Security in GSM

Dr. Yeffry Handoko Putra

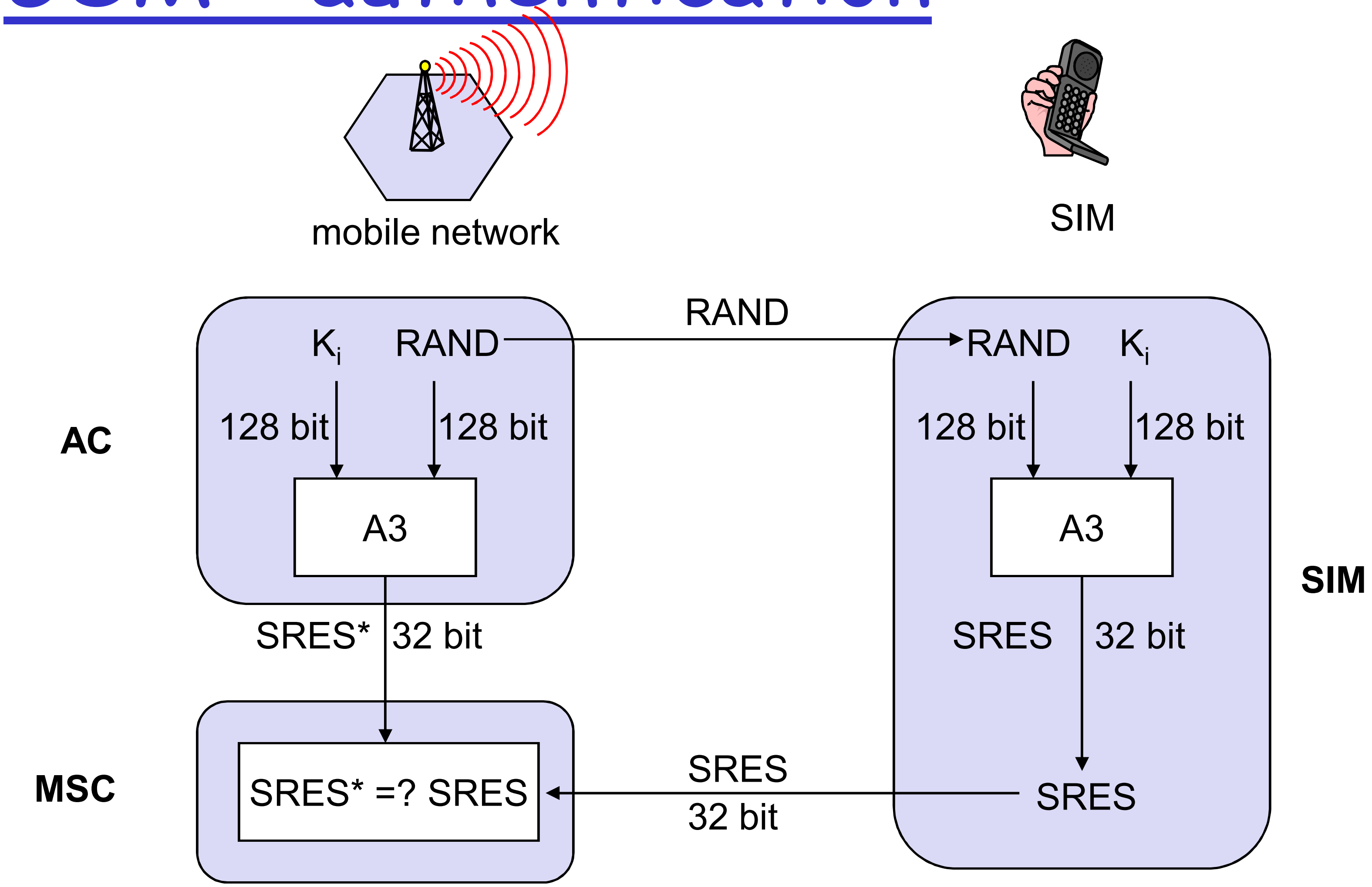
Department of Computer Engineering
Universitas Komputer Indonesia

Security in GSM

- Security services
  - access control/authentication
    - user ⇔ SIM (Subscriber Identity Module): secret PIN (personal identification number)
    - SIM ⇔ network: challenge response method
  - confidentiality
    - voice and signaling encrypted on the wireless link (after successful authentication)
  - anonymity
    - temporary identity TMSI (Temporary Mobile Subscriber Identity)
    - newly assigned at each new location update (LUP)
    - encrypted transmission
- 3 algorithms specified in GSM
  - A3 for authentication ("secret", open interface)
  - A5 for encryption (standardized)
  - A8 for key generation ("secret", open interface)

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

GSM - authentication



mobile network

SIM

AC

K_i

RAND

128 bit

128 bit

A3

SRES*

32 bit

MSC

SRES* =? SRES

RAND

RAND

K_i

128 bit

128 bit

A3

SRES

32 bit

SIM

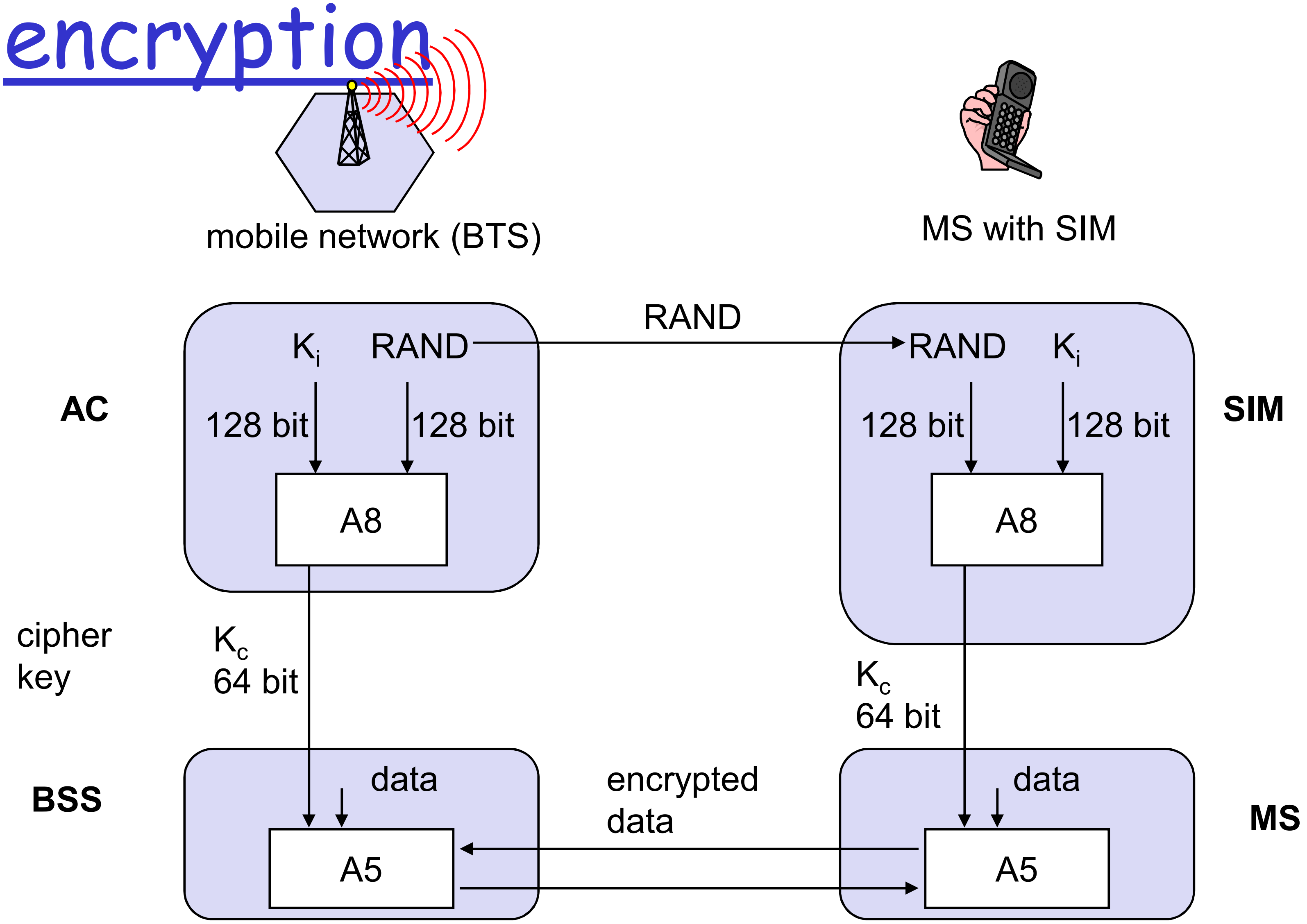
SRES

SRES

32 bit

K_i: individual subscriber authentication key SRES: signed response

GSM - key generation and encryption



mobile network (BTS)

MS with SIM

AC

K_i

RAND

128 bit

128 bit

A8

RAND

RAND

K_i

128 bit

128 bit

A8

SIM

cipher key

K_c 64 bit

K_c 64 bit

BSS

data

A5

encrypted data

data

A5

MS

Data services in GSM I

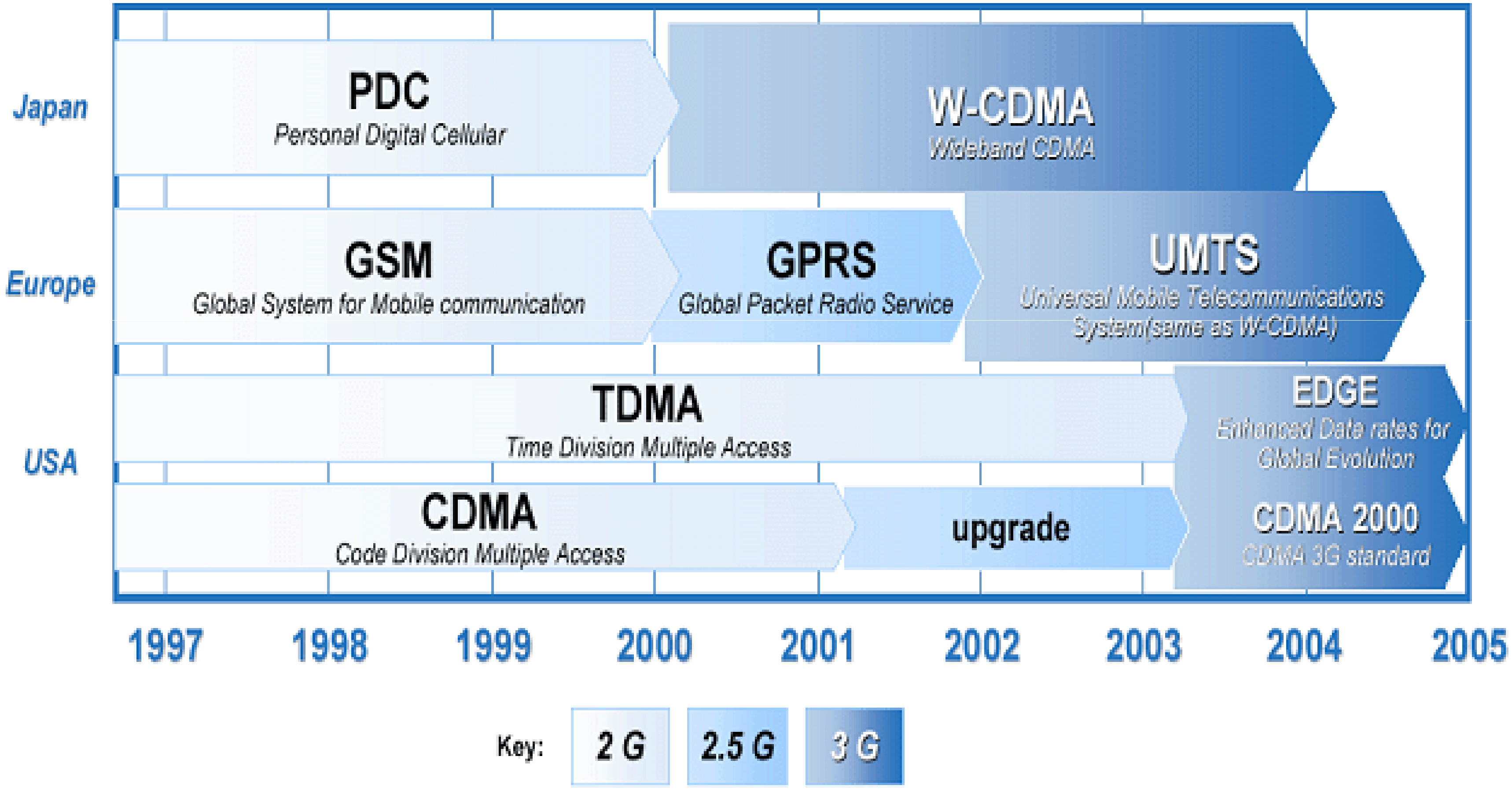
- Data transmission standardized with only 9.6 kbit/s
  - advanced coding allows 14.4 kbit/s
  - not enough for Internet and multimedia applications
- HSCSD (High-Speed Circuit Switched Data)
  - mainly software update
  - bundling of several time-slots to get higher AIUR (Air Interface User Rate, e.g., 57.6 kbit/s using 4 slots @ 14.4)
  - advantage: ready to use, constant quality, simple
  - disadvantage: channels blocked for voice transmission

AIUR [kbit/s]	TCH/F4.8	TCH/F9.6	TCH/F14.4
4.8	1		
9.6	2	1	
14.4	3		1
19.2	4	2	
28.8		3	2
38.4		4	
43.2			3
57.6			4

Data services in GSM II

- GPRS (General Packet Radio Service)
  - packet switching
  - using free slots only if data packets ready to send (e.g., 50 kbit/s using 4 slots temporarily)
  - standardization 1998, introduction 2001
  - advantage: one step towards UMTS, more flexible
  - disadvantage: more investment needed (new hardware)
- GPRS network elements
  - GSN (GPRS Support Nodes): GGSN and SGSN
  - GGSN (Gateway GSN)
    - interworking unit between GPRS and PDN (Packet Data Network)
  - SGSN (Serving GSN)
    - supports the MS (location, billing, security)
  - GR (GPRS Register)
    - user addresses

Timeline of Technology Evolution


Japan
Europe
USA
PDC
Personal Digital Cellular
W-CDMA
Wideband CDMA
GSM
Global System for Mobile communication
GPRS
Global Packet Radio Service
UMTS
Universal Mobile Telecommunications System(same as W-CDMA)
TDMA
Time Division Multiple Access
EDGE
Enhanced Data rates for Global Evolution
CDMA
Code Division Multiple Access
upgrade
CDMA 2000
CDMA 3G standard
1997
1998
1999
2000
2001
2002
2003
2004
2005
Key:
2 G
2.5 G
3 G

GPRS quality of service

Reliability class	Lost SDU probability	Duplicate SDU probability	Out of sequence SDU probability	Corrupt SDU probability
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}

Delay class	SDU size 128 byte		SDU size 1024 byte	
	mean	95 percentile	mean	95 percentile
1	< 0.5 s	< 1.5 s	< 2 s	< 7 s
2	< 5 s	< 25 s	< 15 s	< 75 s
3	< 50 s	< 250 s	< 75 s	< 375 s
4	unspecified			

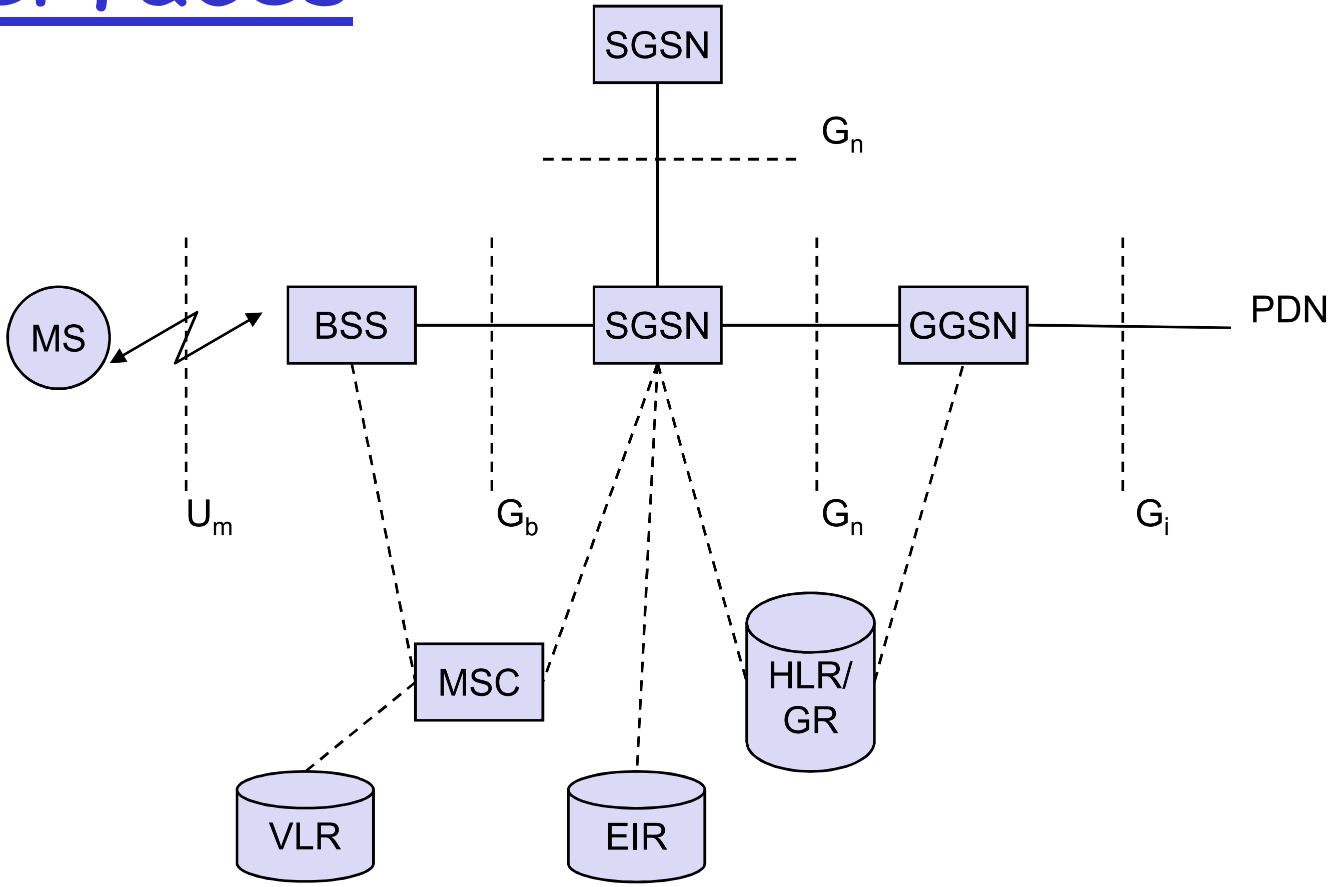
Examples for GPRS device classes

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

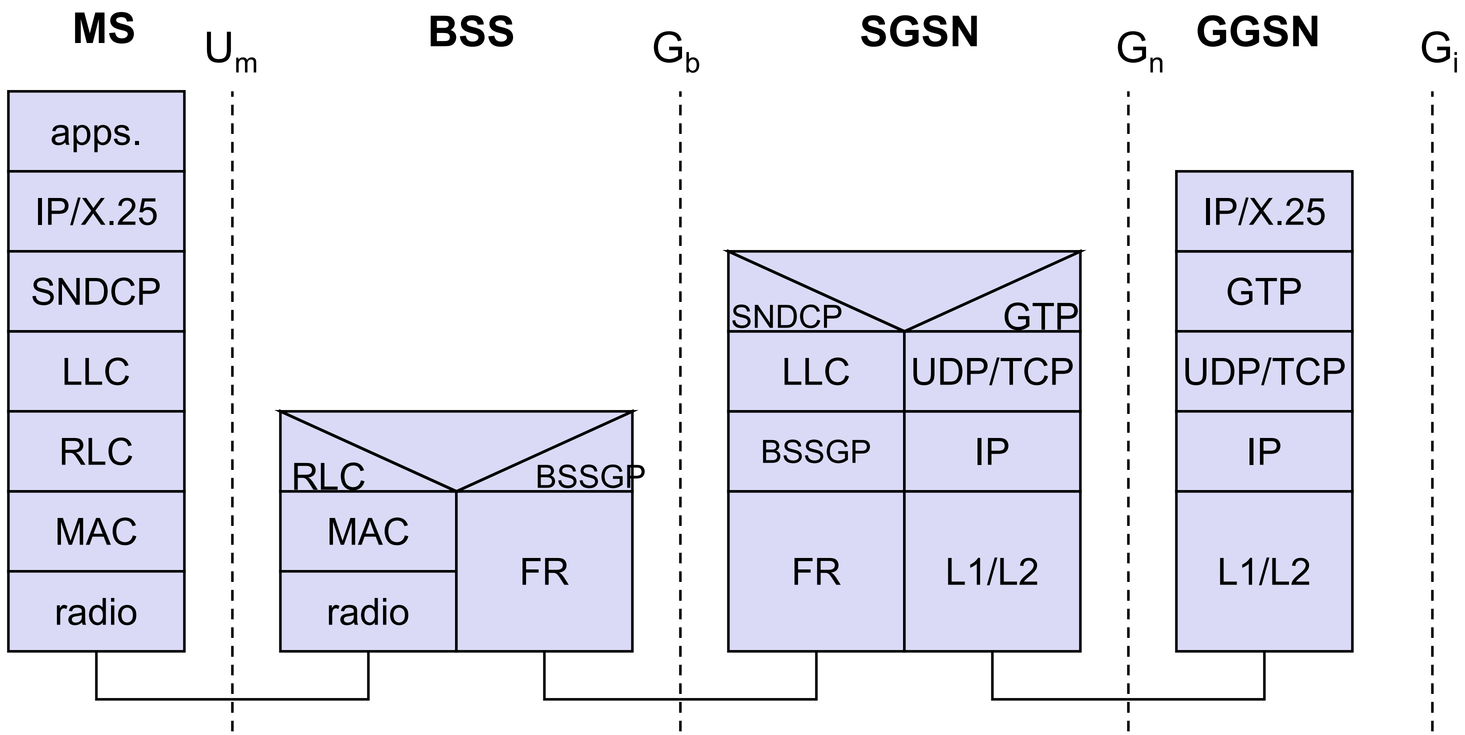
GPRS user data rates in kbit/s

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

GPRS architecture and interfaces



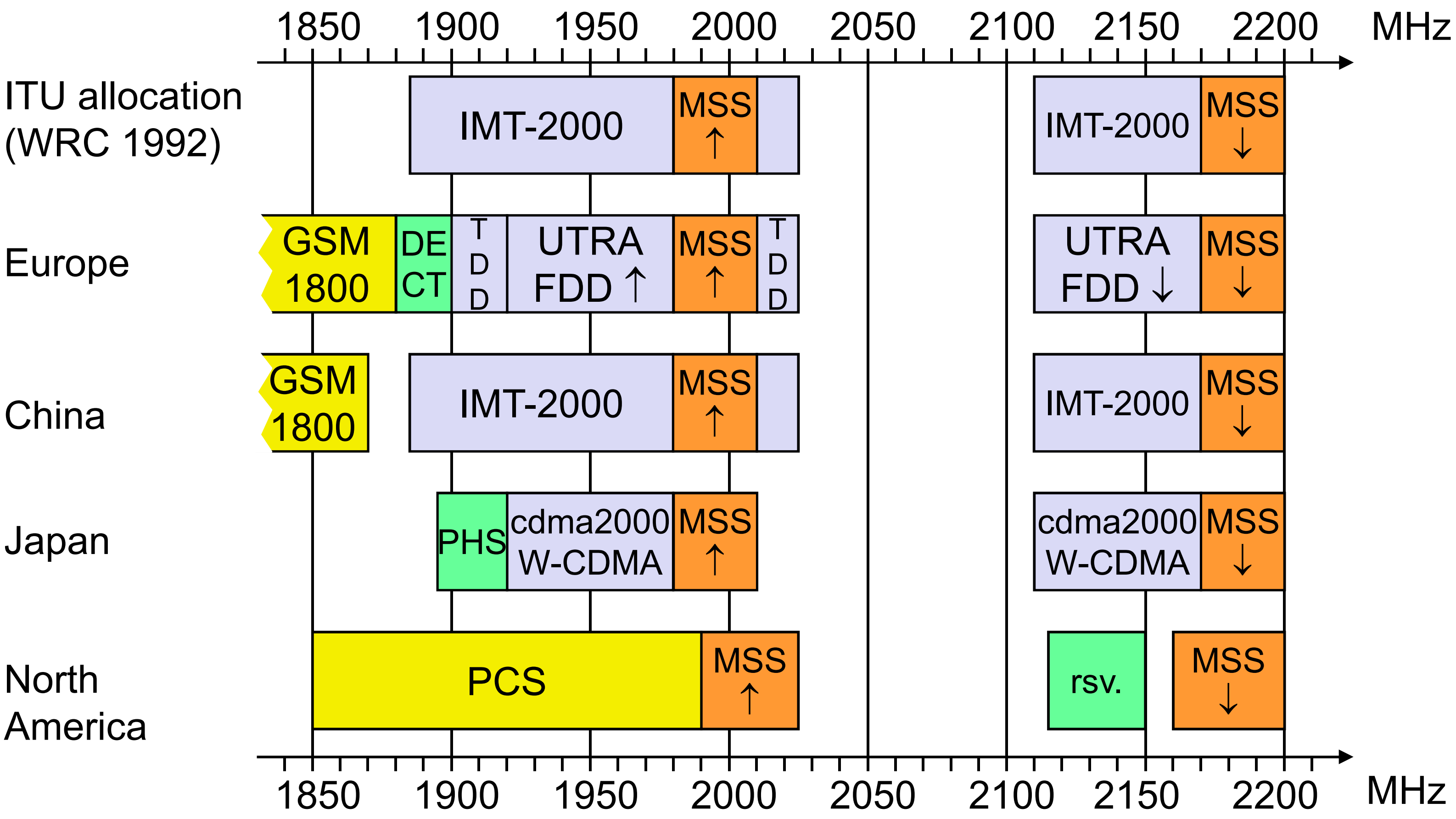
GPRS protocol architecture



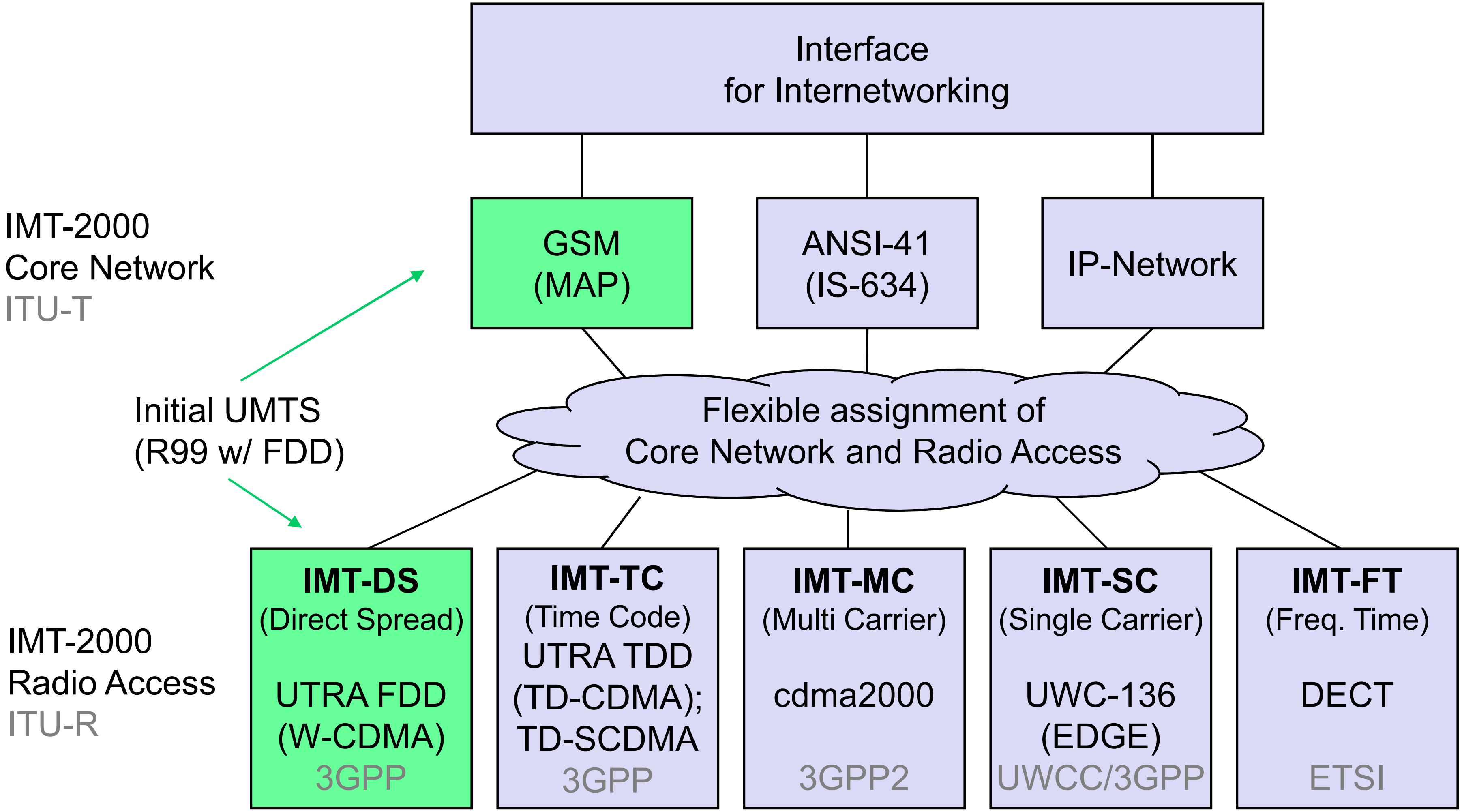
UMTS and IMT-2000

- Proposals for IMT-2000 (International Mobile Telecommunications)
  - UWC-136, cdma2000, WP-CDMA
  - UMTS (Universal Mobile Telecommunications System) from ETSI
- UMTS
  - UTRA (was: UMTS, now: Universal Terrestrial Radio Access)
  - enhancements of GSM
    - EDGE (Enhanced Data rates for GSM Evolution): GSM up to 384 kbit/s
    - CAMEL (Customized Application for Mobile Enhanced Logic)
    - VHE (virtual Home Environment)
  - fits into GMM (Global Multimedia Mobility) initiative from ETSI
  - requirements
    - min. 144 kbit/s rural (goal: 384 kbit/s)
    - min. 384 kbit/s suburban (goal: 512 kbit/s)
    - up to 2 Mbit/s urban

Frequencies for IMT-2000



IMT-2000 family



Interface
for Internetworking

IMT-2000
Core Network
ITU-T

GSM
(MAP)

ANSI-41
(IS-634)

IP-Network

Initial UMTS
(R99 w/ FDD)

Flexible assignment of
Core Network and Radio Access

IMT-2000
Radio Access
ITU-R

IMT-DS
(Direct Spread)
UTRA FDD
(W-CDMA)
3GPP

IMT-TC
(Time Code)
UTRA TDD
(TD-CDMA);
TD-SCDMA
3GPP

IMT-MC
(Multi Carrier)
cdma2000
3GPP2

IMT-SC
(Single Carrier)
UWC-136
(EDGE)
UWCC/3GPP

IMT-FT
(Freq. Time)
DECT
ETSI

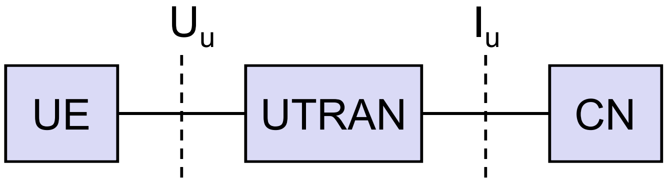
GSM and UMTS Releases

- Stages
  - (0: feasibility study)
  - 1: service description from a service-user's point of view
  - 2: logical analysis, breaking the problem down into functional elements and the information flows amongst them
  - 3: concrete implementation of the protocols between physical elements onto which the functional elements have been mapped
  - (4: test specifications)
- Note
  - "Release 2000" was used only temporarily and was eventually replaced by "Release 4" and "Release 5"
- Additional information:
  - www.3gpp.org/releases
  - www.3gpp.org/ftp/Specs/html-info/SpecReleaseMatrix.htm

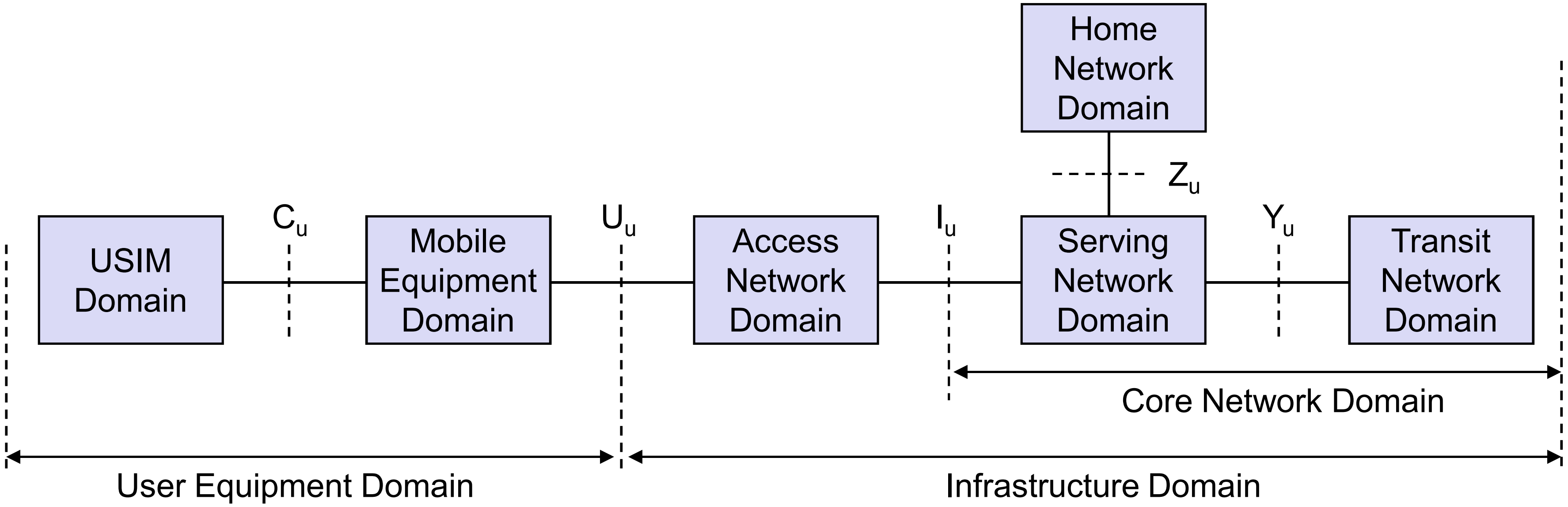
Rel	**Spec version number**	**Functional freeze date, indicative only**
Rel-10	10.x.y	Stage 1 ?
		Stage 2 ?
		Stage 3 ?
Rel-9	9.x.y	Stage 1 freeze December 2008
		Stage 2 June 2009?
		Stage 3 freeze December 2009?
Rel-8	8.x.y	Stage 1 freeze March 2008
		Stage 2 freeze June 2008
		Stage 3 freeze December 2008
Rel-7	7.x.y	Stage 1 freeze September 2005
		Stage 2 freeze September 2006
		Stage 3 freeze December 2007
Rel-6	6.x.y	December 2004 - March 2005
Rel-5	5.x.y	March - June 2002
Rel-4	4.x.y	March 2001
R00	4.x.y	see note 1 below
	9.x.y	
R99	3.x.y	March 2000
	8.x.y	
R98	7.x.y	early 1999
R97	6.x.y	early 1998
R96	5.x.y	early 1997
Ph2	4.x.y	1995
Ph1	3.x.y	1992

UMTS architecture (Release 99 used here!)

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



UMTS domains and interfaces I



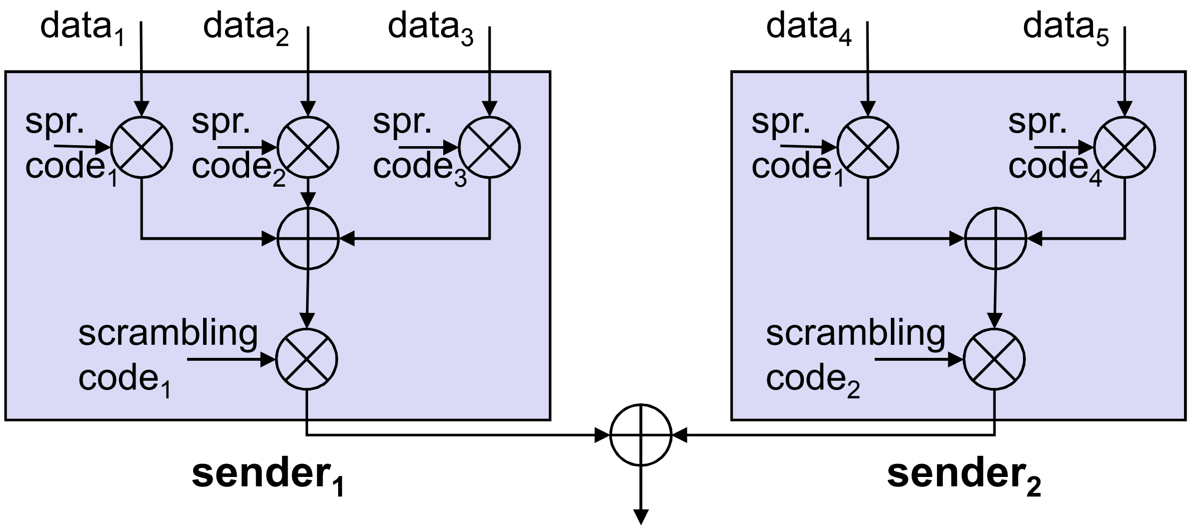
- User Equipment Domain
  - Assigned to a single user in order to access UMTS services
- Infrastructure Domain
  - Shared among all users
  - Offers UMTS services to all accepted users

UMTS domains and interfaces II

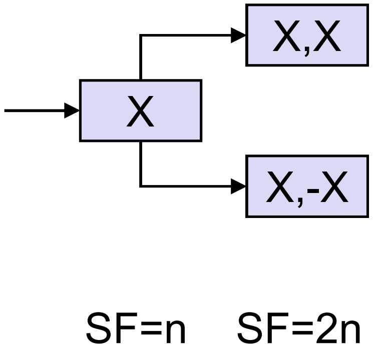
- Universal Subscriber Identity Module (USIM)
  - Functions for encryption and authentication of users
  - Located on a SIM inserted into a mobile device
- Mobile Equipment Domain
  - Functions for radio transmission
  - User interface for establishing/maintaining end-to-end connections
- Access Network 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

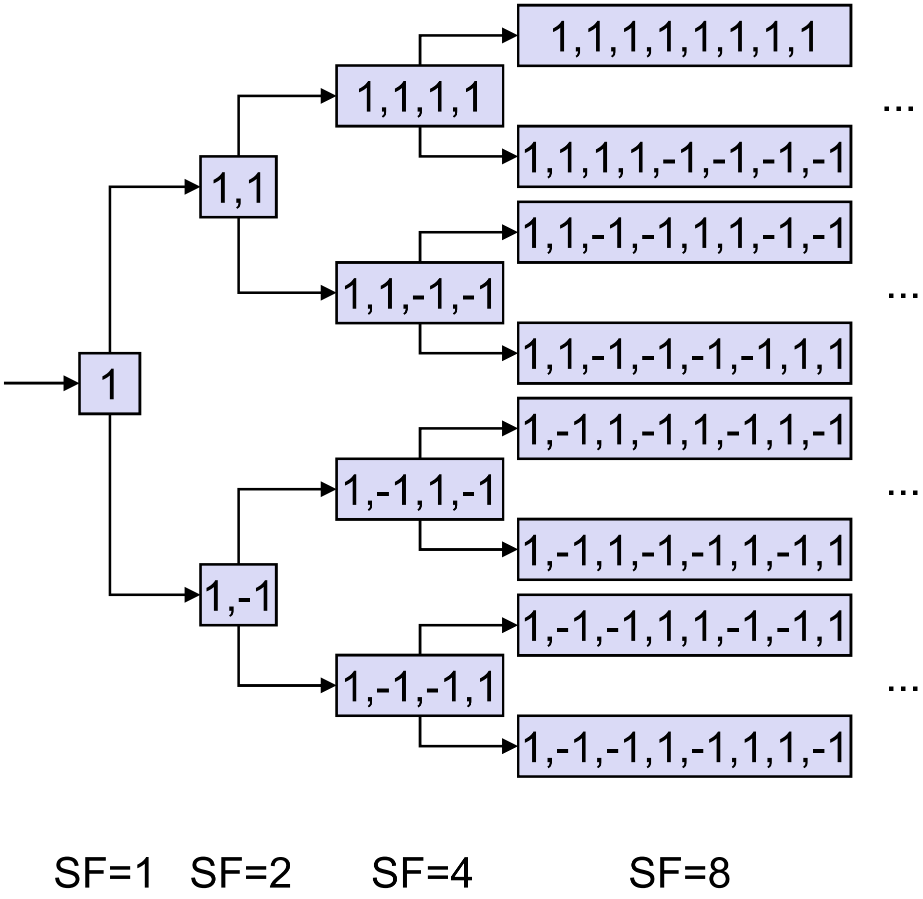
Spreading and scrambling of user data

- 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



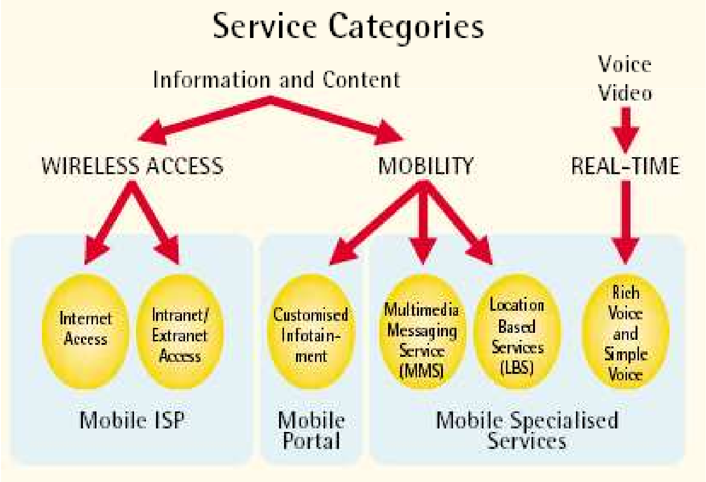
OSVF coding


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

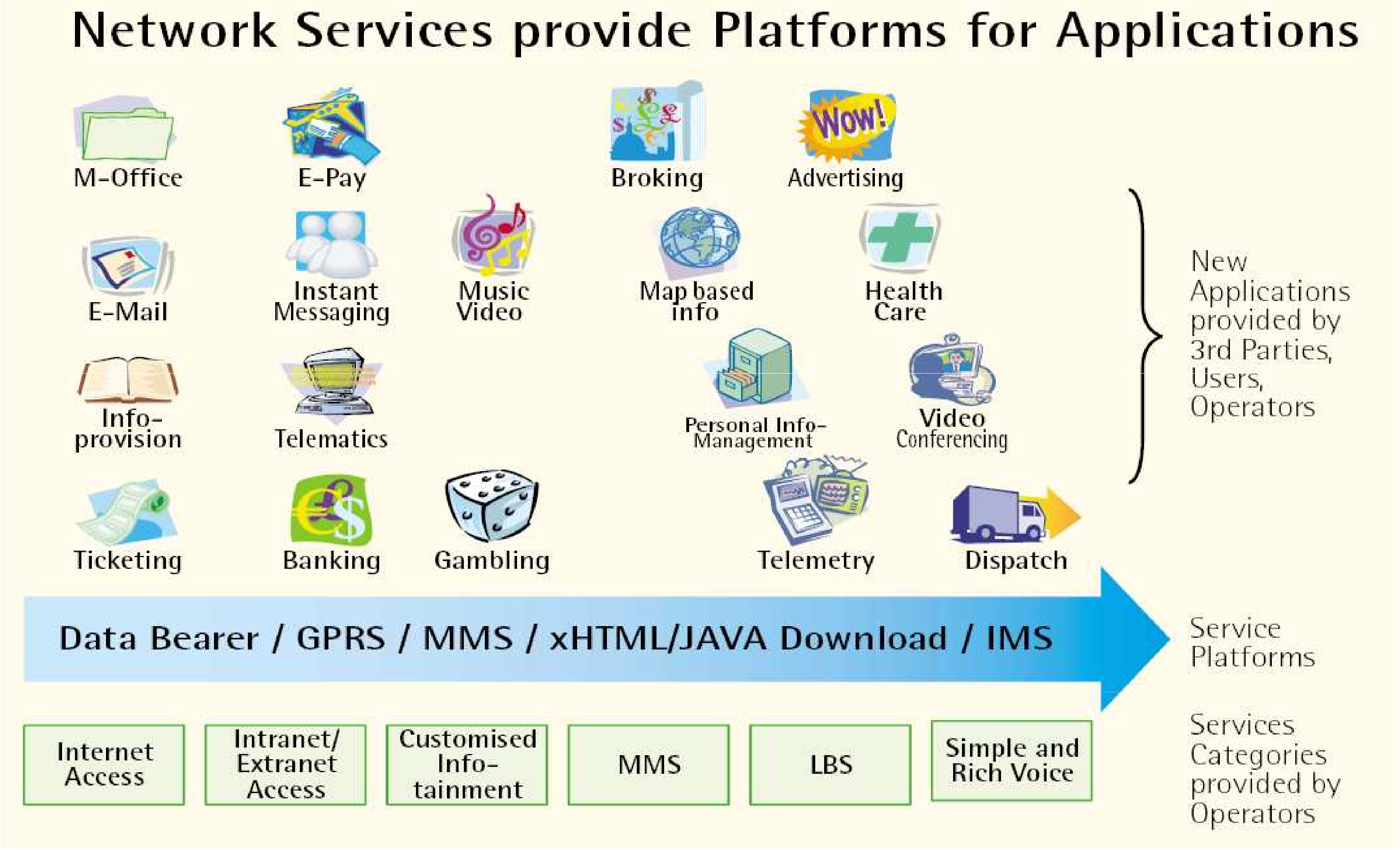
Services

- In shaping future mobile services, the following characteristics should be taken into consideration: mobility, interactivity, convenience, ubiquity, easy access, immediacy, personalization, multimedia
- Services for 3G will evolve within 3 different areas:
  - Personal Communication
  - Wireless Internet
  - Mobile Media (e.g. music, sports, news services)



- Voice traffic will remain the primary business of 3G mobile networks

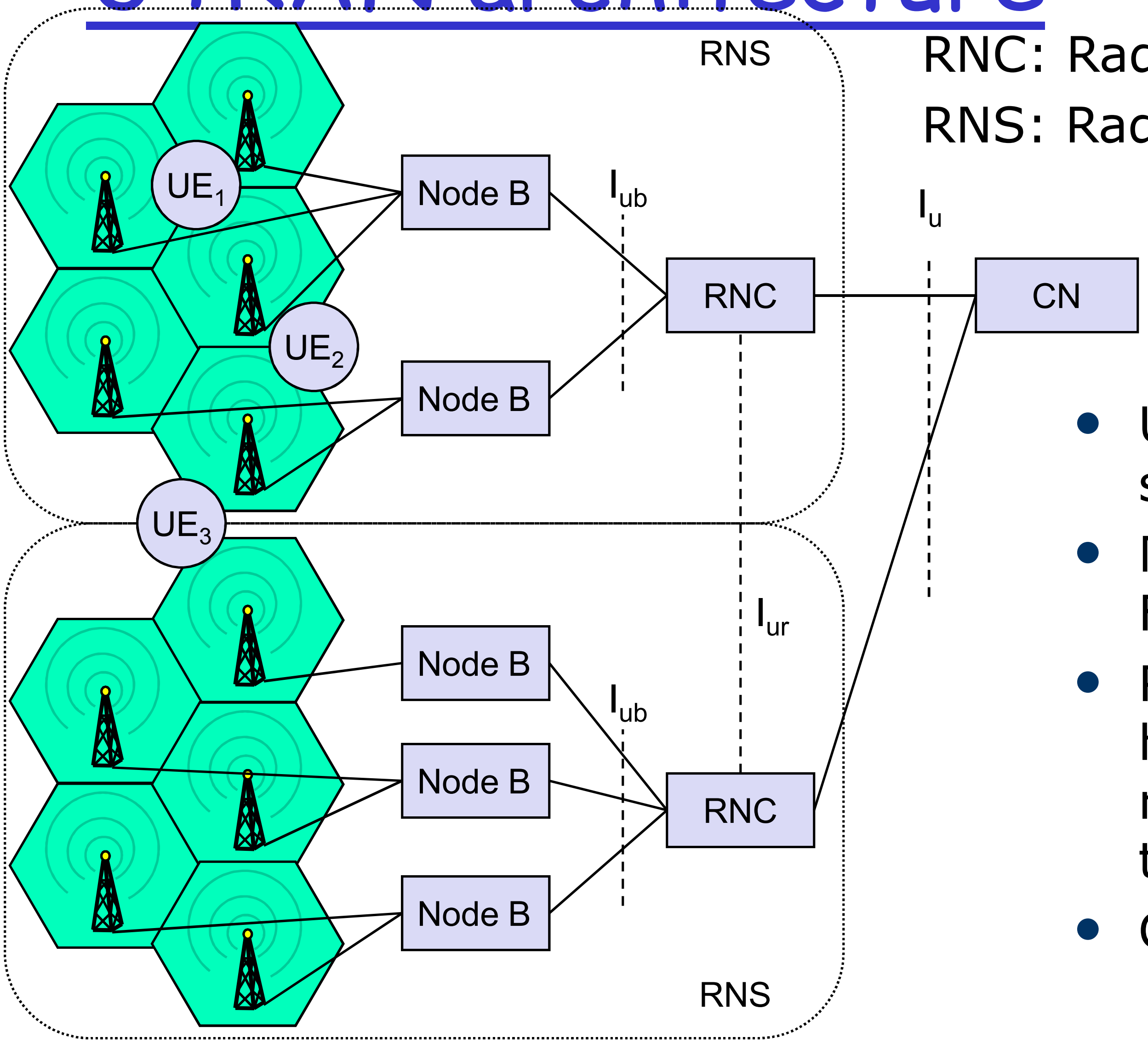
Services


Network Services provide Platforms for Applications
M-Office
E-Pay
Broking
Advertising
E-Mail
Instant Messaging
Music Video
Map based info
Health Care
Info-provision
Telematics
Personal Info-Management
Video Conferencing
Ticketing
Banking
Gambling
Telemetry
Dispatch
New Applications provided by 3rd Parties, Users, Operators
Data Bearer / GPRS / MMS / xHTML/JAVA Download / IMS
Service Platforms
Internet Access
Intranet/ Extranet Access
Customised Info-tainment
MMS
LBS
Simple and Rich Voice
Services Categories provided by Operators

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

UTRAN architecture



RNC: Radio Network Controller

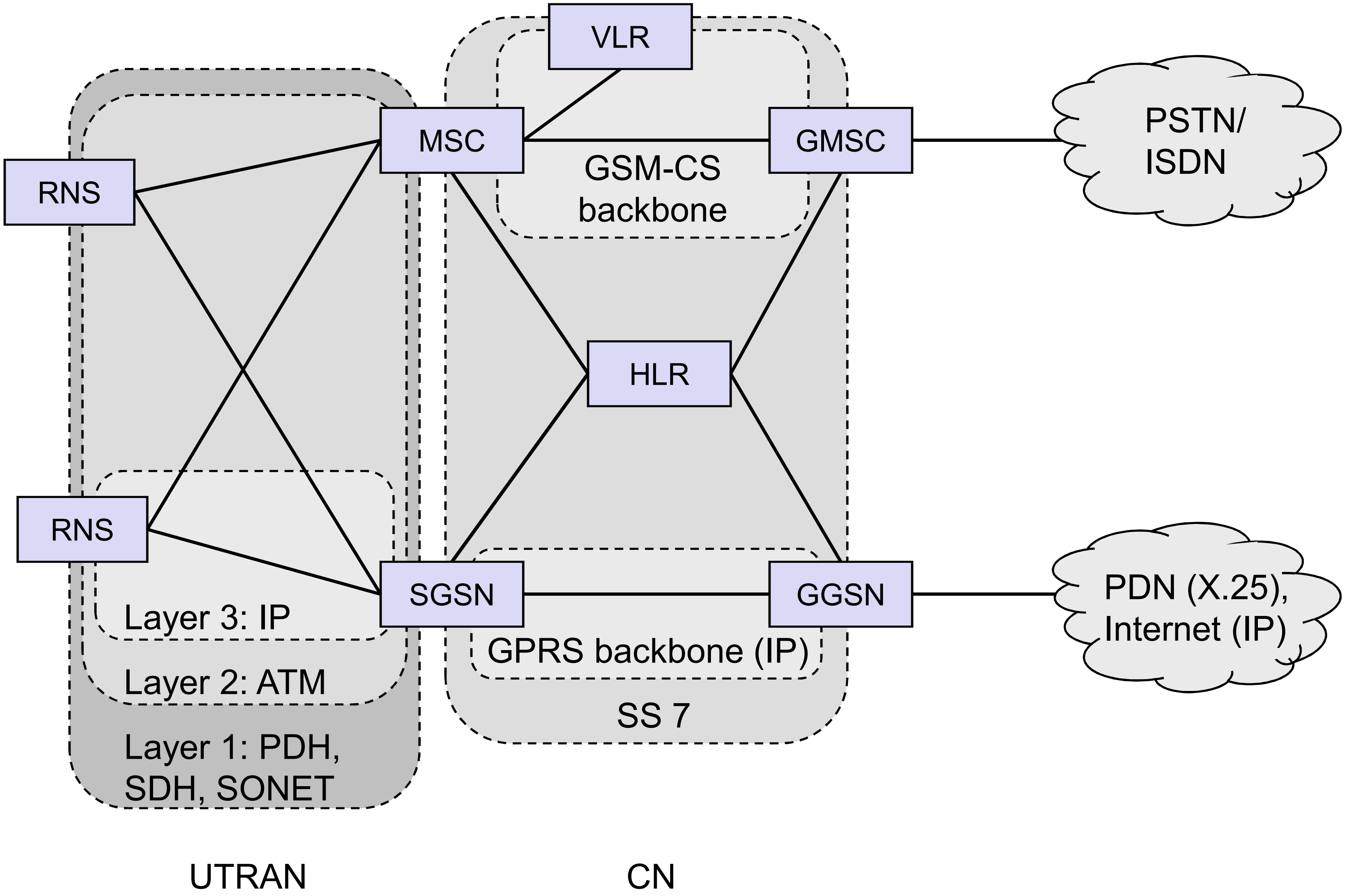
RNS: Radio Network Subsystem

- 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

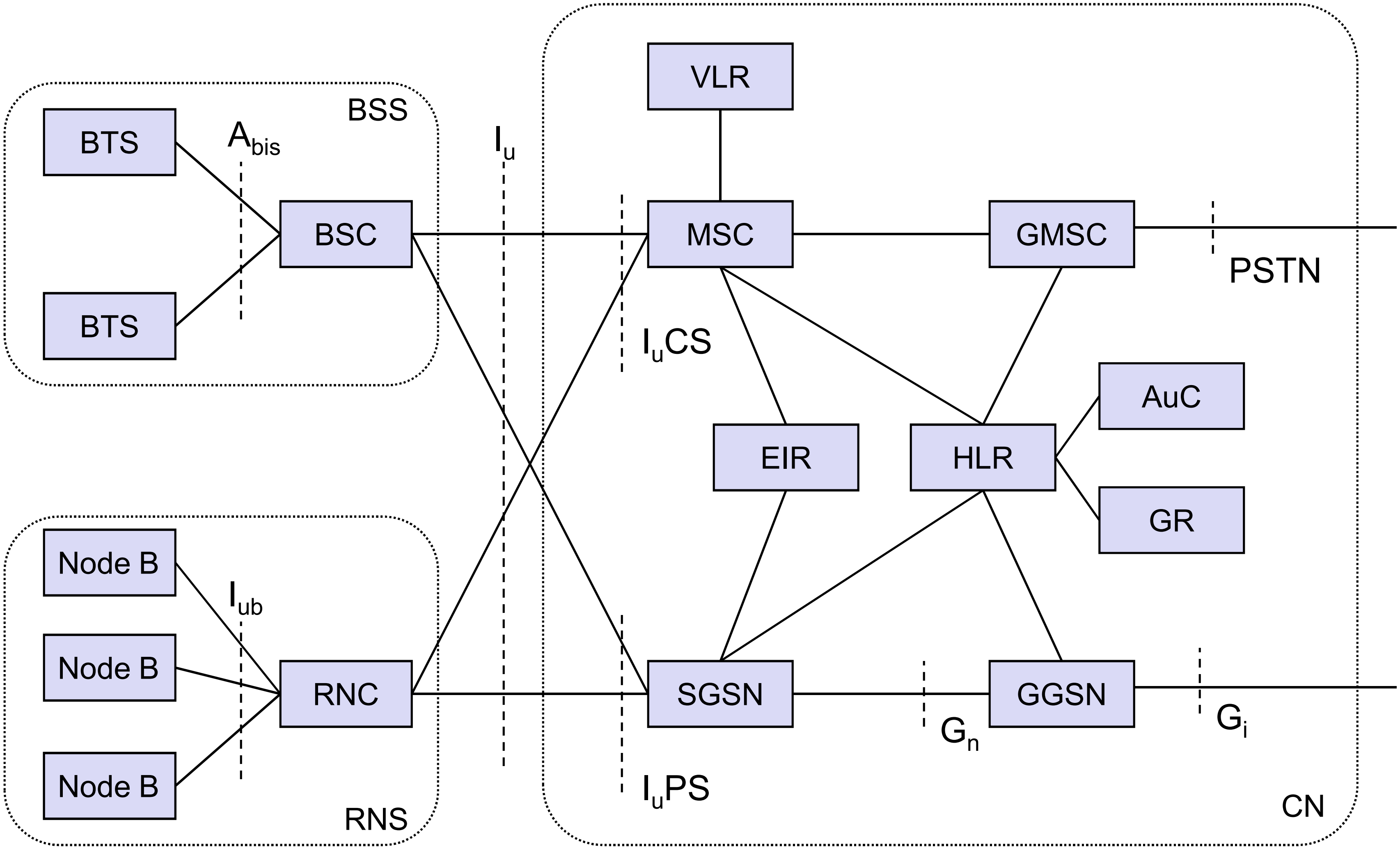
UTRAN functions

- Admission control
- Congestion control
- System information broadcasting
- Radio channel encryption
- Handover
- SRNS moving
- Radio network configuration
- Channel quality measurements
- Macro diversity
- Radio carrier control
- Radio resource control
- Data transmission over the radio interface
- Outer loop power control (FDD and TDD)
- Channel coding
- Access control

Core network: protocols



Core network: architecture

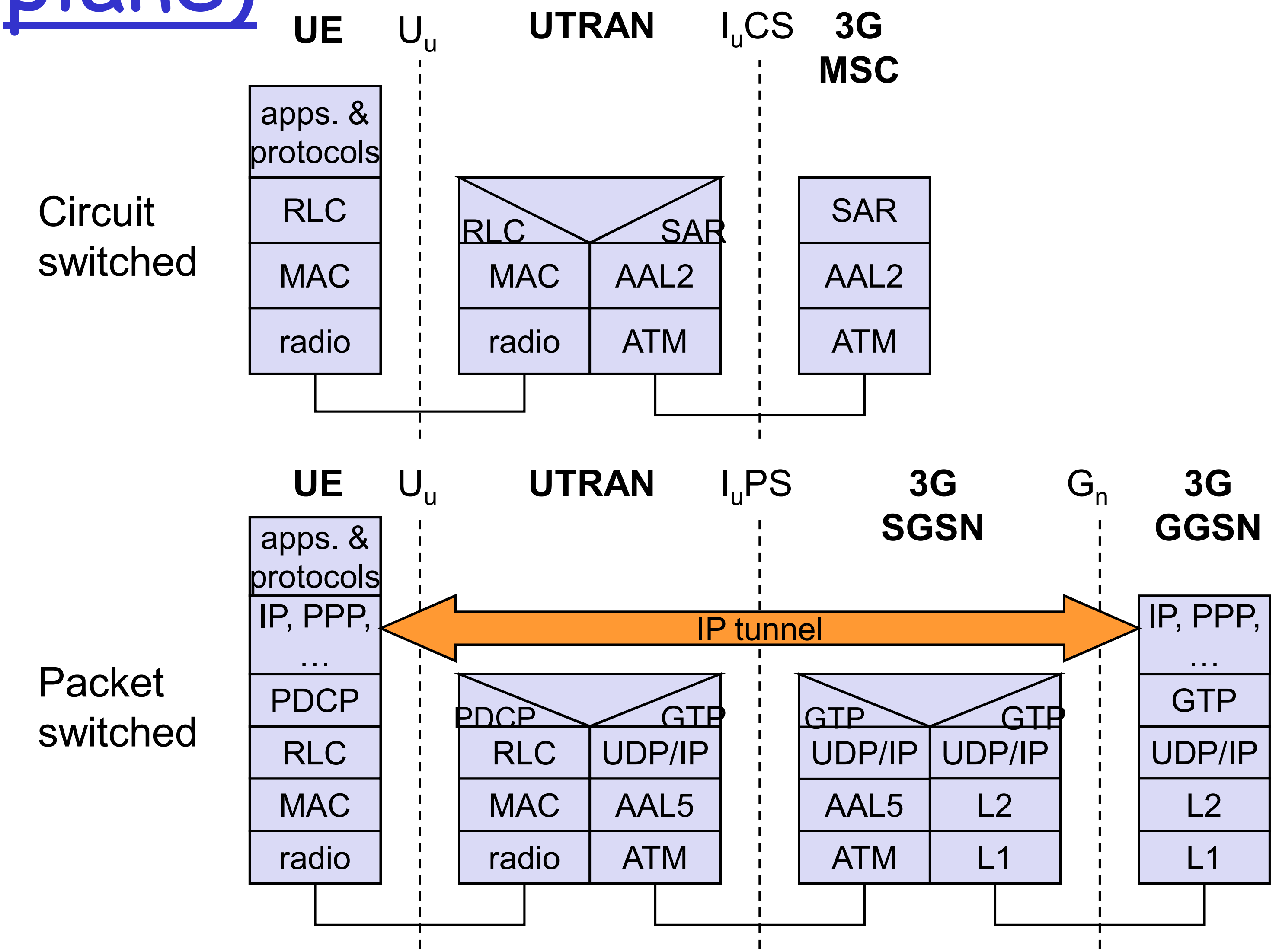


Core network

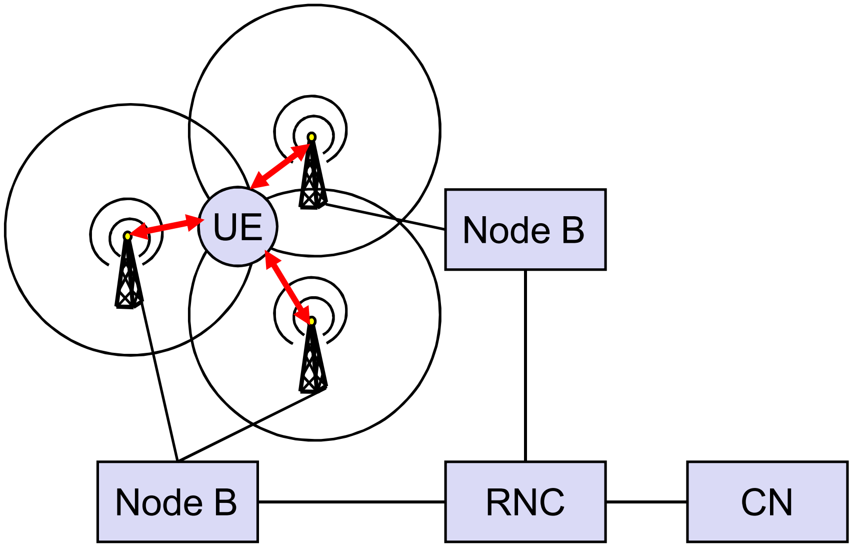
- The Core Network (CN) and thus the Interface I_u, too, are separated into two logical domains:
- Circuit Switched Domain (CSD)
  - Circuit switched service incl. signaling
  - Resource reservation at connection setup
  - GSM components (MSC, GMSC, VLR)
  - I_uCS
- Packet Switched Domain (PSD)
  - GPRS components (SGSN, GGSN)
  - I_uPS

- Release 99 uses the GSM/GPRS network and adds a new radio access!
  - Helps to save a lot of money …
  - Much faster deployment
  - Not as flexible as newer releases (5, 6)

UMTS protocol stacks (user plane)



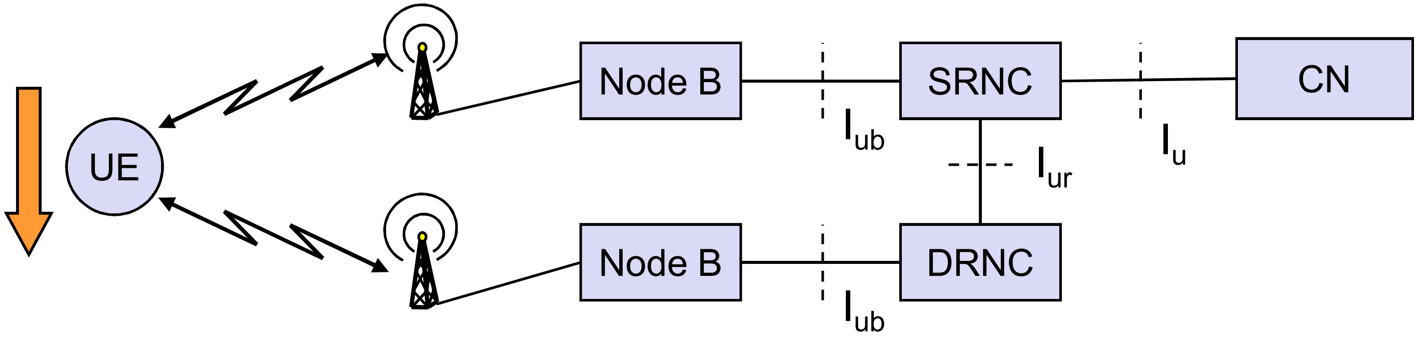
Support of mobility: macro diversity



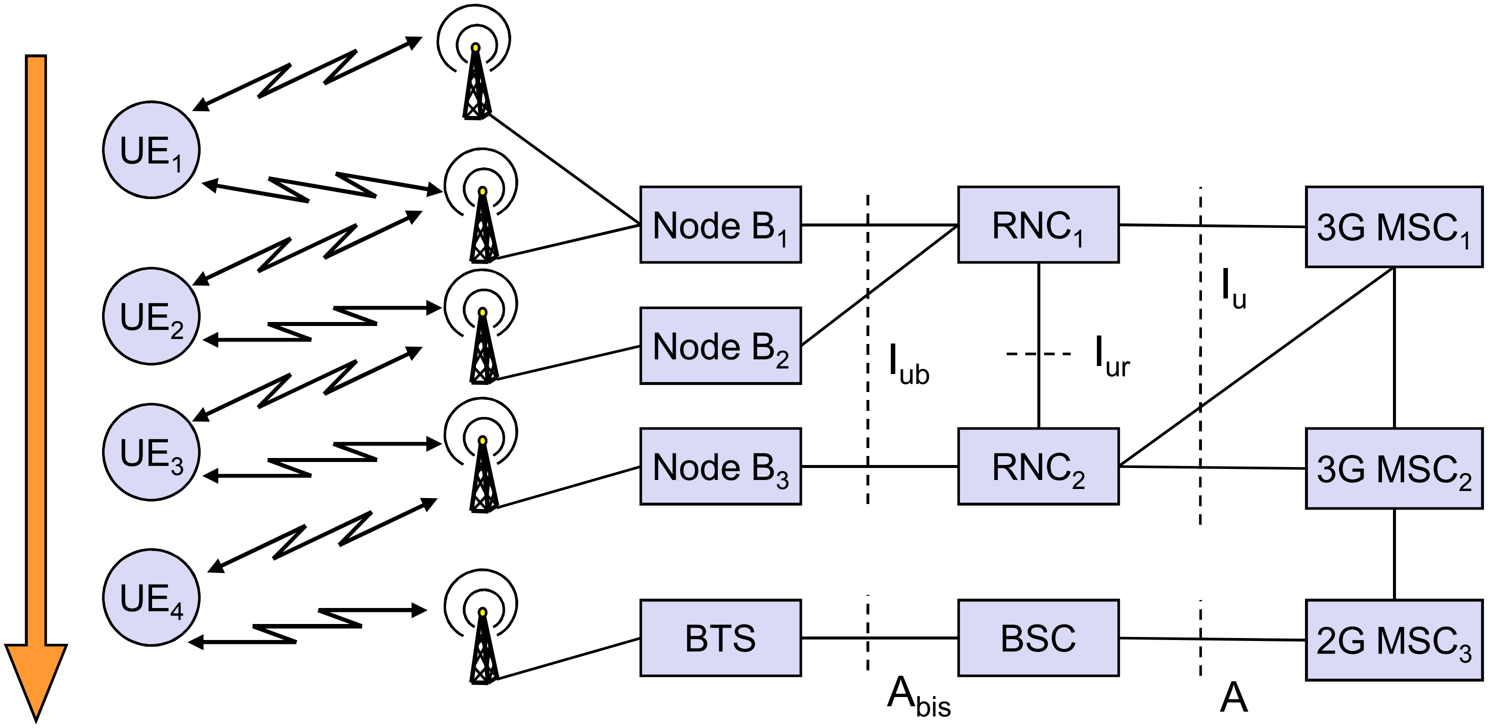
- Multicasting of data via several physical channels
  - Enables soft handover
  - FDD mode only
- Uplink
  - simultaneous reception of UE data at several Node Bs
  - Reconstruction of data at Node B, SRNC or DRNC
- Downlink
  - Simultaneous transmission of data via different cells
  - Different spreading codes in different cells

Support of mobility: handover

- From and to other systems (e.g., UMTS to GSM)
  - This is a must as UMTS coverage will be poor in the beginning
- RNS controlling the connection is called SRNS (Serving RNS)
- RNS offering additional resources (e.g., for soft handover) is called Drift RNS (DRNS)
- End-to-end connections between UE and CN only via I_u at the SRNS
  - Change of SRNS requires change of I_u
  - Initiated by the SRNS
  - Controlled by the RNC and CN



Example handover types in UMTS/GSM



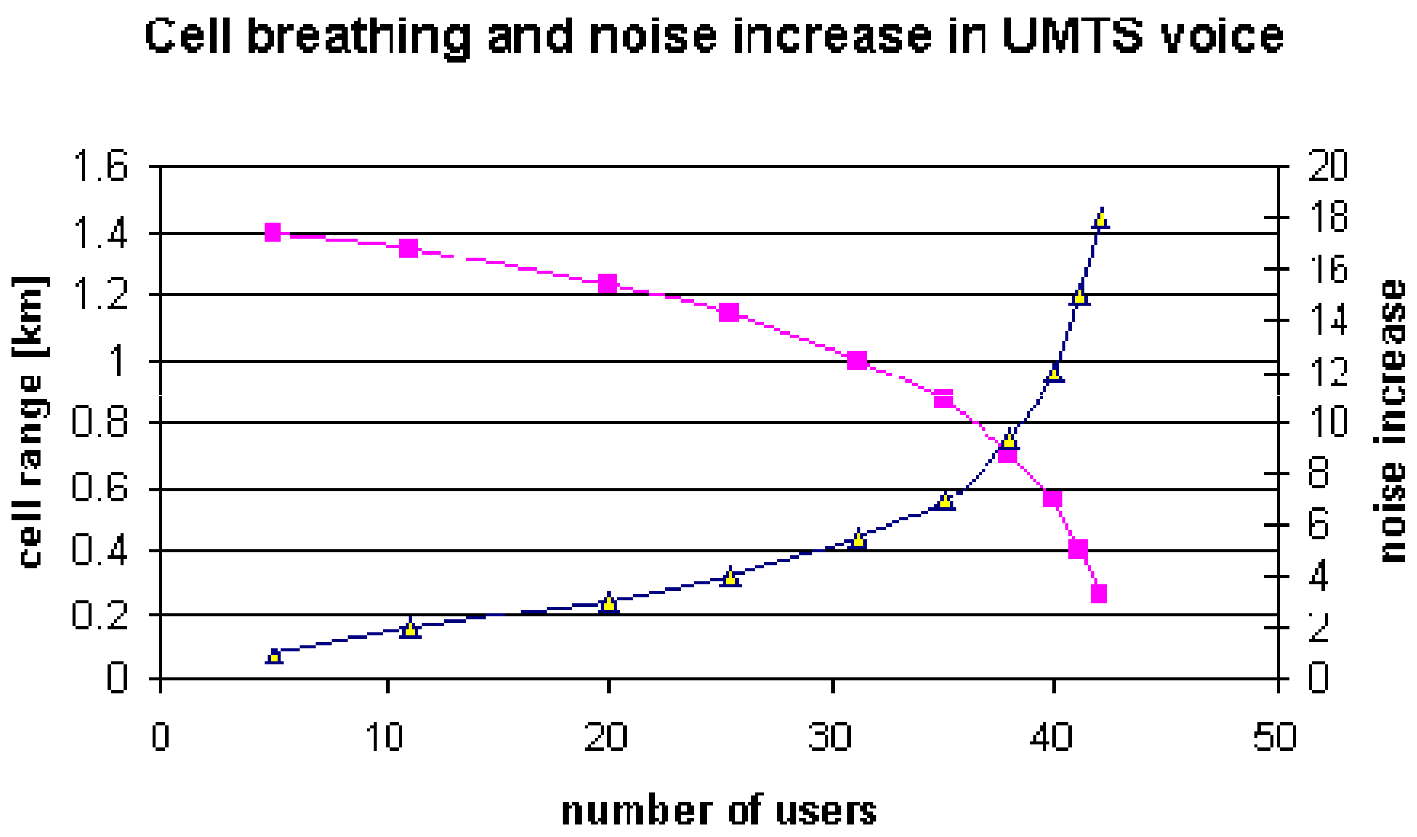
Breathing Cells

- GSM
  - Mobile device gets exclusive signal from the base station
  - Number of devices in a cell does not influence cell size

- UMTS
  - Cell size is closely correlated to the cell capacity
  - Signal-to-nose ratio determines cell capacity
  - Noise is generated by interference from
    - other cells
    - other users of the same cell
  - Interference increases noise level
  - Devices at the edge of a cell cannot further increase their output power (max. power limit) and thus drop out of the cell ⇨ no more communication possible
  - Limitation of the max. number of users within a cell required

  - Cell breathing complicates network planning

Breathing Cells: Example



UMTS services (originally)

- Data transmission service profiles

Service Profile	Bandwidth	Transport mode	
High Interactive MM	128 kbit/s	Circuit switched	Bidirectional, video telephone
High MM	2 Mbit/s	Packet switched	Low coverage, max. 6 km/h
Medium MM	384 kbit/s	Circuit switched	asymmetrical, MM, downloads
Switched Data	14.4 kbit/s	Circuit switched	
Simple Messaging	14.4 kbit/s	Packet switched	SMS successor, E-Mail
Voice	16 kbit/s	Circuit switched	

- Virtual Home Environment (VHE)
  - Enables access to personalized data independent of location, access network, and device
  - Network operators may offer new services without changing the network
  - Service providers may offer services based on components which allow the automatic adaptation to new networks and devices
  - Integration of existing IN services

Some current enhancements

- GSM
  - EMS/MMS
    - EMS: 760 characters possible by chaining SMS, animated icons, ring tones, was soon replaced by MMS (or simply skipped)
    - MMS: transmission of images, video clips, audio
      - see WAP 2.0 / chapter 10
  - EDGE (Enhanced Data Rates for Global [was: GSM] Evolution)
    - 8-PSK instead of GMSK, up to 384 kbit/s
    - new modulation and coding schemes for GPRS ➔ EGPRS
      - MCS-1 to MCS-4 uses GMSK at rates 8.8/11.2/14.8/17.6 kbit/s
      - MCS-5 to MCS-9 uses 8-PSK at rates 22.4/29.6/44.8/54.4/59.2 kbit/s

- UMTS
  - HSDPA (High-Speed Downlink Packet Access)
    - initially up to 10 Mbit/s for the downlink, later > 20 Mbit/s using MIMO-(Multiple Input Multiple Output-) antennas
    - can use 16-QAM instead of QPSK (ideally > 13 Mbit/s)
    - user rates e.g. 3.6 or 7.2 Mbit/s
  - HSUPA (High-Speed Uplink Packet Access)
    - initially up to 5 Mbit/s for the uplink
    - user rates e.g. 1.45 Mbit/s