

GSM Framing Structure



- 1250 bits over 4.615ms across 8 users ➔ gross data rate of ~270.8Kbps
- After discounting overhead: 24.7Kbps per user before error correction and **13Kbps** after error correction
- GSM encodes speech at 13kbps and 12.2 kbps

GSM Framing Structure (contd.)

- There is also a 51 slot multiframe with some slots used for control channels, e.g.,
  - *Broadcast control channel* over downlink with continuous broadcast of base station identity and channel status; also used by mobiles to monitor signal strength from base station
  - *Dedicated control channel* to keep VLR up-to-date via location updating, registration and call setup
  - *Common control channel* divided further into *three logical subchannels*
    - *Paging channel*: used by base stations to announce incoming calls to mobiles
    - *Random access channel*: for mobile to request a slot on dedicated control channel
    - *Access grant channel*: used to inform mobile of assigned slot in response to request on random access channel
- Handoff procedure different from AMPS
  - *Mobile Assisted HandOff (MAHO)*: each mobile uses idle slots to measure signal quality to nearby base stations and informs BSC to help it in making handoff decision

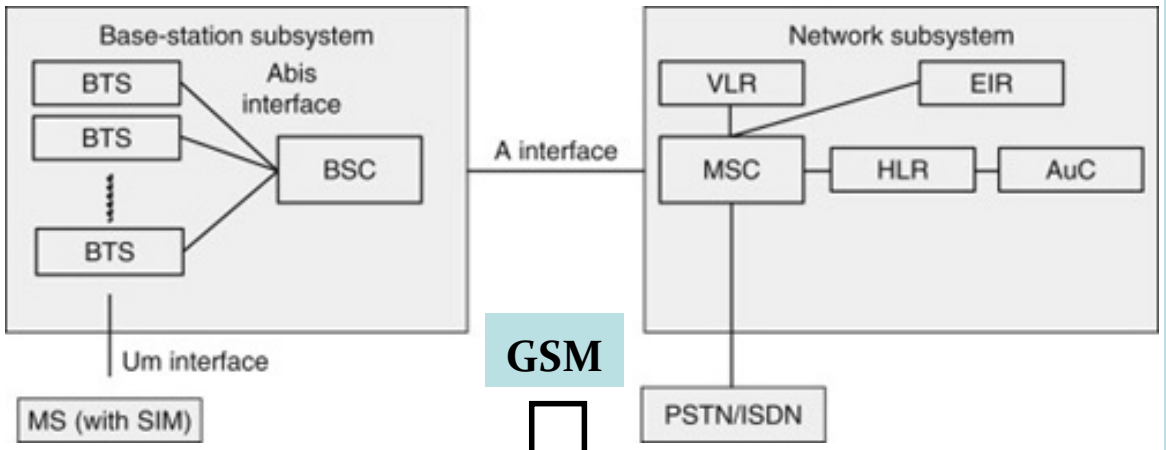
GSM Evolution ➔ HSCSD, GPRS and EDGE

- Examples of 2.5G cellular wireless technologies
- Aimed at improving data rates from ~10Kbps with GSM to better support data services (e.g., e-mail, web browsing)
- High-Speed Circuit-Switched Data (HSCSD) is the first step in this direction towards higher data rates with GSM
- New features with HSCSD:
  - 14.4 Kbps data rate per time slot by reducing error correction overhead
  - Higher data rates up to **57.6 Kbps** by using multiple 14.4 Kbps time slots

General Packet Radio Service (GPRS)

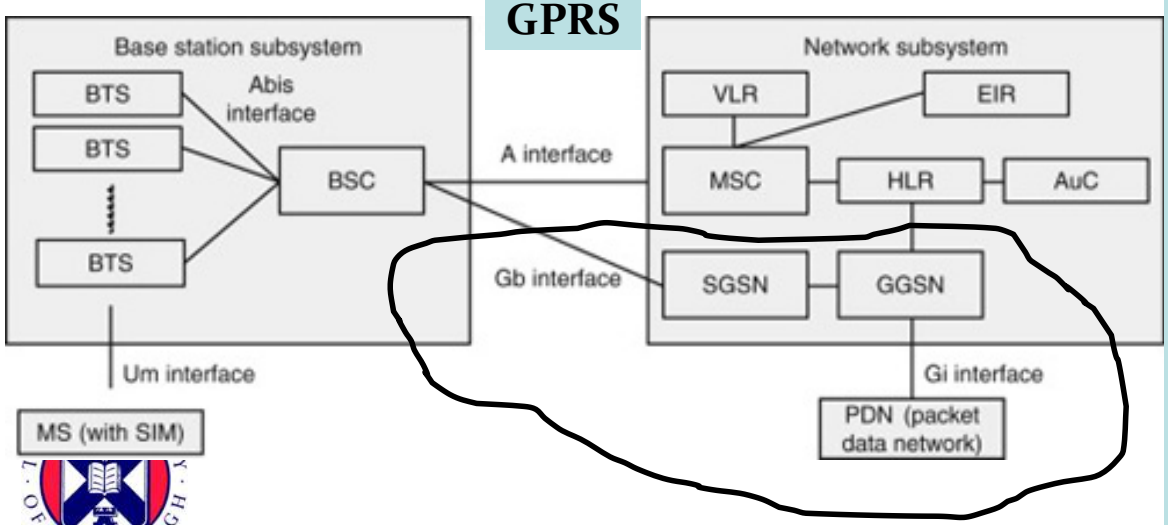
- Unlike HSCSD, GPRS takes a packet-oriented approach to data transmission
- In GPRS, data transmissions are supported on-demand without prior connection establishment and reservation of channels
- Like with HSCSD, a data transfer operation can use multiple time slots in a 8-slot TDM frame
  - Number of time slots available for data transmission limited by slots reserved for voice communication as GPRS needs to coexist with voice services
- Introduced 4 bit-rates (ranging from 9.05Kbps to 21.4 Kbps per time slot), all with GMSK modulation but using 4 different coding rates
- Maximum data rate supported is **171.2Kbps** but expected data rate is typically around 115Kbps

GPRS Architecture



GSM

GPRS



- Two new components:
  1. Serving GPRS support node (SGSN)
  2. Gateway GPRS support node (GGSN)
- SGSN and GGSN are packet-switched counterparts of MSC and GMSC
  - GGSN does NAT, and enables communication between GPRS mobile and external PDN (e.g., Internet) via SGSN over GPRS Tunnelling Protocol (GTP)
  - Also does authentication and accounting
- Mobile stations need GPRS terminal functionality, and BTSs need a software upgrade
- Packet control unit (PCU) device in the BSC to separate/multiplex circuit-switched and packet-switched traffic

Enhanced Data rates for Global Evolution (EDGE)

- GPRS enhancement to support data rates up to **384Kbps**
- Via introduction of a new modulation scheme 8-PSK that allows 3 data bits per symbol over the air interface as opposed to 1 bit per symbol with GMSK
- Features 9 different modulation and coding schemes (MCSs) in all, each supporting different bit-rates per time slot
  - Higher bit-rates via 8-PSK modulation whereas lower bit-rates MCSs use GMSK modulation
  - Can automatically switch between them to optimise higher data rate or reliability based on measured channel quality (SNR)

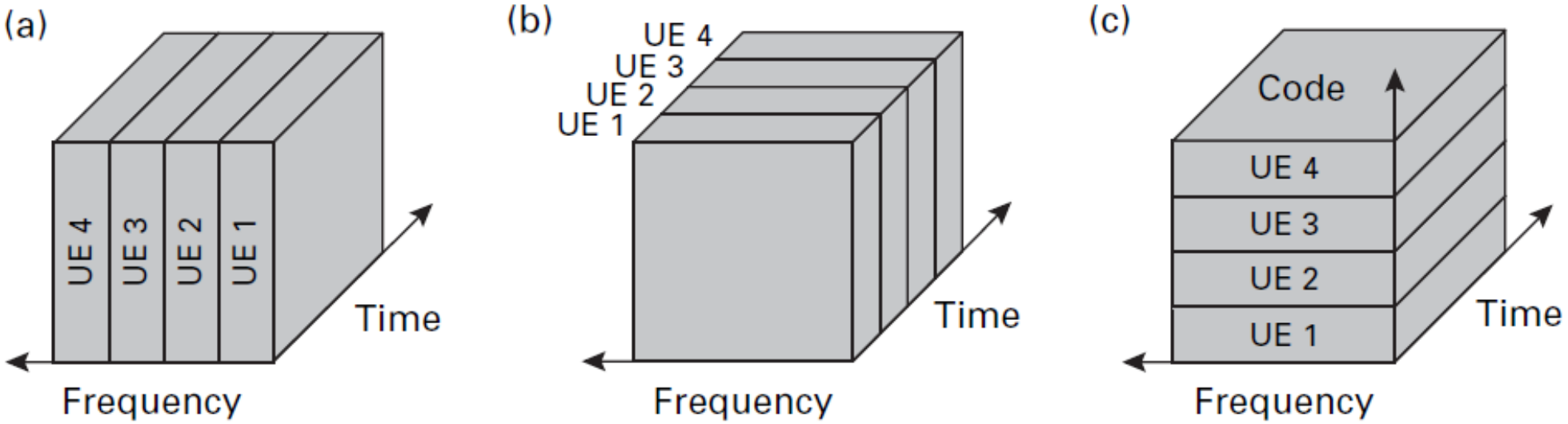
3G Cellular Wireless Technologies
Overview

- Still digital like 2G but higher data rates through changes to the air interface, aimed at supporting advanced data-oriented services (e.g., Internet access)
  - To support growing mobile data traffic which was anticipated to exceed voice traffic; in fact, it did in 2010
  - Cater to "converged" mobile devices, e.g., likes of iPhones
- In 1997, ITU set out blueprint under the name "International Mobile Telecommunications 2000 (IMT-2000)"
  - For standardization of single worldwide third generation cellular technology by 2000
  - For use by a single type of device in contrast to 2G case (GSM vs. CDMA)

3G Cellular Wireless Technologies
Overview (contd.)

- IMT-2000 requirements
  - Provide ubiquitous and always-on access
  - Support diverse services with QoS guarantees: voice, messaging, multimedia, Internet access, …
  - Target data rates: >= 2Mbps for stationary/indoor users, >= 384Kbps for walking users; >144Kbps in a moving vehicle
- Several proposals selected of which two are of primary interest, both based on *CDMA*:
  - **Universal Mobile Telecommunications System (UMTS) aka Wideband CDMA (WCDMA)**
    - From EU (Ericsson et al.), successor to GSM
    - Uses **5MHz** channels
  - **CDMA2000**
    - From US (Qualcomm), successor to cdmaOne
    - Uses 1.25MHz channels

Recall: Code Division Multiple Access (CDMA)



(a) FDMA, (b) TDMA, (c) CDMA.

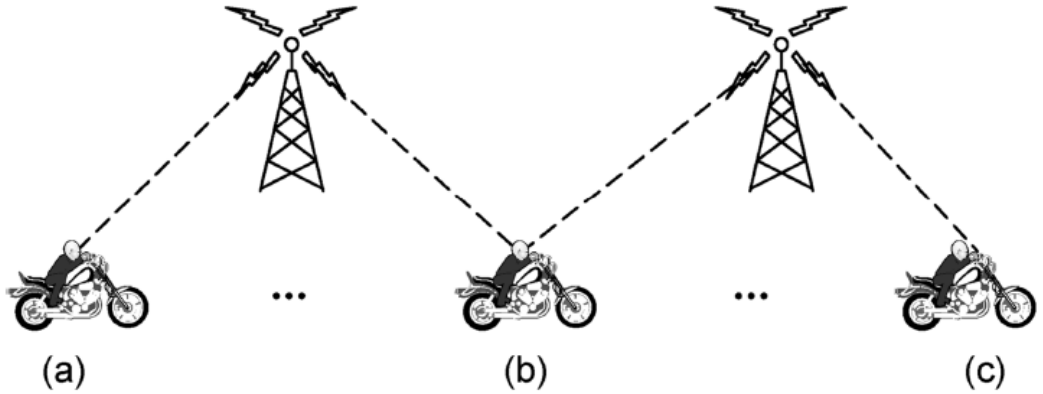
- Allows multiple users to operate on the same frequency at the same time by separating their transmissions with orthogonal codes

CDMA Advantages

1. Improves capacity
   - Allows using all frequencies in all cells
     - Obviates the need for frequency planning required in AMPS and GSM systems
   - Cell capacity limited by interference ➔ no interference when mobile not transmitting or receiving
     - Silence periods during voice calls can be exploited to increase number of simultaneous calls
     - Also exploits the times with fewer *active* users (or low interference periods)
   - Short chip duration allows receiver to do multipath diversity processing via rake receiver to counter fading, thereby obviate the need for higher received signal power (and consequent possibility of higher interference)

CDMA Advantages (contd.)

2. Facilitates soft handoffs for seamless movement between cells
   - By allowing association with both old and new base stations during the transition period
   - Naturally possible because all frequencies are used in every cell



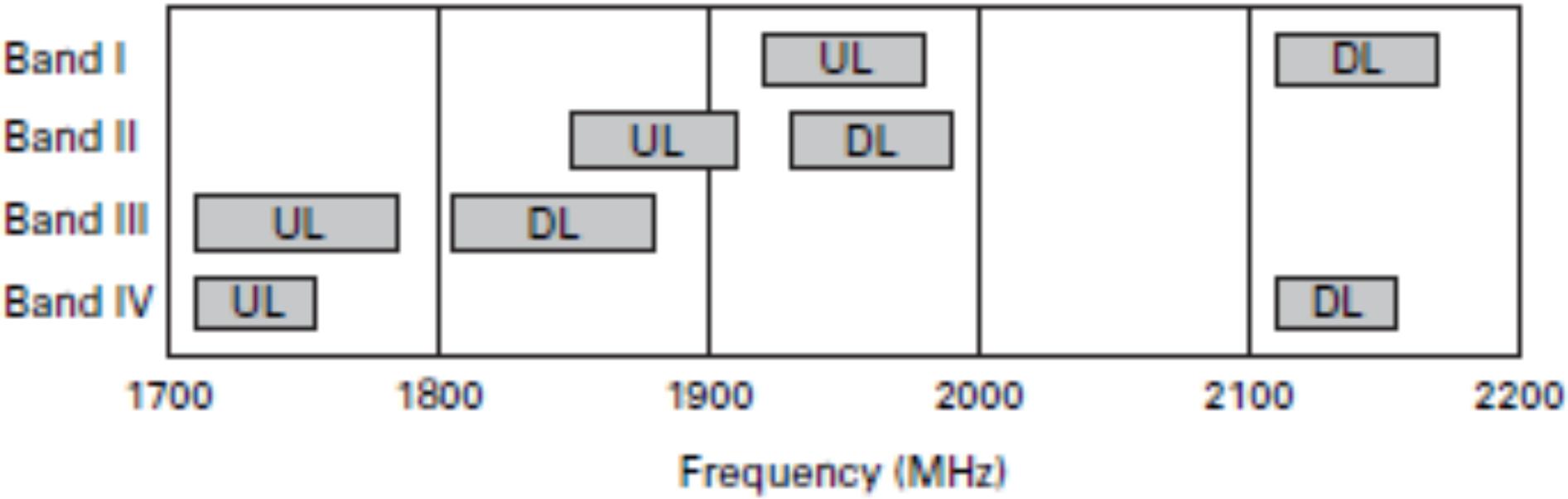
Soft handoff (a) before, (b) during, and (c) after.

CDMA in Practice

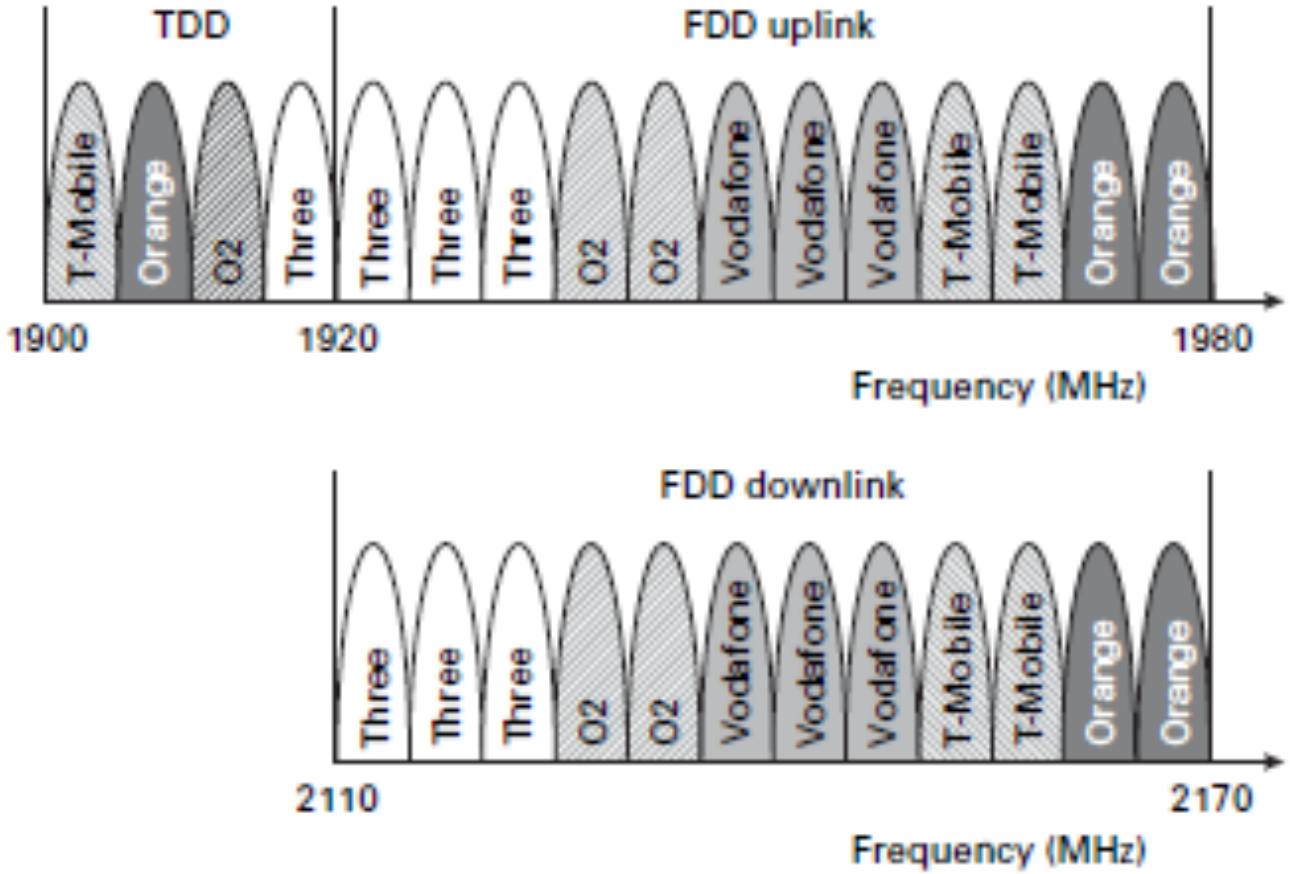
- Synchronization issue:
  - Our earlier discussion on CDMA implicitly assumed that when there is more than one transmitter, they all are time synchronized besides using orthogonal codes (chip sequences)
  - An unrealistic assumption in uplink direction, so need codes that are orthogonal with each other *at all time offsets*
  - Also need sufficient number of codes to use same set of carrier frequencies in all cells
  - The above two requirements approximated by *long pseudorandom sequences (scrambling codes in UMTS parlance)*
- Near-far problem:
  - Use of scrambling codes not enough if received signal powers from different mobiles not same, otherwise interference between signals from different mobiles
    - A signal from nearby mobile can drown out the signal from a distant one (near-far problem)
    - Need *dynamic transmit power control* to counter this effect
- Radio network planning more complex as cells can cause interference to each other and thus cannot be planned independently

UMTS Worldwide Frequency Allocations

- UMTS has two modes of operation: FDD and TDD
- FDD variant is more common, except in China
- Key FDD bands: mostly, Band I: 1920-1980MHz (uplink) and 2110-2170MHz (downlink) with 12 full duplex channels, each 5MHz wide

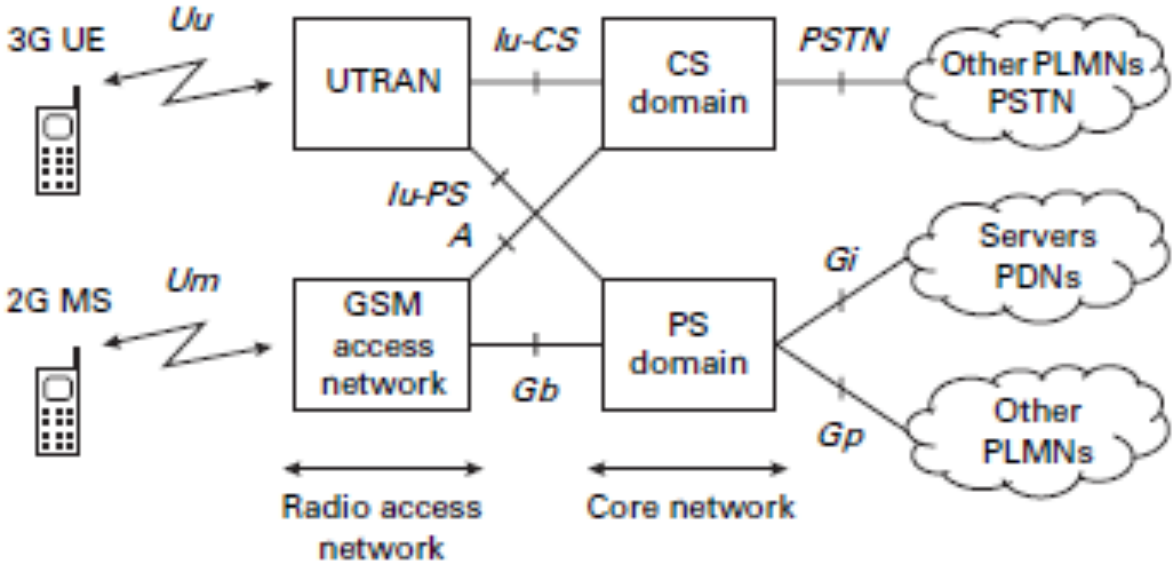


UMTS Frequency Allocation in the UK



- Given UMTS based on CDMA, different full duplex channels used:
  - For cells of different sizes: macrocells, microcells, picocells
  - Or, to increase capacity of any of these type of cells

High Level Architecture of UMTS Network



UTRAN: UMTS Terrestrial Radio Access Network

PLMN: Public Land Mobile Network

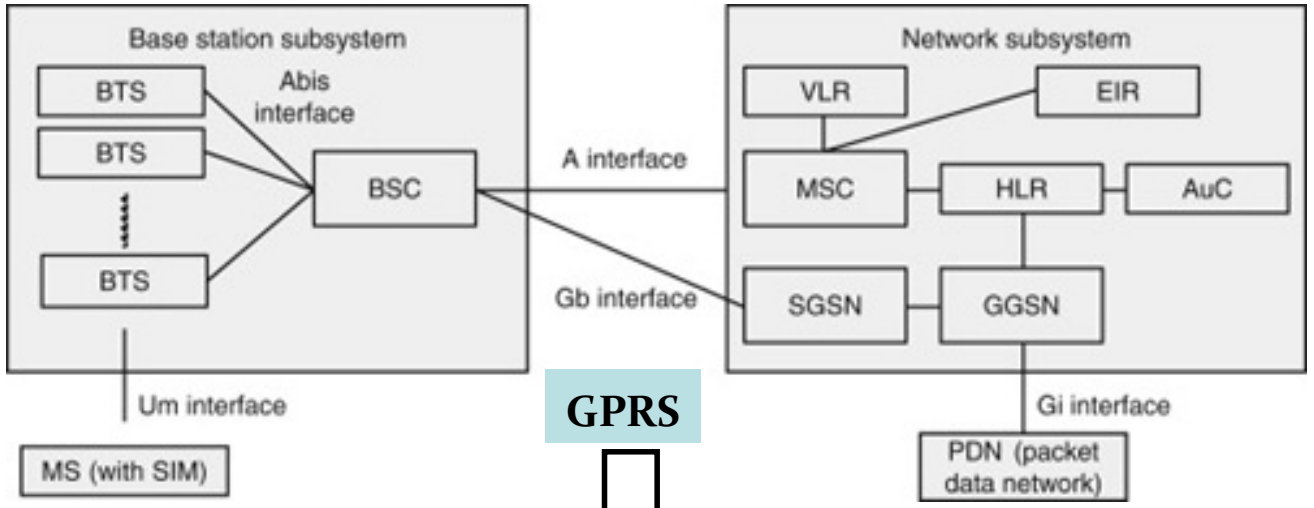
PSTN: Public Switched Telephone Network

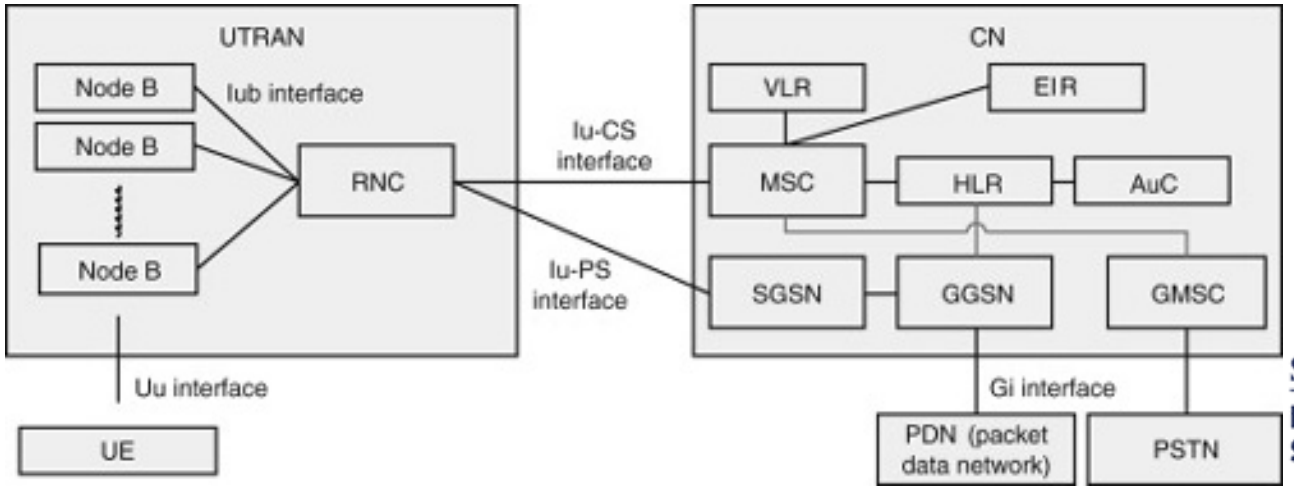
PDN: Packet Data Network

- Like in GPRS and EDGE networks, two domains in core network: circuit switched (CS) and packet switched (PS)
- UTRAN is the UMTS radio access network but the system designed to maintain backward compatibility with GSM via GSM radio access network (and GSM-enabled user devices)
- Interfaces between different system components have their own protocol stacks
- Multiplexing mechanism over the air interface: CDMA within TDMA slots, which are available in multiple frequencies ➔ combined use of FDM, TDM and CDM approaches

School of Informatics
Institute for Computing Systems Architecture

UMTS vs. GPRS/GSM Architectural Differences



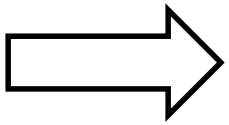


School of Informatics
Institute for Computing Systems Architecture

GSM ➔ UMTS Terminology Changes

GSM

1. Mobile Station (MS)
2. Base Transceiver Station (BTS)
3. Base Station Controller (BSC)
4. Base Station Subsystem (BSS)

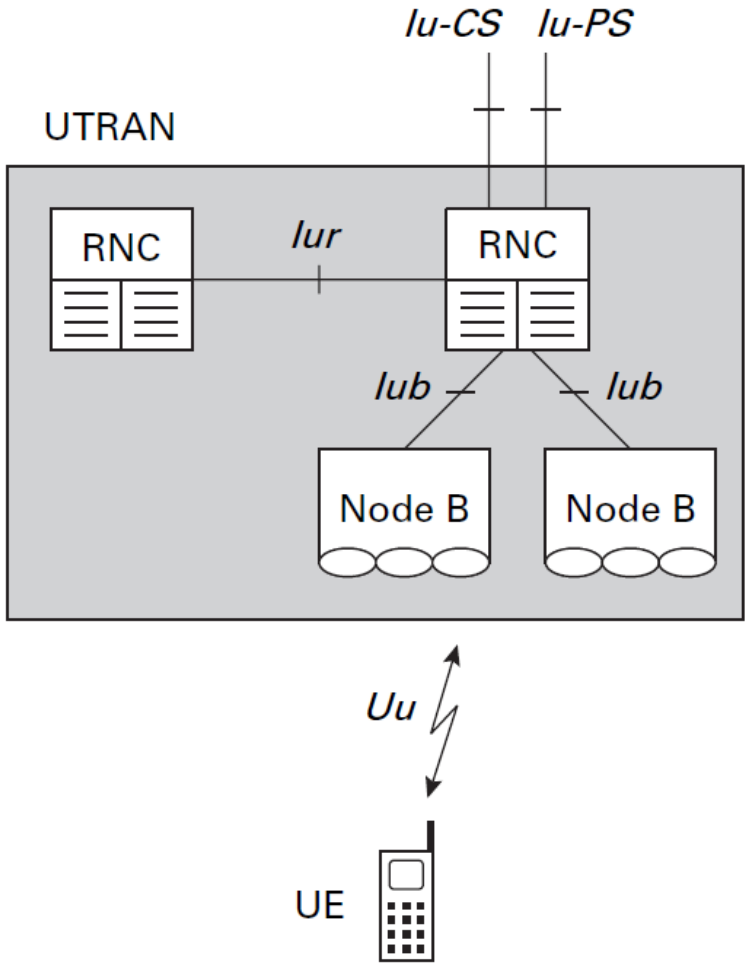


UMTS

1. User Equipment (UE)
2. Node B
3. Radio Network Controller (RNC)
4. UMTS Terrestrial Radio Access Network (UTRAN)

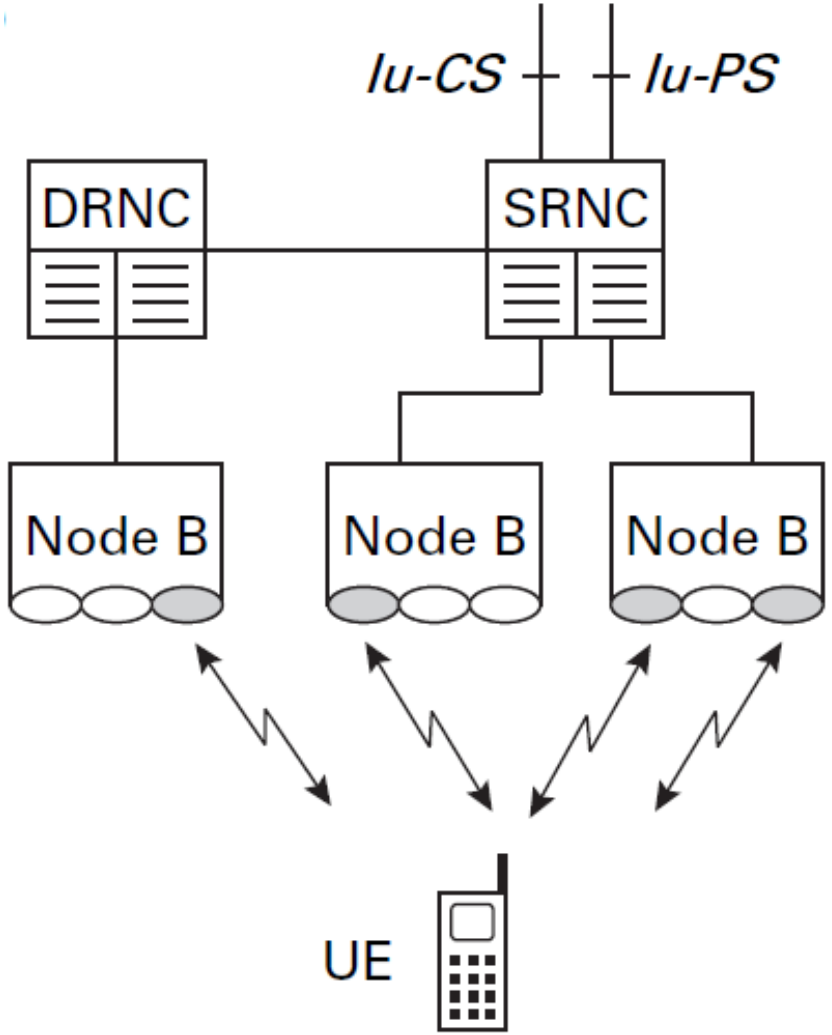
UTRAN Architecture

- Node B (UMTS base station) controls one or more cells
- UE can communicate with more than one cell at a time (e.g., during soft handover periods)



RNC Functions

- A typical operator's network may contain a few tens of RNCs, each of which controlling a few hundred base stations (NodeBs).
- **Controlling RNC (CRNC)**: the RNC controlling a Node B
- **Serving RNC (SRNC)**: the RNC serving a UE
- **Drift RNC (DRNC)**: RNC controlling a Node B with which UE is communicating but not served by
- SRNC and DRNC functions illustrated in the soft handover situation shown on the right

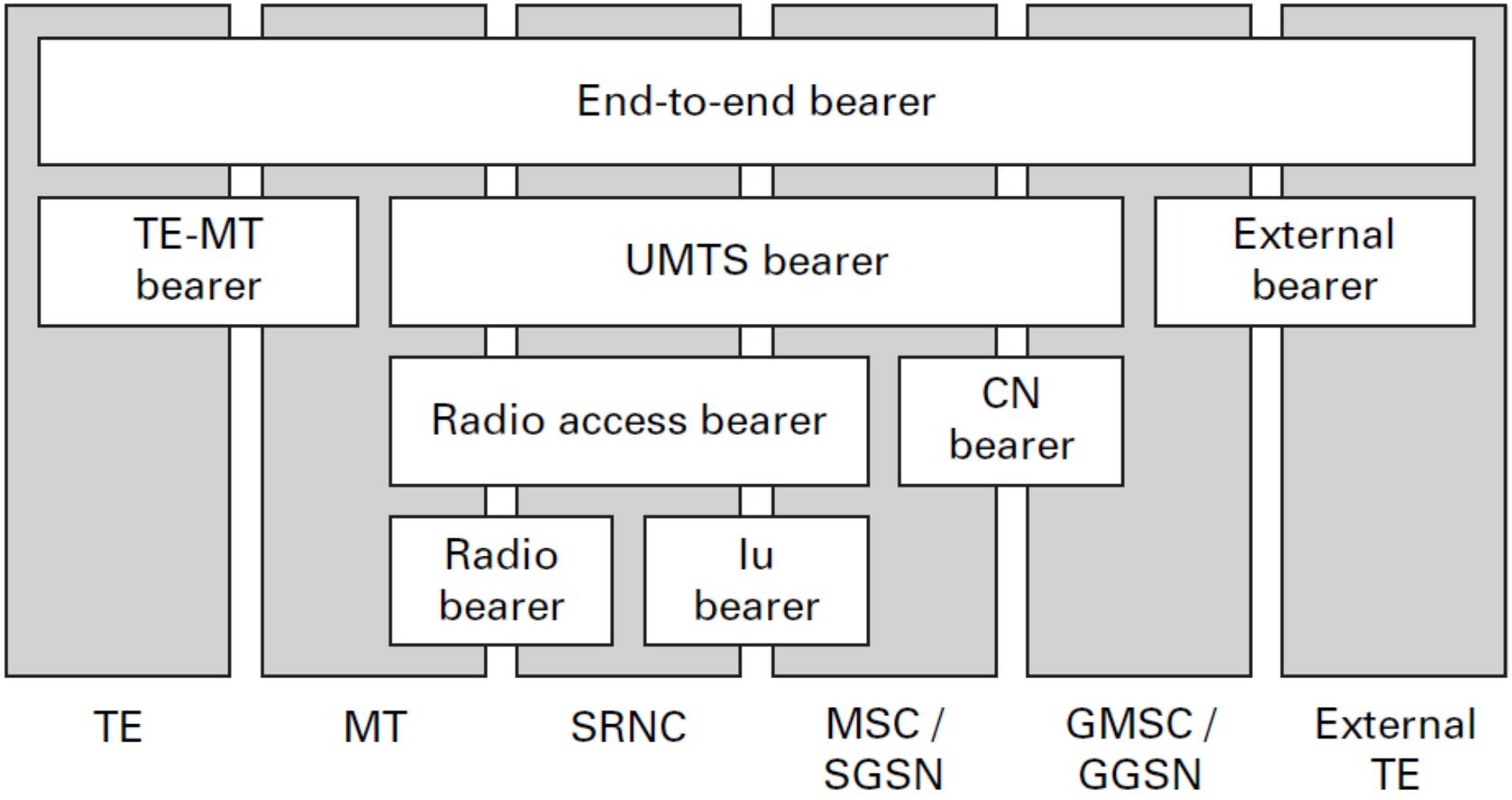


Important New Concepts of UMTS

- The Radio Access Bearer (RAB)
- The Access Stratum and Non-Access Stratum
- Common protocols for circuit-switched (CS) and packet-switched (PS) modes
  - a single lower layer protocol, **RLC/MAC**, instead of separate protocols used in GSM/GPRS for different types of data

UMTS Data Streams: Bearers

- A *bearer* is a data stream that spans some part of the system and has a specific quality of service (QoS)
- Most important bearers in UMTS shown below

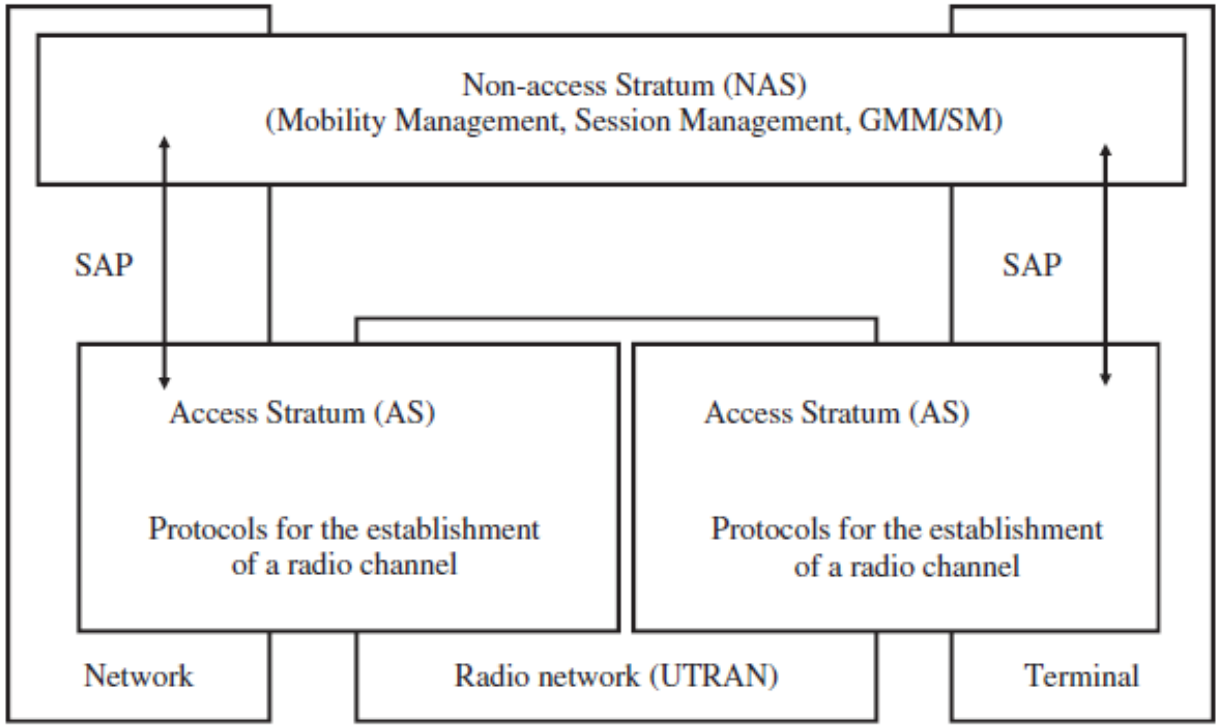


The Radio Access Bearer (RAB)

- RAB is a description of the virtual connection (or communication pipe) between the network and a user
  - Divided into radio bearer on the air interface and the Iu bearer in the radio network (UTRAN)
  - Needs to be established before data can be exchanged between a user and the network
  - This connection used for both signalling and user data
  - RAB established by a request of MSC/SGSN, which indicates only a description of required channel properties as listed below:
    - service class (conversational, streaming, interactive or background);
    - maximum speed;
    - guaranteed speed;
    - delay;
    - error probability.
  - UTRAN maps these properties to a physical connection
    - RAB properties also influence the settings of parameters like coding scheme, logical and physical transmission channel selected

The Access Stratum and Non-Access Stratum

- UMTS aims to separate core network functionalities from those of the access network as much as possible, to allow each of them to evolve independently
- Access Stratum (AS) covers all functionalities that are associated with the radio network ('the access') and the control of active connections between a user and the radio network, e.g., handover control

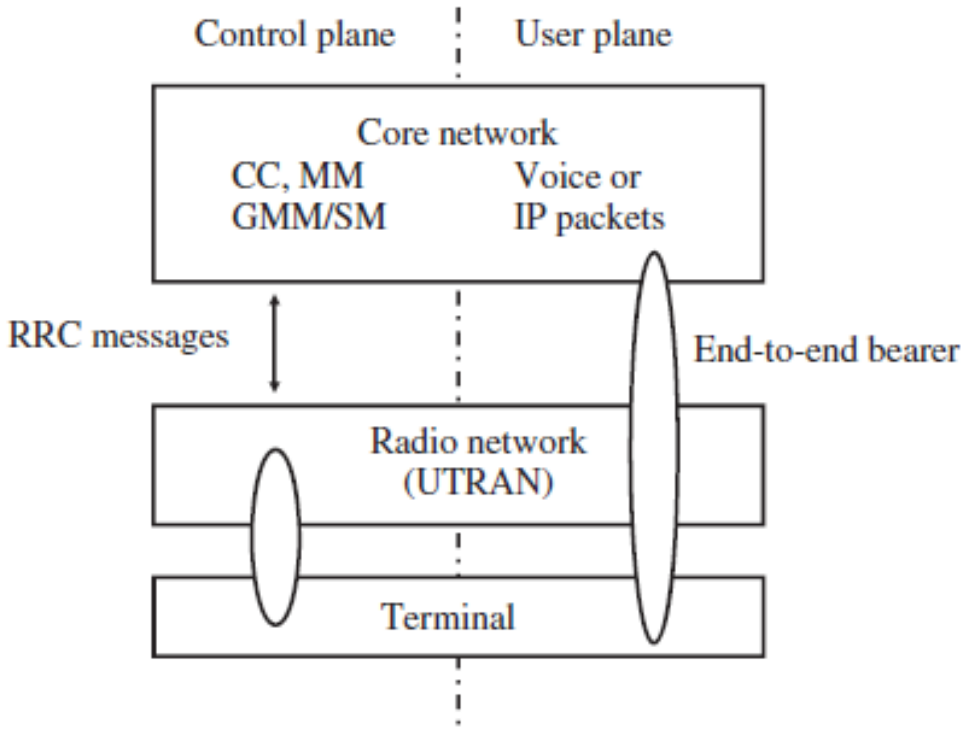


Non-Access Stratum

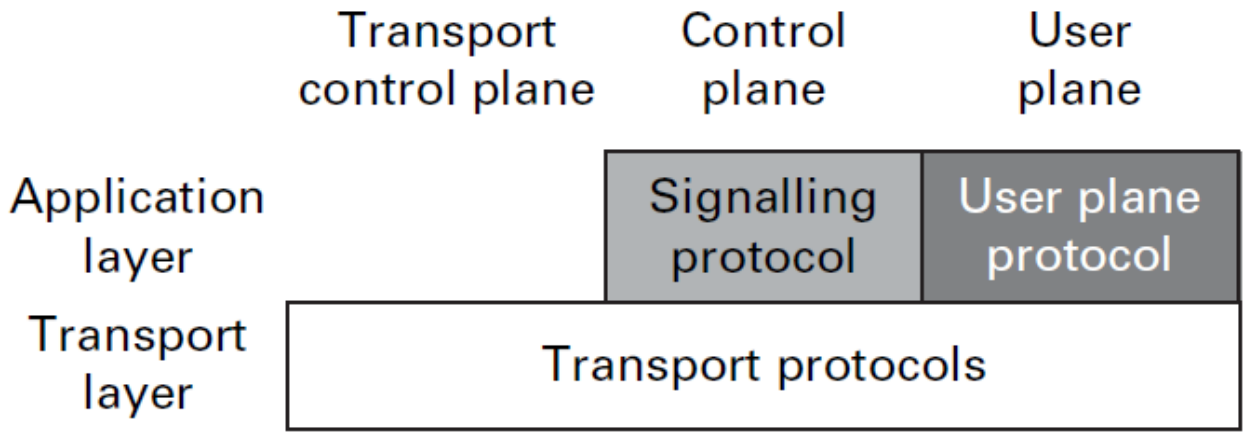
- The NAS contains all functionalities and protocols that are used directly between the mobile device (UE) and the core network
  - No direct influence on the properties of the established RAB and its maintenance
  - NAS protocols transparent to the access network
  - NAS functionalities are those controlled via MSC and SGSN (e.g., mobility and session management)
- Some NAS protocols (e.g., call control, session management) need to request bearer establishment, modification or termination which is enabled by three different service access points (SAPs):
  - notification SAP (Nt, e.g., for paging);
  - dedicated control SAP (DC, e.g., for RAB setup);
  - general control SAP (GC, e.g., for modification of broadcast messages, optional).

UMTS User and Control Planes

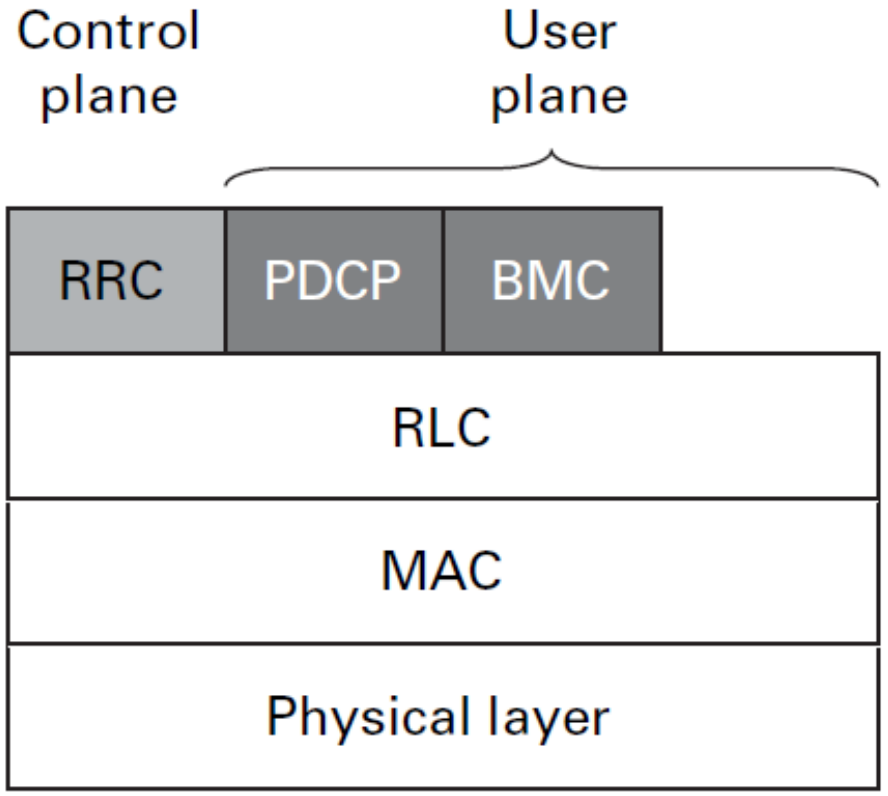
- User plane deals with actual voice data or IP packets to/from end-users
- Control plane deals with signalling data (e.g., call establishment, location update)



Model of (Interface) Protocol Stacks in UMTS

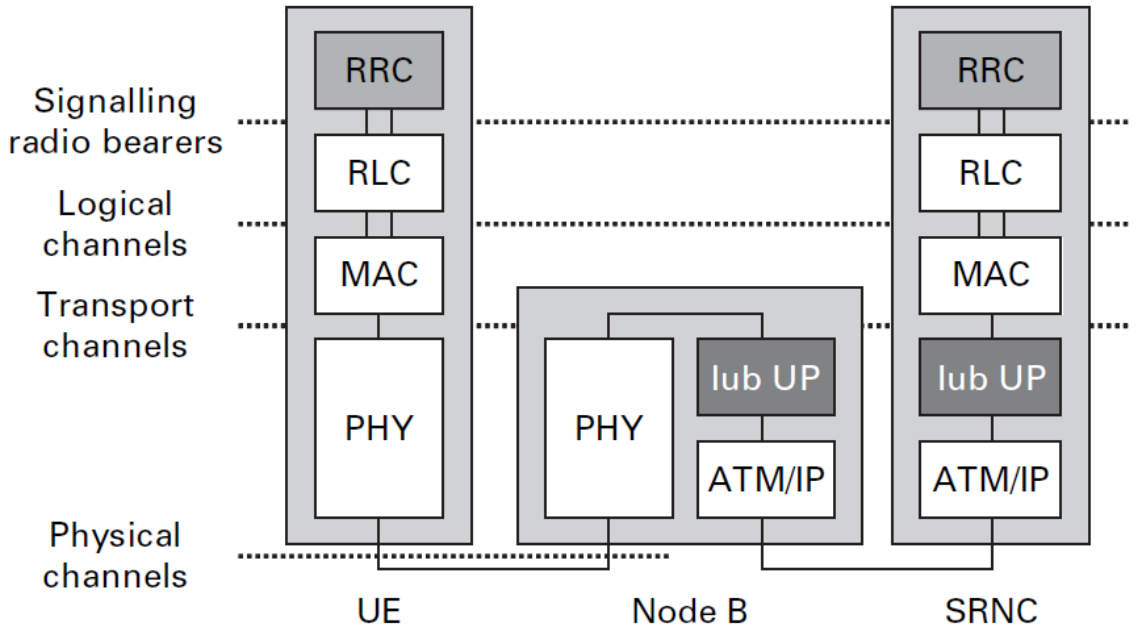


- Example: protocol stack for Uu interface between UE and UTRAN
  - Transport protocols:
    - RLC: Radio Link Control
    - MAC: Medium Access Control
    - PHY: Air interface physical layer



UMTS Data Streams: Channels

- With respect to the air interface, data flows between different protocols are called *channels*
  1. *Logical channels* between RLC and MAC protocols
  2. *Transport channels* between the MAC and PHY
  3. *Physical channels* below the air interface's physical layer
     - Each physical channel is roughly a CDMA code allocated for a specific purpose
- Example below illustrates channels and bearers



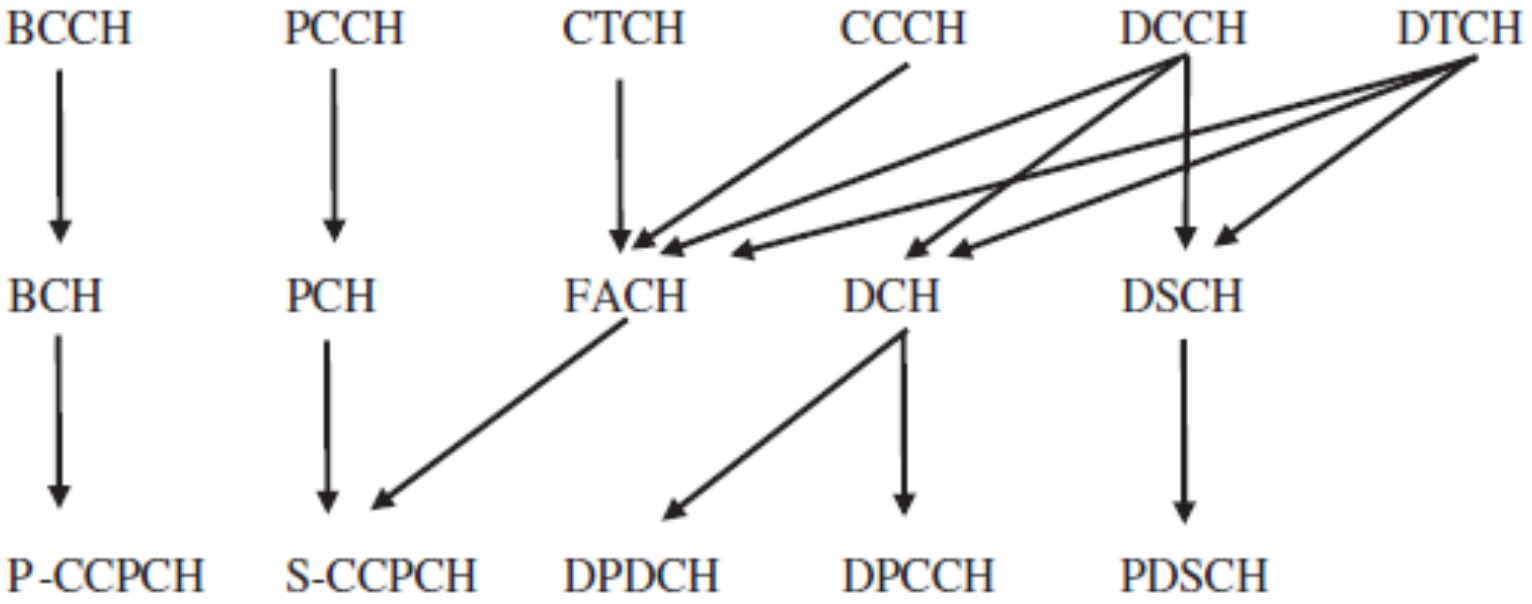
Logical, Transport and Physical Channels

- Three different channel *layers* introduced in UMTS to separate physical properties of the air interface from the logical data transmission
  1. **Logical channels** describe different flows of info like user data and signalling data. Contain no info about characteristics of transmission channel
  2. **Transport channels** prepare data packets received from logical channels for transmission over air interface, also defining channel coding schemes to be used
  3. **Physical channels** are concerned with sending data from transport channels over the air interface and applying channel coding/decoding to the incoming data streams

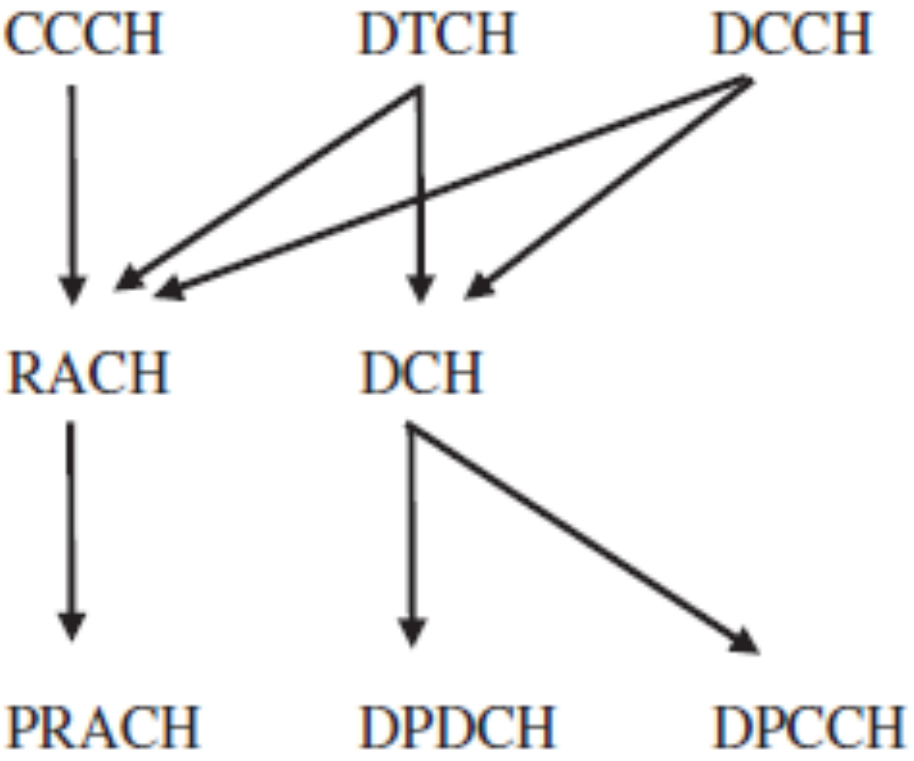
Common and Dedicated Channels

- "Channels" are used to transfer both user and control plane data over the UMTS air interface
- There are three kinds of channels:
  1. **Dedicated channels** to transfer data for a single user (e.g., for a voice connection, for IP packets between user and network, location update message)
  2. **Common channels**: data sent on common channels destined for all users in a cell
     - E.g., broadcast channel transmits general info about the network to all users of a cell (network cell belongs to, current network state, ..)
  3. **Shared channels**: like common channels but only monitored by devices instructed by the network to do so

Logical, Transport and Physical Channels
Downlink Direction

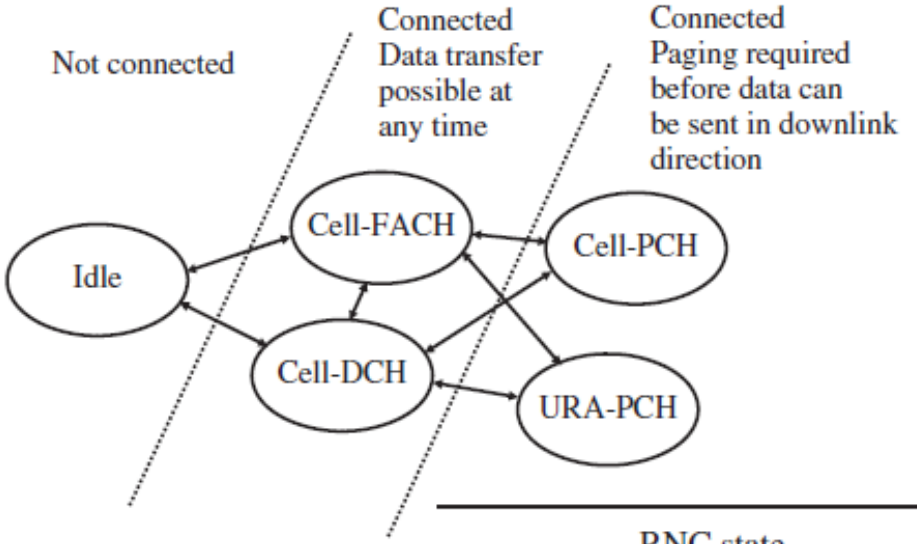


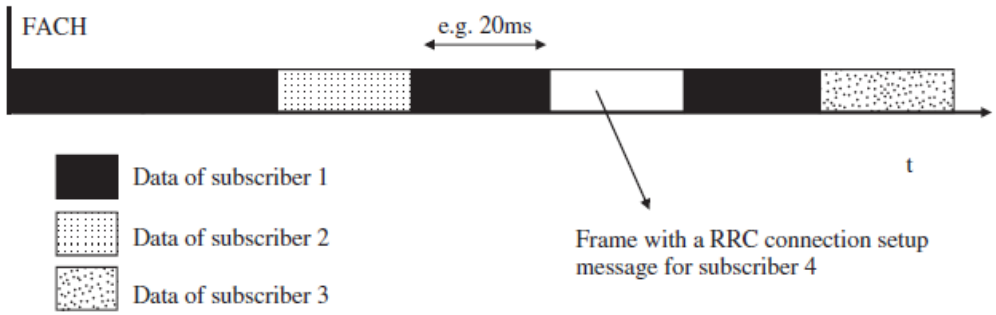
Logical, Transport and Physical Channels
Uplink Direction



Radio Resource Control (RRC) States

- Reflect the state of the device (UE) and the way data transferred between device and the network

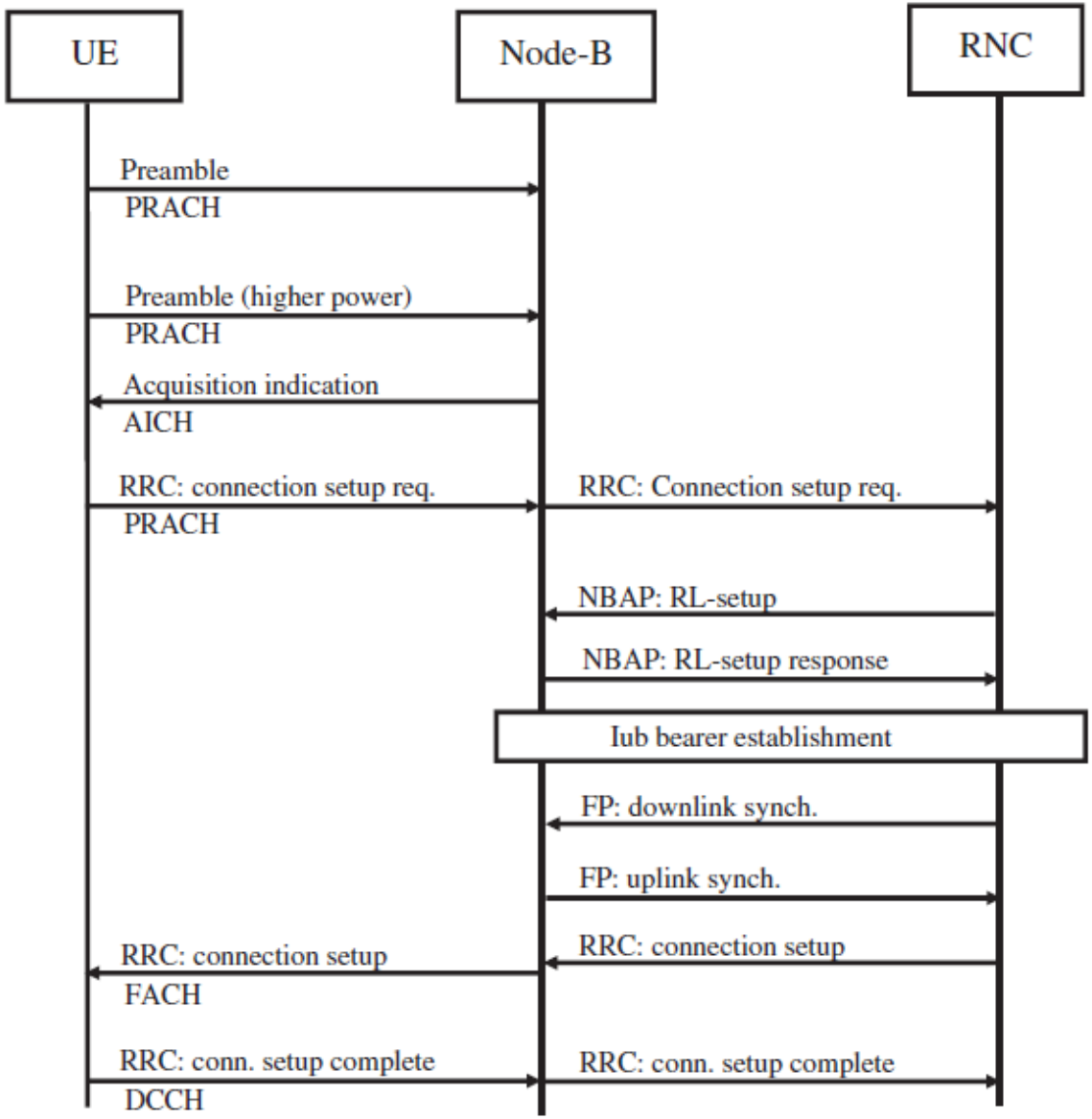




	RNC state	SGSN state
Idle	Not connected	Not connected
Cell-DCH	Connected, data is sent via the DCH or HS-DSCH	Connected
Cell-FACH	Connected, incoming data is sent immediately via the FACH (Common Channel)	Connected
Cell-PCH	Connected, but subscriber has to be paged and needs to reply before data can be forwarded. Once the answer to the paging has been received, the subscriber is put in either Cell-FACH or Cell-DCH state	Connected
URA-PCH	Same as Cell-PCH. Furthermore, the network only needs to be informed of a cell change in case the mobile device is moved into a cell, which is part of a different UTRAN Registration Area	Connected

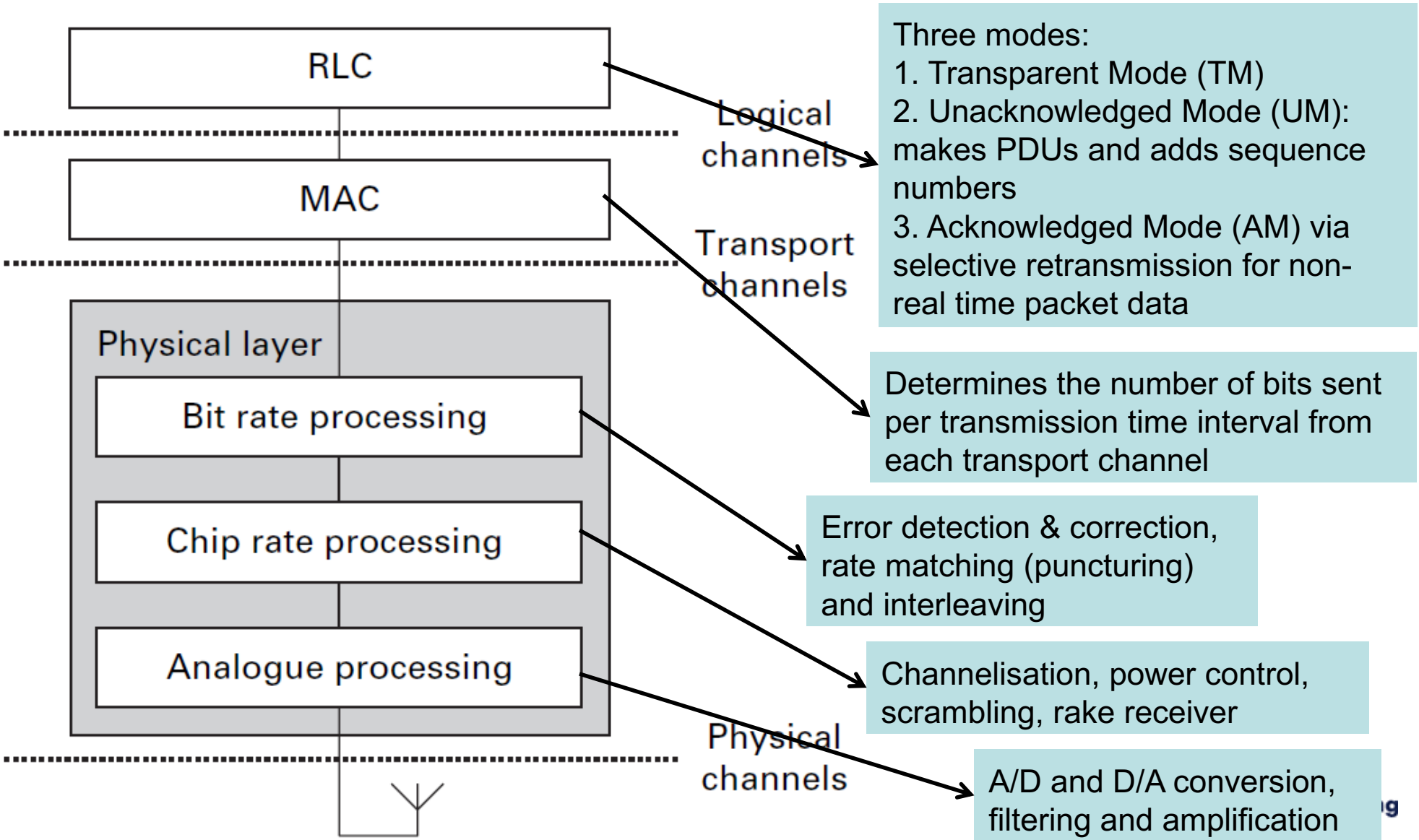
Initial Network Access Procedure

- Performed when device is in Idle state to establish connection with the network (for making a call, (re-)starting a data session, etc.)



UMTS Air Interface

- Enables a maximum downlink/uplink data rate of 2Mbps



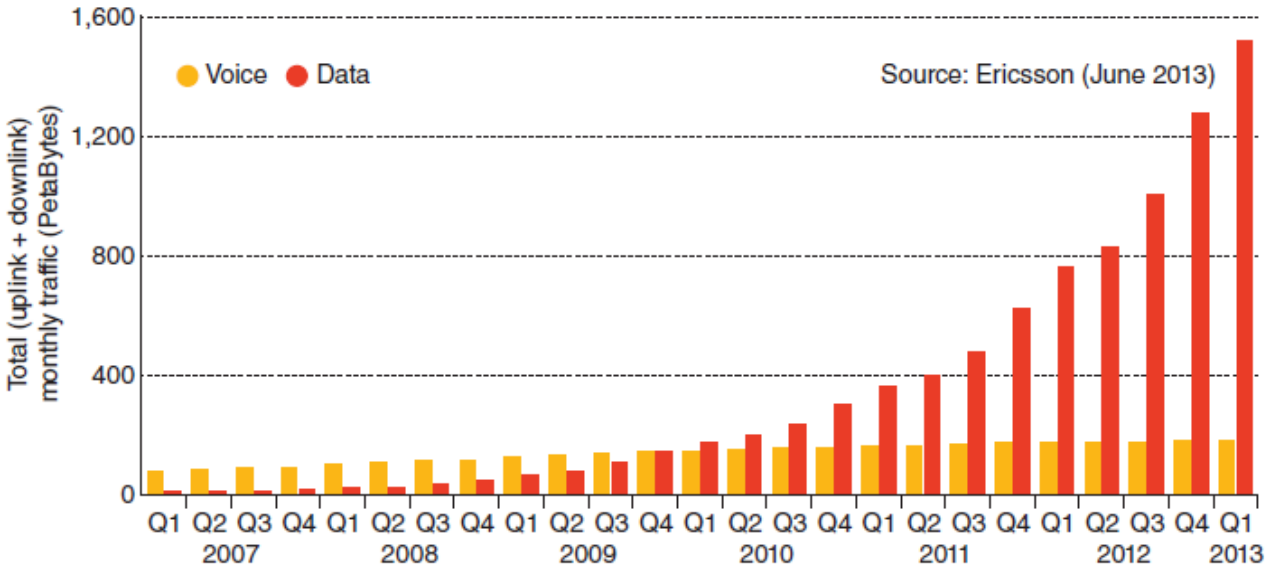
UMTS Evolution ➔ HSDPA, HSUPA, HSPA+

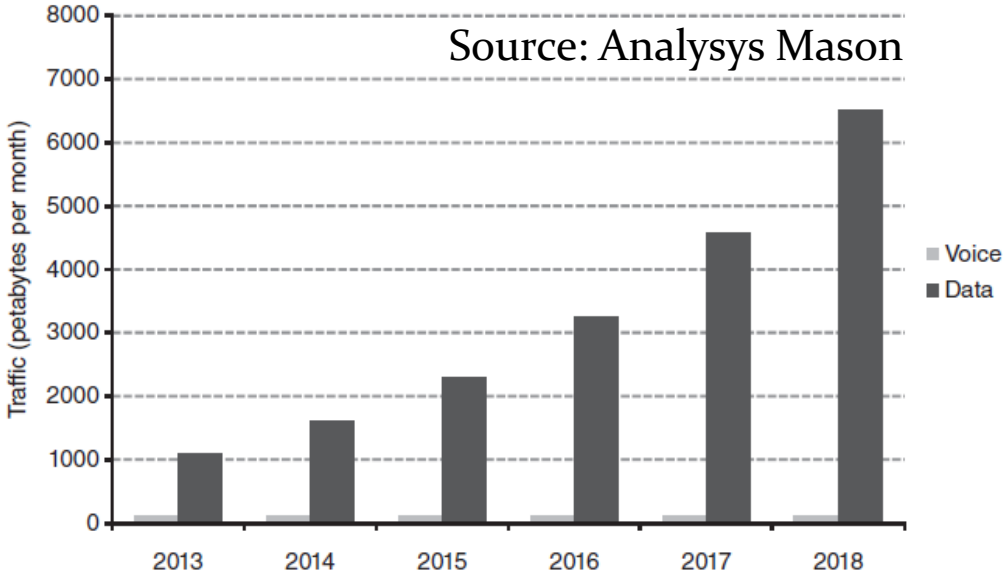
- Examples of 3.5G cellular wireless technologies for increased data rates with non-real time packet data
- High-Speed Downlink Packet Access (HSDPA)
  - Increases the downlink data rate up to 14Mbps
  - Uses a combination of Hybrid ARQ with soft combining, fast scheduling (at the Node B), and adaptive modulation and coding (also at Node B)
- High-Speed Uplink Packet Access (HSUPA)
  - Increases uplink data rate up to 5.7Mbps
  - Uses a combination of Hybrid ARQ with soft combining, and fast scheduling (at the Node B)
- High-Speed Packet Access Evolution (HSPA+)
  - Enables significant increase in max downlink and uplink speeds to 84Mbps and 11Mbps, respectively
  - Via the use of 2x2 MIMO, higher bit-rate modulation schemes in both uplink and downlink directions, etc.

Motivations for 4G

- Increase system capacity to meet growing demand for mobile data (see next slide for historical/forecasted mobile voice/data traffic growth)
- Reduced capital and operational expenditure for mobile operators by maintaining only one (packet-switched) core network instead of two with 2G/3G (circuit-switched for voice and packet-switched for data)
- Reduce end-to-end delay (from ~100ms with 3G networks for data applications)
- Improving system performance without the need to support legacy devices; in other words, a lower complexity solution approach

Mobile Data Traffic Growth





3GPP Requirements for the 4G Air Interface

- Peak data rates
  - 100Mbps in downlink
  - 50 Mbps in uplink
- Spectral efficiency (cell capacity per unit bandwidth) relative to WCDMA (Release 6)
  - 3-4 times greater in downlink
  - 2-3 times greater in uplink
- Latency
  - Less than 5ms latency between mobile and fixed network
  - Less than 100ms to switch from standby to active state
- Coverage
  - Optimized for cell sizes up to 5Km, degraded performance up to 30Km and support cell sizes up to 100Km
- Mobility
  - Optimized for mobile speeds up to 15Km/h, work with high performance up to 120Km/h and support speeds up to 350Km/h

3GPP Requirements for 4G Core Network

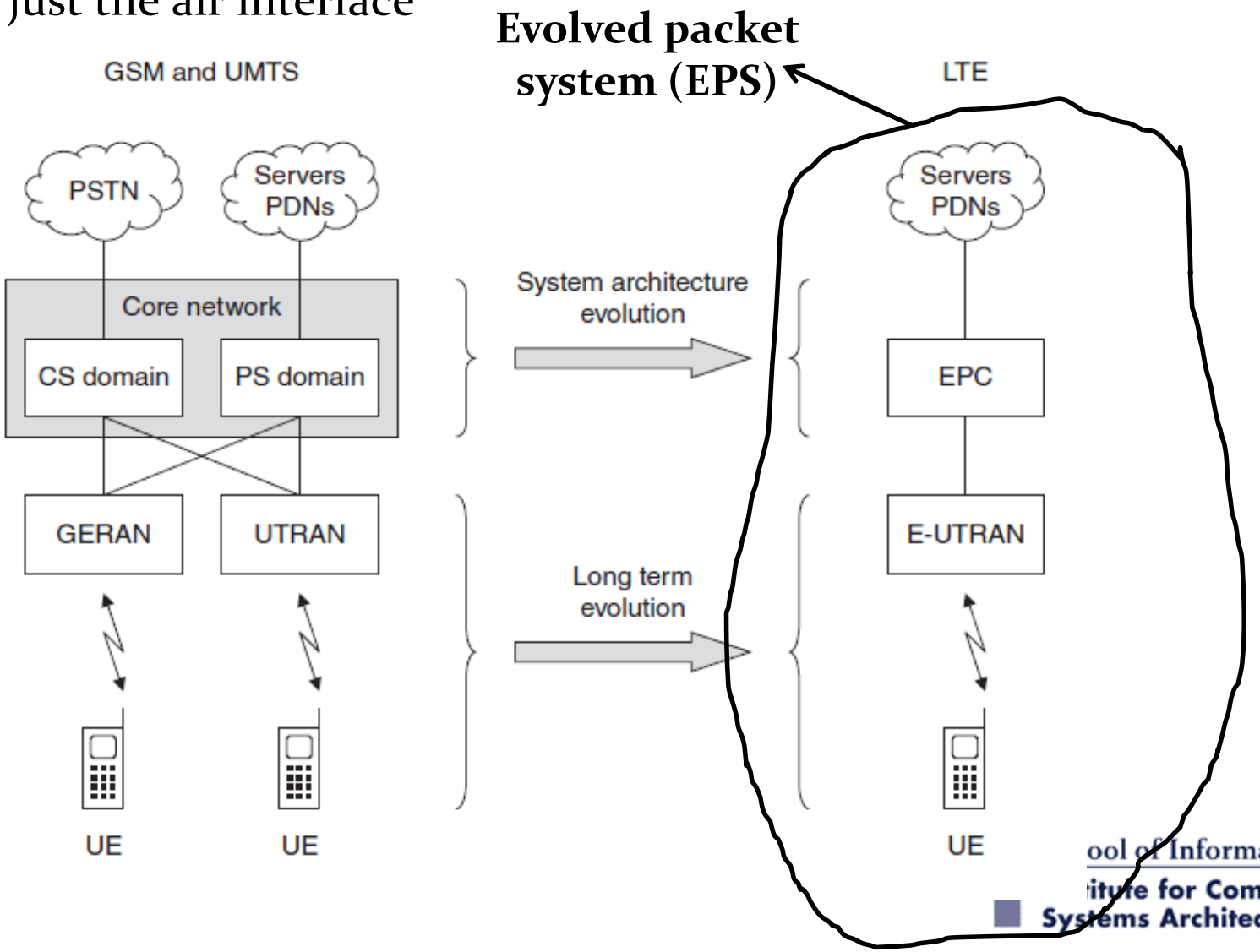
- Route packets using IP
- Provide always-on connectivity
- 10ms user-plane latency for non-roaming mobile, 50ms in a roaming scenario
- Support inter-system handovers both with older 3GPP and non-3GPP systems

Need for a New Air Interface Technology

- Increasing the carrier bandwidth natural way to enable higher data rates and increased system capacity
- UMTS (Wideband CDMA) however exhibits poor scaling and increased susceptibility to multipath fading as the carrier bandwidth is increased due to the use of one *single* wide carrier (5MHz in UMTS)
- This issue is overcome through the use of OFDM, where a carrier is made up of multiple narrow subcarriers
- So 4G air interface (called Long Term Evolution or LTE) is OFDM based with flexibility in the set of bandwidths supported (1.25MHz to 20MHz) by increasing or decreasing the number of 180KHz wide subcarriers
  - 10, 15 and 20MHz channels typically used
  - 20MHz carrier ➔ >100Mbps data rates in good channel conditions
- Additionally, all LTE devices have to support MIMO too

Architectural differences between GSM/GPRS/UMTS and LTE

- LTE acronym used in practice to refer to EPS, i.e., the whole system instead of just the air interface



3GPP Specifications for LTE

3GPP specification releases for UMTS and LTE

Release	Date frozen	New features
R99	March 2000	WCDMA air interface
R4	March 2001	TD-SCDMA air interface
R5	June 2002	HSDPA, IP multimedia subsystem
R6	March 2005	HSUPA
R7	December 2007	Enhancements to HSPA
R8	December 2008	LTE, SAE
R9	December 2009	Enhancements to LTE and SAE
R10	June 2011	LTE-Advanced
R11	June 2013	Enhancements to LTE-Advanced
R12	September 2014	Enhancements to LTE-Advanced

3GPP specification series used by UMTS and LTE

Series	Scope
21	High-level requirements
22	Stage 1 service specifications
23	Stage 2 service and architecture specifications
24	Non-access stratum protocols
25	WCDMA and TD-SCDMA air interfaces and radio access network
26	Codecs
27	Data terminal equipment
28	Tandem free operation of speech codecs
29	Core network protocols
30	Programme management
31	UICC and USIM
32	Operations, administration, maintenance, provisioning and charging
33	Security
34	UE test specifications
35	Security algorithms
36	LTE air interface and radio access network
37	Multiple radio access technologies

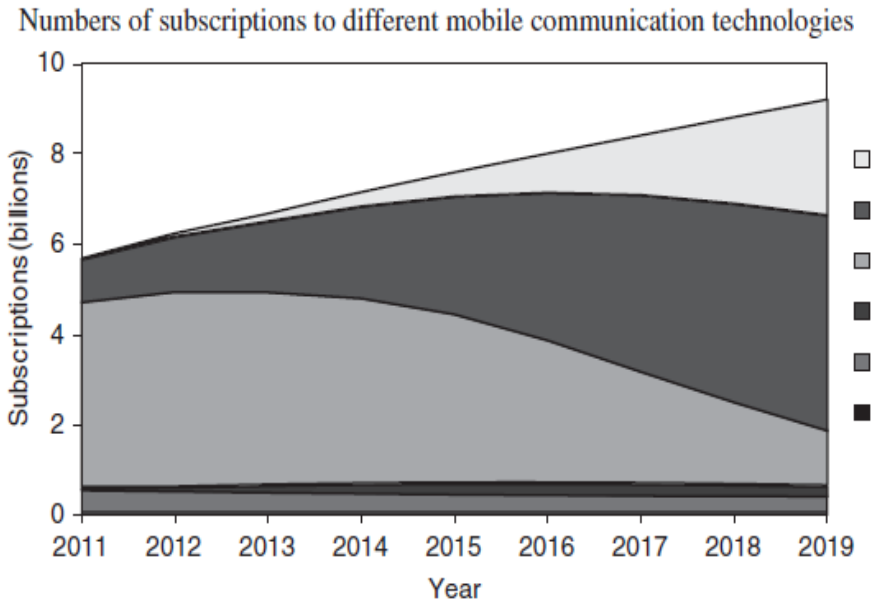
4G / LTE Overview

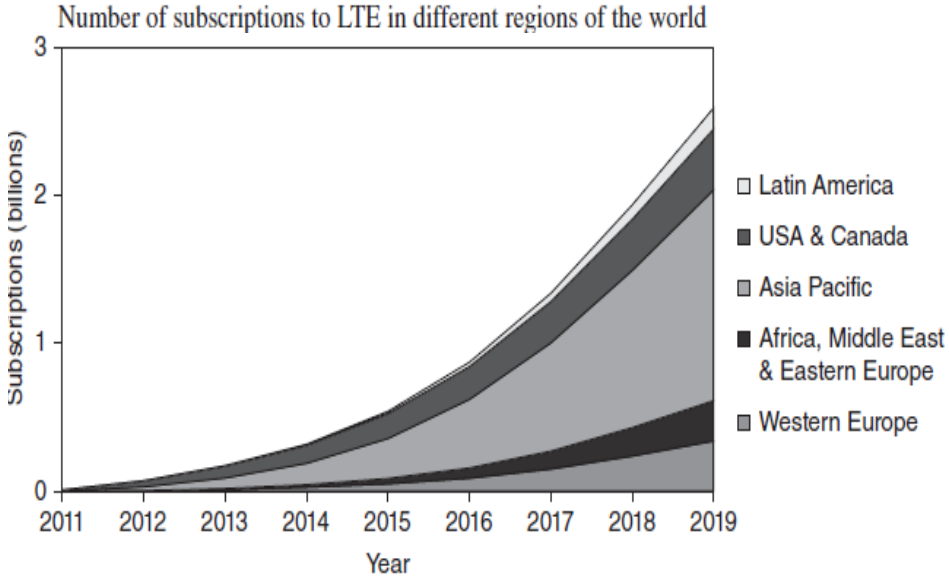
- LTE Air Interface based on OFDM (with flexible bandwidth support) and MIMO
  - Orthogonal Frequency Division Multiple Access (OFDMA) in the downlink and Single Carrier Frequency Division Multiple Access (SC-FDMA) in the uplink
  - FDD and TDD modes specified in the same standard with differences only in the lower 2 layers (L1 and L2) of air interface
- All IP core network with the exception of SMS (that are transported over signaling messages)
- All interfaces are IP based ➔ simplification and do away with legacy, slow and expensive technologies
- Fewer logical and physical network components in LTE ➔ further simplification and reduced delay (<20-30ms round-trip times)
- Optimized signaling for connection establishment and mobility management procedures ➔ better user experience (network connection time ~few hundred ms, quick entry/exit from power save states)
- Interfaces to other 3GPP based RATs for seamless access

LTE Growth in #Subscriptions

- Historical data up to 2013, forecast thereafter

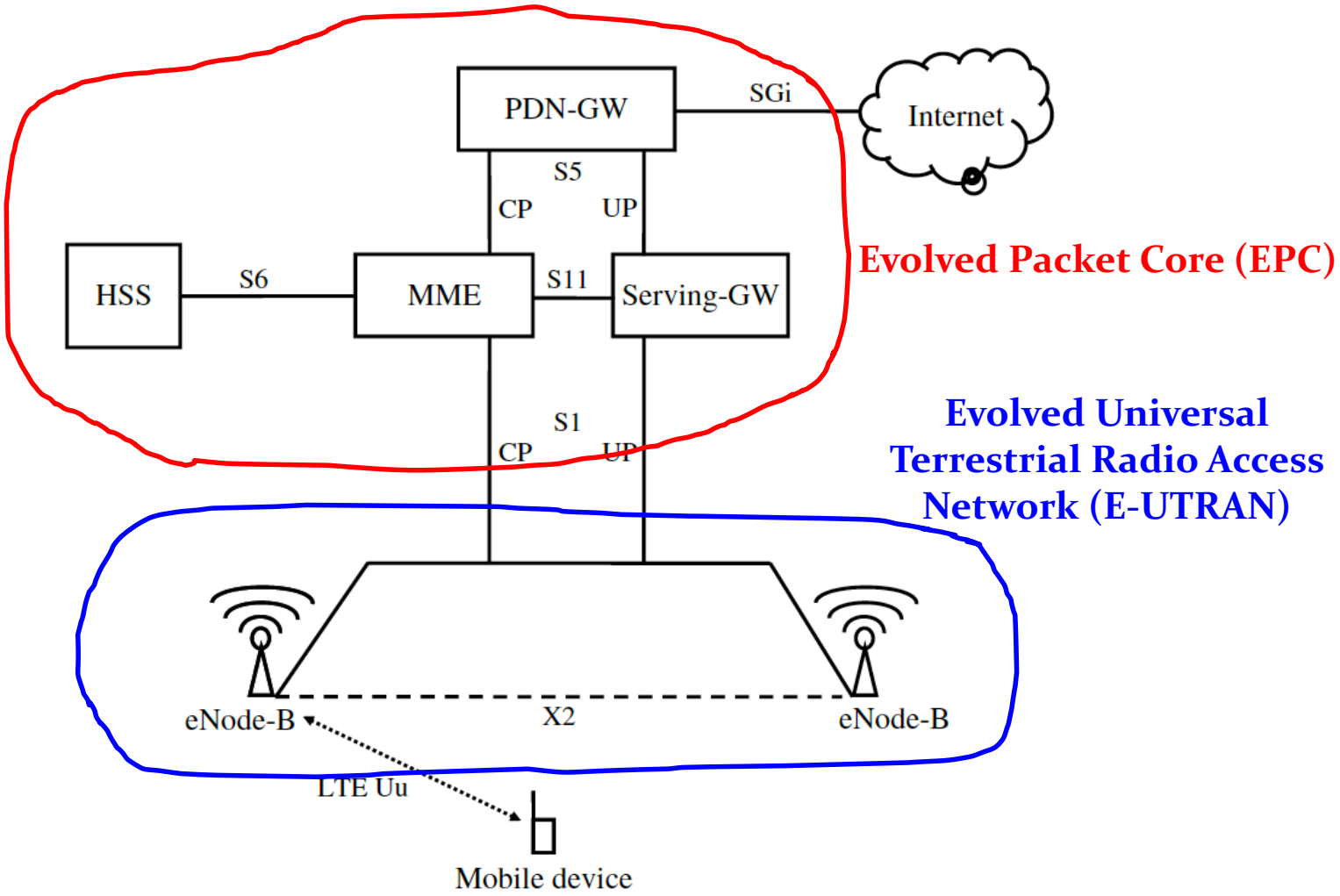
Source: Ericsson





- Also check out Ofcom mobile availability checker and maps at https://checker.ofcom.org.uk/mobile-coverage

LTE System Architecture Overview



LTE Mobile Devices

- As in UMTS, LTE mobile device called user equipment (UE)
- Several UE categories defined (to refer to UEs with different hardware capabilities)

UE category	Maximum number of bits in a subframe		Maximum number of downlink MIMO layers
	Downlink	Uplink	
1	10296	5160	1
2	51024	25456	2
3	102048	51024	2
4	150752	51024	2
5	299552	75376	4

Selection of Typical UE Device Categories

Category	3	4	6	9	12
Maximum downlink datarate with carrier aggregation	100	150	300	450	600
Typical number of aggregated carriers in downlink	1	1	2	3	4
Maximum uplink datarate	50	50	50	50	100
Typical number of aggregated carriers in uplink	1	1	1	1	2
Number of receive antennas	2	2	2	2	2
Number of MIMO downlink streams	2	2	2	2	2
Support for 64-QAM in the uplink direction	No	No	No	No	No

LTE Mobile Devices (contd.)

- In downlink, all UEs support 64-QAM in downlink, antenna diversity and MIMO (2x2 common today) ➔ peak downlink data rates between 100 and 150Mbps in a 20MHz carrier with 2x2 MIMO and even higher with carrier aggregation
- Only 16-QAM required in the uplink for UE classes 1-4 ➔ peak uplink data rate of 50Mbps in a 20MHz carrier
- Besides UE category, feature group indicators also used to indicate other different UE capabilities
  - E.g., support for inter-frequency handover, periodic measurements for self-optimized networks, inter-RAT measurements, intra-subframe frequency hopping in the uplink, simultaneous transmission of uplink control info, semi-persistent scheduling

Bearer

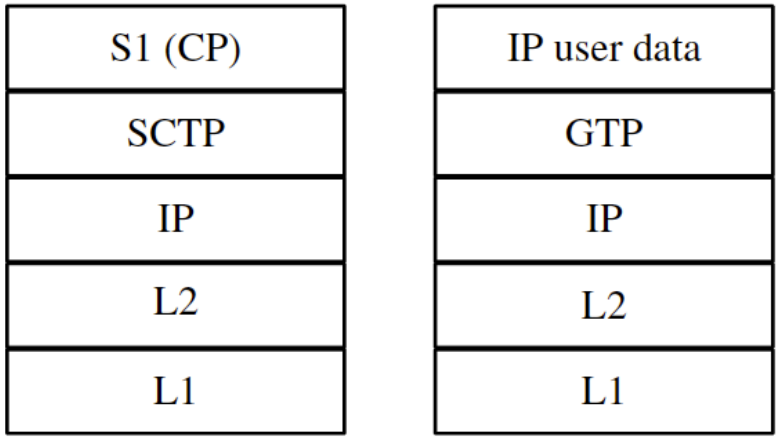
- Logical connection between network entities and describes Quality of Service (QoS) attributes such as latency, maximum throughput, etc. for the data flows over it
- **Radio Access Bearer (RAB)** manages all communication between a mobile device and a base station, and includes:
  - **Signaling Radio Bearer (SRB)** for exchanging session management, mobility management and radio resource configuration (RRC) messages
  - At least one **Data Radio Bearer (DRB)** for transferring IP user data packets

eNode-B (LTE Base Station)

- eNode-B consists of three major elements: antennas, radio modules and digital modules
  - **Remote Radio Head (RRH)**: combination of radio module and antennas installed close to each other
  - Typical these days for RRH to be separated from the digital module by an optical connection
- Unlike in UMTS, eNode-Bs are autonomous units and are responsible for:
  - Managing the air interface (LTE Uu interface)
  - User management in general and scheduling air interface resources
  - Ensuring QoS
  - Load balancing between different simultaneous radio bearers to diff. users
  - Mobility management (handing over to neighbouring e-NodeB and informing higher layer network nodes afterwards)
  - Interference management (reducing inter-cell interference)

S1 Interface

- Interface between the base station and core network
- Split into two logical parts over the same physical connection
  - S1 User Plane (S1-UP) for user data: tunneled through IP using GPRS Tunneling Protocol (GTP)
  - S1 Control Plane (S1-CP) for control/signaling data: both for eNode-B's interaction with the core network and for transferring user related signaling messages (e.g., for bearer establishment, user authentication, providing encryption keys for air interface)
    - ➢ SCTP used to allow multiple independent signaling connections



X2 Interface

- For direct communication between LTE base stations
- Used for two purposes:
  - Handover to a neighboring cell reachable over the X2 interface (otherwise, via S1 interface)
    - Base station neighbor relations either configured by operator or detected via info from mobile devices (*aka* Automatic Neighbor Relation (ANR) feature)
  - Interference coordination
    - Full frequency reused among neighboring base stations by default in LTE, as in UMTS
    - But this can cause interference to UEs in overlapping coverage area
    - X2 interface can used for relevant base stations to coordinate and mitigate/reduce such interference
- X2 user plane stack similar to that of S1 user plane
- X2 control plane uses X2 application protocol in the top layer, otherwise similar to S1-CP stack (SCTP/IP/..)
- In practice, X2 interface is transported over the same backhaul link as the S1 interface up to the first IP aggregation router

EPC Functions

- Mobile core network providing the following functions:
  - **Mobility management**: signaling support between UE and network using NAS protocols
  - **Session management**: establishment and management of data bearers
  - **Security management**: data encryption and authentication services for the users
  - **Policy control and charging**: operator prescribed access and control of services
    - E.g., QoS management, metering, service control based on user classification, policy control enforcement, charging and billing of services

EPC Entities

- Mainly three:
  1. **Mobility Management Entity (MME)**
     - Control entity of the EPC
     - Main functionalities provided: NAS signaling and security, P-GW and S-GW selection, roaming support, user authentication, bearer management, and idle-state mobility handling
  2. **Serving Gateway (S-GW)**
     - Manages user data plane between eNBs and P-GW
     - Also serves as a mobility anchor when UEs move between different eNBs
  3. **Packet Data Network Gateway (P-GW)**
     - Provides data connectivity to external packet data networks
     - Functions: packet filtering and routing, IP address allocation, charging and policy enforcement via PCRF, lawful interception

Mobility Management Entity (MME)

- In LTE, overall user control is centralized in the core network with MME playing a key role
  - Some of this control is delegated to eNode-Bs to autonomously handle users after their radio bearers are established
- MME responsible for all Non-Access Stratum (NAS) Signaling, i.e., signaling exchanges between base stations and the core network, and between users and the core network
- Many MMEs in large networks to cope with the amount of signaling
- Similar to SGSN in GPRS and UMTS networks except that it does not handle user data forwarding between core and radio network; Serving Gateway (S-GW) deals with the latter in LTE

MME Tasks

- **Authentication.** On attachment, user is authenticated by MME with info from Home Subscriber Server (HSS) and then encryption keys are sent to eNode-B for ciphering messages over the air interface
- **Establishment of bearers.** MME communicates with other core network components to establish IP tunnel for each user between its eNode-B and an Internet gateway
- **NAS mobility management.** Page all eNode-Bs in the Tracking Area (TA) of an idle device with arriving data from the Internet, and re-establish bearer(s)
- **Handover support.** Forward handover messages between two eNode-Bs when no X2 interface, and also modify user data IP tunnel after a handover if needed
- **Interworking with other radio networks.** When a device moves out of the LTE coverage area, hand it over to an available GSM/UMTS network
- **SMS and voice support.** Support these traditional services over a pure IP based LTE network

Voice Calls in LTE

- Voice calls in earlier standards supported via the circuit-switched part of the core network
- Since LTE is fully packet-switched, voice calls supported via:
  - **Circuit switched fallback (CSFB)**: voice calls made over legacy 2G/3G via their circuit-switched domain
  - **IP multimedia subsystem (IMS)**: external network that includes signalling functions needed to set up, manage and tear down a voice over IP call

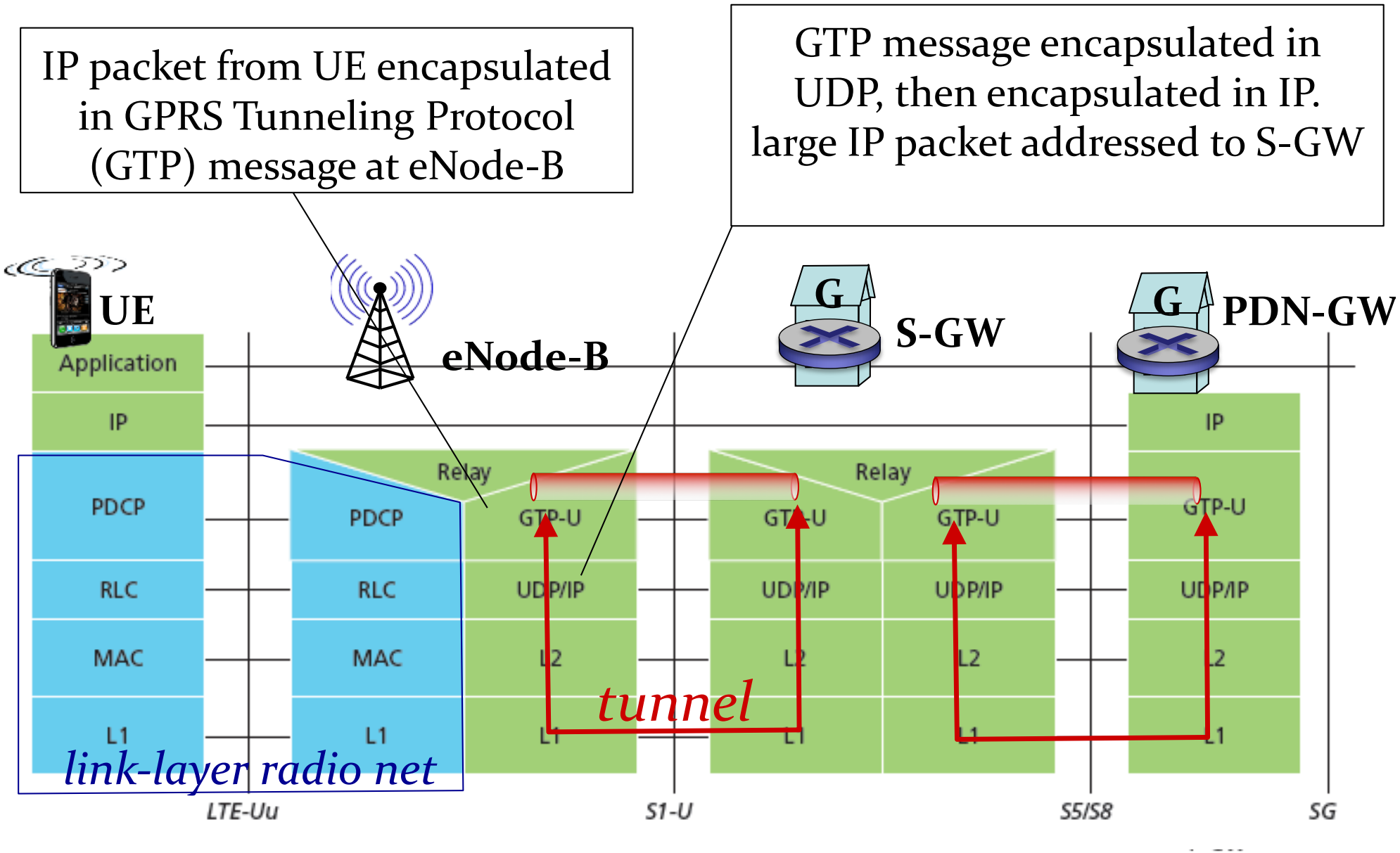
Serving Gateway (S-GW)

- Manages user data tunnels between eNode-Bs in the radio network and the Packet Data Network Gateway (PDN-GW), which is the gateway router to the Internet
- On the radio network side, it terminates S1-UP GTP tunnels
- On the core network side, it terminates the S5-UP GTP tunnels to the Internet gateway
- S1 and S5 tunnels for a single user are independent of each other and can be changed separately as required
- Tunnel creation and modification are controlled by the MME via commands sent to the S-GW over the S11 interface
- S11 interface reuses GTP-C protocol of GPRS and UMTS with new messages and has UDP and IP below it

PDN-Gateway (PDN-GW)

- Gateway node to the Internet and terminates S5-UP tunnels
- Some operators also use it to interconnect intranets of large companies over an encrypted tunnel for direct access to their private internal networks
- Also responsible for assigning IP addresses to mobile devices via MME over the S5 control plane protocol
  - A mobile device can be assigned multiple IP addresses, e.g., one to connect to the Internet and another to access the IP Multimedia Subsystem (IMS) for voice over LTE
  - Often PDN-GW implements a NAT to assign only local addresses internally; this protects mobile devices and helps them conserve power in presence of malicious connection attempts
- Also plays an important part in international roaming scenarios – GTP tunnel between S-GW in the visited network and a PDN-GW in the user's home network over S8 interface (home routing)

Radio + Tunneling: UE ⟷ eNode-B ⟷ PDN-GW



Home Subscriber Server (HSS)

- Subscriber database, shared with GSM and UMTS
- LTE uses IP-based DIAMETER protocol to exchange info with the database (S6 interface)
- Each subscriber has a record in the HSS incl. the following key parameters:
  - User's International Mobile Subscriber Identity (IMSI)
    - Uniquely identifies a subscriber and implicitly includes Mobile Country Code (MCC) and Mobile Network Code (MNC)
    - A copy of the IMSI is stored on the subscriber's SIM card
  - Authentication info to authenticate the subscriber and generate encryption keys on a session basis
  - Circuit-switched service properties such as user's telephone number (MSISDN number) and services user is allowed to use (e.g., SMS, call forwarding)
  - Packet-switched service properties such as Access-Point Names (APNs) the subscriber is allowed to use
  - IMS specific info
  - The ID of the current serving MME

Billing, Prepaid and Quality of Service

- For offline or postpaid billing, billing records are created on the MME
- Online charging or prepaid billing requires interaction with core network components such as MME, S-GW and PDN-GW
- Policy and Charging Rules Function (PCRF) is a standardized QoS node to request a certain QoS profile for a data flow and have it enforced through commands to the core and access network
  - Only for network operator services needing QoS, e.g., voice over LTE (VoLTE)

Key Features of Core Networks of UMTS and LTE

Feature	UMTS	LTE
IP version support	IPv4 and IPv6	IPv4 and IPv6
USIM version support	Release 99 USIM onwards	Release 99 USIM onwards
Transport mechanisms	Circuit & packet switching	Packet switching
CS domain components	MSC server, MGW	n/a
PS domain components	SGSN, GGSN	MME, S-GW, P-GW
IP connectivity	After registration	During registration
Voice and SMS applications	Included	External

LTE Frequency Bands

- Typical LTE frequency bands simultaneously supported by high-end devices, sorted by region
- List not complete, new bands frequently added
- LTE band 20 called *Digital Dividend* band
- Band 8 (900MHz) originally meant for GSM is now partially used for LTE up to 10MHz

Band	Downlink (DL) (MHz)	Uplink (UL) (MHz)	Duplex mode	Carrier bandwidth (MHz) typically used	Total bandwidth available in the band
Europe					
3	1805–1880	1710–1785	FDD	20	75
7	2620–2690	2500–2570	FDD	20	70
8	925–960	880–915	FDD	10	35
20	791–821	832–862	FDD	10	30
38	2570–2620	2570–2620	TDD	20	50
Japan					
1	2110–2170	1920–1980	FDD	20	60
18	860–875	815–830	FDD	15	15
19	875–890	830–845	FDD	15	15
28	758–803	703–748	FDD	20	45
United States					
2	1930–1990	1850–1910	FDD	10–20	60
4	2110–2155	1710–1755	FDD	10	45
5	869–894	824–849	FDD	10	25
12	729–746	699–716	FDD	15	15
13	746–756	777–787	FDD	10	10
17	734–746	704–716	FDD	10	10
25	1930–1995	1850–1915	FDD	10–20	55
26	859–894	814–849	FDD	10	35
27	852–869	807–824	FDD	10–15	15
China					
38	2570–2620	2570–2620	TDD	10–20	50
39	1880–1920	1880–1920	TDD	20	40
40	2300–2400	2300–2400	TDD	20	100
41	2496–2690	2496–2690	TDD	20	90

4G Spectrum Allocation in the UK

- Result of Ofcom's 4G spectrum auction from March 2013

Licensee	Frequencies assigned
Everything Everywhere Limited	796 to 801 MHz and 837 to 842 MHz
	2535 to 2570 MHz and 2655 to 2690 MHz
Hutchison 3G UK Limited	791 to 796 MHz and 832 to 837 MHz
Niche Spectrum Ventures Limited	2520 to 2535 MHz and 2640 to 2655 MHz
	2595 to 2620 MHz
Telefónica UK Limited	811 to 821 MHz and 852 to 862 MHz
Vodafone Limited	801 to 811 MHz and 842 to 852 MHz
	2500 to 2520 MHz and 2620 to 2640 MHz
	2570 to 2595 MHz

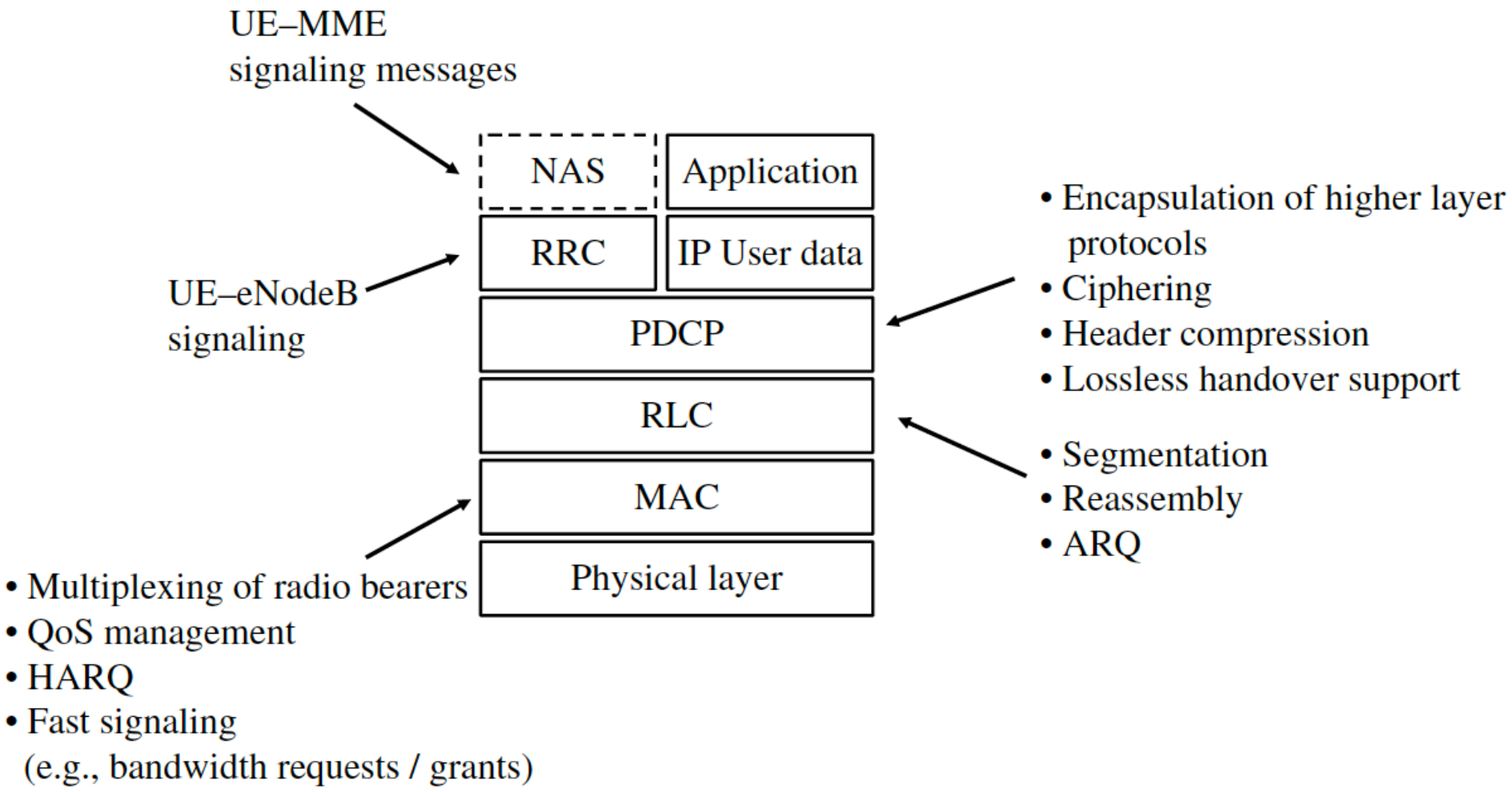
Additional LTE Frequency Bands Coming Soon

- Band 1 (2100 MHz) originally meant for UMTS is also expected to be used for LTE in future
- Digital Dividend 2 (700MHz) band: 758-788MHz (downlink) and 703-733MHz (uplink)
- Band 32 (1452-1492MHz): 40MHz downlink only would be available for carrier aggregation purposes
- On-going Ofcom spectrum auction in the UK for:
  - 40MHz in 2.3GHz band
  - 150MHz in 3.4GHz band

Antenna and Receiver Design Challenge for Multi-Band LTE Devices

- Most LTE-capable devices also support other radio access technologies (RATs) such as GSM and UMTS
- So a typical high-end LTE device needs to support:
  - 20 LTE frequency bands (in the range of 700-2600MHz)
  - plus bands for other RATs (900 and 1800MHz for GSM; 900 and 2100MHz for UMTS; 850 and 1900MHz for international GSM and UMTS roaming; …)
- Antenna design challenge: sensitivity of device's antennas must be equally good in all supported bands
- Adding more input ports to support increasing number of bands reduces overall receiver sensitivity ➔ challenge for receiver chips that needs to be compensated by advances in receiver technology

LTE Air Interface Protocol Stack

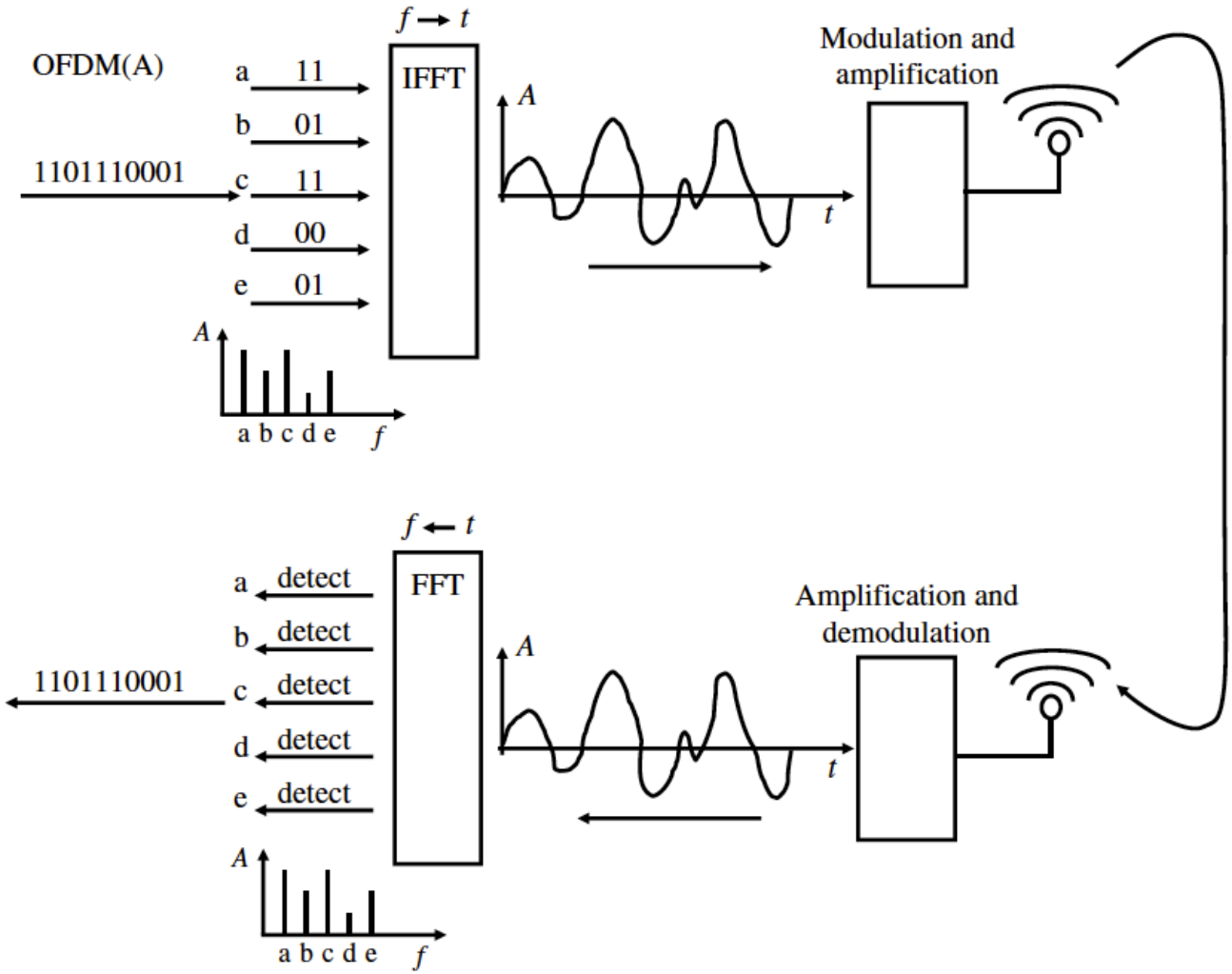


LTE Radio Transmission Scheme

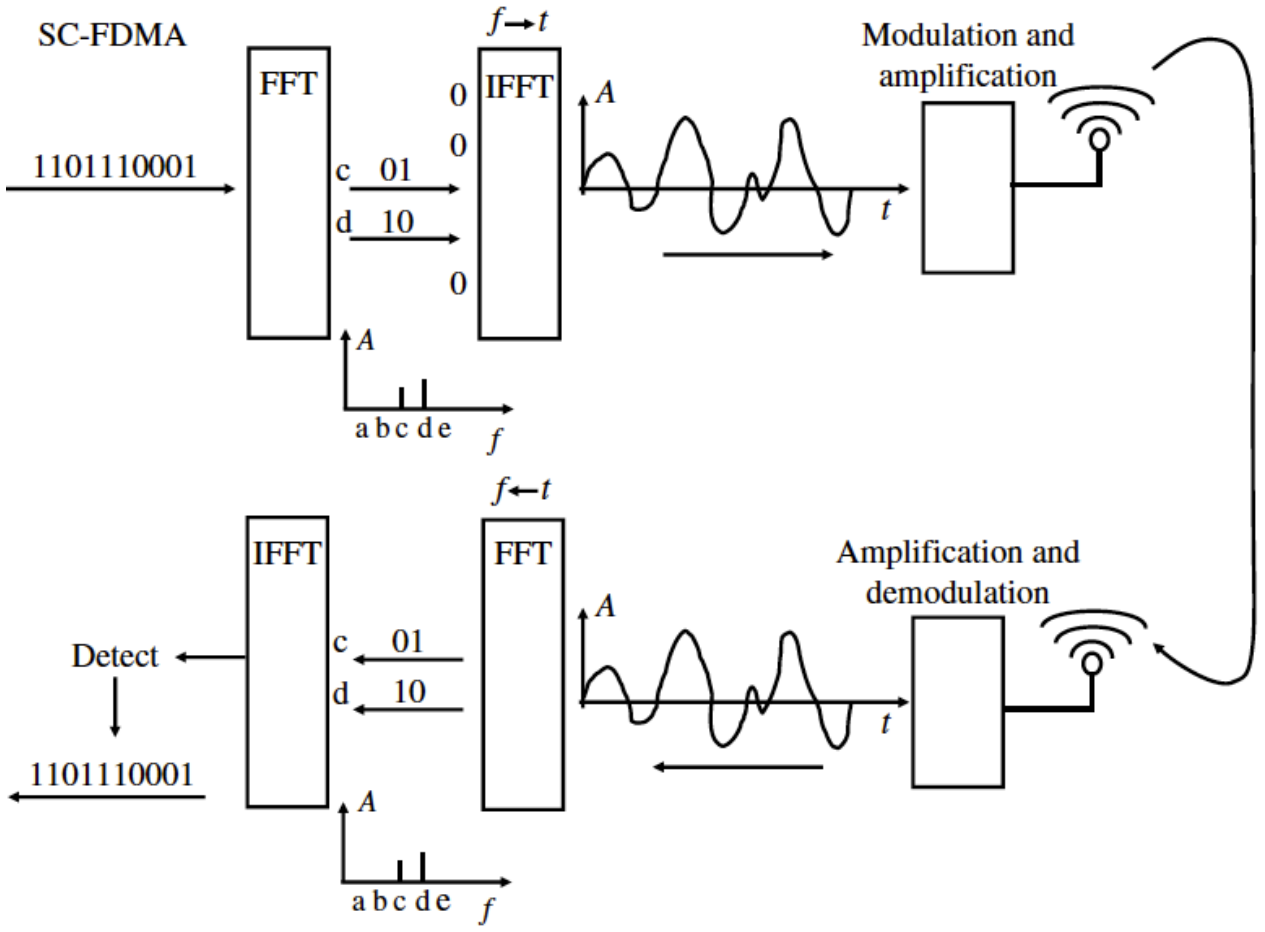
- **Orthogonal Frequency Division Multiple Access (OFDMA) for the downlink**: OFDM based multiple access scheme that allocates different users to different subsets of subcarriers
- A variant of OFDMA called **single carrier FDMA (SC-FDMA) in the uplink direction** to suit lower cost and battery operated mobile transmitters with non-linear amplifiers

School of Informatics
Institute for Computing Systems Architecture

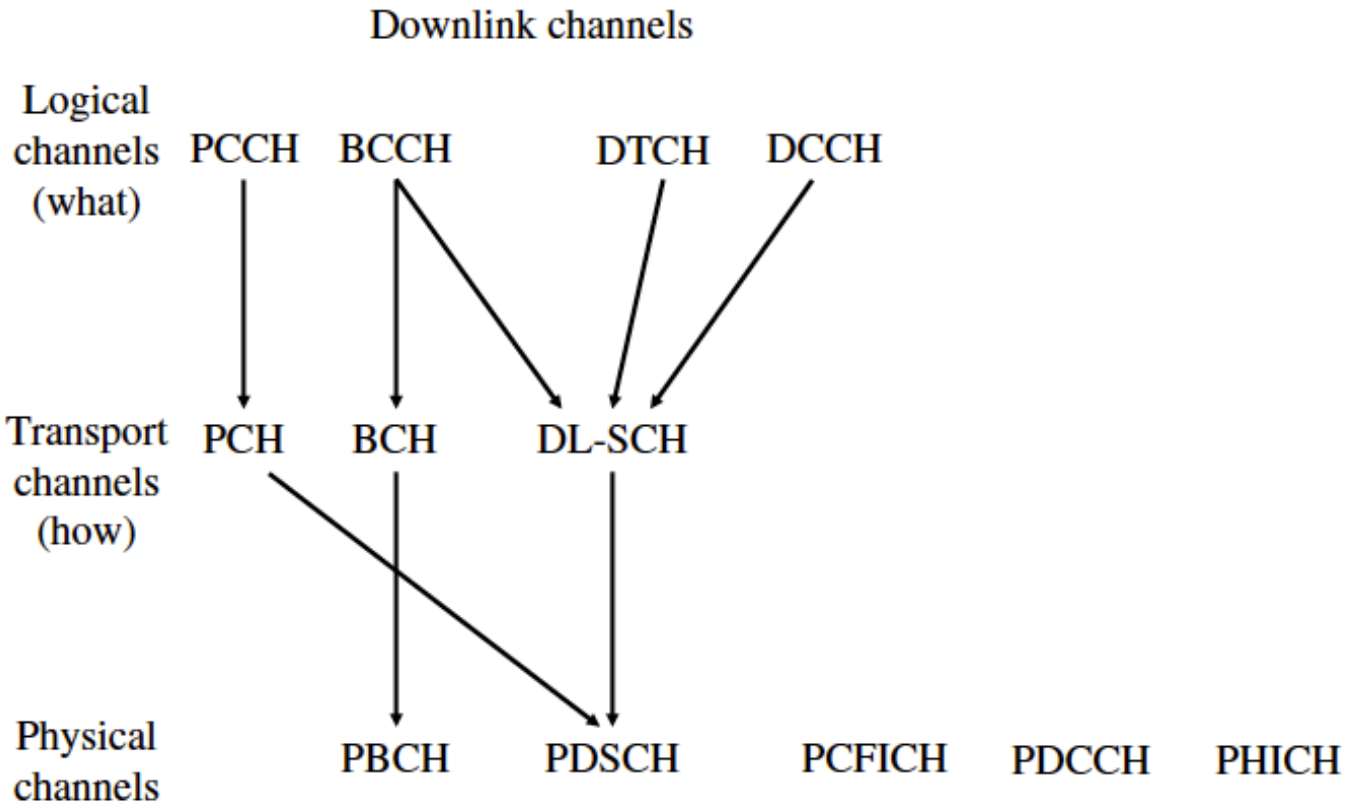
OFDMA



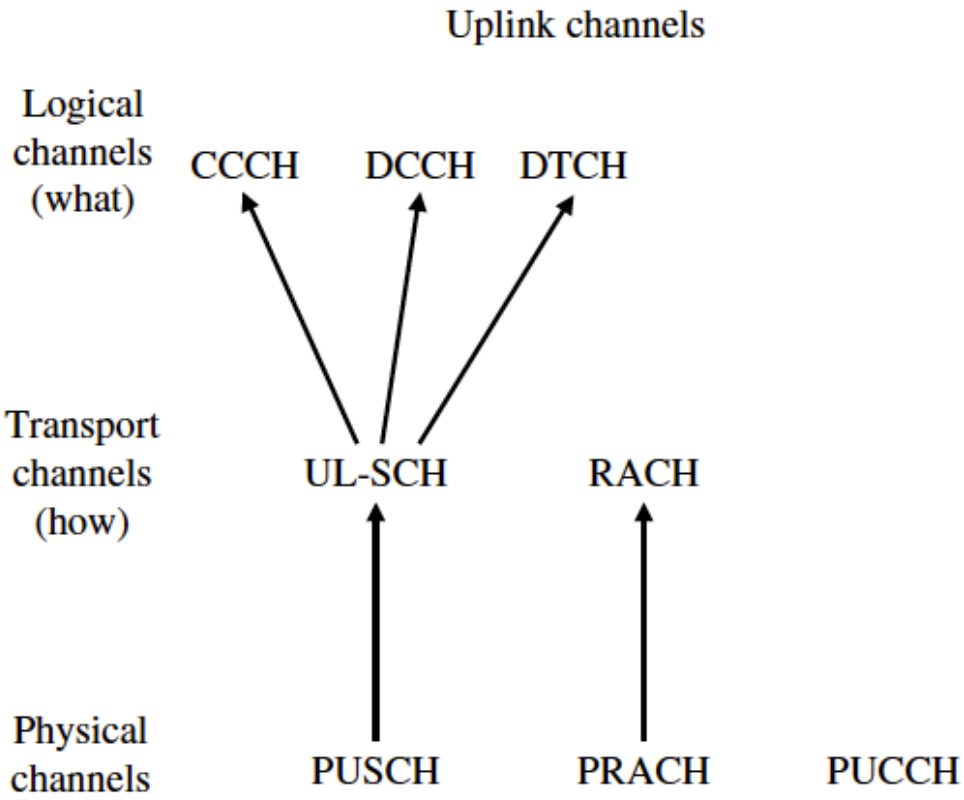
SC-FDMA



LTE Downlink Channels

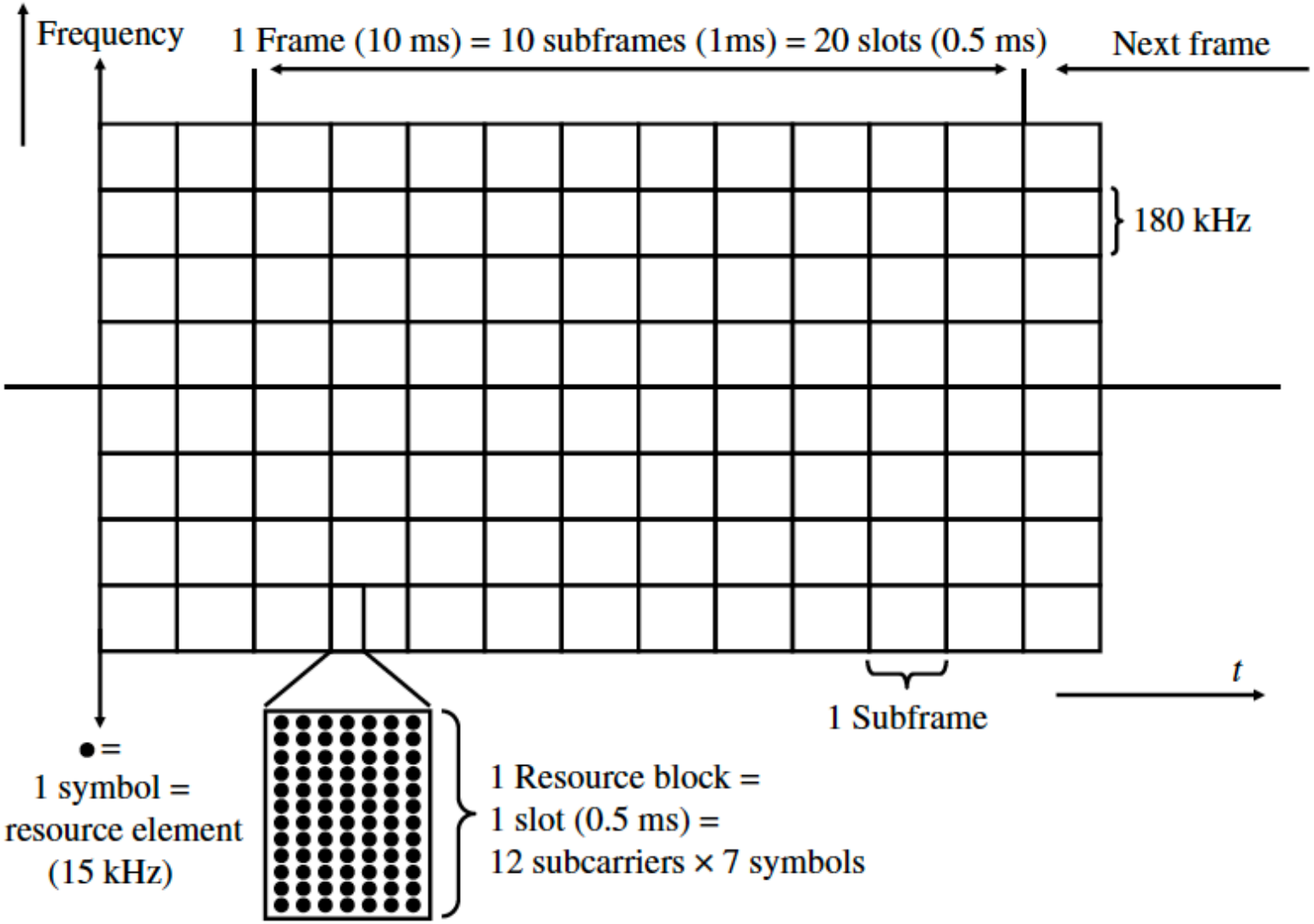


LTE Uplink Channels



LTE Resource Grid

- Resource block (RB) is the smallest unit of resource allocated to a user



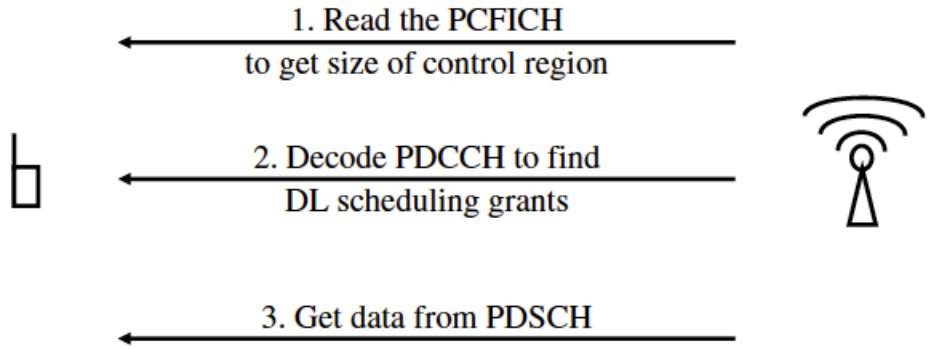
Scheduling

- In LTE, both uplink and downlink data transmissions are controlled by the eNode-B (network)
- The resource scheduling problem concerns who to allocate resources in each scheduling round and how much in both downlink and uplink
- This decision is influenced by several factors incl. user QoS requirements, channel conditions
- In LTE, scheduling done at the granularity of subframes (i.e., every 1 millisecond)
- No. of RBs in each subframe dependent on system bandwidth (e.g., 50 RBs with a 10MHz carrier)

Bandwidth (MHz)	Number of subcarriers
1.25	76
2.5	150
5	300
10	600
15	900
20	1200

Downlink Scheduling

- Dynamic scheduling
  - In each subframe, eNode-B decides the number of users it wants to schedule and the number of RBs that are assigned to each user ➔ determines the size of the control region in the PDCCH for each device to decode its scheduling grant
  - eNode-B has several ways to indicate a resource allocation:
    - Type 0 allocation give a bitmap of assigned RB groups
    - Type 1 also use a bitmap but allocation spread across groups
    - Type 2 allocation specifies starting point in the frequency domain and number of allocated resources



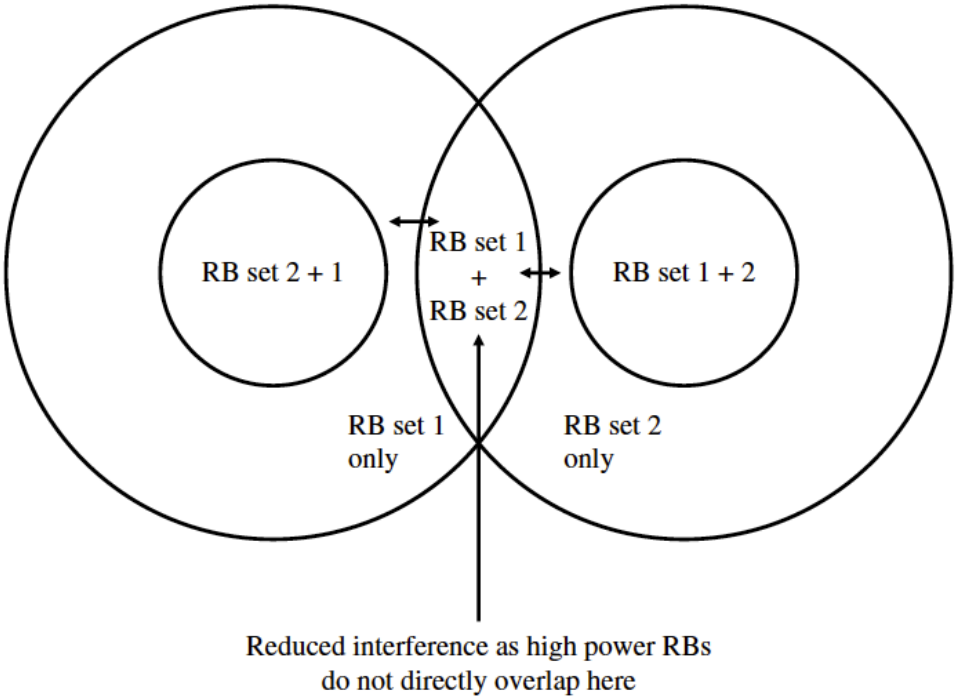
- For low-rate periodic data (e.g., voice calls), **semi-persistent scheduling** can be used to reduce assignment overhead

Uplink Scheduling

- To get resources assigned on the uplink shared channel (PUSCH), a mobile device needs to send an assignment request to the eNode-B
- Assignment of uplink resources performed via PDCCH messages
- Mobile devices expected to send buffer status reports in the header of each packet when actively communicating, or via uplink control channel (PUCCH) when no uplink shared resources are allocated to the device
- eNode-B uses the power headroom reports in the uplink direction to decide on the appropriate modulation and coding scheme and number of RBs

Single Frequency Network and Cell Edge Performance

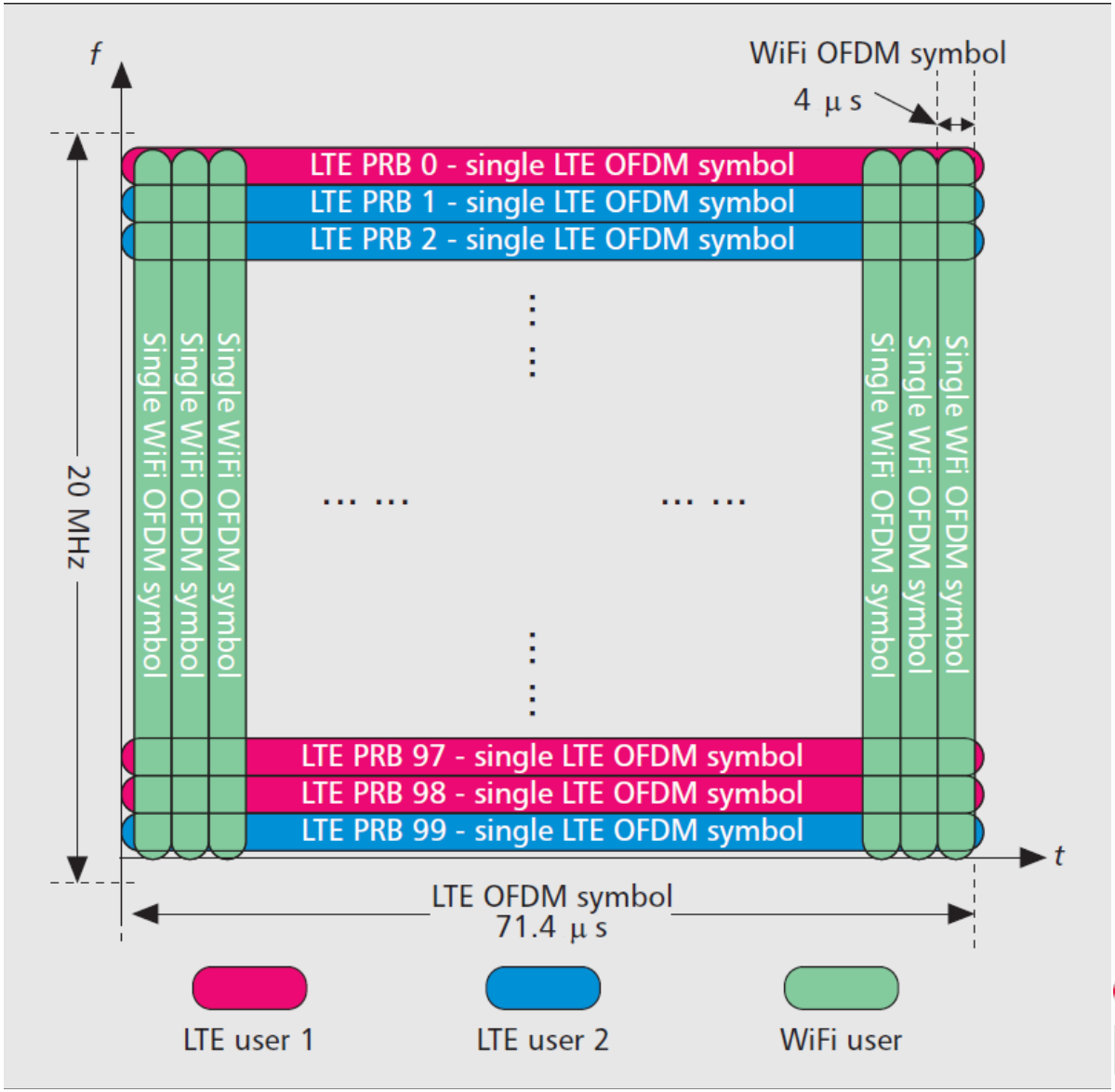
- By default, LTE is a single frequency network meaning all cells reuse the same carrier frequencies (i.e., frequency reuse factor of 1)
- Devices in the overlapping coverage area of multiple neighboring cells can be subject to high interference due to receiving signals from several cells
- Neighboring eNBs can coordinate via the X2 interface to reduce interference to cell edge users ➔ **fractional frequency reuse (FFR)**
- Additionally, power control at the RB level can be used by each eNB
- Uplink interference management can be done by each eNB via its RB allocation



Key Features of Air Interfaces of WCDMA (in UMTS) and LTE

Feature	WCDMA	LTE
Multiple access scheme	WCDMA	OFDMA and SC-FDMA
Frequency re-use	100%	Flexible
Use of MIMO antennas	From Release 7	Yes
Bandwidth	5 MHz	1.4, 3, 5, 10, 15 or 20 MHz
Frame duration	10 ms	10 ms
Transmission time interval	2 or 10 ms	1 ms
Modes of operation	FDD and TDD	FDD and TDD
Uplink timing advance	Not required	Required
Transport channels	Dedicated and shared	Shared
Uplink power control	Fast	Slow

Comparing LTE and Wi-Fi



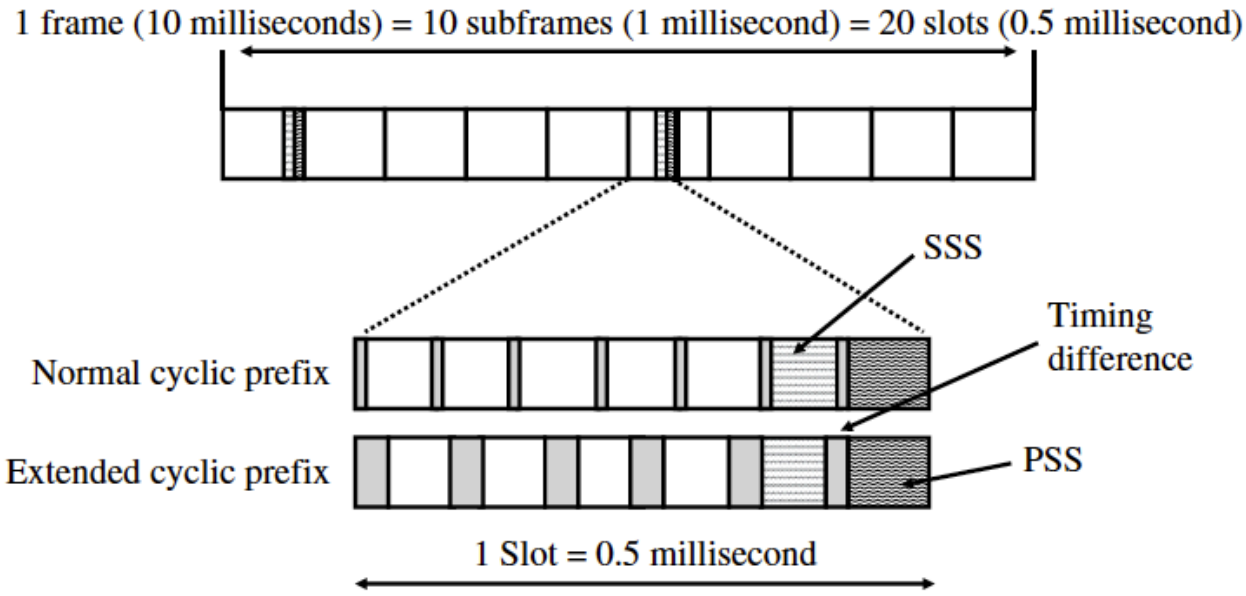
School of Informatics
Institute for Computing Systems Architecture

Cell Search

- When a device is powered on, first task is to search for a suitable network and then attempt to register
  - Guided by the info stored on the SIM card (e.g., access technology field)
- Search process is shortened via stored parameters of the last cell used before switching off
- If can't find previous cell with stored info, then **full search**
  1. Search all channels in all supported frequency bands to pick up primary synchronization signal (PSS), broadcasted twice per frame
  2. Locate secondary synchronization signal (SSS)
     - SSS content alternated in every frame to help device find the start of frame

PSS and SSS in an LTE FDD frame

- PSS and SSS broadcast only on the inner 1.25MHz of the channel, irrespective of the channel bandwidth
- Both PSSs and SSSs implicitly contain the Physical Cell Identity (PCI) to distinguish neighboring cells transmitting on same frequency
- PSS and SSS detection also allows the device to determine if the cell is using normal or extended cyclic prefix because of their timing differences

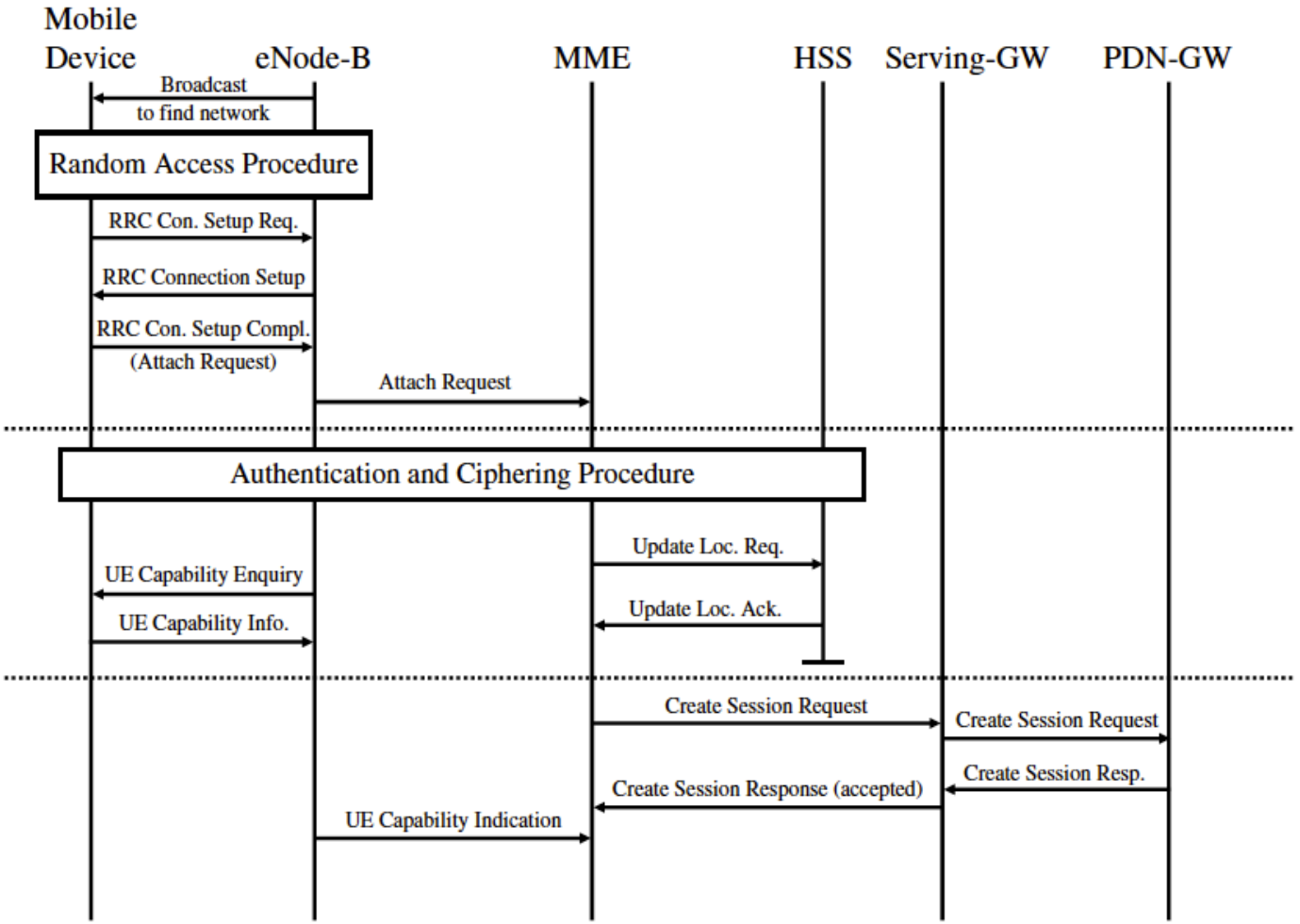


Cell Search (contd.)

- Full search procedure (contd.)
  3. Read the MIB from PBCH, broadcast every 40ms in inner 1.25MHz of the channel
     - Contains the most important info about configuration of the channel, incl. channel bandwidth, structure of HARQ indicator channel, system frame number (SFN)
  4. With info from MIB, begin search for SIB 1, broadcast on downlink shared channel every 80ms, to get the following info:
     - MCC and MNC of the cell, NAS cell identifier, tracking area code (TAC), cell barring status, minimum reception level, scheduling list of when other SIBs are sent
  5. With info in SIB 1, device can decide if it wants to communicate with the cell and accordingly search for and decode further system info messages
     - E.g., SIB 2 contains further parameters incl. configurations of RACH, paging channel, downlink shared channel, PUCCH; SRS configuration in the uplink; uplink power control info; uplink channel bandwidth

Attach and default bearer activation message flow – Part 1

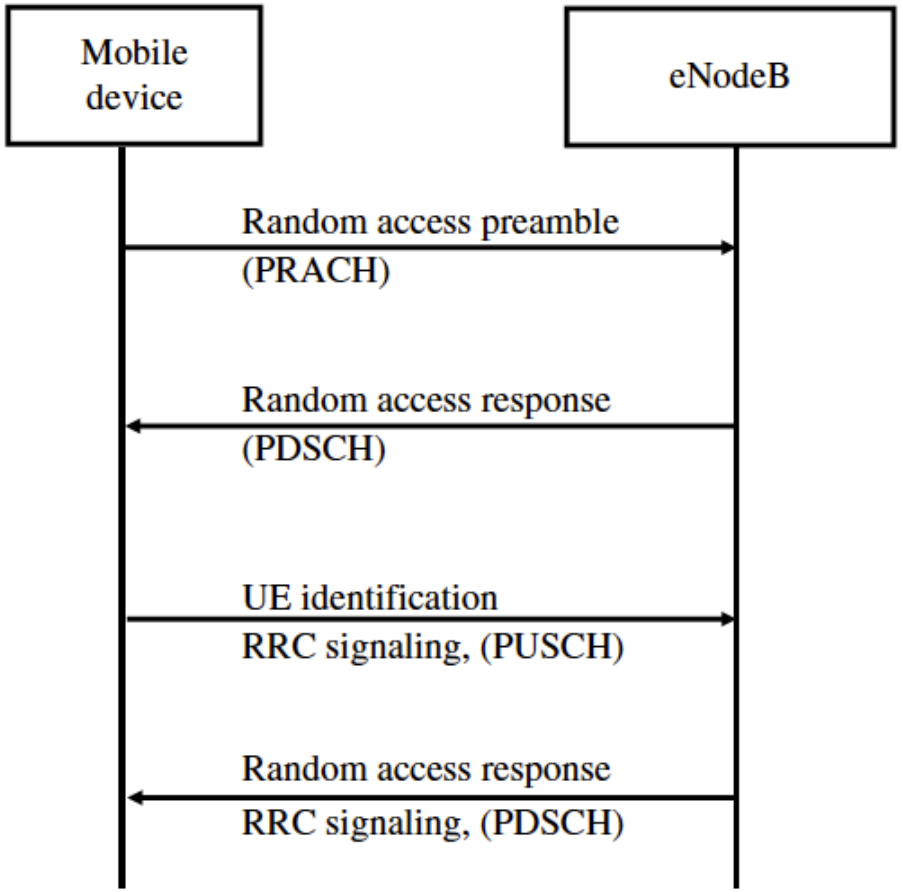
- Once device has required info to access the network after power on, performs **attach** procedure to get IP address and send/receive data over the network



Random Access Procedure

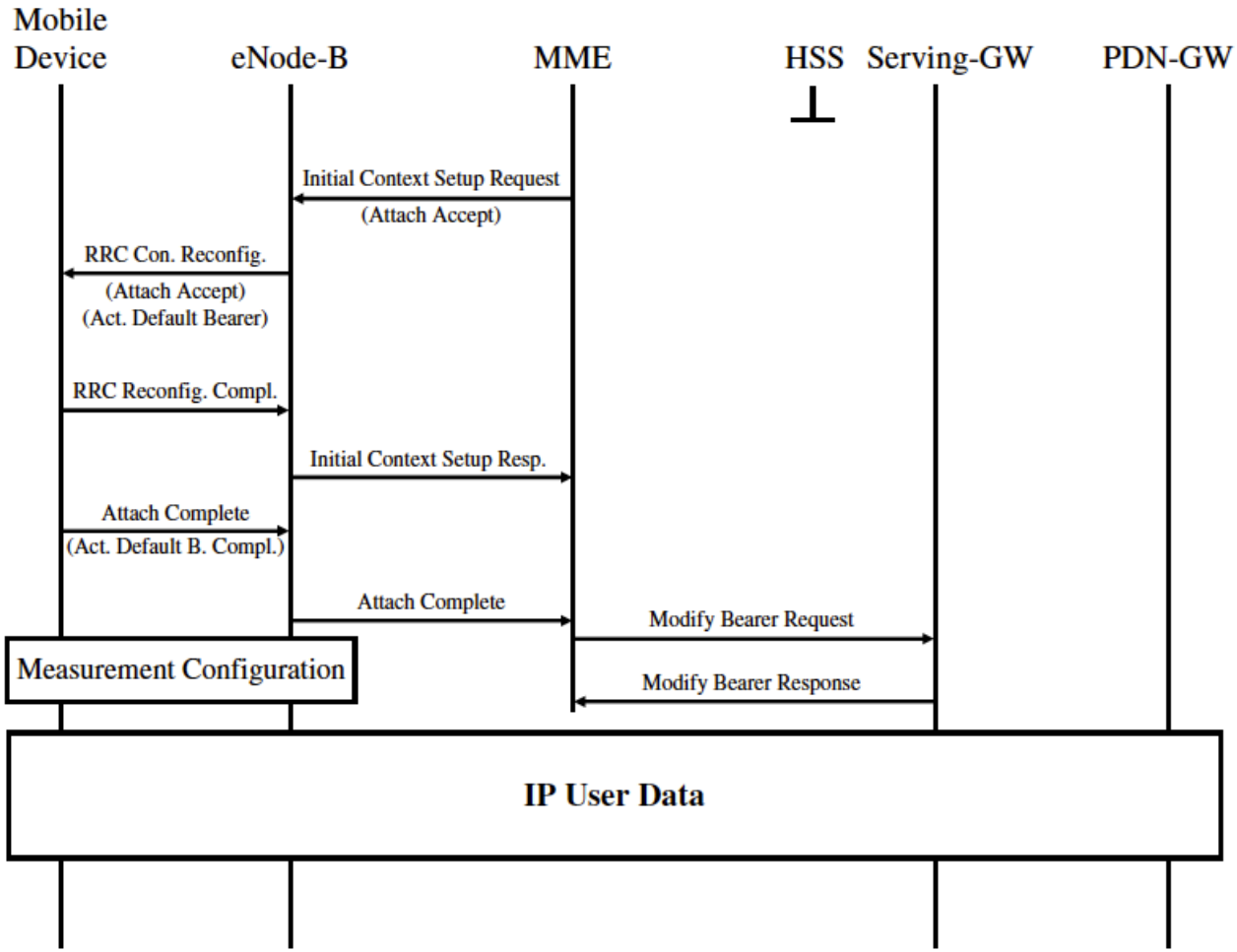
- Once this procedure has been performed, the mobile device is known to the eNode-B and has been assigned a Cell Radio Network Temporary Identity (C-RNTI)

- This MAC-layer ID is used, for example, in scheduling grants that are sent in downlink control channel (PDCCH) messages



Attach and default bearer activation message flow – Part 2

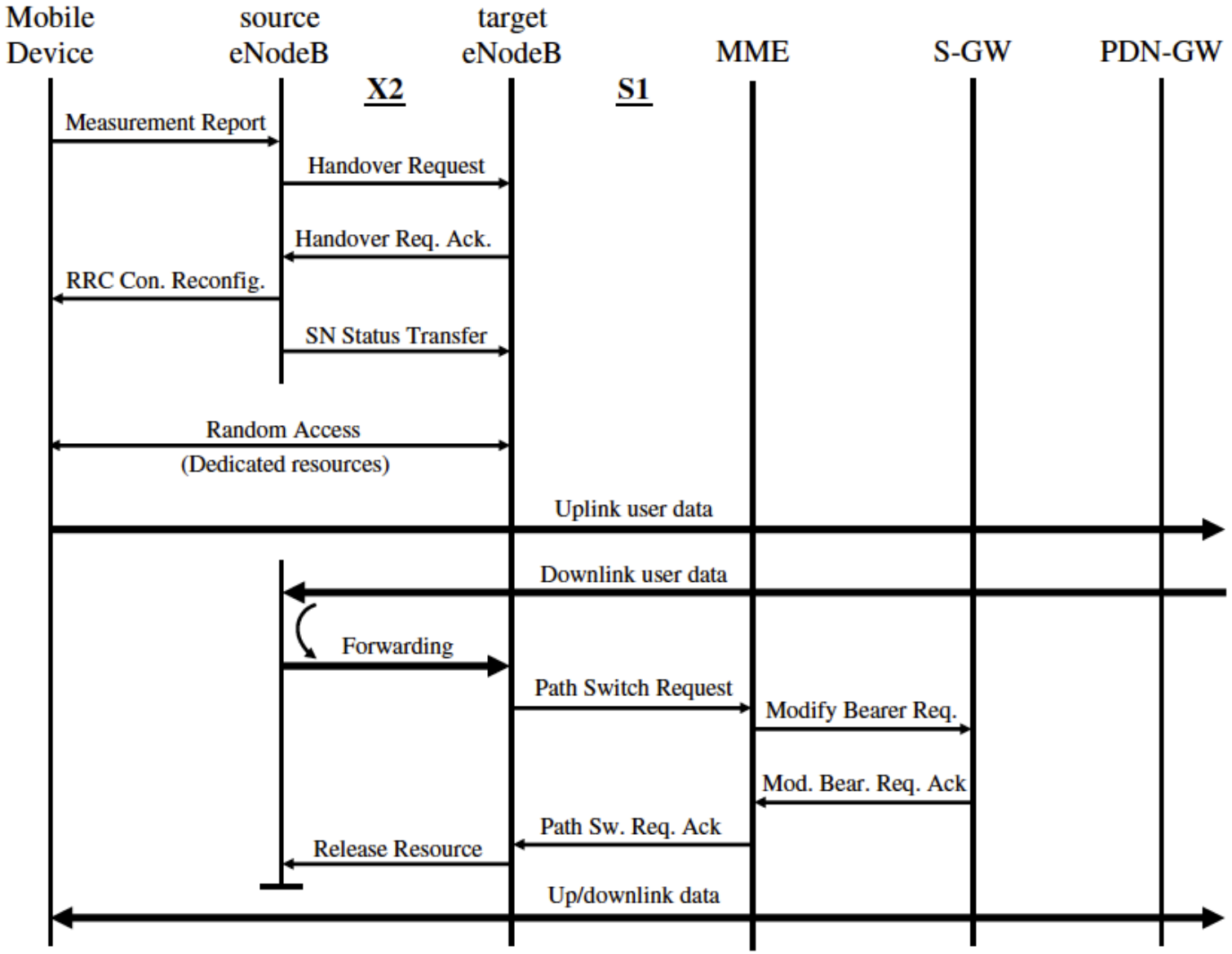
- Rest of the attach procedure establishes the user data tunnel between eNode-B and S-GW, and default data radio bearer (DRB) on the air interface
- The whole procedure executed usually in fraction of a second



Handover Scenarios

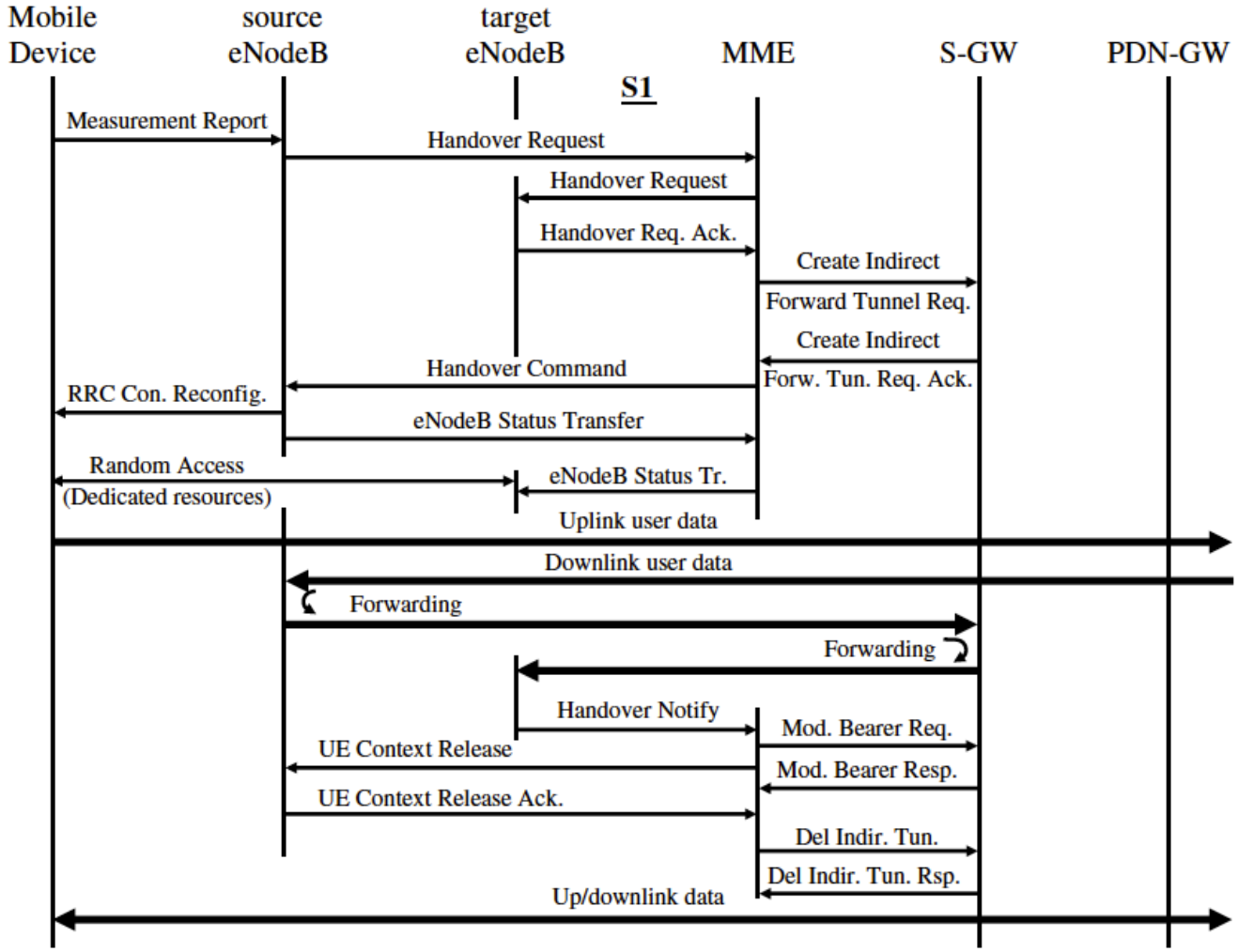
- Based on the measurement info from the device, eNode-B decides if a handover is necessary
- Potential benefits of handover:
  - Avoid connection failure
  - Improve data throughput in both uplink and downlink
  - Reduce power required for uplink transmissions and reduce overall interference
- In LTE, two types of handover:
  - **X2 handover**: source and target eNode-Bs directly communicate with each other over the X2 interface
  - **S1 handover**: handover signaling takes place over the S1 interface and MME assists in the process

X2 Handover



S1 Handover

- From a mobile device viewpoint, no difference between X2 and S1 handovers
- S1 handover takes a bit longer than X2 handover but typically executed within just a few hundred milliseconds



Further Cases

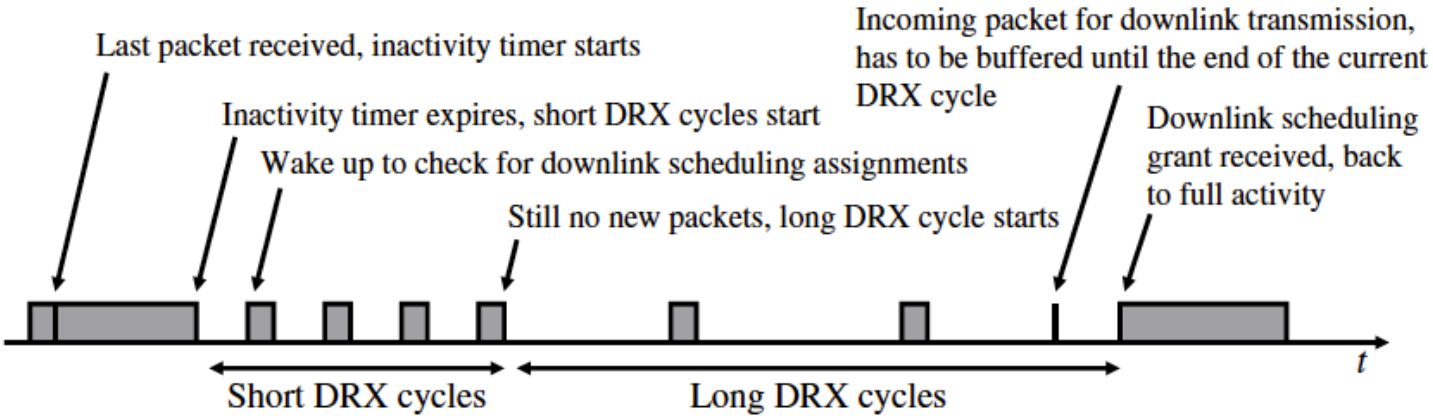
- Tracking area update
- Core network node (MME, S-GW) changes
- Establishing dedicated bearers to match QoS requirements
- Additional IP addresses to the device with corresponding default and dedicated bearers

Mobility Management and Power Optimization

- In LTE, devices generally in one of two activity states: radio resource control (RRC) connected and RRC idle
- **Mobility management in RRC connected state:** when device in RRC connected state, it is fully synchronized with the network in both uplink and downlink directions, and can send/receive data at any time
  - Device actively monitors signals from serving and neighboring cells and reports measurements to serving eNode-B
  - Handover decision made by eNode-B based on those measurements (RSRP, RSSI, RSRQ = RSRP/RSSI)
  - Handover procedures as discussed so far

Discontinuous Reception (DRX) in Connected State to Save Power

- Continuously scanning for scheduling grants in each subframe every millisecond power consuming if throughput requirements of device low
- So LTE allows configuring a device to only periodically check for scheduling assignments *aka* DRX
- In DRX state, device has to continue to send occasional measurement reports (downlink channel quality indications, uplink transmissions for measurements on network side, power headroom reports)
  - This can be turned off at the expense of random access procedure to resume communication



Mobility Management in RRC Idle State

- Device enters RRC idle state after long period of inactivity to reduce the amount of signaling and power required to maintain the connection
  - Autonomously performs cell reselections so long as within same tracking area
  - No physical radio bearer and S1 user data tunnel between eNB and S-GW
  - Radio module on the device can be deactivated for long periods specified by the paging interval (1-2 seconds) ➔ **DRX in the Idle State**
  - When data needs to be sent on uplink, switch to connected state (similar to search and attach procedure)
  - On arrival of data in the downlink direction, device paged via all eNBs in the whole tracking area

School of Informatics
Institute for Computing Systems Architecture

Mobility Management and State Changes in Practice

- Some example configurations by network operators in practice

Network 1:

- Time until DRX is enabled: 100 ms;
- DRX short cycle time: 80 ms;
- DRX long cycle time: 200 ms;
- On-duration: 10 ms;
- Time alignment: 10.2 seconds;
- Time until idle: –.

Network 2:

- Time until DRX is enabled: 200 ms;
- DRX short cycle time: 40 ms;
- DRX long cycle time: 320 ms;
- On-duration: 10 ms;
- Time alignment: infinity;
- Time until idle: –.

Network 3:

- Time until DRX is enabled: 200 ms;
- DRX short cycle time: none;
- DRX long cycle time: 80 ms;
- On-duration: 4 ms;
- Time alignment: 1.92 seconds;
- Time until idle: 30 seconds.

Network 4:

- No DRX configured;
- Time until idle: 5 seconds.

Key Features of Radio Access Networks of UMTS and LTE

Feature	UMTS	LTE
Radio access network components	Node B, RNC	eNB
RRC protocol states	CELL_DCH, CELL_FACH, CELL_PCH, URA_PCH, RRC_IDLE	RRC_CONNECTED, RRC_IDLE
Handovers	Soft and hard	Hard
Neighbour lists	Always required	Not required

School of Informatics
Institute for Computing Systems Architecture

Functional split of major LTE components