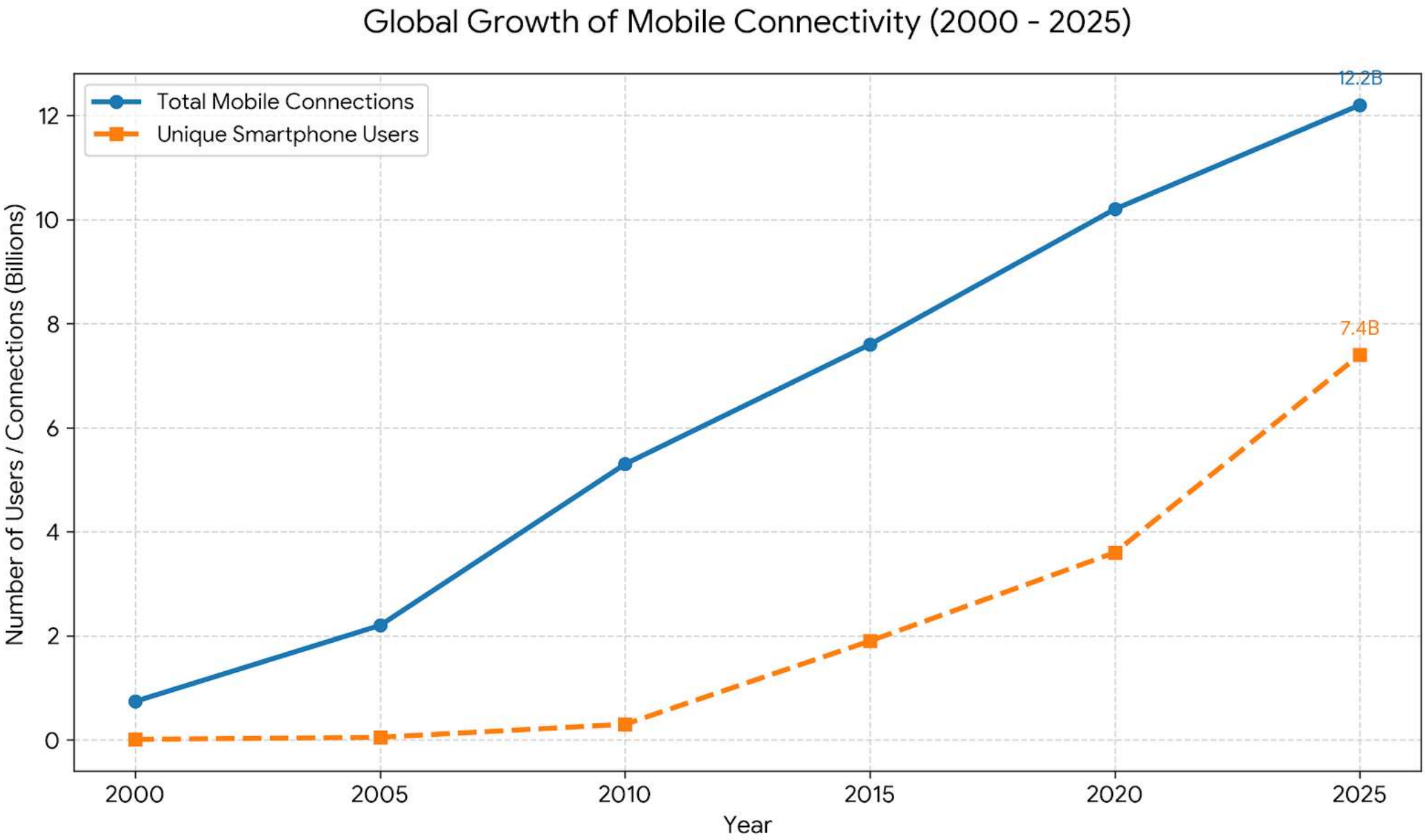
Cellular Networks

Outline

- Introduction
- Frequency reuse
- Channel assignment strategies
- Techniques to increase capacity
- Handoff
- Cellular standards

Mobile Phone Subscribers



Cellular Concept

- Challenge: limited spectrum allocation (government regulation)
- A single high-powered transmitter
  - good coverage
  - interference: impossible to reuse the same frequency
- Example:
  - One tower system in New York City in 1970
    - Maximum 12 simultaneous calls/1000 square miles

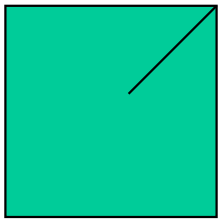
Cellular Concept

- developed by Bell Labs 1960's-70's
- areas divided into cells
- a system approach, no major technological changes
- a few hundred meters in some cities, 10s km at country side
- each served by base station with lower power transmitter
- each gets portion of total number of channels
- neighboring cells assigned different groups of channels, interference minimized

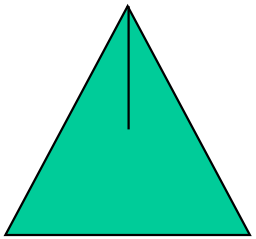
Cell Shape

- Factors
  - Equal area
  - Non overlap between cells

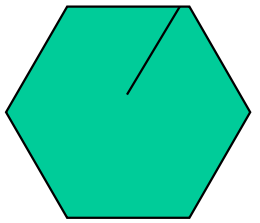
- Choices



A1



A2

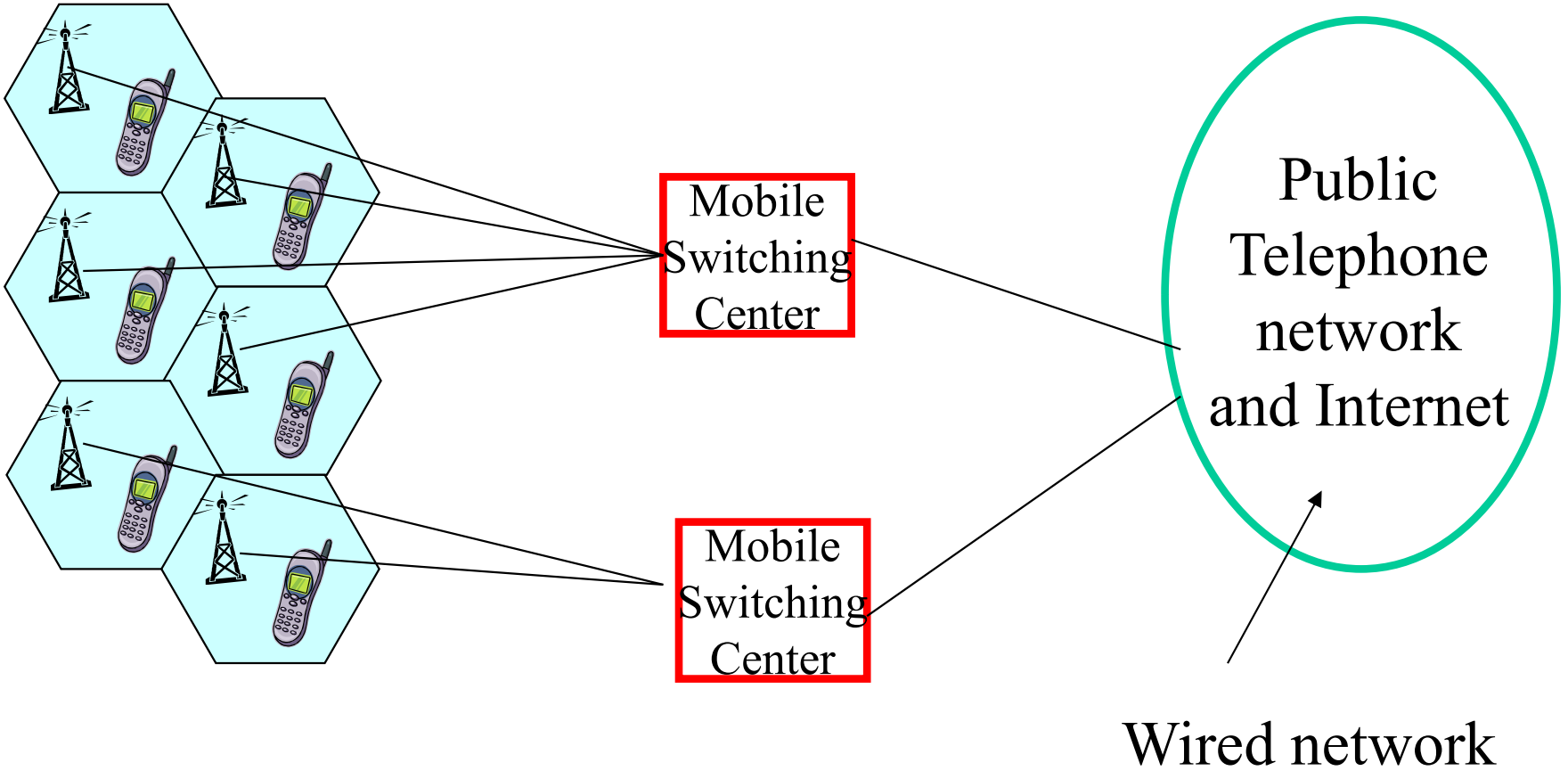


A3

For a given S

- A3 > A1
- A3 > A2
- A3 provides maximum coverage area for a given value of S
- By using hexagon geometry, the fewest number of cells covers a given geographic region
- Actual cellular footprint is determined by the contour of a given transmitting antenna

Cellular Network Architecture



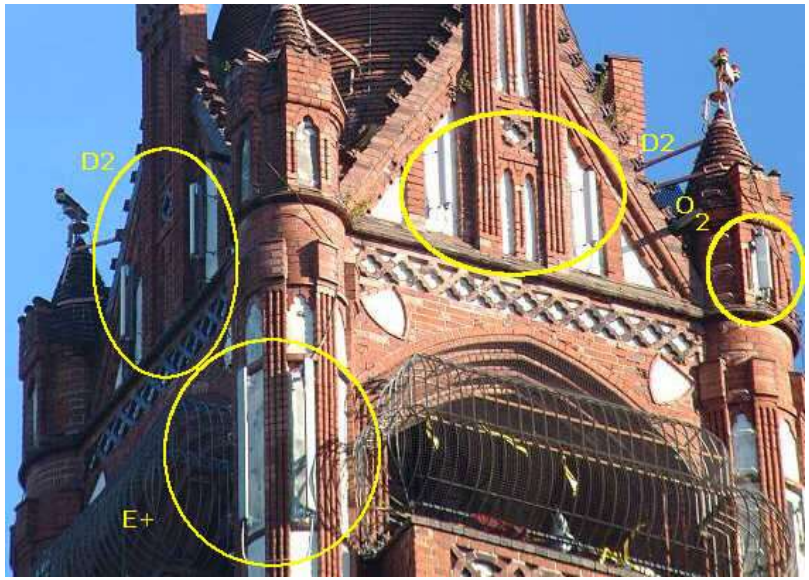
Cellular Network Architecture

- Cell
  - Covers geographic region
  - Base station (BS): analogous to 802.11 AP
  - Mobile users attach to network through BS
  - Air interface: physical and link layer protocol between mobile and BS
- MSC
  - Connects cells to wide area network
  - Manages call setup
  - Handles mobility

Ingredients 1: Mobile Phones, PDAs & Co.

The visible but smallest part of the network!

Ingredients 2: Antennas



Still visible – cause many discussions…

Ingredients 3: Infrastructure 1

Base Stations

Cabling

Microwave links

Ingredients 3: Infrastructure 2

Switching units

Management

Data bases

Monitoring

Not “visible“, but comprise the major part of the network (also from an investment point of view…)

Cellular networks: the first hop

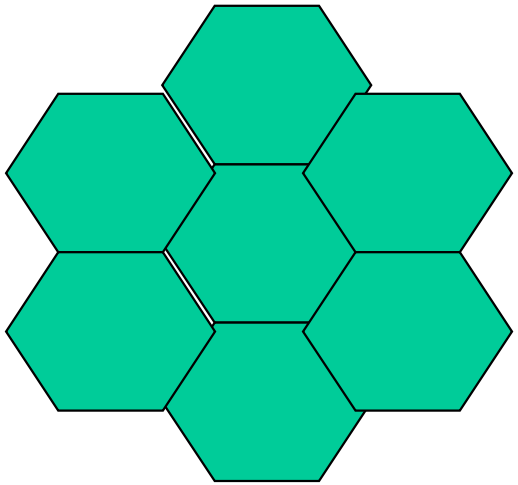
- Two techniques for sharing mobile-to-BS radio spectrum
  - combined FDMA/TDMA:
    - divide spectrum in frequency channels, divide each channel into time slots
  - CDMA:
    - code division multiple access

Frequency Reuse

- Adjacent cells assigned different frequencies to avoid interference or crosstalk
- Objective is to reuse frequency in nearby cells
  - 10 to 50 frequencies assigned to each cell
  - transmission power controlled to limit power at that frequency escaping to adjacent cells
  - the issue is to determine how many cells must intervene between two cells using the same frequency

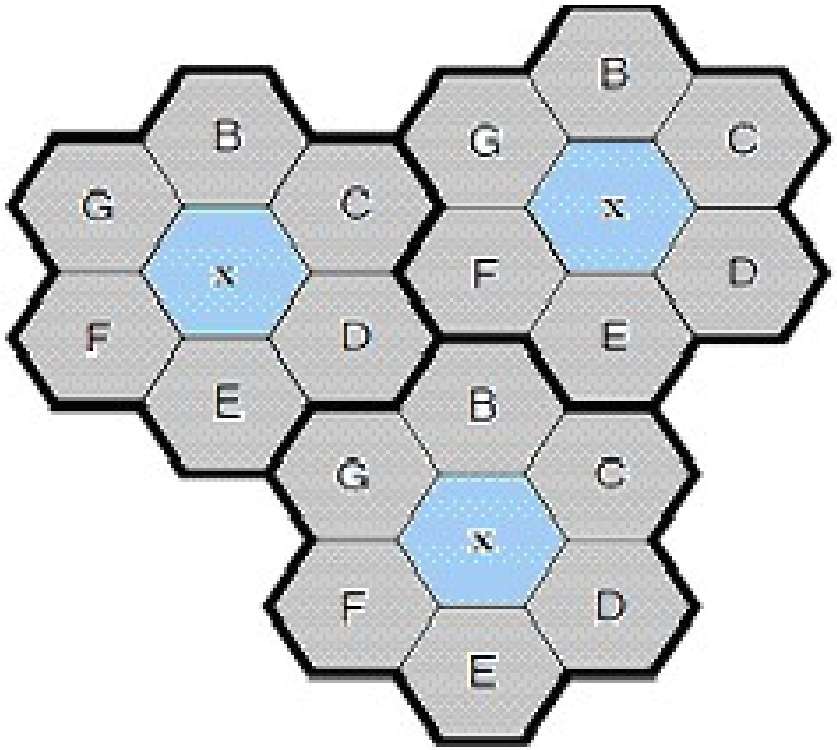
Frequency Reuse

- each cell allocated a group k channels
  - a cluster has N cells with unique and disjoint channel
- groups, N typically 4, 7, 12
- total number of duplex channels S = kN



System Capacity

- Cluster repeated M times in a system
- Total number of channels that can be used (capacity)
  - C = MkN = MS



Example 1

- If a particular cellular telephone system has a total bandwidth of 33 MHz, and if the phone system uses two 25 KHz simplex channels to provide full duplex voice and control channels.

- compute the number of channels per cell if N = 4, 7, 12.

Solution 1

- Total bandwidth = 33 MHz
- Channel bandwidth = 25 KHz x 2 = 50 KHz
- Total avail. channels = 33 MHz / 50 KHz = 660
- N = 4
  - Channel per cell = 660 / 4 = 165 channels
- N = 7
  - Channel per cell = 660 / 7 = 95 channels
- N = 12
  - Channel per cell = 660 / 12 = 55 channels

Little's Theorem

- # users in system = arrival rate * service time
- Applies to any non-preemptive system regardless of arrival and service process distribution

Example 2

- A mobile phone system covers 1 mile long segment of a highway. Users enter and leave the segment of the highway at the rate of 20 users/minute. Assume that all the users drive a the constant speed of 55 miles/hour. On average, 25% cars use a mobile phone system in this highway segment. Assume that all the calls initiate and terminate outside this highway segment. How many users on average are using the system at any time instant?

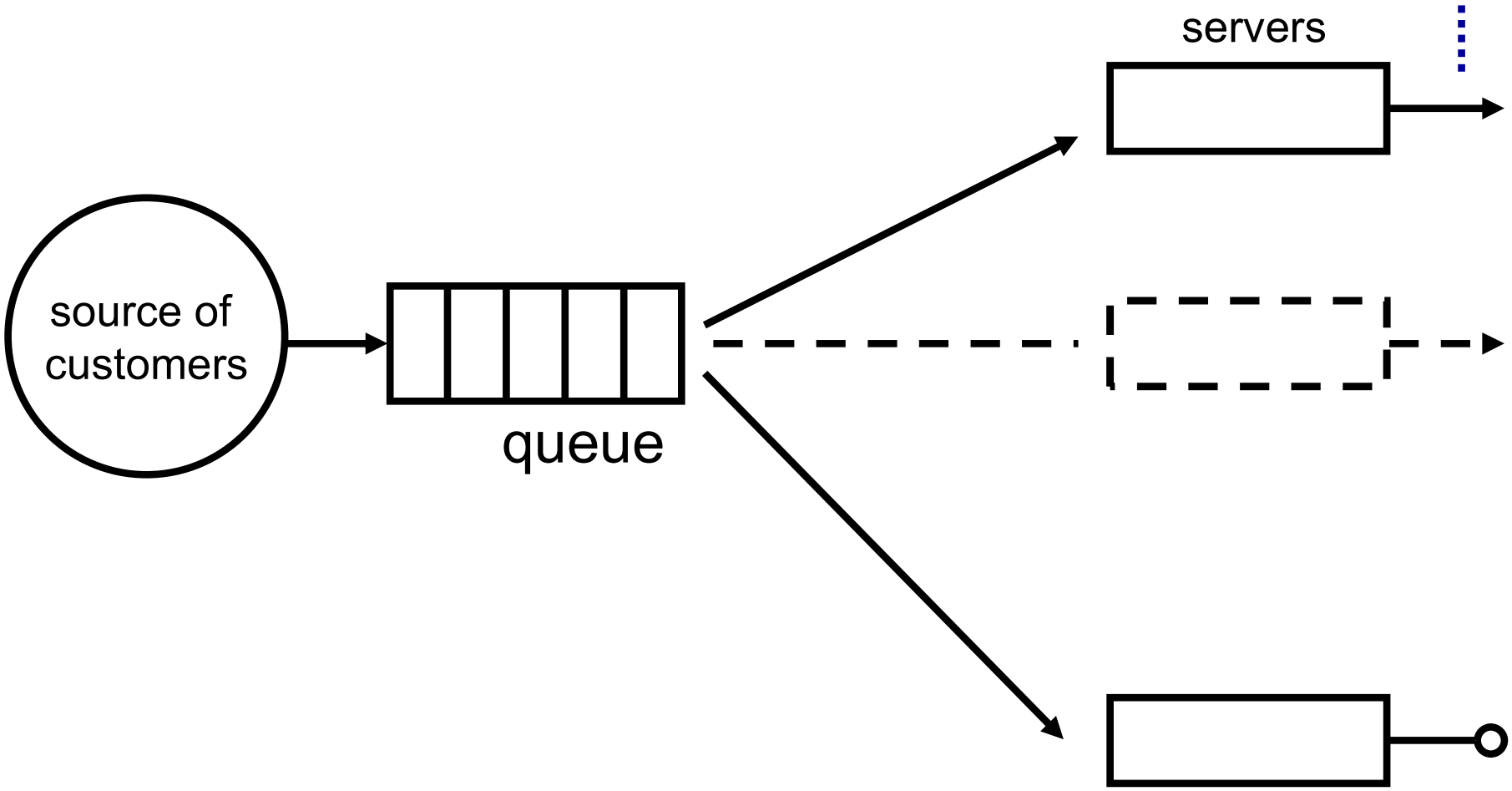
Solution 2

- The mobiles arrive at the mobile phone system a rate of $\lambda=20*25\% = 5$ users/min
- Service time = 1/(55/60) = 1.09 min
- # users in the system = 5*1.09 = 5.45 users

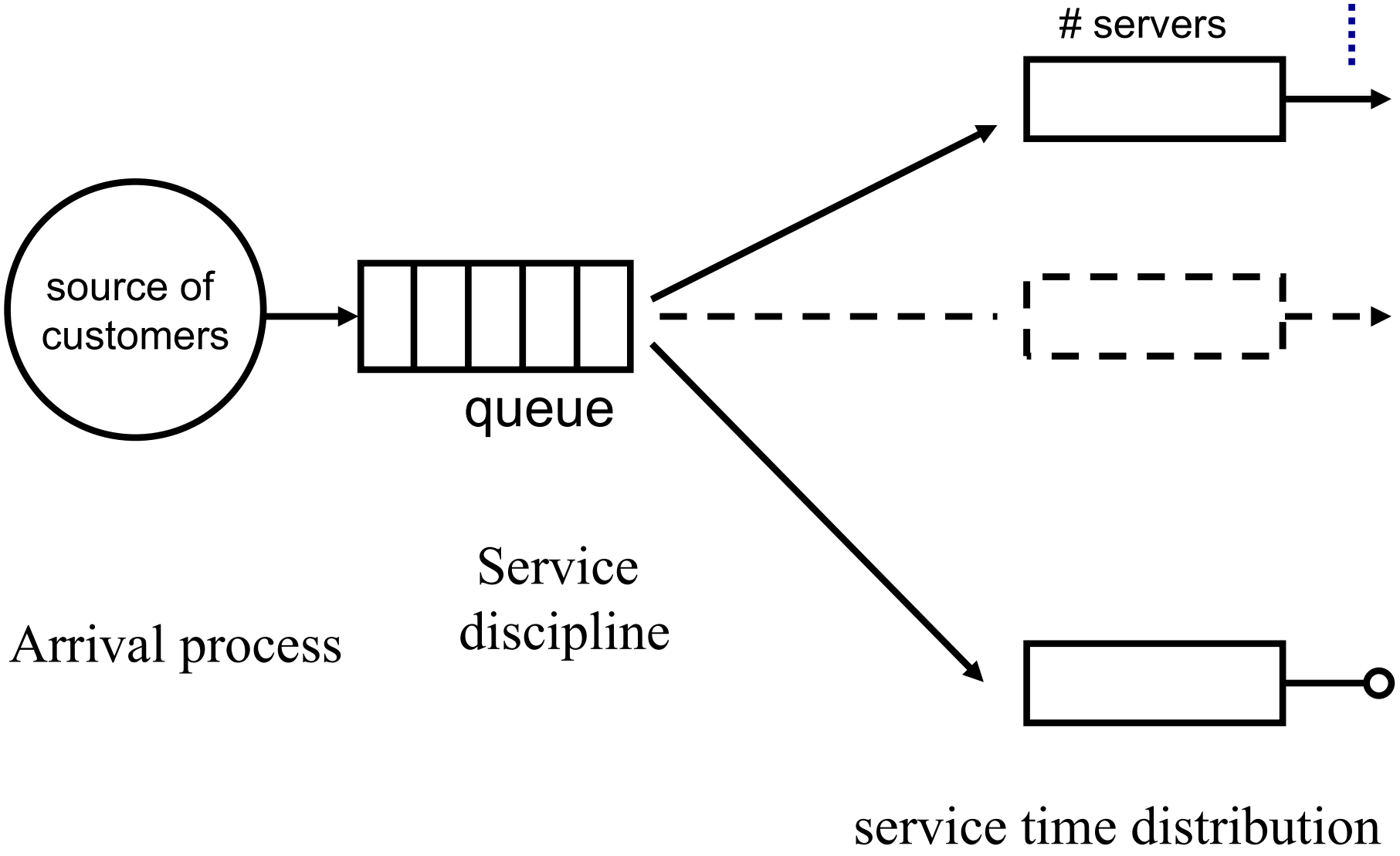
Another Example of Little's Theorem

- A monitor on a disk server showed that the average time to satisfy an I/O request was 100 milliseconds. The I/O rate was about 100 requests per second. What was the mean number of requests at the disk server?

Queuing Systems



Queuing System



Arrival Process

- Arrival times: t1, t2, …, tj
- Interarrival times: $\tau j = tj - t(j-1)$
- τj form a sequence of Independent and Identically Distributed (IID) random variables
- Exponential + IID ⇒ Poisson
- Notation
  - M = Memoryless = Poisson
  - E = Erlang
  - H = Hyper-exponential
  - G = General ⇒ Results valid for all distributions

Service Time Distribution

- Time each customer spends at the terminal
- Service times are IID
- Distribution: M, E, H, or G
- Device = Service center = Queue
- Buffer = Waiting positions

Service Disciplines

- First-Come-First-Served (FCFS)
- Last-Come-First-Served (LCFS)
- Last-Come-First-Served with Preempt and Resume (LCFS-PR)
- Round-Robin (RR) with a fixed quantum
- Small Quantum ⇒ Processor Sharing (PS)
- Infinite Server: (IS) = fixed delay
- Shortest Processing Time first (SPT)
- Shortest Remaining Processing Time first (SRPT)
- Shortest Expected Processing Time first (SEPT)
- Shortest Expected Remaining Processing Time first (SERPT).
- Biggest-In-First-Served (BIFS)
- Loudest-Voice-First-Served (LVFS)

Kendall Notation
A/S/c/K/m/Z

A – Arrival process
S - service time distribution
c - number of servers
K - system's queue capacity
m – population size
Z – service discipline

K, m, and Z can be omitted if the queue and source are infinite and queue is FIFO

M denotes the most widely used exponential distribution

D - discrete

G - general

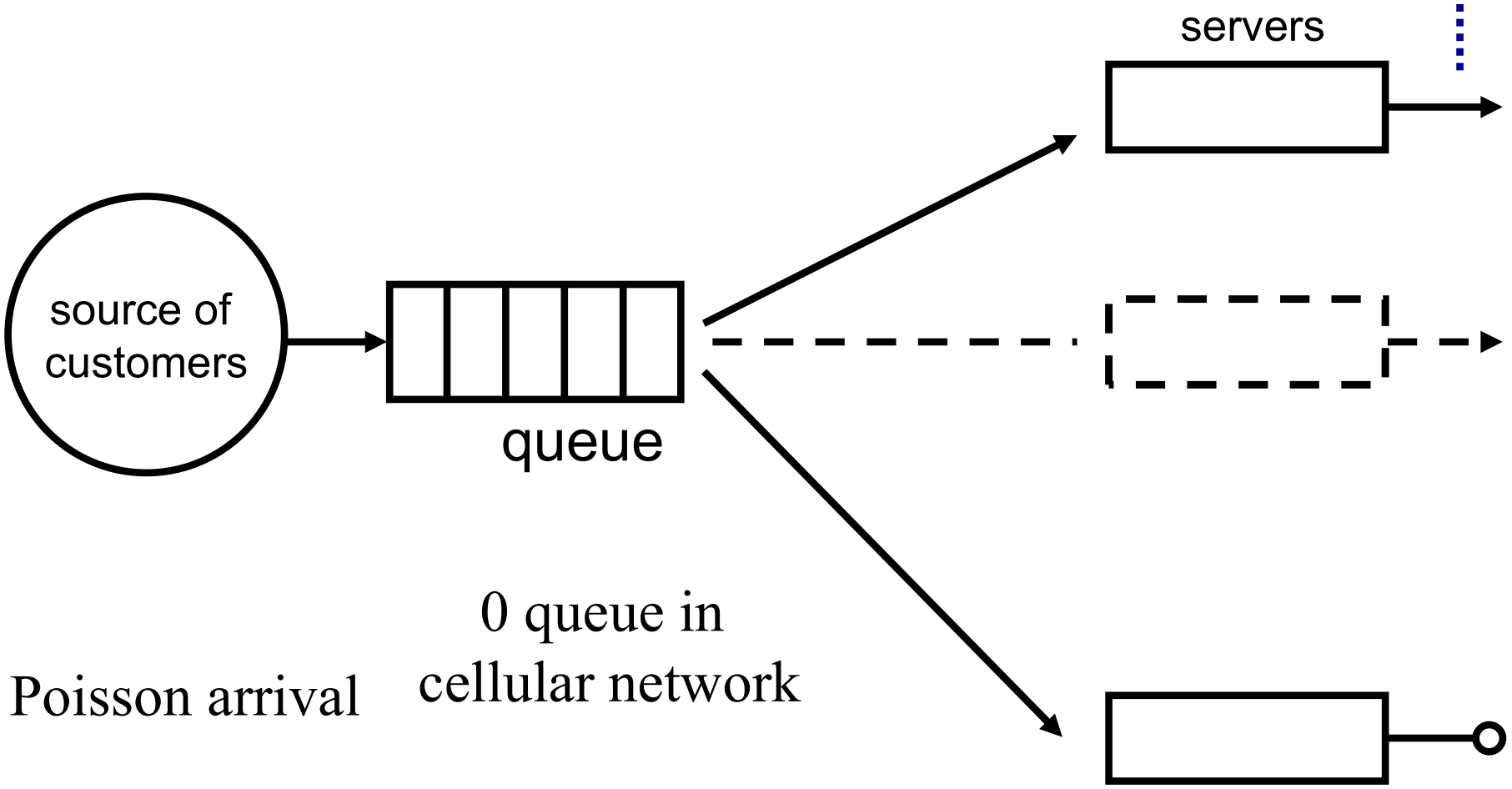
Common Distribution

- M: Exponential
- Ek: Erlang with parameter k
- Hk: Hyper-exponential with parameter k
- D: Deterministic ⇒ constant
- G: General ⇒ All
- Memoryless
  - Expected time to the next arrival is always $1/\lambda$ regardless of the time since the last arrival
  - Remembering the past history does not help.

M/M/c/c Queue

- Poisson arrival
- Exponential distributed service time
- c servers
- Buffer size: c
- Blocking probability = $(\alpha^c/c!)/\sum_{i=0..c}(\alpha^i/i!)$ where α is Offered load

M/M/c/c Queuing System



Poisson arrival

0 queue in cellular network

c servers

Exponential service time

Queuing Models for Cellular Networks

Generation	Primary Voice Model	Primary Data Model	Focus Metric
2G (GSM)	M/M/c/c	N/A (Circuit Switched)	Blocking Probability
3G (UMTS)	M/M/c/c	M/M/1 / M/G/1	Throughput & Delay
4G (LTE)	M/M/c/c (VoLTE)	M/G/1 / M/D/1	Latency & Jitter
5G (NR)	M/M/c/c (Vo5G)	Priority Queuing / Slicing	QoS & Reliability

1G - 6G

Generation	Launch Era	Key Physical Layer Innovation	Primary Queuing Model	Focus Metric & Social Impact
1G	1980	Analog Signals (FDAMA)	M/M/c/c (Loss)	Voice Quality: The birth of mobile mobility.
2G	1991	Digital Encoding & TDMA	M/M/c/c (Digital)	Blocking Rate: Texting (SMS) becomes a global phenomenon.
3G	2001	Packet Switching & WCDMA	M/M/1 (Delay)	Throughput: Always-on internet; the "App Economy" begins.
4G	2010	OFDMA & Deterministic Scheduling	M/D/1 (Deterministic)	Latency/Jitter: High-definition video streaming and Uber/Lyft.
5G	2020	Massive MIMO & Beamforming	Priority Queuing	Reliability: Network Slicing for Industry 4.0 and Remote Surgery.
6G	~2030 (Est)	Smart Surfaces (RIS) & THz	Predictive Queuing	Ubiquity: Integrated sensing; AI-native "Internet of Intelligence."

Example 3

- Same as Example 2, if 10 voice channels are available, what is the dropping rate, i.e., the probability that a user cannot get a channel assignment and his call is interrupted?

- If the system is redesigned, how many more channels are needed to achieve 1% dropping probability?

Solution 3

- α = Offered load = N_{active} * 1.0 [Erlangs/user] = 5.45 Erlangs
- Number of trunks = 10 trunks
- Blocking probability = $(\alpha^c/c!)/\sum_{i=0..c}(\alpha^i/i!)$
  - Looking at table, dropping probability = 0.03
  - http://onlinelibrary.wiley.com/doi/10.1002/0470842849.app2/pdf

Solution 3

- Find c' s.t. $(\alpha^{c'}/c'!)/\sum_{i=0..c'}(\alpha^{i}/i!)$
  - Table lookup, ?? channels are needed to achieve ≤ 1% dropping rate under 5.45 Erlangs
  - 12 channels

- Lookup exercises

Cell-size Tradeoff

Cell Size: Tradeoff

- Smaller cells ➔ higher M ➔ higher C
  - + Channel reuse ➔ higher capacity
  - + Lower power requirements for mobiles
  - – Additional base stations required
  - – More frequent handoffs
  - – Greater chance of ‘hot spots’

Effect of cluster size N

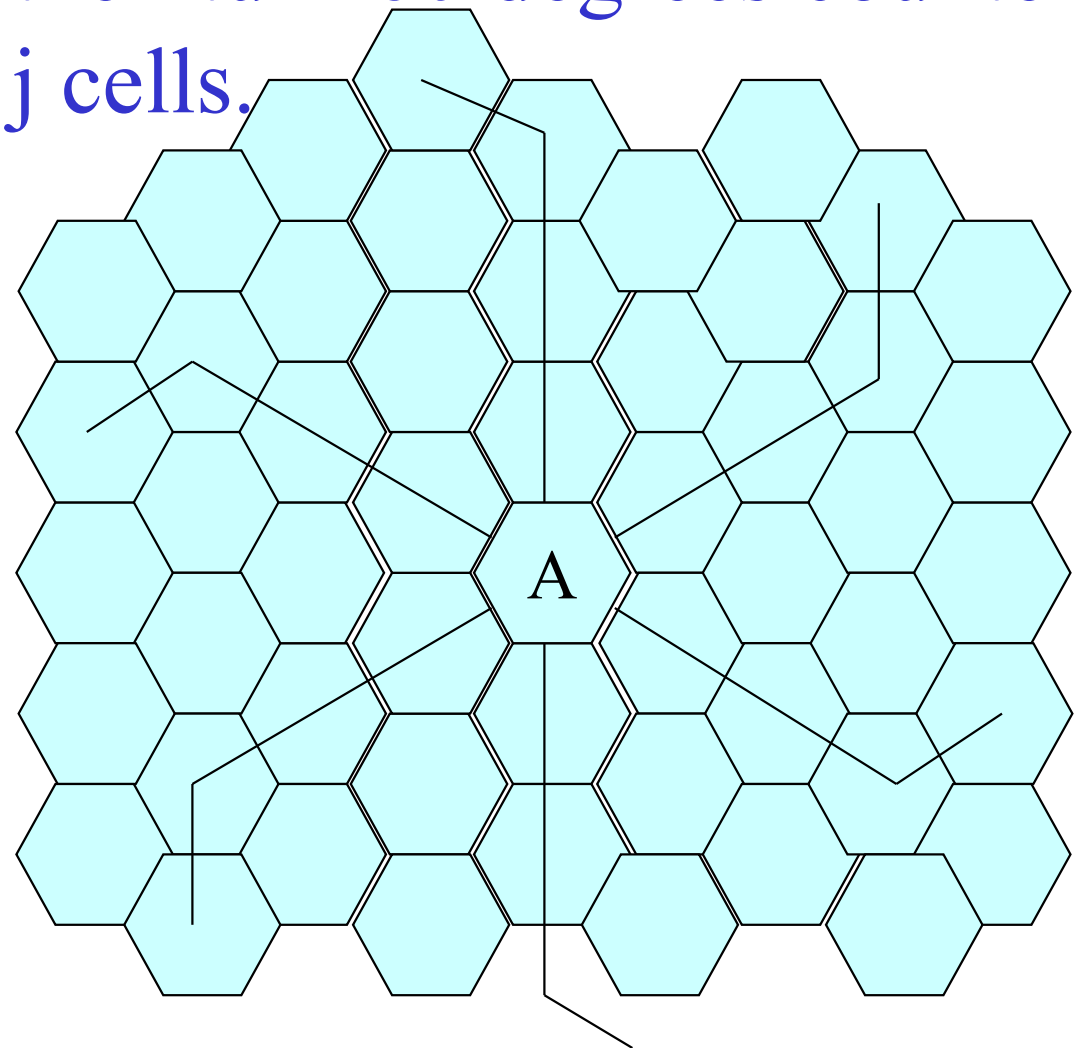
- channels unique in same cluster, repeated over clusters
- keep cell size same
  - large N : weaker interference, but lower capacity
  - small N: higher capacity, more interference need to maintain certain S/I level
- frequency reuse factor: 1/N
  - each cell within a cluster assigned 1/N of the total available channels

Design of cluster size

- In order to connect without gaps between adjacent cells (to Tessellate)
- $N = i^2 + ij + j^2$ where i and j are non-negative integers
- Example $i = 2, j = 1$
  - $N = 2^2 + 2(1) + 1^2 = 4 + 2 + 1 = 7$

Nearest Co-channel Neighbor

- move i cells along any chain or hexagon.
- then turn 60 degrees counterclockwise and move j cells.



N=19
(i=3, j=2)

Channel Assignment Strategies: Fixed Channel Assignments

- Each cell is allocated a predetermined set of voice channels.
- If all the channels in that cell are occupied, the call is blocked, and the subscriber does not receive service.
- Variation includes a borrowing strategy: a cell is allowed to borrow channels from a neighboring cell if all its own channels are occupied. This is supervised by the MSC.

Channel Assignment Strategies: Dynamic Channel Assignments

- Voice channels are not allocated to different cells permanently.
- Each time a call request is made, the serving base station requests a channel from the MSC.
- The switch then allocates a channel to the requested call based on a decision algorithm taking into account different factors: frequency re-use of candidate channel and cost factors.
- Dynamic channel assignment is more complex (real time), but reduces likelihood of blocking.

Interference and System Capacity

- major limiting factor in performance of cellular radio systems
- two main types:
  - co-channel interference
  - adjacent channel interference
- effect of interference:
  - voice channel: cross talk
  - control channel: missed or blocked calls
- sources of interference:
  - other mobiles in same cell
  - a call in progress in a neighboring cell
  - other base stations operating in the same frequency band
  - Non-cellular system leaking energy into the cellular frequency band

Co-Channel Interference

- cells that use the same set of frequencies are called co-channel cells.
- Interference between the co-channel cells is called co-channel interference.
- Co-channel reuse ratio: Q = D/R
  - R: radius of cell
  - D: distance between nearest co-channel cells

  $$Q = \sqrt{3N}$$
- Small Q ➔ small cluster size N ➔ large capacity
- large Q ➔ good transmission quality
- tradeoff must be made in actual cellular design

Co-Channel Interference

- Signal to interference ratio (SIR) or S/I for a mobile receiver is given by

  $S/I = SIR = S/\sum_{i=1..i0} I_i$

- S = signal power from designated base station
- I_i = interference power caused by the i-th interfering co-channel cell

Assumptions

- For any given antenna (base station) the power at a distance d is given by $Pr = Po\ (d/do)^{-\alpha}$ where α is path loss exponent

- $S/I = R^{-\alpha}/\sum_{i=1..i0}(D_i)^{-\alpha}$

Co-channel Interference

- If the mobile is at the center of the cell, Di = D
  - $S/I = R^{-\alpha}/D^{-\alpha} \sum_{i=1..i0} 1 = (R/D)^{-\alpha}/i_0$
- What's S/I in a hexagonal geometry?

Co-channel Interference (Cont.)

- **For a hexagonal geometry**
  - $D / R = \sqrt{3N}$ = Q - co-channel reuse ratio
  - $S / I = [\sqrt{3N}]^{\alpha} / i_0$

Example 4

- consider 6 closest co-channel cells, i0 = 6
  - $\alpha = 4$
  - require SIR > 18 dB
- Q: what is the minimum cluster size?

Example 4

- consider 6 closest co-channel cells, i0 = 6
  - $\alpha = 4$
  - require SIR > 18 dB
- Q: what is the minimum cluster size?
- A: $S / I = [\sqrt{3N}\,]^{\alpha} / i_0 = 9N^2/6 = 3N^2/2$

  $10 \log (3N^2/2) > 18$

  $N > 6.49$

Co-Channel Interference

- Co-channel interference

  $S/I = SIR = S/\sum_{i=1..i0} I_i$

  – For a hexagonal geometry

    - $D / R = \sqrt{3N}$ = Q - co-channel reuse ratio
    - $S / I = [\sqrt{3N}]^{\alpha} / i_0$

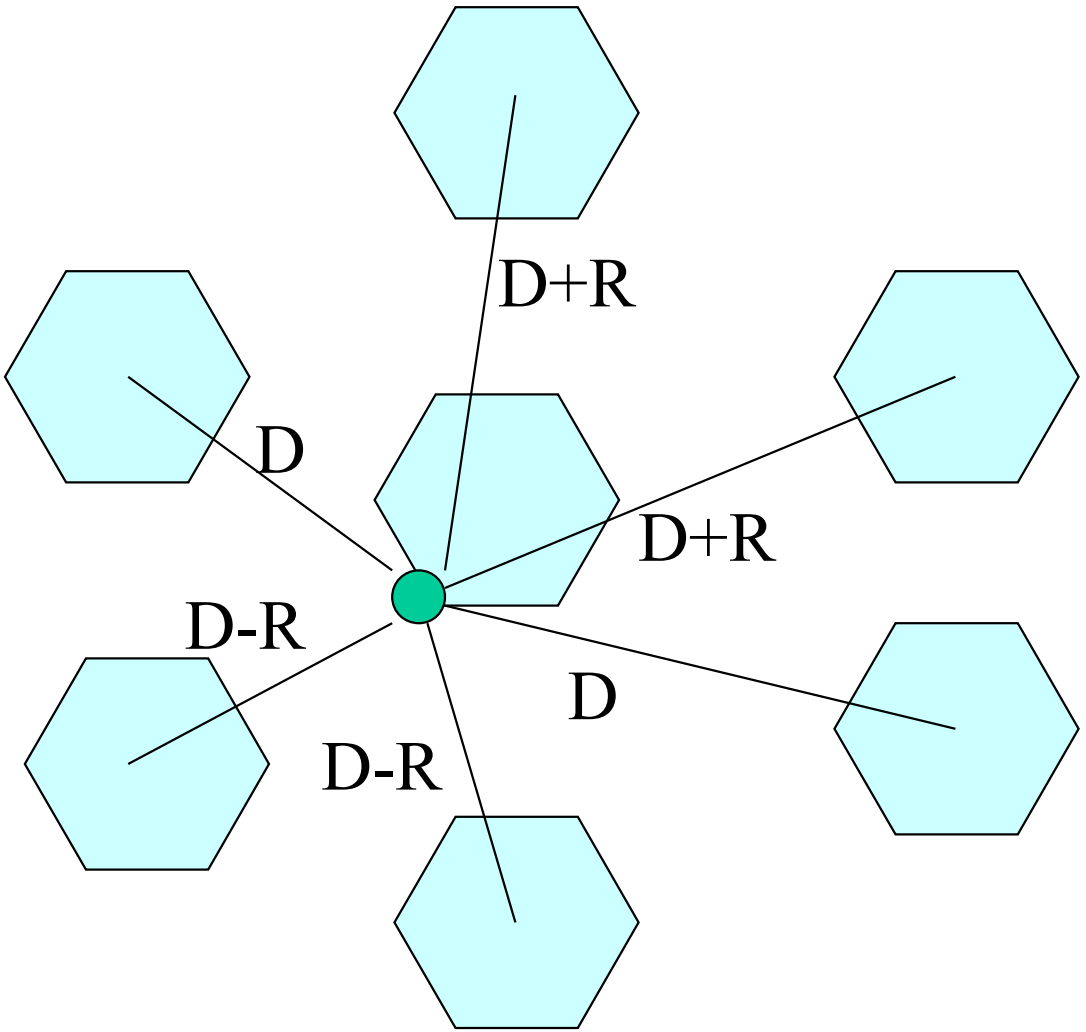
- Worst case co-channel interference

Worst Case Interference

- When the mobile is at the cell boundary (point A), it experiences worst case co-channel interference on the forward channel.
- The marked distances between the mobile and different co-channel cells are based on approximations made for easy analysis.

Worst Case Interference

- $S/I \sim R^{-4} / [2(D-R)^{-4} + 2(D+R)^{-4} + 2D^{-4}]$



Adjacent Channel Interference

- Interference resulting from signals where are adjacent in frequency to the desired signal.
- Due to imperfect receiver filters that allow nearby frequencies to leak into pass band.

Adjacent Channel Interference

- Interference resulting from signals where are adjacent in frequency to the desired signal.
- Due to imperfect receiver filters that allow nearby frequencies to leak into pass band.
- Can be minimized by careful filtering and assignments, and by keeping frequency separation between channel in a given cell as large as possible, the adjacent channel interference may be reduced considerably.

Increasing Capacity in Cellular Systems

- As demand for wireless services increases, the number of channels assigned to a cell is not enough to support the required number of users.
- Solution is to increase channels per unit coverage area.

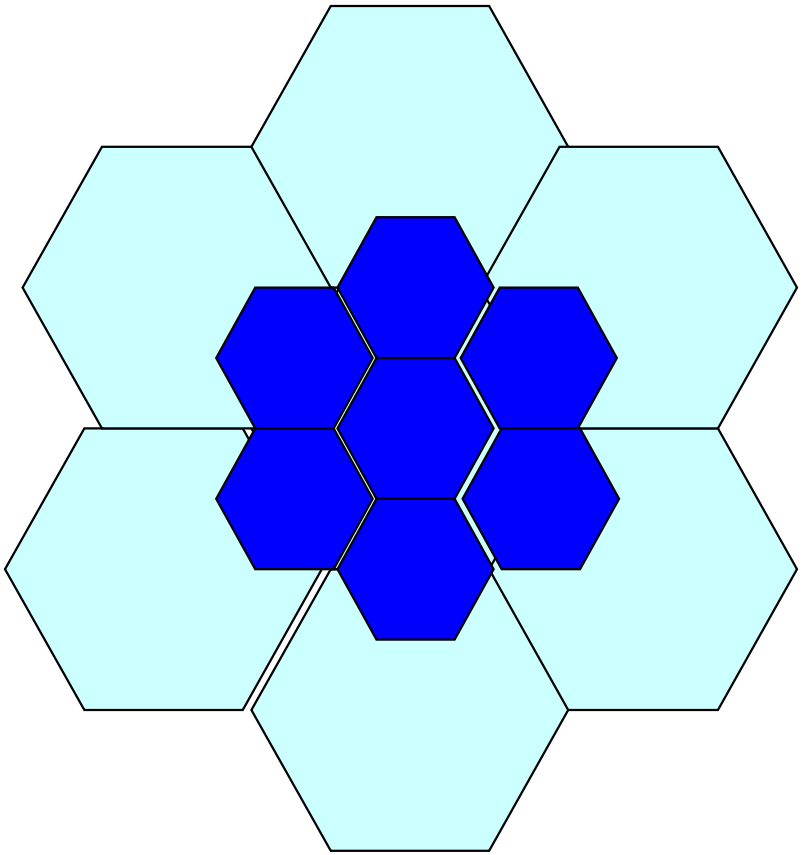
Approaches to Increasing Capacity

- Frequency borrowing
  - frequencies are taken from adjacent cells by congested cells
- Cell splitting
  - cells in areas of high usage can be split into smaller cells
- Cell sectoring
  - cells are divided into a number of wedge-shaped sectors, each with their own set of channels
- Microcells
  - antennas move to buildings, hills, and lamp posts

Cell Splitting

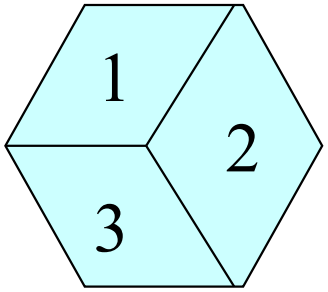
- subdivide a congested cell into smaller cells
- each with its own base station, reduction in antenna and transmitter power
- more cells ➔ more clusters ➔ higher capacity
- achieves capacity improvement by essentially rescaling the system.

Cell Splitting from radius R to R/2

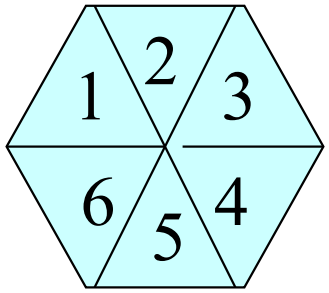


Sectoring

- In basic form, antennas are omnidirectional
- Replacing a single omni-directional antenna at base station with several directional antennas, each radiating within a specified sector.



3 sectors



6 sectors

Sectoring

- achieves capacity improvement by essentially rescaling the system.
- less co-channel interference, number of cells in a cluster can be reduced
- Larger frequency reuse factor, larger capacity

Micro Cell Zone Concept

- Large control base station is replaced by several lower powered transmitters on the edge of the cell.
- The mobile retains the same channel and the base station simply switches the channel to a different zone site and the mobile moves from zone to zone.
- Since a given channel is active only in a particular zone in which mobile is traveling, base station radiation is localized and interference is reduced.

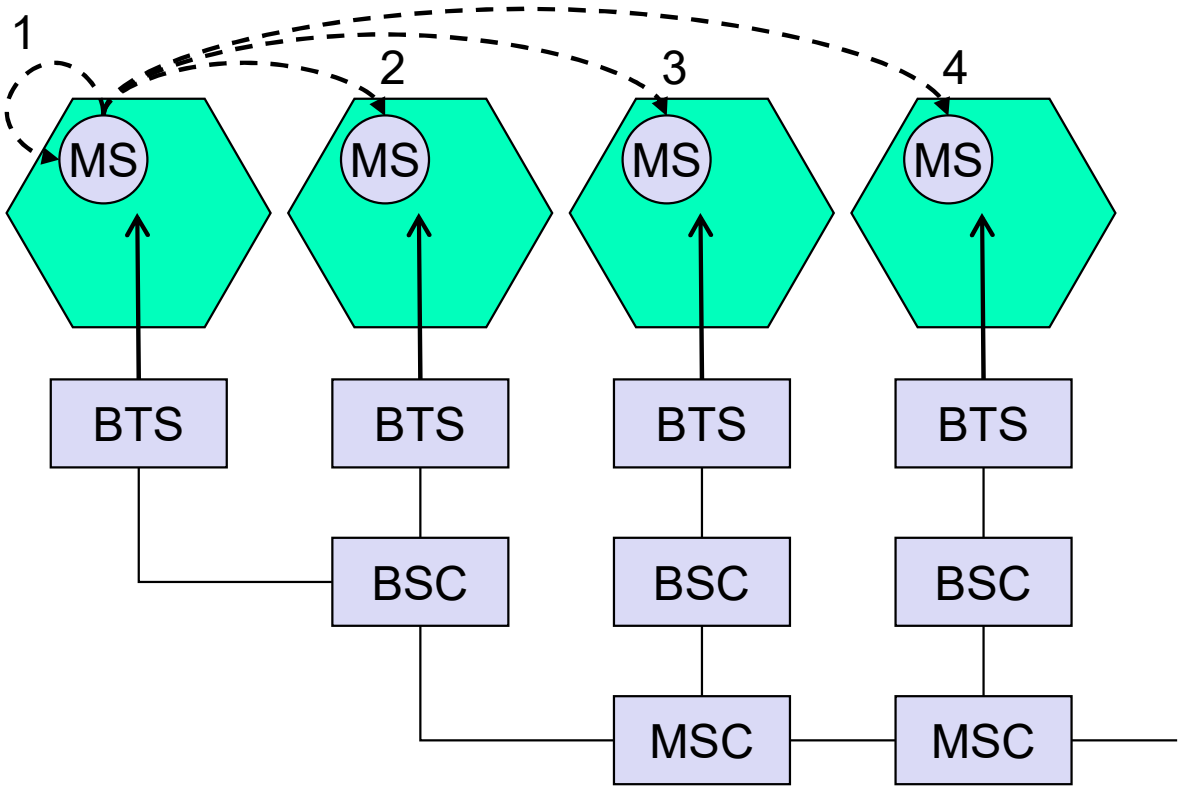
Handoffs

- Handoff - when a mobile moves into a different cell while a conversation is in progress, the MSC automatically transfers the call to a new channel belonging to the new base station

Handoffs

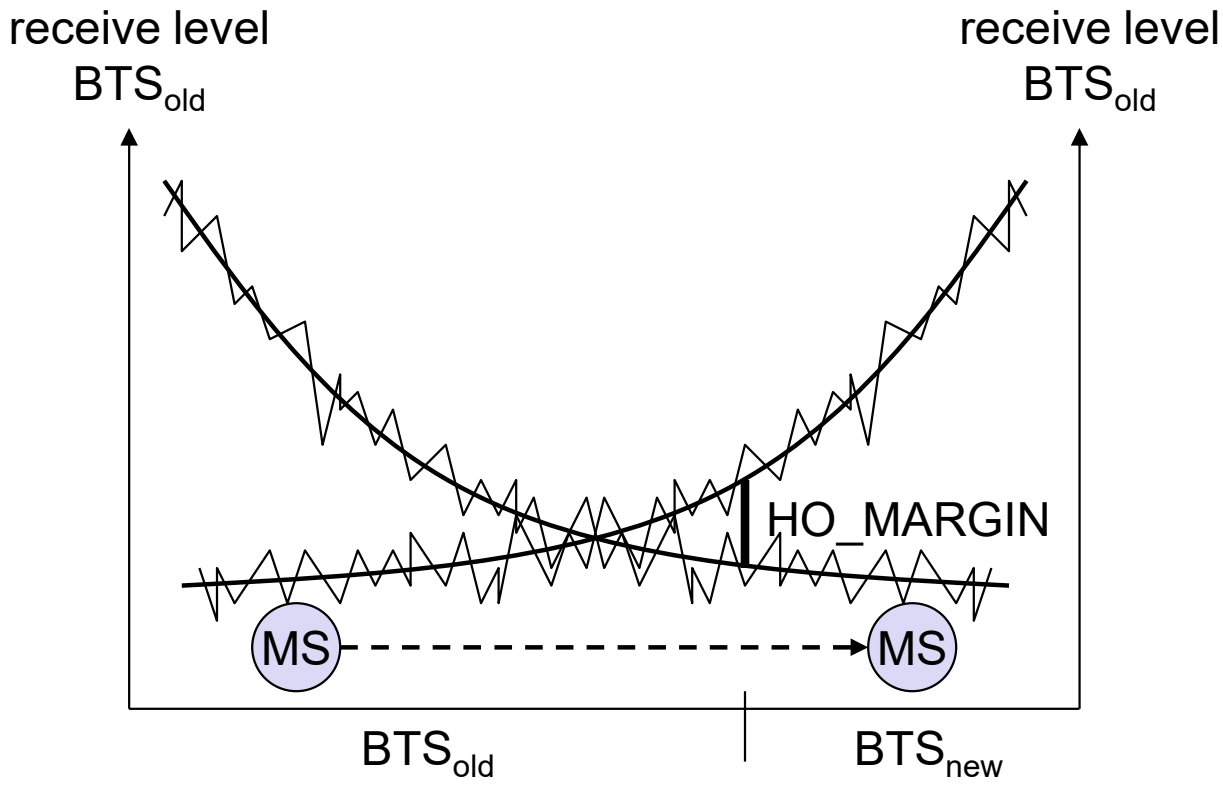
- important task in any cellular radio system
- must be performed successfully, infrequently, and imperceptible to users.
- identify a new base station
- channel allocation in new base station
- high priority than initiation request (block new calls rather than drop existing calls)

4 types of handover

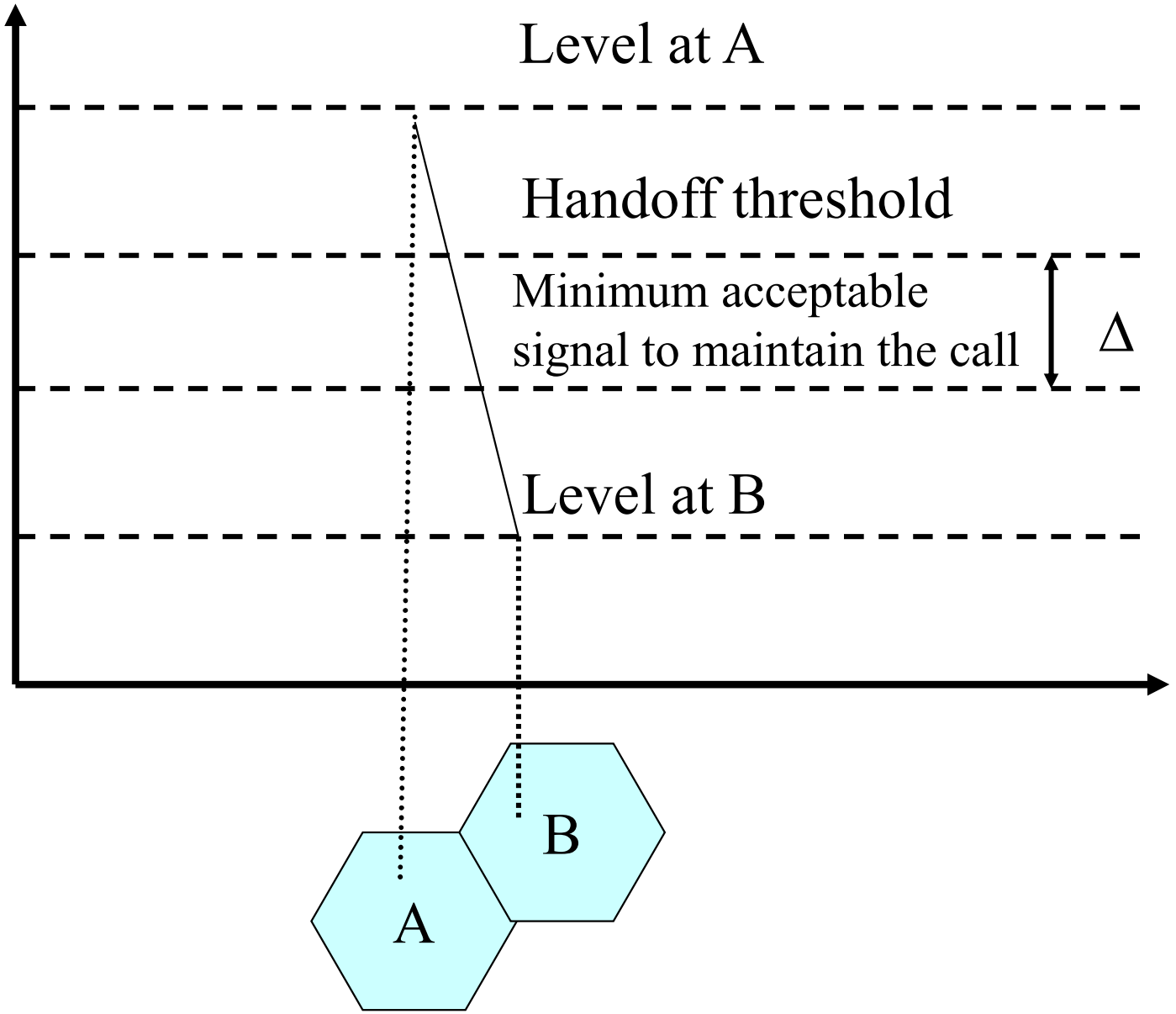


Intra-cell Inter-cell, Inter-BSC, Inter-MSC
Intra-BSC Intra-MSC

Handover decision



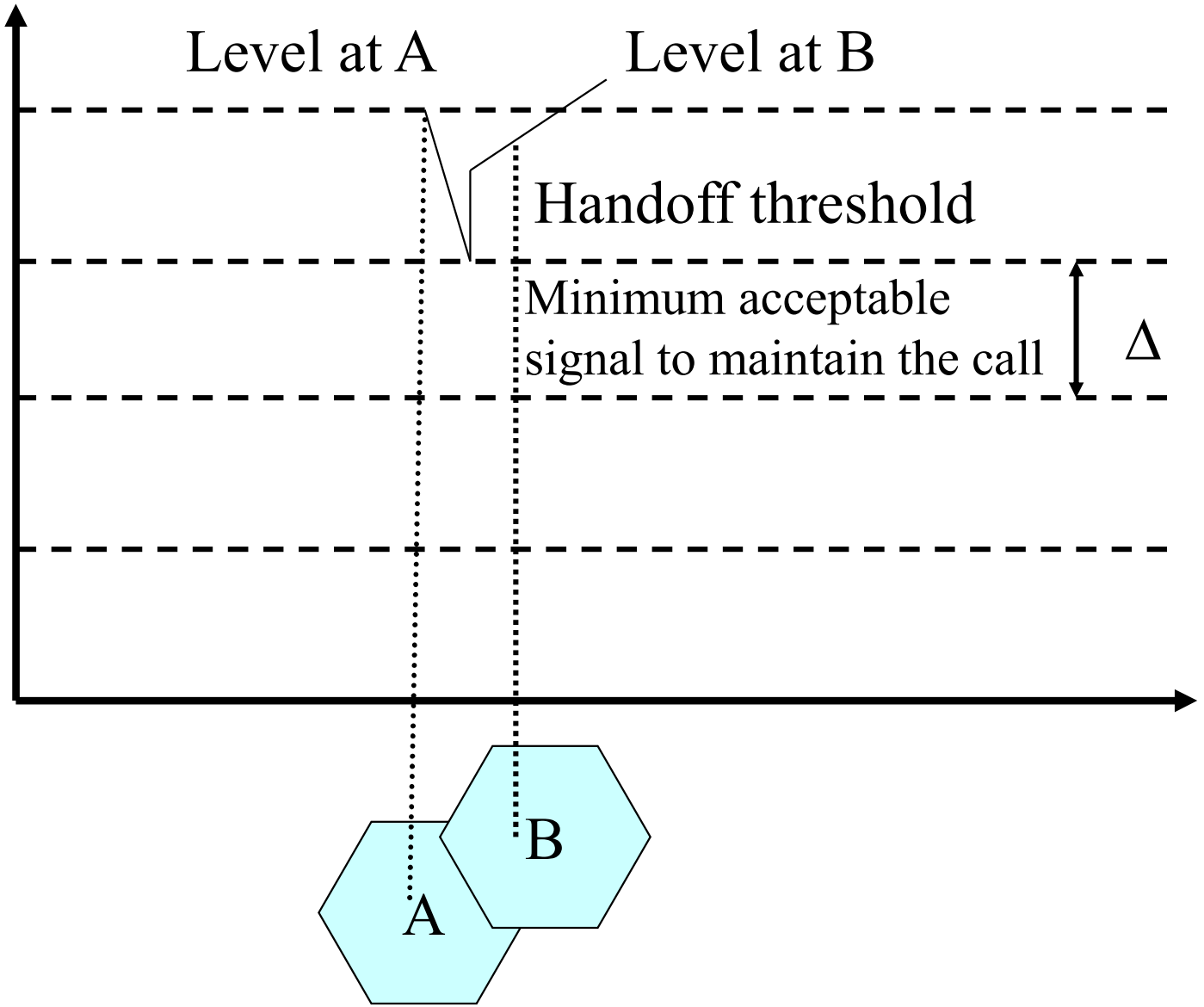
Handoffs


Level at A
Handoff threshold
Minimum acceptable
signal to maintain the call
Δ
Level at B
B
A

Choice of Margin

- Δ too small:
  - Insufficient time to complete handoff before call is lost
  - More call losses
- Δ too large:
  - Too many handoffs
  - Burden for MSC

Proper Handoff



Styles of Handoff

- Network Controlled Handoff (NCHO)
  - in first generation cellular system, each base station constantly monitors signal strength from mobiles in its cell
  - based on the measures, MSC decides if handoff necessary
  - mobile plays passive role in process
  - burden on MSC

Styles of Handoff

- Mobile Assisted Handoff (MAHO)
  - present in second generation systems
  - mobile measures received power from surrounding base stations and report to serving base station
  - handoff initiated when power received from a neighboring cell exceeds current value by a certain level or for a certain period of time
  - faster since measurements made by mobiles, MSC don't need monitor signal strength

Types of Handoff

- Hard handoff - (break before make)
  - FDMA, TDMA
  - mobile has radio link with only one BS at anytime
  - old BS connection is terminated before new BS connection is made.

Types of Handoff

- Soft handoff (make before break)
  - CDMA systems
  - mobile has simultaneous radio link with more than one BS at any time
  - new BS connection is made before old BS connection is broken
  - mobile unit remains in this state until one base station clearly predominates

Brief Outline of Cellular Process

- Telephone call placed to mobile user
- Telephone call made by mobile user

Telephone call to mobile user

- Step 1 – The incoming telephone call to Mobile X is received at the MSC.
- Step 2 – The MSC dispatches the request to all base stations in the cellular system.
- Step 3 – The base stations broadcast the Mobile Identification Number (MIN), telephone number of Mobile X, as a paging message over the FCC throughout the cellular system.

Telephone call to mobile user

- Step 4 – The mobile receives the paging message sent by the base station it monitors and responds by identifying itself over the reverse control channel.
- Step 5 – The base station relays the acknowledgement sent by the mobile and informs the MSC of the handshake.
- Step 6 – The MSC instructs the base station to move the call to an issued voice channel within the cell.

Telephone call to mobile user

- Step 7 – The base station signals the mobile to change frequencies to an unused forward and reverse voice channel pair.
- At the same time, another data message (alert) is transmitted over the forward voice channel to instruct the mobile to ring.

Telephone Call Placed by Mobile

- Step 1 – When a mobile originates a call, it sends the base station its telephone number (MIN), electronic serial number (ESN), and telephone number of called party. It also transmits a station class mark (SCM) which indicates what the maximum power level is for the particular user.
- Step 2 – The cell base station receives the data and sends it to the MSC.

Telephone Call Placed by Mobile

- Step 3 – The MSC validates the request, makes connection to the called party through the PSTN and validates the base station and mobile user to move to an unused forward and reverse channel pair to allow the conversation to begin.

Roaming

- All cellular systems provide a service called roaming. This allows subscribers to operate in service areas other than the one from which service is subscribed.
- When a mobile enters a city or geographic area that is different from its home service area, it is registered as a roamer in the new service area.

Roaming (Cont.)

- Registration
  - MSC polls for unregistered mobiles
  - Mobiles respond with MINs
  - MSC queries mobile's home for billing info
- Calls
  - MSC controls call and bills mobile's home

Example 5

- The US AMPS system is allocated 50 MHz of spectrum in the 800 MHz range and provides 832 channels. 42 of those channels are control channels. The forward channel frequency is exactly 45 MHz greater than the reverse channel frequency.
- a. Is the AMPS system simplex, half-duplex or duplex? What is the bandwidth for each channel, and how is it distributed between the base station and the subscriber?

Solution (a)

- AMPS system is duplex.
- Total bandwidth = 50 MHz
- Total number of channels = 832
- Bandwidth for each channel = 50 MHz / 832 = 60 KHz
- 60 KHz is split into two 30 KHz channels (forward and reverse channels). The forward channel is 45 MHz > reverse channel.

Example 5 (Cont.)

- b. Assume a base station transmits on channel 352 operating at 880.56 MHZ. What is the transmission frequency of a subscriber unit transmitting on channel 352?

Solution (b.)

- For $F_{fw} = 880.560$ MHz
- $F_{rev} = F_{fw} - 45$ MHz $= 835.560$ MHz

Example 5 (Cont.)

- c. The A side and B side cellular carriers evenly split the AMPS channels. Find the number of voice channels and number of control channels for each carrier?

Solution (c.)

- Total number of channels = 832 = N
- Total number of control channels Ncon = 42
- Total number of voice channels Nvo = 832 – 42 = 790
- Number of voice channels for each carrier = 790 / 2 = 395 channels
- Number of control channels for each carrier = 42 / 2 = 21 channels

Example 5 (Cont.)

- d. For an ideal hexagonal cellular layout which has identical cell sites, what is the distance between the centers of the two nearest co-channel cells:
  - For 7 cell reuse?
  - For 4 cell reuse?

Solution (d.)

- N = 7
  - $Q = D/R = (3N)^{1/2} = 21^{1/2} = 4.58$ ➔ D=4.58R
- N=4
  - $Q = 12^{1/2} = 3.46$ ➔ D = 3.46R

Example 6

- What is the number of users per cell when the system has 63 voice channels, the cluster size of 7, blocking probability of 1%, and average user load of 0.03 [Erlang].

Solution 6

- Each cell has 63/7 = 9 channels
- 9 channels @ block rate = 1% ➔ 3.783 [Erlang]
- 3.783/0.03 = 126 users

Example 7

- You are in charge of AMPS system composed of 49 cells (7 clusters) and total of 126 channels. The current statistics of the system indicate that there is 50% call blocking probability and the users are complaining about the poor quality of service. You propose to improve the system performance by splitting each cell into 3 smaller cells.
- (a) What's the new blocking rate?
- (b) To reduce the interference, you propose to use 120 degree sectors (no frequency reuse among the sectors within a cell). What is the new blocking probability?

Solution 7

- Each cell has 126/7 = 18 channels
- 18 channels @ 50% blocking rate ➔ offered load = 34.173
- Each smaller cell has 34.173/3 = 11.391 Erlang
- 18 channels under 11.391 Erlang ➔ blocking rate ~ 2%

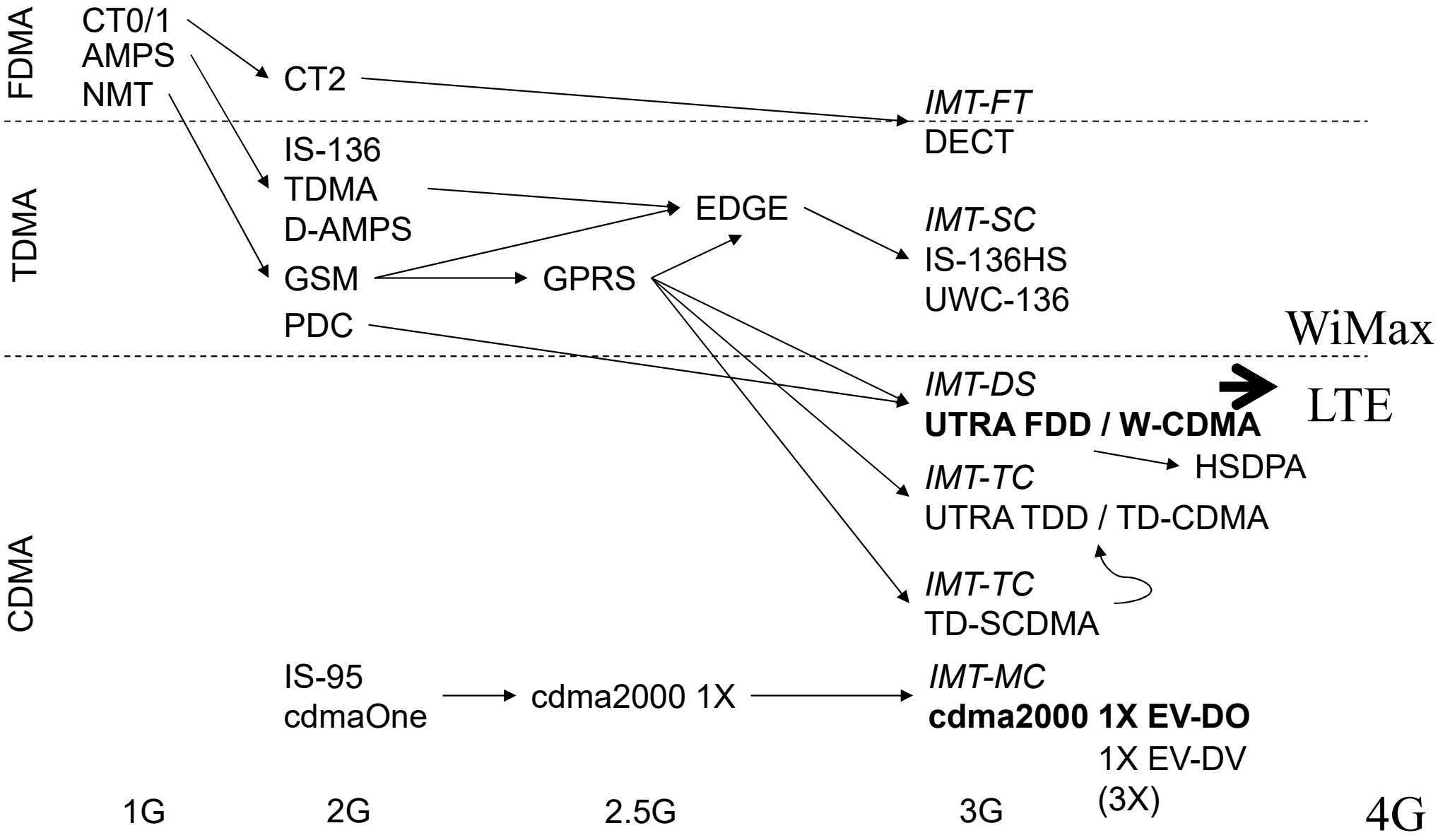
Solution 7

- Splitting into 3 sectors/cell ➔ each sector has offered load = 11.391/3 = 3.797 Erlang @ 18/3 = 6 channels ➔ blocking rate ~ 10%

Cellular Networks

- Introduction
- Frequency reuse
- Channel assignment strategies
- Techniques to increase capacity
- Handoff
- Roaming
- Cellular network provision
- Cellular standards

Development of mobile telecommunication systems



1G

- 1G system (1980)
  - Started in 1980
  - Analog and only voice channels
  - 2.4 Kbps

2G

- Digital and voice channels (1991)
  - Data: SMS, picture msgs, MMS
  - 50 Kbps
  - 10 km range
  - IS-136 TDMA: combined FDMA/TDMA (north America)
  - GSM (global system for mobile communications): combined FDMA/TDMA
  - most widely deployed
  - Circuit switched data
- IS-95 CDMA: code division multiple access

2G (Cont.)

- 2.5 G systems: voice and data channels
  - for those who can't wait for 3G service: 2G extensions
  - enhanced data rates for global evolution (EDGE)
    - also evolved from GSM, using enhanced modulation
    - Data rates up to 384K
  - general packet radio service (GPRS)
    - first always-on data service
    - evolved from GSM
    - data sent on multiple channels (if available)
- CDMA-2000 (phase 1)
  - data rates up to 144K
  - evolved from IS-95

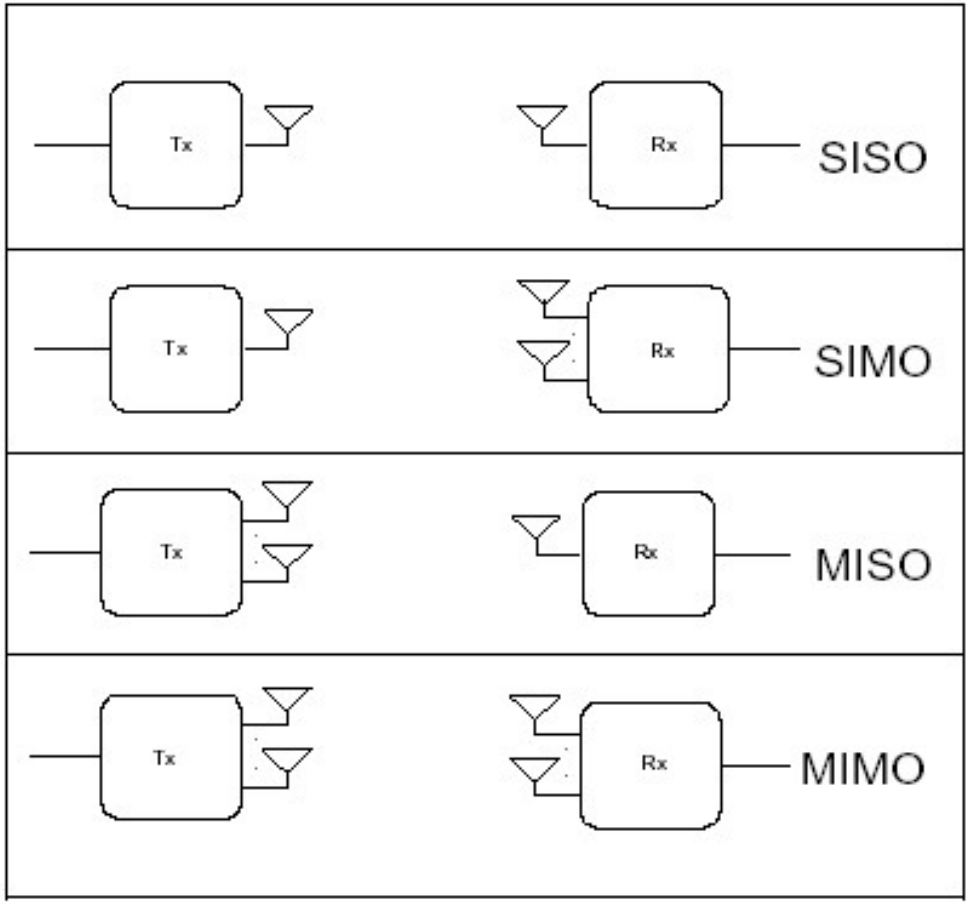
3G

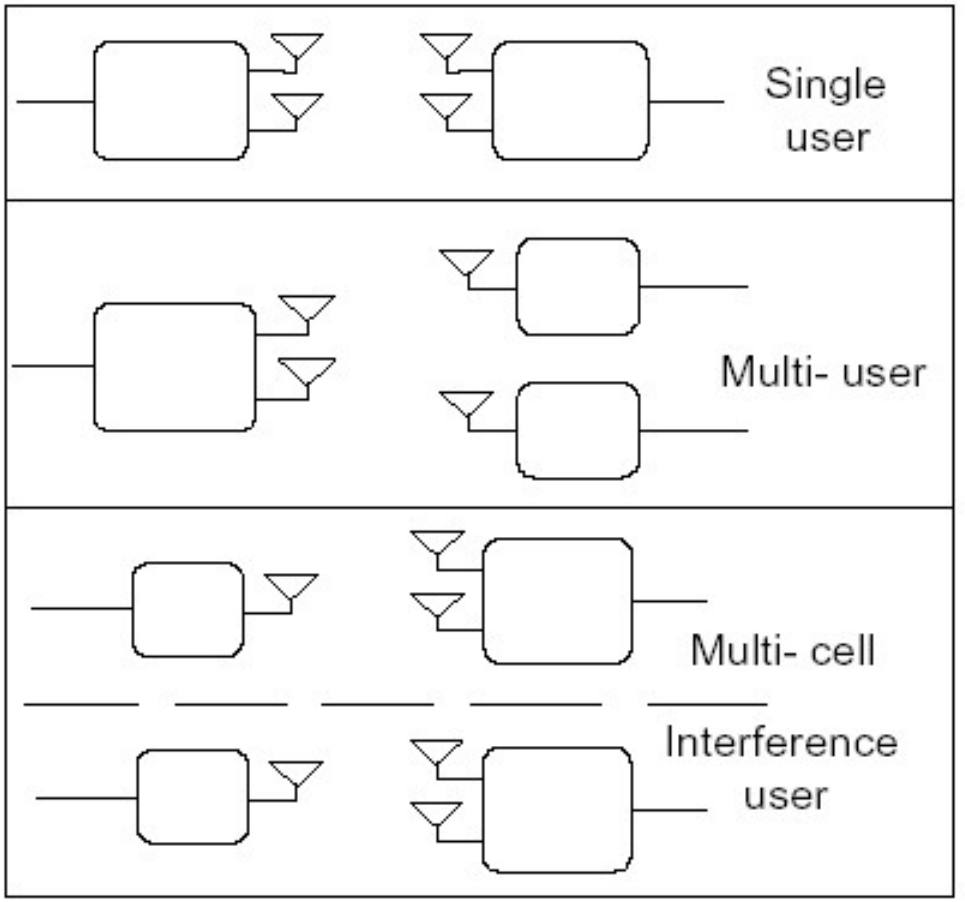
- UN's International Telecommunications Union IMT-2000 standard requires stationary speeds of 2Mbps and mobile speeds of 384kbps for a "true" 3G (1998)
  - Universal Mobile Telecommunications Service (UMTS)
    - GSM next step, but using CDMA
  - CDMA-2000
  - Edge
  - WCDMA
  - EVDO

4G

- Theoretical data rates: ~10Mbps downstream, ~5Mbps upstream
- LTE and WiMAX
- MIMO
- OFDMA

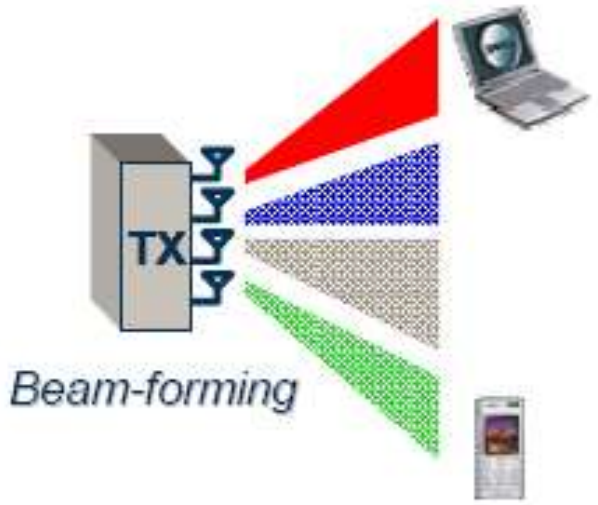
MIMO


Tx
Rx
SISO
Tx
Rx
SIMO
Tx
Rx
MISO
Tx
Rx
MIMO


Single user
Multi- user
Multi- cell
Interference user

Advanced Antenna Techniques

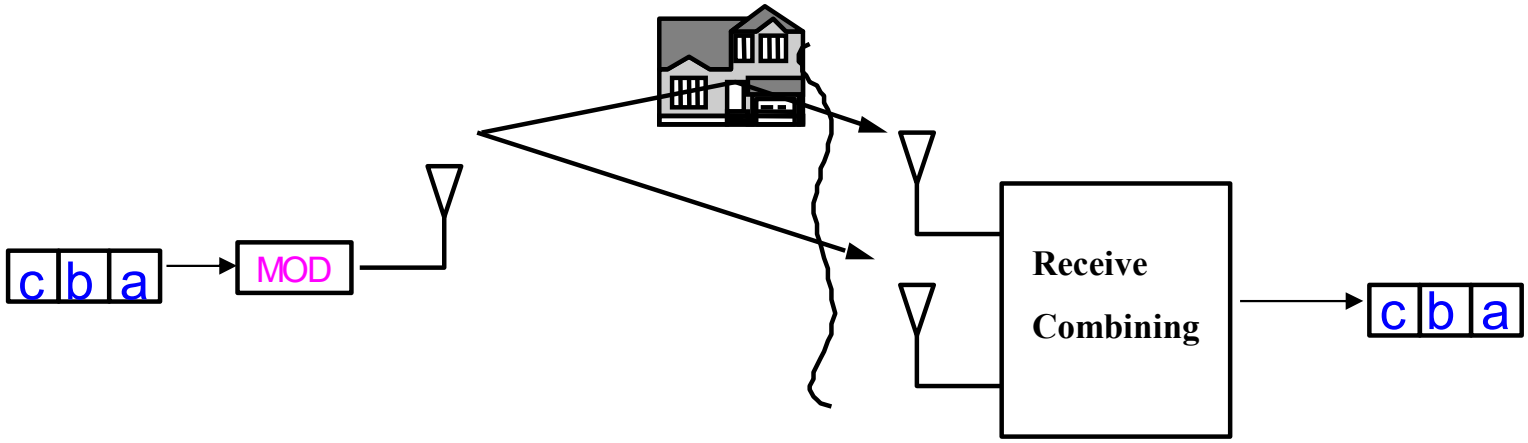
- Single data stream / user
- Beam-forming
  - ➢ Coverage, longer battery life
- Spatial Division Multiple Access (SDMA)
  - ➢ Multiple users in same radio resource
- Multiple data stream / user Diversity
  - ➢ Link robustness
- Spatial multiplexing
  - ➢ Spectral efficiency, high data rate support



Beam-forming

Multi-layer transmission ("MIMO")

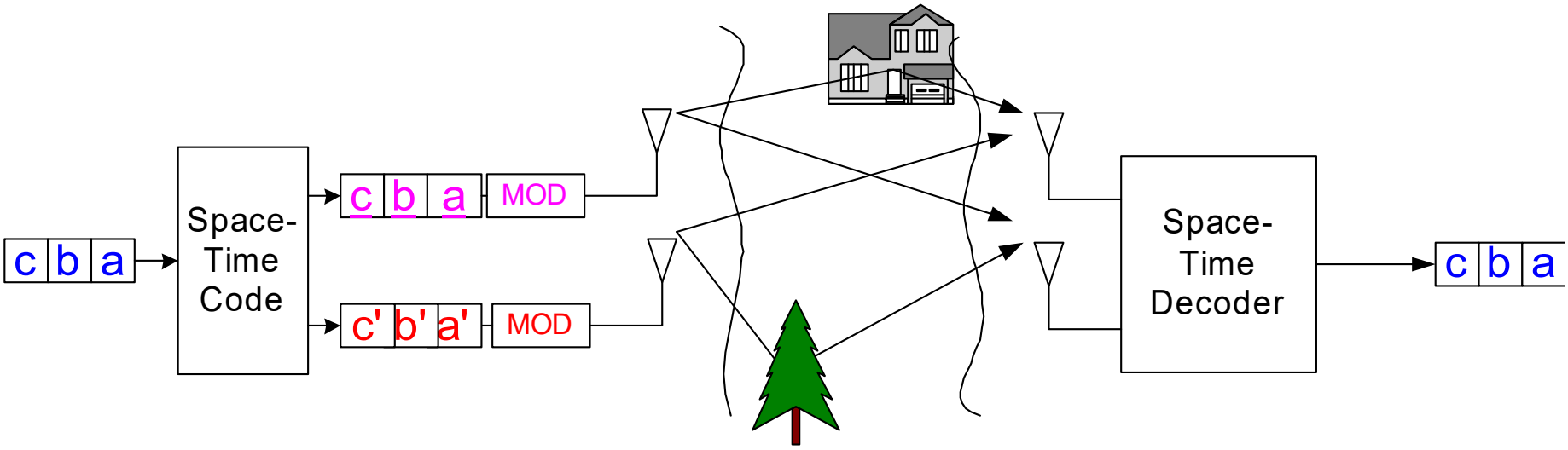
Diversity Gain



- Receive diversity
  - Transmitter modulates bits with R bits / s / Hz
  - Receiver combines signals from different paths
  - Systems works with as little as one of Mr paths

Presence of multiple paths ensures “quality”

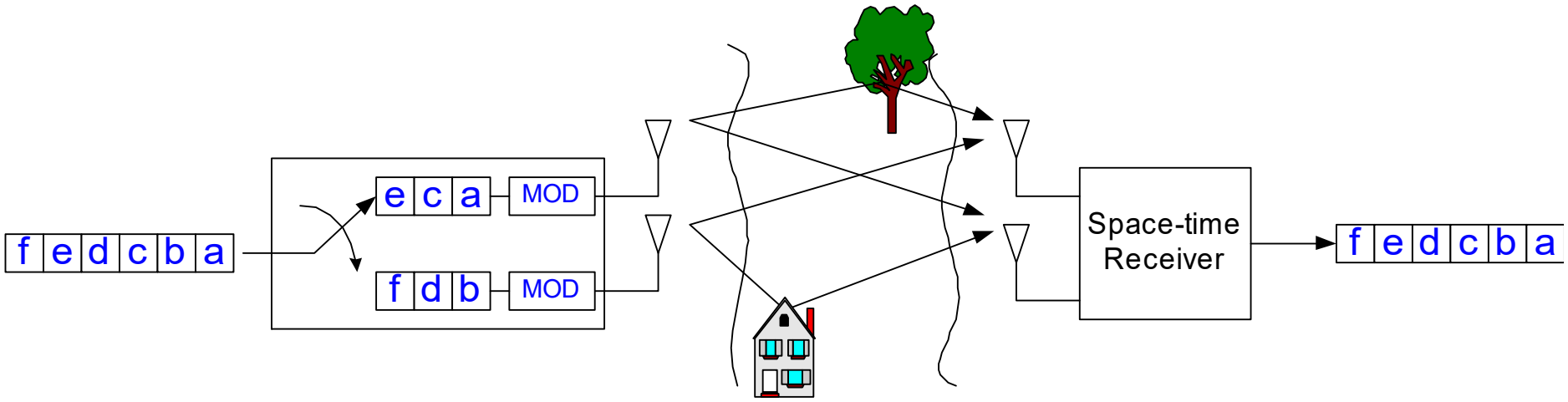
Diversity Gain



- Transmit diversity
  - Transmitter modulates bits with R bits / s / Hz
  - Diversity encoder ensures every bit -> every antenna
  - Systems works with as little as one of Mt Mr paths

Redundancy across multiple paths ensures “quality”

Multiplexing Gain



- Spatial multiplexing [Paulraj & Kailath'94] [Foschini'96]
  - Transmitter demultiplexes bits into Mt streams
  - Bits modulated onto symbols with R bits / s / Hz
  - Total spectrum efficiency is Mt R bits / s / Hz
  - Symbols separated at receiver and demultiplexed

Multiplexing takes advantage of multiple spatial data pipes

MIMO Diversity

Technique	Description	Complexity	Hardware Requirement	Performance (SNR Gain)	Key Advantage
Maximal Ratio Combining (MRC)	Weights each branch by its SNR and aligns phases before summing.	High	Full RF chain for every antenna	Optimal (Best SNR)	Maximizes signal quality by utilizing all available energy.
Selection Combining (SC)	"Selects the best one" by choosing the branch with the highest instantaneous SNR.	Low	Only 1 RF chain needed (with a switch)	Lowest (Significant loss vs MRC)	Simplest to implement; reduced power and cost.
Equal Gain Combining (EGC)	Aligns the phases of all branches but uses equal weights (no amplitude scaling).	Medium	Full RF chain for every antenna	Near-Optimal (Slightly below MRC)	Avoids the need for continuous amplitude estimation.
Precoding (Beamforming)	Processing done at the Transmitter. Uses Channel State Information (CSI) to "steer" the signal.	High	Multiple TX chains + Feedback link	Very High	Focuses energy toward the receiver; improves range.
Switch & Stay Combining (SSC)	Stays with one antenna until its SNR drops below a threshold, then switches.	Very Low	1 RF chain	Low (Similar to SC)	Reduces switching frequency compared to SC; saves power.

MIMO Detection

- Solve $y = Hx + n$

- Maximum likelihood ➔ exponential
  - $x = \text{argmin } x \in X \|y-Hx\|^2$

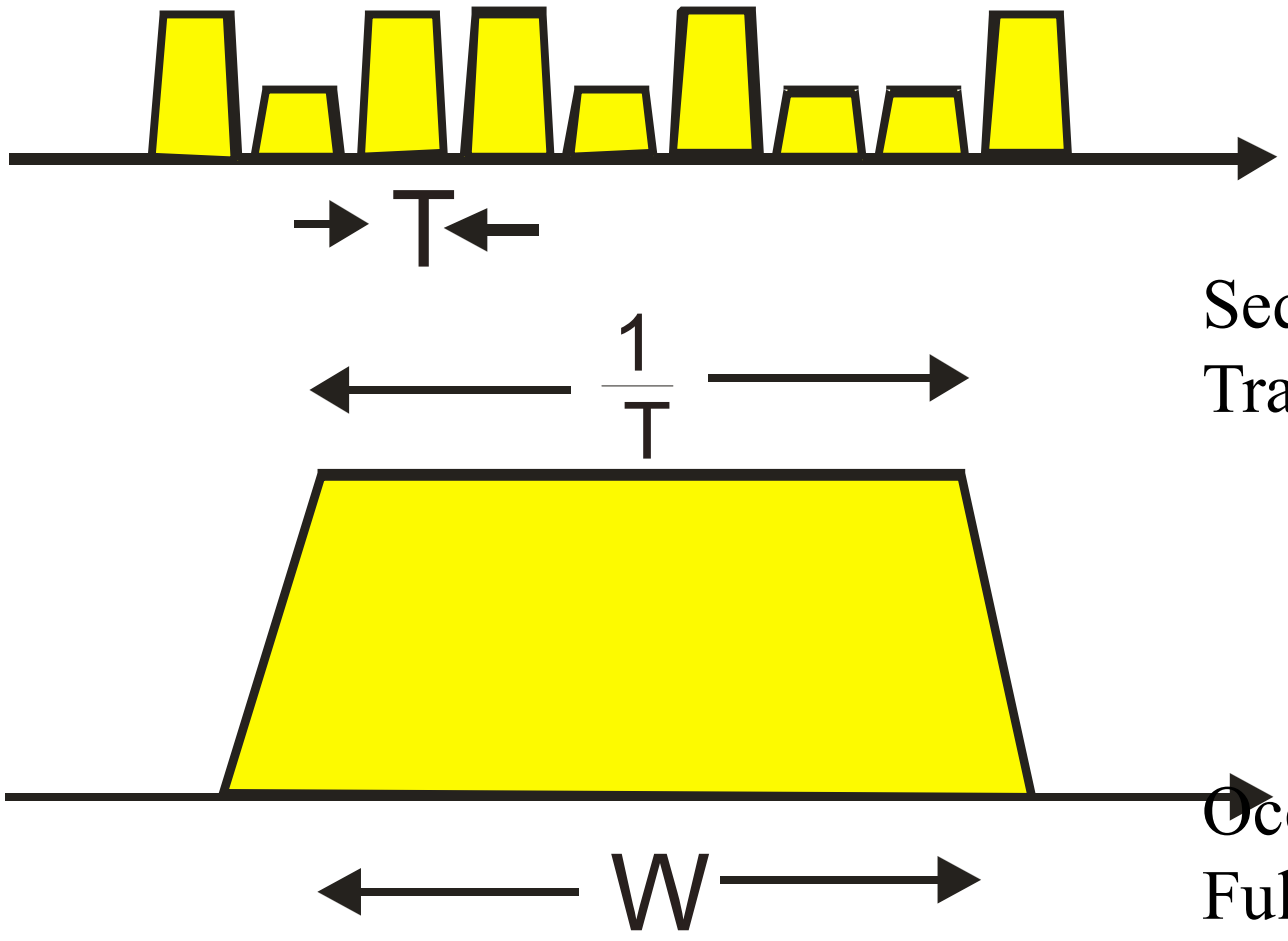
MIMO Detection

Decoding Scheme	Type	Performance (BER)	Complexity	Key Characteristic
Maximum Likelihood (ML)	Non-Linear	Optimal	Exponential	Compares received signal to all possible transmitted combinations. Impractical for high-order MIMO.
Zero Forcing (ZF)	Linear	Poor (Low SNR)	Low	Multiplies by the pseudo-inverse of the channel. Suffers from noise amplification.
MMSE	Linear	Moderate	Low	Minimizes mean square error. Balances noise reduction and interference suppression.
SIC (V-BLAST)	Non-Linear	Good	Medium	Decodes the strongest stream first, then "subtracts" it from the total signal to decode the rest.
Sphere Decoding (SD)	Non-Linear	Near-ML	Variable	Searches only a "sphere" around the received signal. Achieves ML performance with less computation.

Cellular Standards: Brief Overview

- 4G systems
  - Theoretical data rates: ~10Mbps downstream, ~5Mbps upstream
  - LTE and WiMAX
  - MIMO
  - OFDMA

Single Carrier System

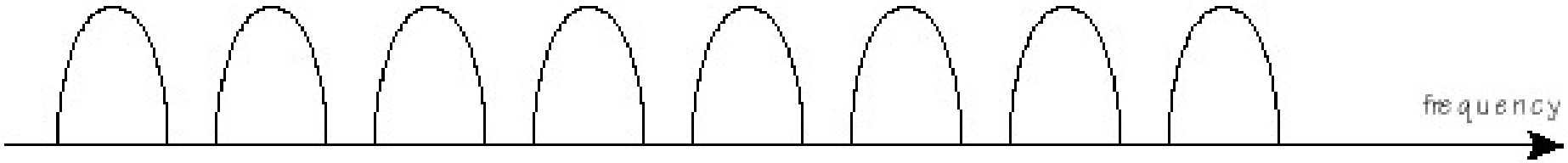


Sequential Transmission of Waveforms

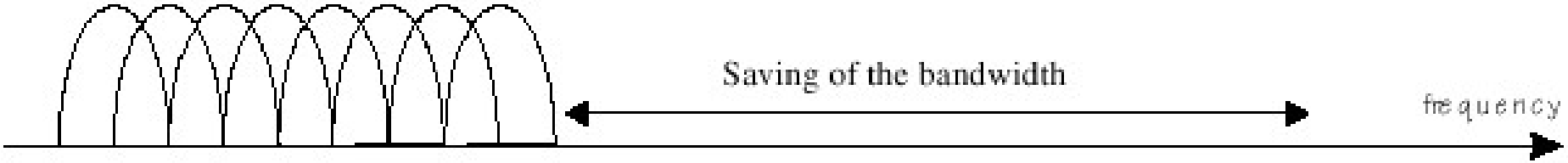
Waveforms are Short Duration T

Waveforms Occupy Full System Bandwidth 1/T

FDM vs. OFDM



Conventional Frequency Division Multiplex (FDM) multicarrier modulation technique

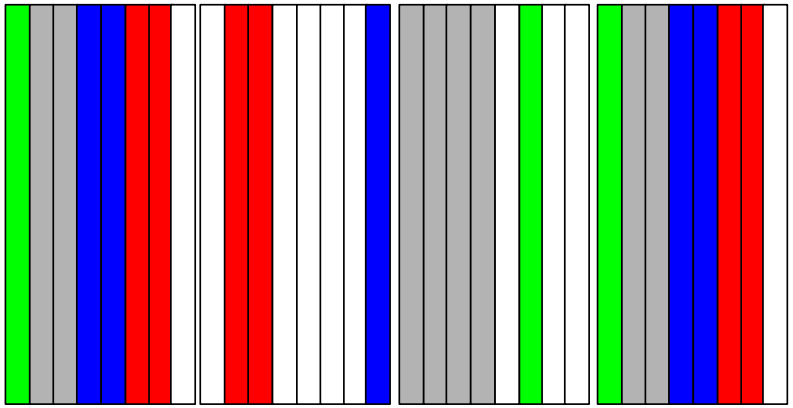


Orthogonal Frequency Division Multiplex (OFDM) multicarrier modulation technique

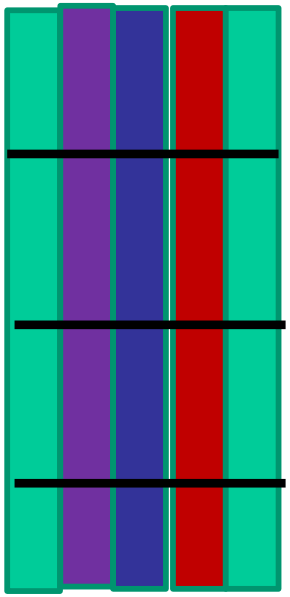
From OFDM to OFDMA

TDMA

t

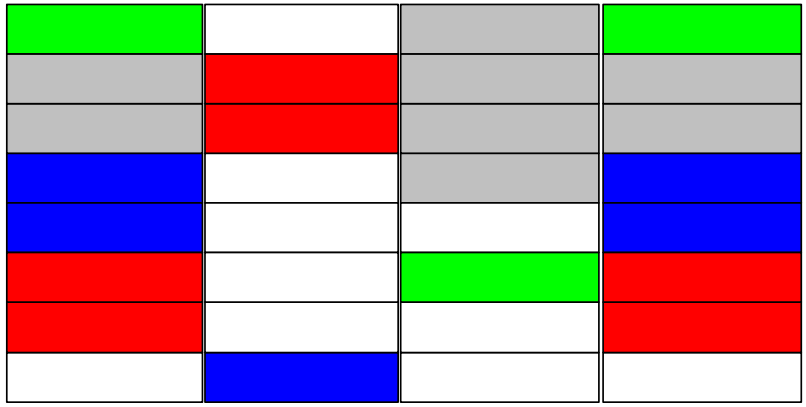


f



TDMA\OFDMA

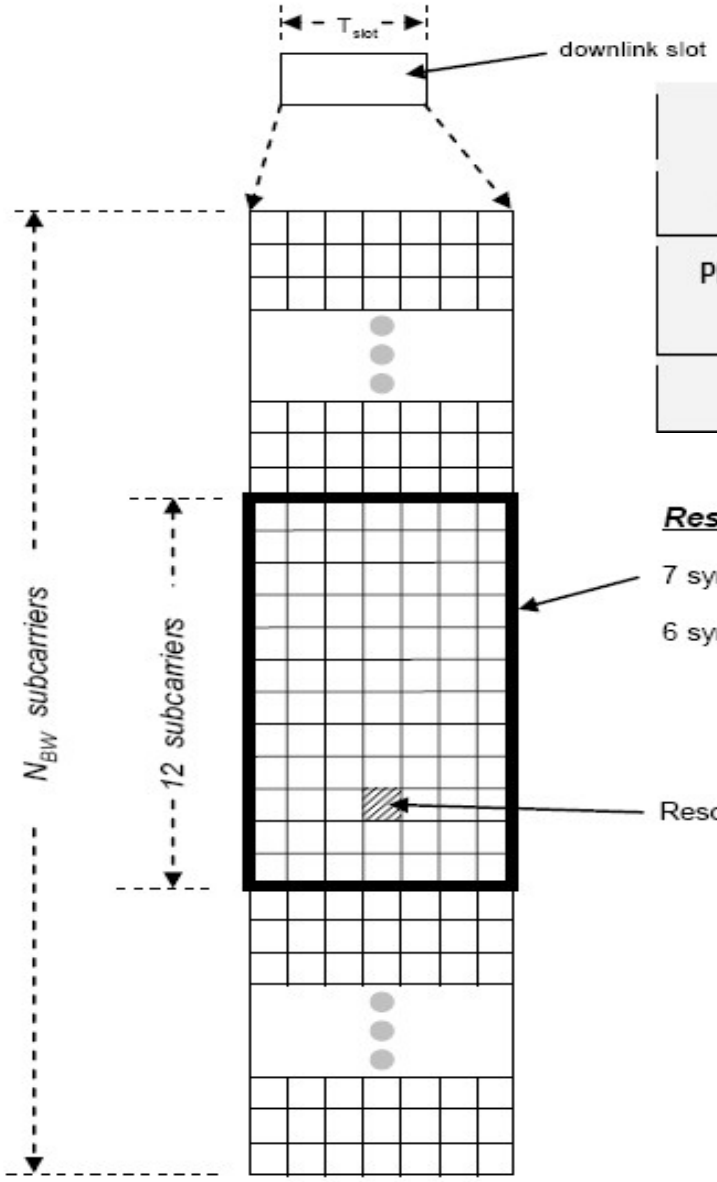
m



N

OFDM

LTE Generic Frame structure



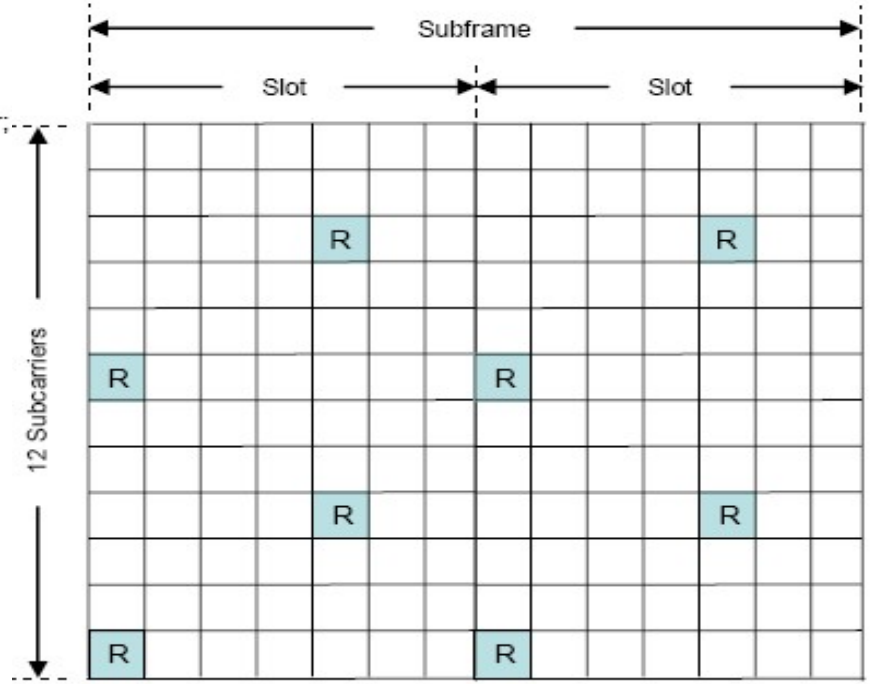
Available Downlink Bandwidth is Divided into Physical Resource Blocks

Bandwidth (MHz)	1.25	2.5	5.0	10.0	15.0	20.0
Subcarrier bandwidth (kHz)	15					
Physical resource block (PRB) bandwidth (kHz)	180					
Number of available PRBs	6	12	25	50	75	100

Resource Block:

7 symbols X 12 subcarriers (short CP), or;

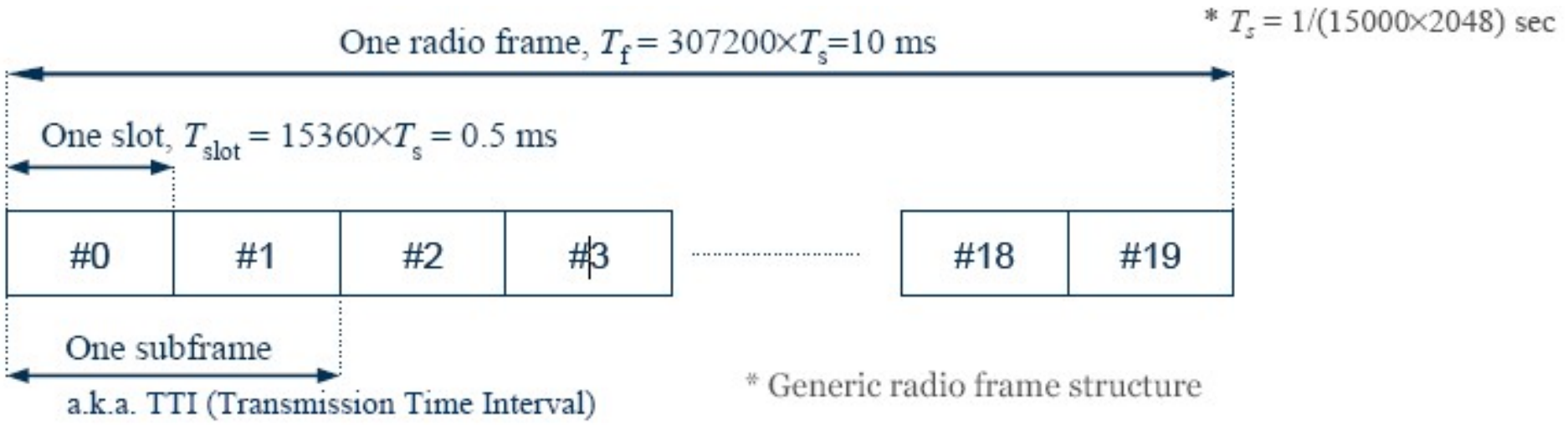
6 symbols X 12 subcarriers (long CP)



LTE Reference Signals are Interspersed Among Resource Elements

[source: 3GPP TR 25.814]

LTE Frame Structure



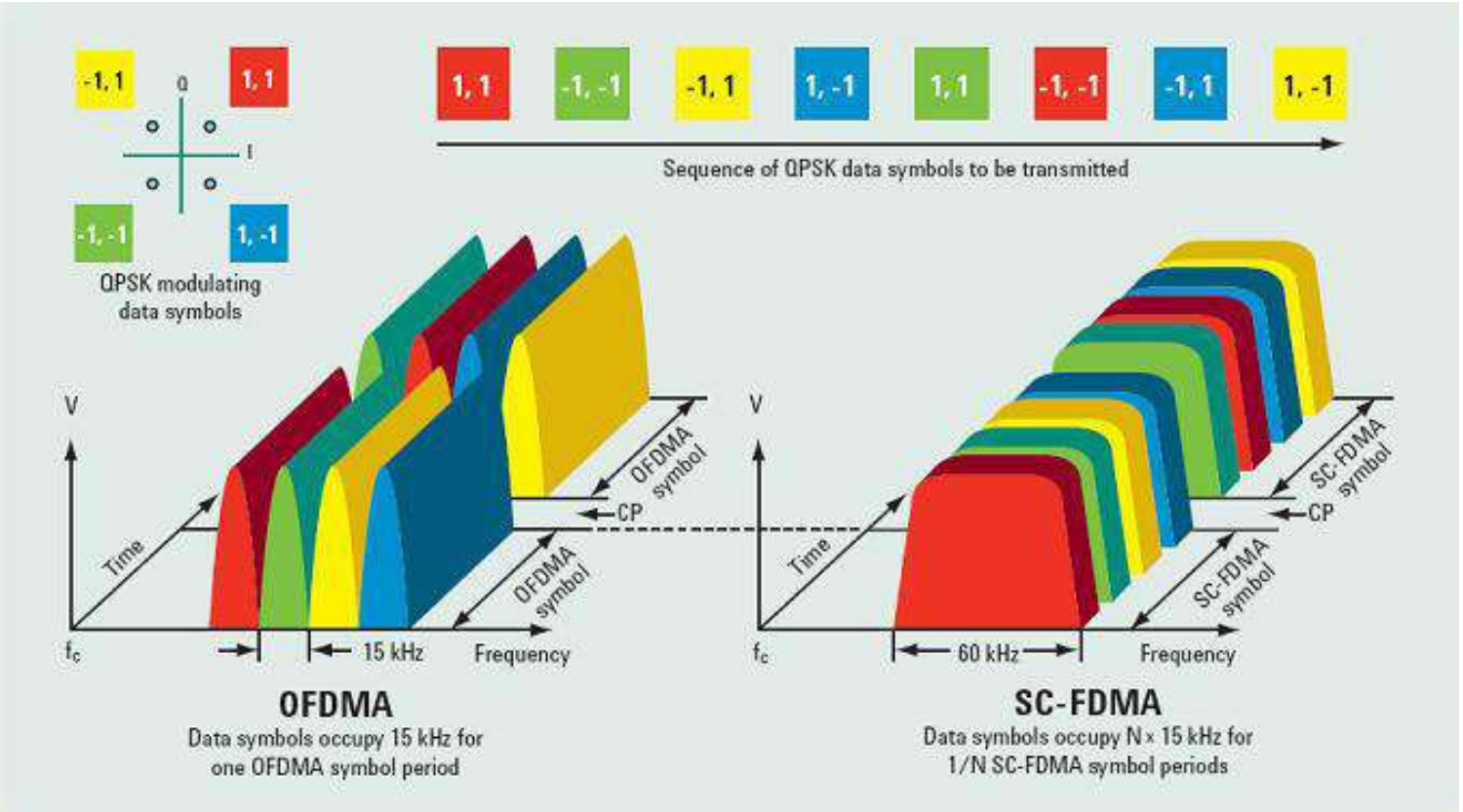
•One element that is shared by the LTE Downlink and Uplink is the generic frame structure. The LTE specifications define both FDD and TDD modes of operation. This generic frame structure is used with FDD. Alternative frame structures are defined for use with TDD.

•LTE frames are 10 msec in duration. They are divided into 10 subframes, each subframe being 1.0 msec long. Each subframe is further divided into two slots, each of 0.5 msec duration. Slots consist of either 6 or 7 ODFM symbols, depending on whether the normal or extended cyclic prefix is employed

[source: 3GPP TR 25.814]

LTE Uplink (SC-FDMA)

- SC-FDMA is a new single carrier multiple access technique which has similar structure and performance to OFDMA



A salient advantage of SC-FDMA over OFDM is low Peak to Average Power Ratio (PAPR) :

Increasing battery life

5G: Service-Aware-Architecture

•**Cloud-Native Core:** Unlike 4G's hardware-dependent core, 5G is "software-defined." It uses a **Service-Based Architecture** where network functions are like apps that can be moved and scaled instantly.

•**Network Slicing:** This is the most critical 5G data innovation. It allows an operator to create "virtual" networks on the same hardware. *Example:* A "Safety Slice" for self-driving cars with 99.999% reliability, completely isolated from a "Gaming Slice" optimized for speed.

5G: 3 Data Modes

- eMBB (Enhanced Mobile Broadband):
  - Goal: Extreme throughput.
  - Capability: 10–20 Gbps peak speeds. Handles 4K/8K video and "Volumetric" data (AR/VR).
- URLLC (Ultra-Reliable Low Latency):
  - Goal: Instant response.
  - Capability: Under 1ms air-interface latency. Essential for V2X (Vehicle-to-Everything) and remote industrial control.
- mMTC (Massive Machine-Type Communications):
  - Goal: Density.
  - Capability: Supports 1 million devices per km^2. Designed for low-power sensors that only send a few bytes but stay connected for 10 years on one battery.

5G: Spectrum Shift

•**Sub-6 GHz (FR1):** The "Coverage Layer." Signals travel through walls and over miles. This is what you usually see on your phone.

•**mmWave (FR2):** The "Capacity Layer." Extremely high frequency (24GHz+). It provides the "insane" multi-gigabit speeds but is blocked by a window or a tree.

5G Technologies

- **Massive MIMO:** 4G used up to 4 antennas; 5G uses **64 or 128**. This allows the tower to talk to dozens of people on the exact same frequency at the same time without interference.
- **Beamforming:** Instead of wasting energy broadcasting signal everywhere, 5G uses "constructive interference" to focus the radio waves into a narrow **beam** that follows the user as they move.
- **Edge Computing (MEC):** To reach <1ms latency, 5G moves the "data brain" closer to the user. Instead of data traveling to a central server 500 miles away, it's processed at the base of the cell tower.
- **CUPS (Control and User Plane Separation):** 5G separates the "directions" (Control) from the "payload" (Data), allowing the network to route data more efficiently and reduce bottlenecks.

6G: From Communication to Perception

•**Network as a Sensor (ISAC):** 6G is the first generation where the radio waves themselves act as a high-resolution radar. The network "sees" the environment without cameras, allowing for centimeter-level tracking of people and objects.

•**Deterministic Service:** Unlike the "best-effort" internet we have today, 6G is being engineered for **guaranteed timing**. This is vital for "Physical AI" like swarms of collaborative robots and synchronized digital twins.

•**AI-Native Architecture:** In 5G, AI is an add-on. In 6G, the **Air Interface** (how your phone talks to the tower) is optimized by AI in real-time to overcome interference that humans can’t program for.

New 6G Usage Scenarios (ITU-R IMT-2030)

- **Immersive Communication:** Supporting **Holographic Telepresence** and the **Internet of Senses** (transmitting haptic/touch and smell data).
- **Integrated AI & Communication:** Distributed computing where your phone offloads heavy AI processing (like real-time language translation or vision) directly into the 6G "Edge Cloud."
- **Ubiquitous Connectivity:** Seamlessly integrating **Non-Terrestrial Networks (NTN)**. Your standard 6G phone will connect to Low-Earth Orbit (LEO) satellites automatically when you are out of range of ground towers.

6G Key Enablers

•**Terahertz (THz) & Sub-THz Frequencies:** * **The Tech:** Utilizing spectrum between 100 GHz and 1 THz.
•**The Data:** Provides a "data highway" so wide it can support **1 Terabit per second (1,000 Gbps)**.
•**Reconfigurable Intelligent Surfaces (RIS):**
•**The Problem:** THz signals are easily blocked by a single sheet of paper.
•**The Solution:** "Smart Mirrors" on walls that electronically "bend" and "focus" 6G beams around corners, eliminating dead zones in urban environments.
•**Integrated Sensing and Communication (ISAC):**
•Uses the same spectrum for both data and "Radar-like" sensing. It enables **gesture control** of devices from across a room and high-accuracy "sees-around-corners" safety for autonomous vehicles.
•**Non-Terrestrial Networks (NTN):** * 6G is a "3D Network." It integrates satellites, high-altitude drones (HAPS), and terrestrial towers into a single, unified handover system. This ensures 100% global coverage—even in the middle of the Pacific Ocean.
•**Giga-MIMO:** * While 5G uses ~64 antennas, 6G will use **thousands of tiny antenna elements** to manage the extreme precision required for THz beams.

5G

- Use more spectrum
  - mmWave, unlicensed spectrum (e.g., TV white space, WiFi)
- Massive MIMO
- Dense small cells
- Tight integration between cellular and WiFi
- New apps: Internet of things

6G

- Data rate: 100 Gbps
- TeraHz
  - sub-mmWave
  - 10 m range
  - Invisible, non-invasive, biologically safe, non-destructive
- Intelligent networks
- Localization
- Applications: VR, AR, IoT, drones, health care

Video tutorial

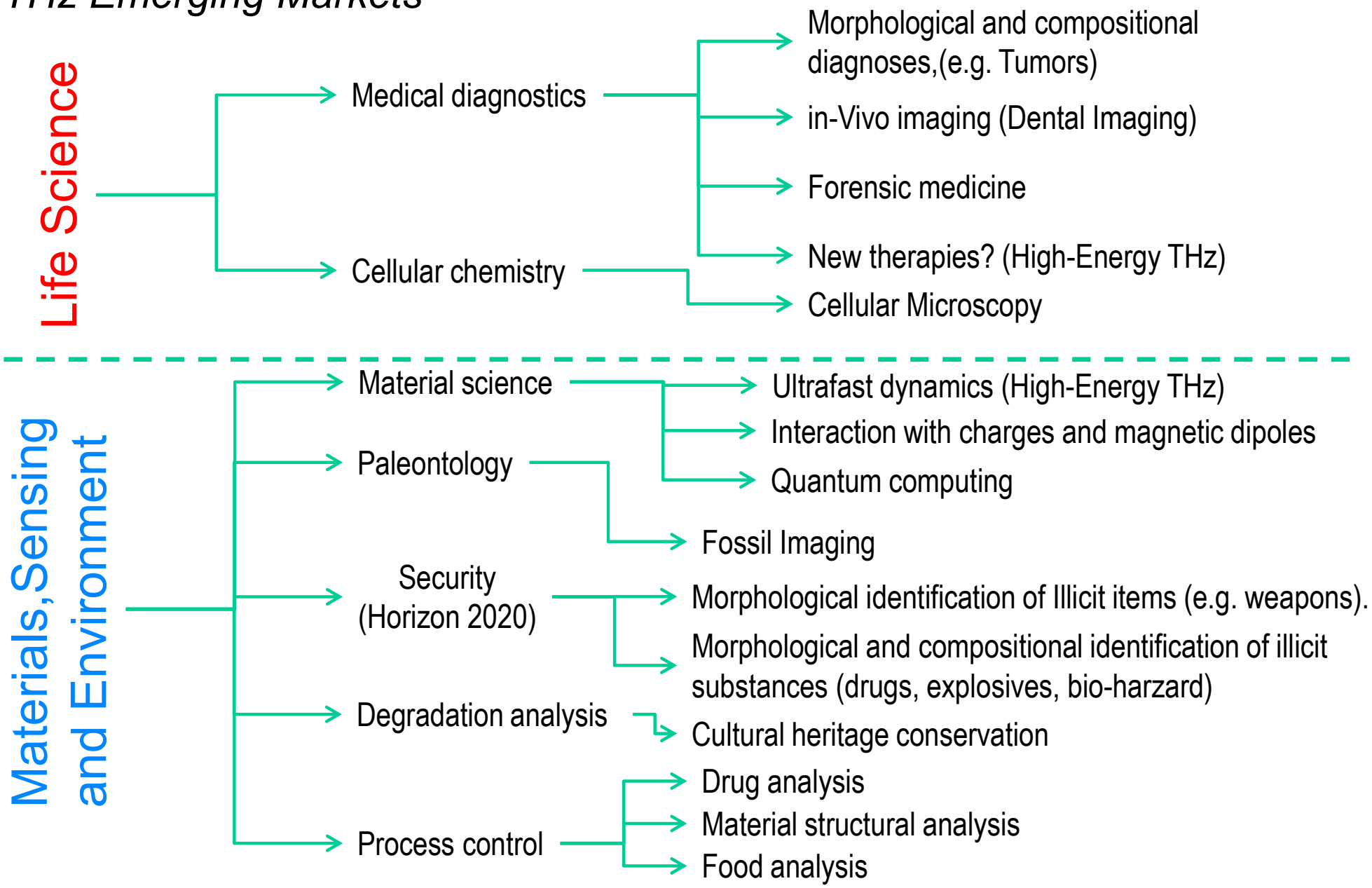
5G

6G?

- Data rate: 100 Gbps
- TeraHz
  - sub-mmWave
  - Invisible, non-invasive, biologically safe, non-destructive
  - 2012 Japanese researchers used 542 GHz to support 3Gbps and 10 m

https://www.newscientist.com/article/dn13500-terahertz-video-transfer-is-foretaste-of-future-wireless/

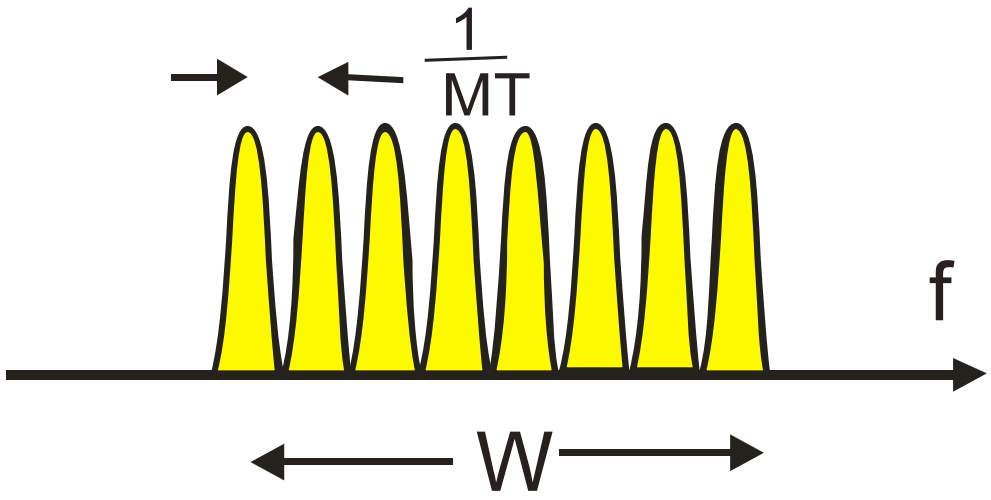
THz Emerging Markets



6G?

- Data rate: 100 Gbps
- TeraHz
- Intelligent networks
- Localization
- Applications: VR, AR, IoT, drones, smart driving, health care

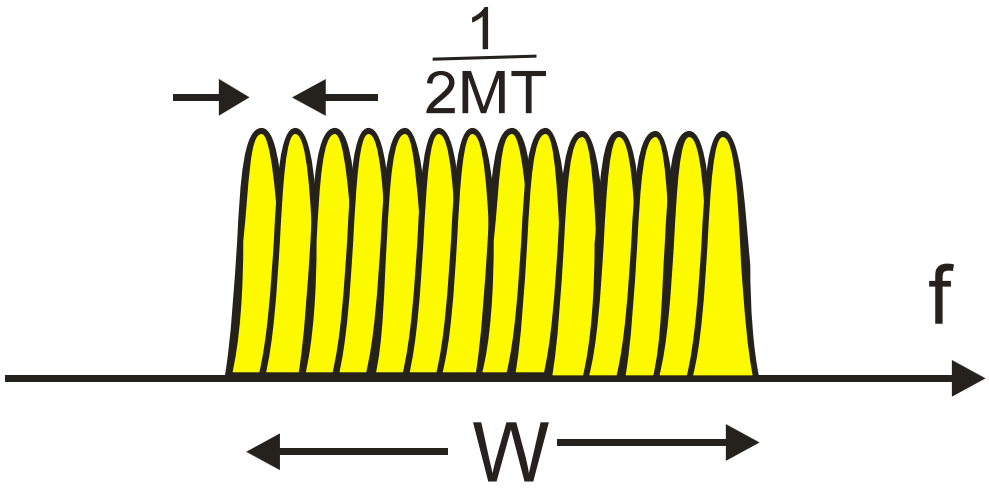
OFDM: Dense Multichannel System



Conventional Multichannel System

Non Overlapping Adjacent Channels.

Channels separated by More Than Their Two Sided bandwidth



OFDM Multichannel System

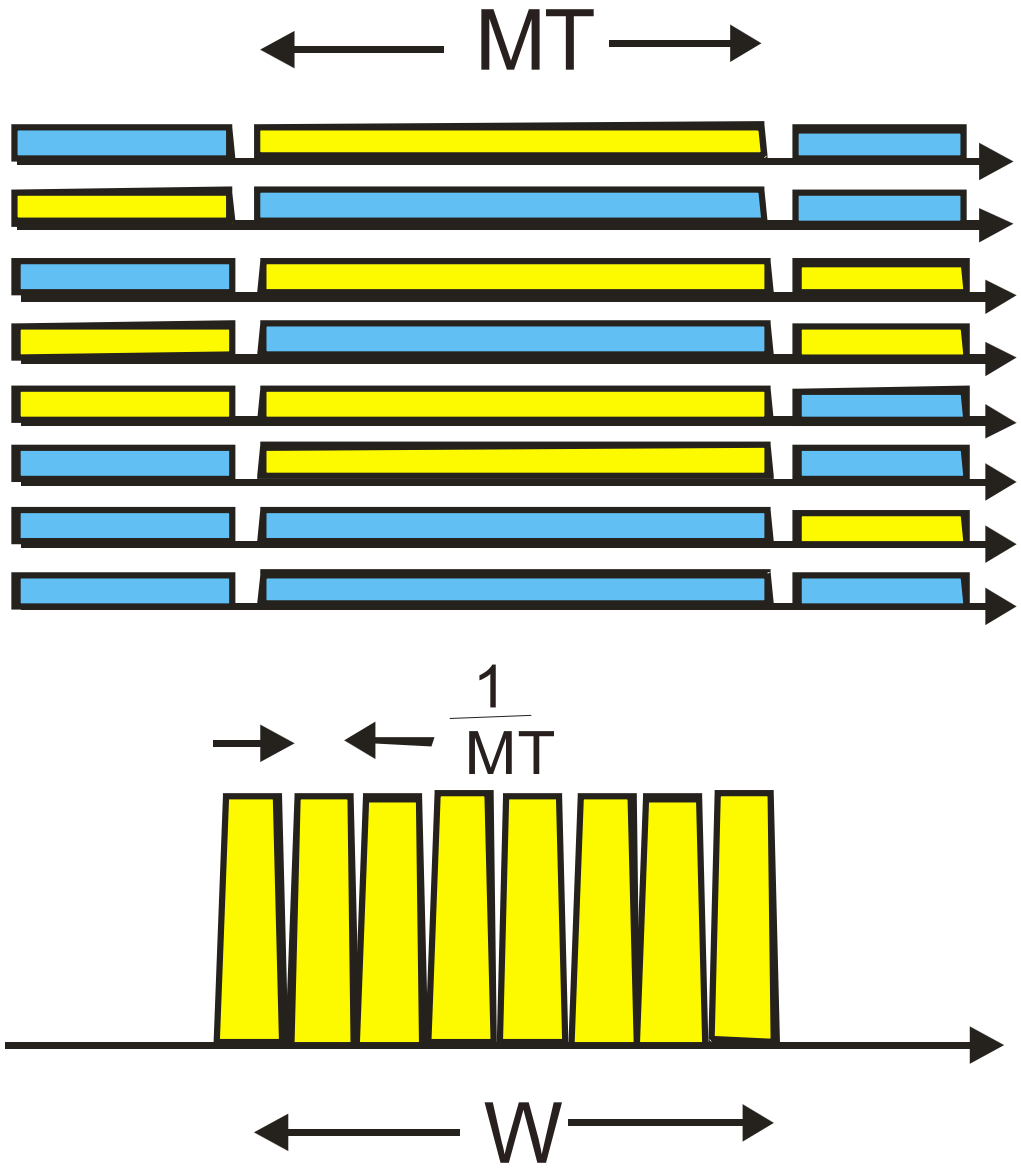
50% Overlap of Adjacent Channels

Available bandwidth is Used Twice

5G?

- No one knows for sure
- Innovations under development
  - Massive dense small cells
  - Tight integration between cellular and WiFi
  - Multihop wireless networks
  - Use more spectrum
    - 60GHz
    - Unlicensed spectrum, e.g., white space
  - New apps: Internet of things, wearable computing

Multi-Carrier System



t

Parallel Transmission of Waveforms

Waveforms are Long Duration MT

Waveforms Occupy 1/M th Of System Bandwidth

1/T

f

Today's agenda

- Recap cellular networks
- Cellular standards: 1G/2G/3G/4G/5G
- Wireless network security

Recap (Cont.)

- Techniques to increase capacity
  - Frequency borrowing
  - Cell splitting
  - Cell sectoring
  - Microcells
- Handoff

Recap (Cont.)

- Roaming
  - Regional roaming within a provider
  - National roaming within a provider
  - National roaming across providers
  - International roaming
  - Inter standard roaming
  - Roaming over non-cellular networks

Recap

- Cellular network provision
  - M/M/c (or M/M/c/c queue)
  - Blocking probability: Erlang distribution

Downlink Physical Layer Procedures

•Downlink Physical Layer Procedures

•For E-UTRA, the following downlink physical layer procedures are especially important:

- Cell search and synchronization:
- Scheduling:
- Link Adaptation:
- Hybrid ARQ (Automatic Repeat Request)

SC-FDMA

•The LTE uplink transmission scheme for FDD and TDD mode is based on SC-FDMA (Single Carrier Frequency Division Multiple Access).

•This is to compensate for a drawback with normal OFDM, which has a very high Peak to Average Power Ratio (PAPR). High PAPR requires expensive and inefficient power amplifiers with high requirements on linearity, which increases the cost of the terminal and also drains the battery faster.

•SC-FDMA solves this problem by grouping together the resource blocks in such a way that reduces the need for linearity, and so power consumption, in the power amplifier. A low PAPR also improves coverage and the cell-edge performance.

•Still, SC-FDMA signal processing has some similarities with OFDMA signal processing, so parameterization of downlink and uplink can be harmonized.

3G Cellular Systems

- UMTS: Universal Mobile Telecommunication Standard Based on core GSM, conforms to IMT-2000.
- Use of different sized cells (macro, micro and pico) in multi-cell environment
- Global roaming: multi-mode, multi-band, low-cost terminal, portable services & QoS
- High data rates for
  - up to 144kbps at vehicular speed (80km/h)
  - up to 384 kbps at pedestrian speed
  - up to 2Mbps indoor
- Multimedia interface to the internet

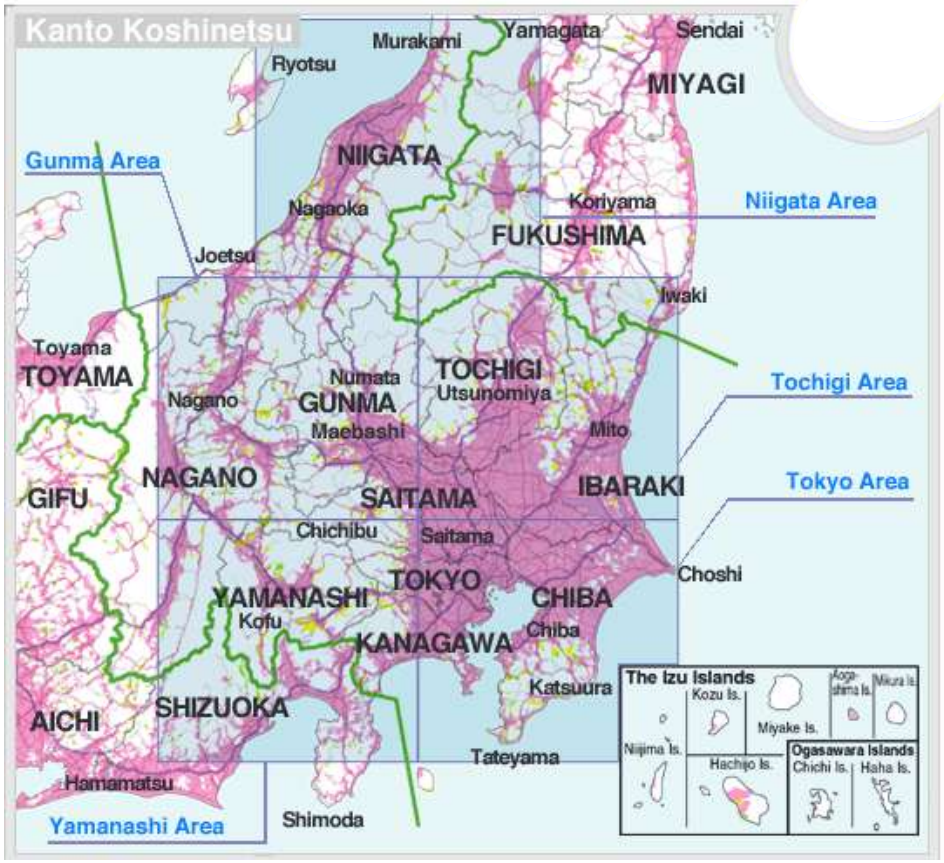
CDMA

- 3G UMTS air interface: CDMA
- CDMA assigns to each user a unique code sequence that is used to code data before transmission
- If a receiver knows the code sequence, it is able to decode the received data
- Several users can simultaneously transmit on the same frequency channel by using different code sequences
- Codes should be orthogonal: with zero cross correlation

CDMA (Cont.)

- Most promising 3G systems is the direct sequence (DS)-CDMA
- The following are based on the DS-CDMA:
- WCDMA:
  - wide band CDMA. In the W-CDMA, the SF can be very large (up to 512). This is why so called wideband.
- TD-CDMA:
  - Time division CDMA is based on a hybrid access scheme in which each frequency channel is structured in frame and time slots.
  - Within each time slots more channels can be allocated and separated by means of DS-CDMA.
  - The number of codes in a time slot is not fixed but depends on the data rate and SF of each physical channel.

Example 3G Networks: Japan



FOMA (Freedom Of Mobile multimedia Access) in Japan

Examples for FOMA phones

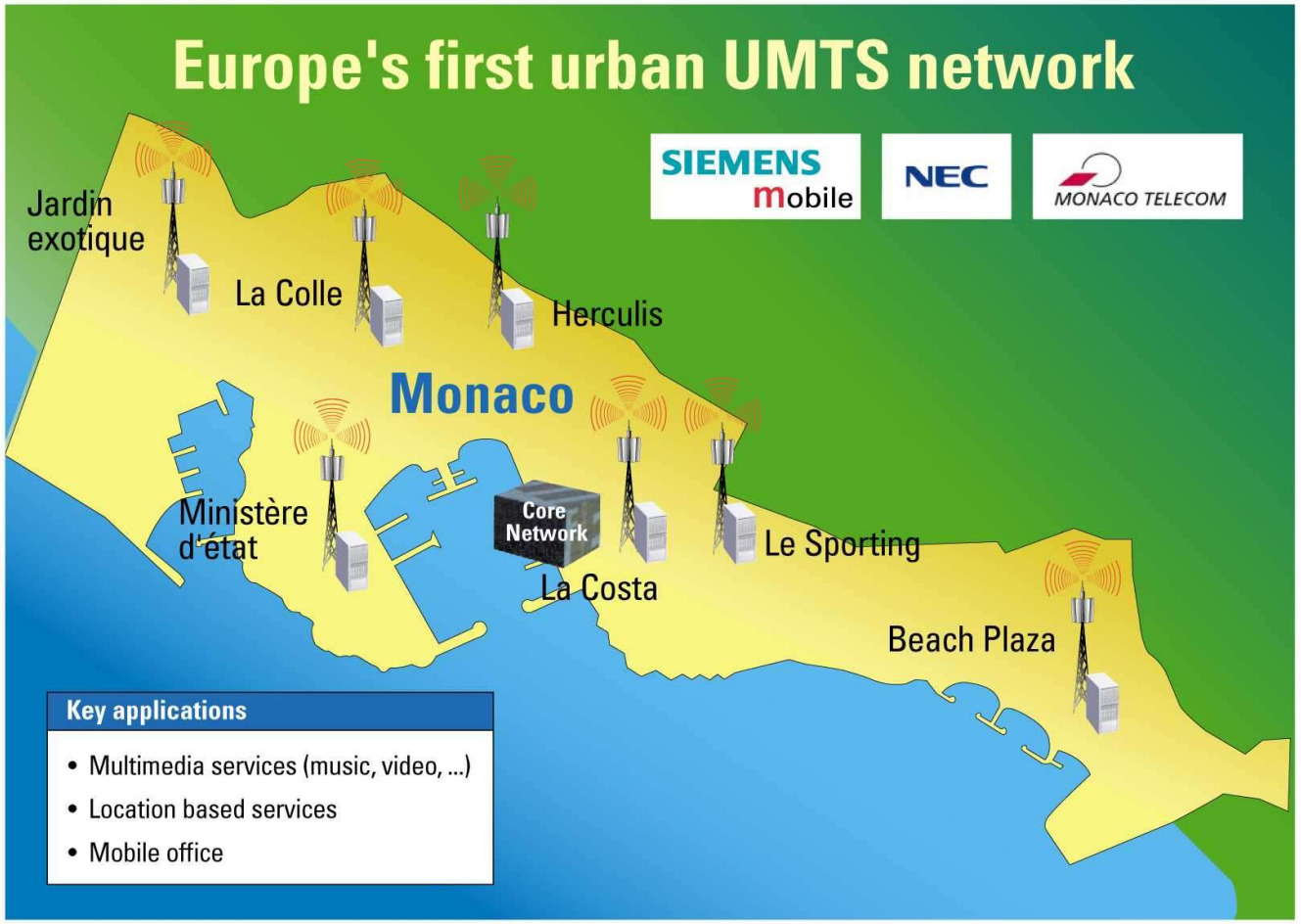
Example 3G networks: Australia

cdma2000 1xEV-DO in Melbourne/Australia

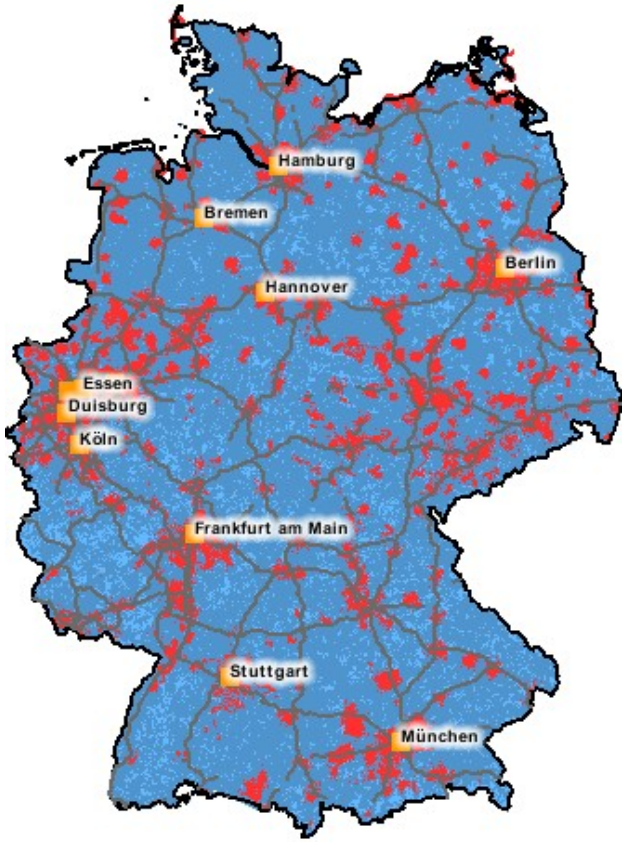
Examples for 1xEV-DO devices

Isle of Man – Start of UMTS in Europe as Test

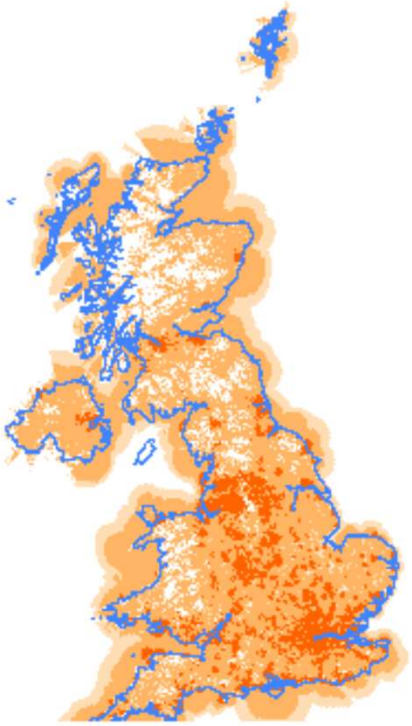
UMTS in Monaco



UMTS in Europe



Vodafone/Germany



Orange/UK

GSM: Overview

- formerly: Groupe Spéciale Mobile (founded 1982)
- now: Global System for Mobile Communication
- Pan-European standard (ETSI, European Telecommunications Standardisation Institute)
- simultaneous introduction of essential services in three phases (1991, 1994, 1996) by the European telecommunication administrations (Germany: D1 and D2)
  ➔ seamless roaming within Europe possible
- today many providers all over the world use GSM (more than 200 countries in Asia, Africa, Europe, Australia, America)
- more than 1.2 billion subscribers in more than 630 networks
- more than 75% of all digital mobile phones use GSM (74% total)
- over 200 million SMS per month in Germany, > 550 billion/year worldwide (> 10% of the revenues for many operators)
  [be aware: these are only rough numbers and are not up-to-date…]

Features of GSM (wrt. analog sys.)

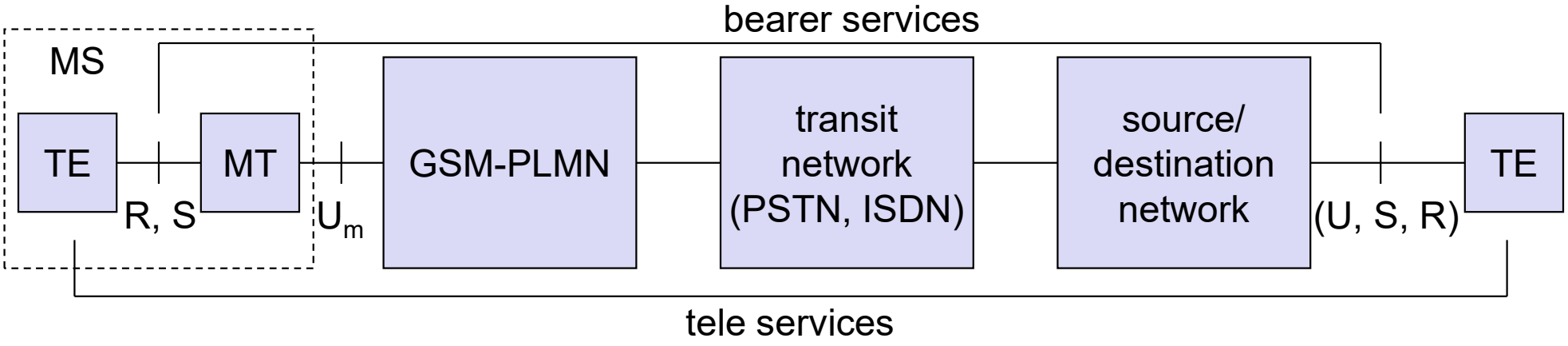
- Communication
  - mobile, wireless communication; support for voice and data services
- Total mobility
  - international access, chip-card enables use of access points of different providers
- Worldwide connectivity
  - one number, the network handles localization
- High capacity
  - better frequency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

Disadvantages of GSM

- There is no perfect system!!
- no end-to-end encryption of user data
- no full ISDN bandwidth of 64 kbit/s to the user, no transparent B-channel
- reduced concentration while driving
- electromagnetic radiation
- abuse of private data possible
- roaming profiles accessible
- high complexity of the system
- several incompatibilities within the GSM standards

GSM: Mobile Services

- GSM offers
  - several types of connections
    - voice connections, data connections, short message service
  - multi-service options (combination of basic services)
- Three service domains
  - Bearer Services
  - Telematic Services
  - Supplementary Services



Bearer Services

- Telecommunication services to transfer data between access points
- Specification of services up to the terminal interface (OSI layers 1-3)
- Different data rates for voice and data (original standard)
  - data service (circuit switched)
    - synchronous: 2.4, 4.8 or 9.6 kbit/s
    - asynchronous: 300 - 1200 bit/s
  - data service (packet switched)
    - synchronous: 2.4, 4.8 or 9.6 kbit/s
    - asynchronous: 300 - 9600 bit/s
- Today: data rates of approx. 50 kbit/s possible

Tele Services I

- Telecommunication services that enable voice communication via mobile phones
- All these basic services have to obey cellular functions, security measurements
- Offered services
  - mobile telephony
    primary goal of GSM was to enable mobile telephony offering the traditional bandwidth of 3.1 kHz
  - Emergency number
    911 in US, common number throughout Europe (112); mandatory for all service providers; free of charge; connection with the highest priority (preemption of other connections possible)
  - Multinumbering
    several ISDN phone numbers per user possible

Tele Services II

- Additional services
  - Non-Voice-Teleservices
    - group 3 fax
    - voice mailbox (implemented in the fixed network supporting the mobile terminals)
    - electronic mail (MHS, Message Handling System, implemented in the fixed network)
    - Short Message Service (SMS)
      - Almost ignored at the beginning
      - Today > 30 billion SMS transferred per month!
      - The only way to reach a mobile phone from within the network
      - Big business for network operators and content providers
        - » Update mobile phone software
        - » Alert services (e.g., stock quotes, road conditions)
        - » Many fun applications (e.g., ring tones, horoscopes)

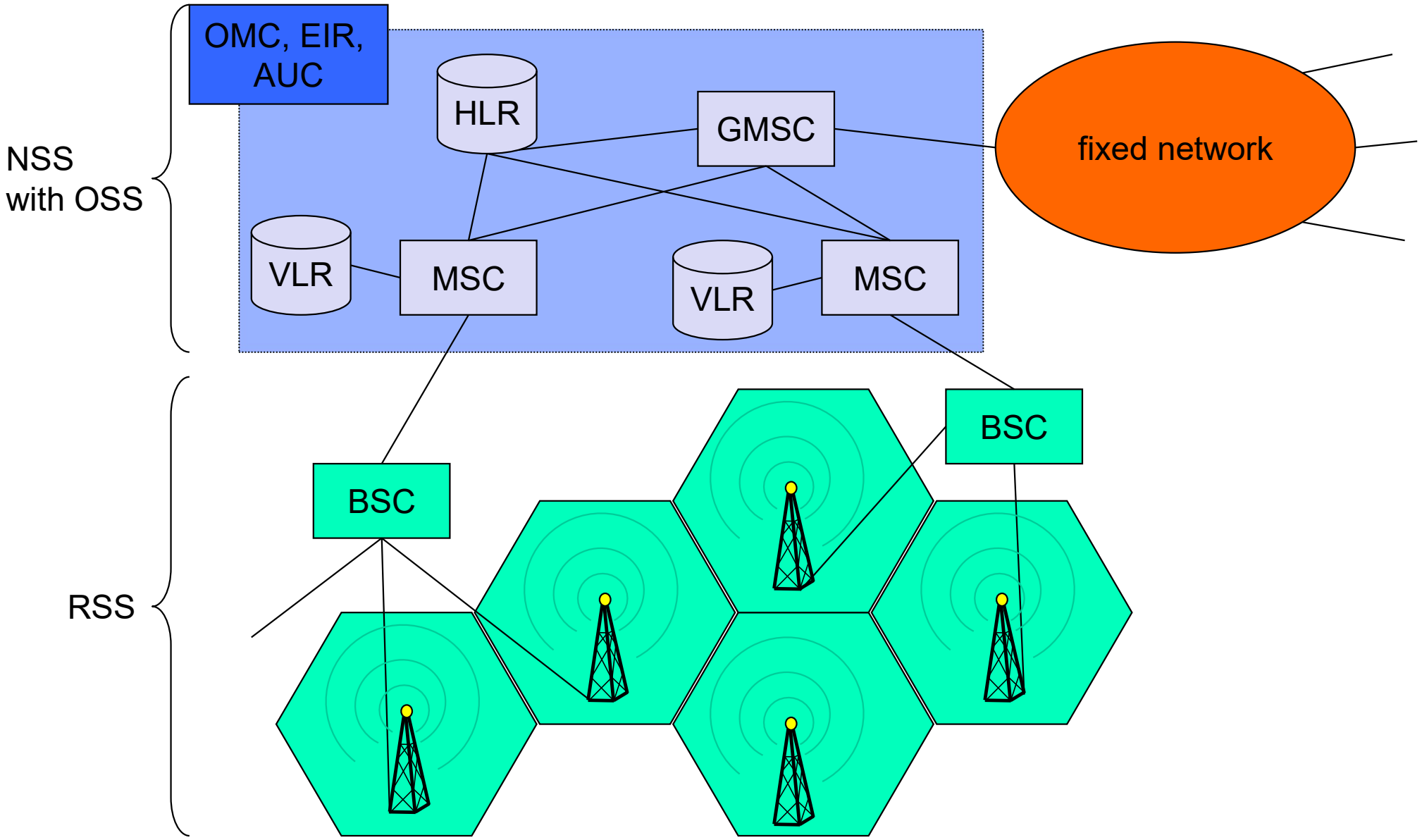
Supplementary Services

- Services in addition to the basic services, cannot be offered stand-alone
- Similar to ISDN services besides lower bandwidth due to the radio link
- May differ between different service providers, countries and protocol versions
- Important services
  - identification: forwarding of caller number
  - suppression of number forwarding
  - automatic call-back
  - conferencing with up to 7 participants
  - locking of the mobile terminal (incoming or outgoing calls)
  - ...

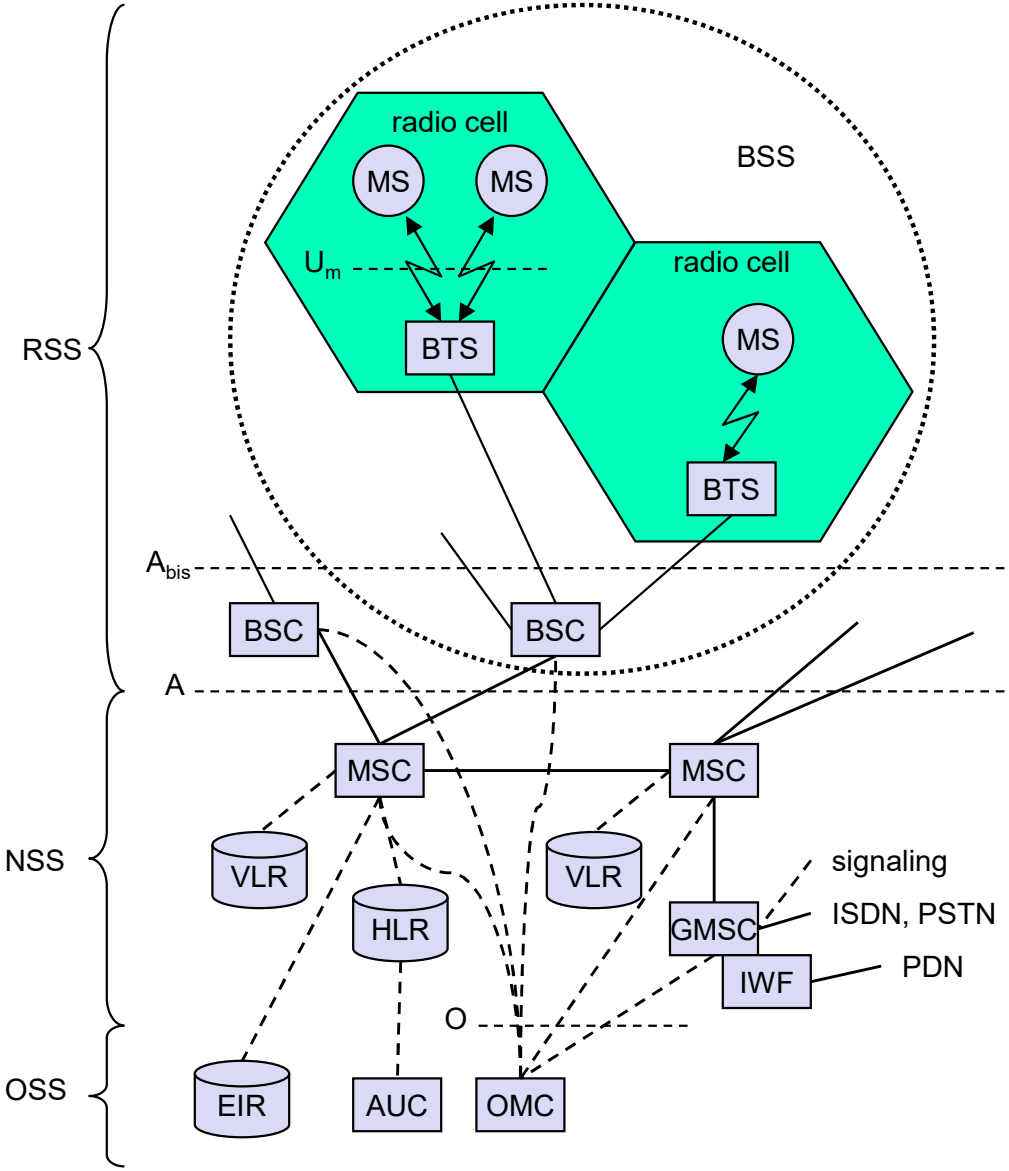
Architecture of the GSM system

- GSM is a PLMN (Public Land Mobile Network)
  - several providers setup mobile networks following the GSM standard within each country
  - components
    - MS (mobile station)
    - BS (base station)
    - MSC (mobile switching center)
    - LR (location register)
  - subsystems
    - RSS (radio subsystem): covers all radio aspects
    - NSS (network and switching subsystem): call forwarding, handover, switching
    - OSS (operation subsystem): management of the network

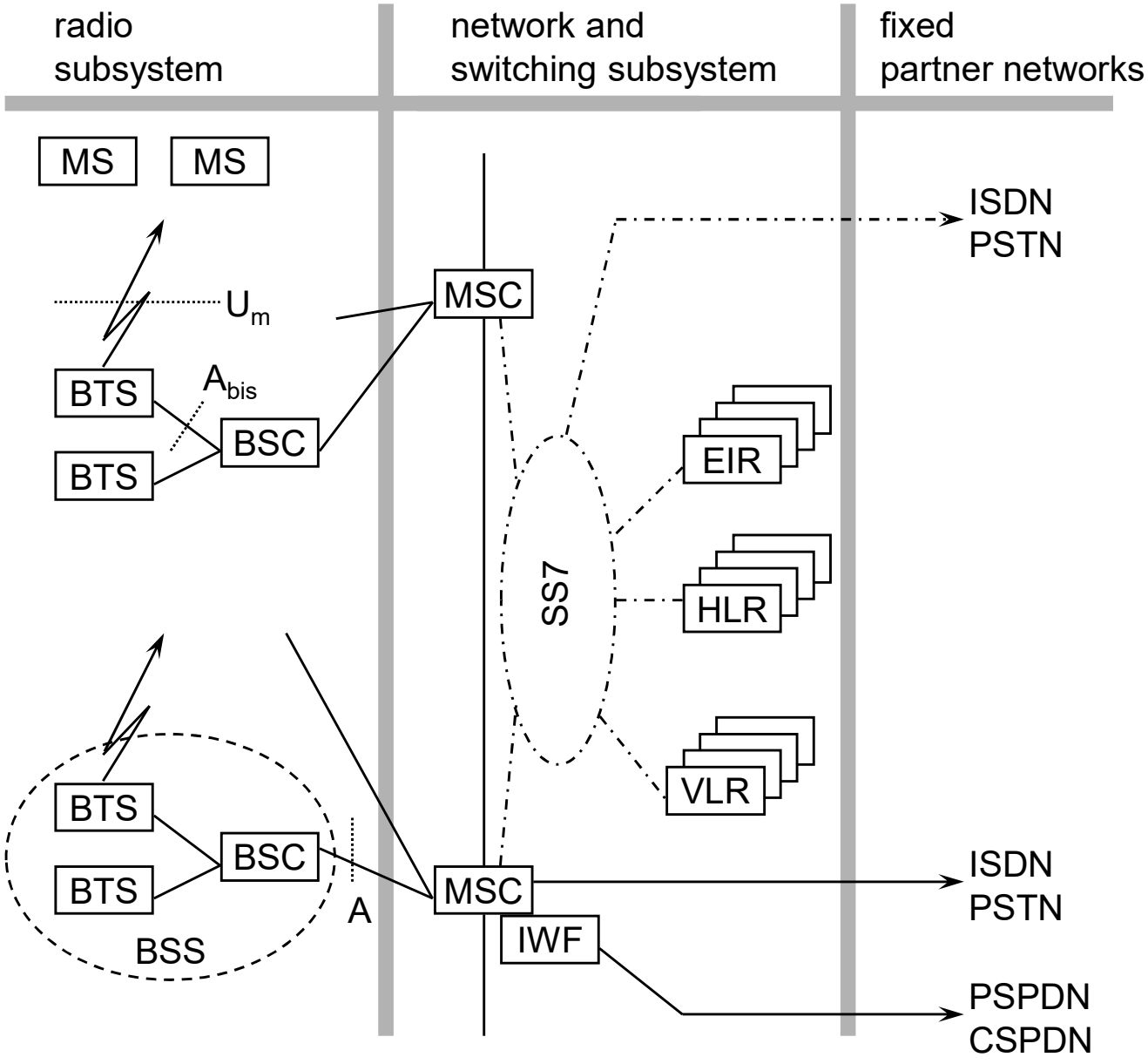
GSM: overview



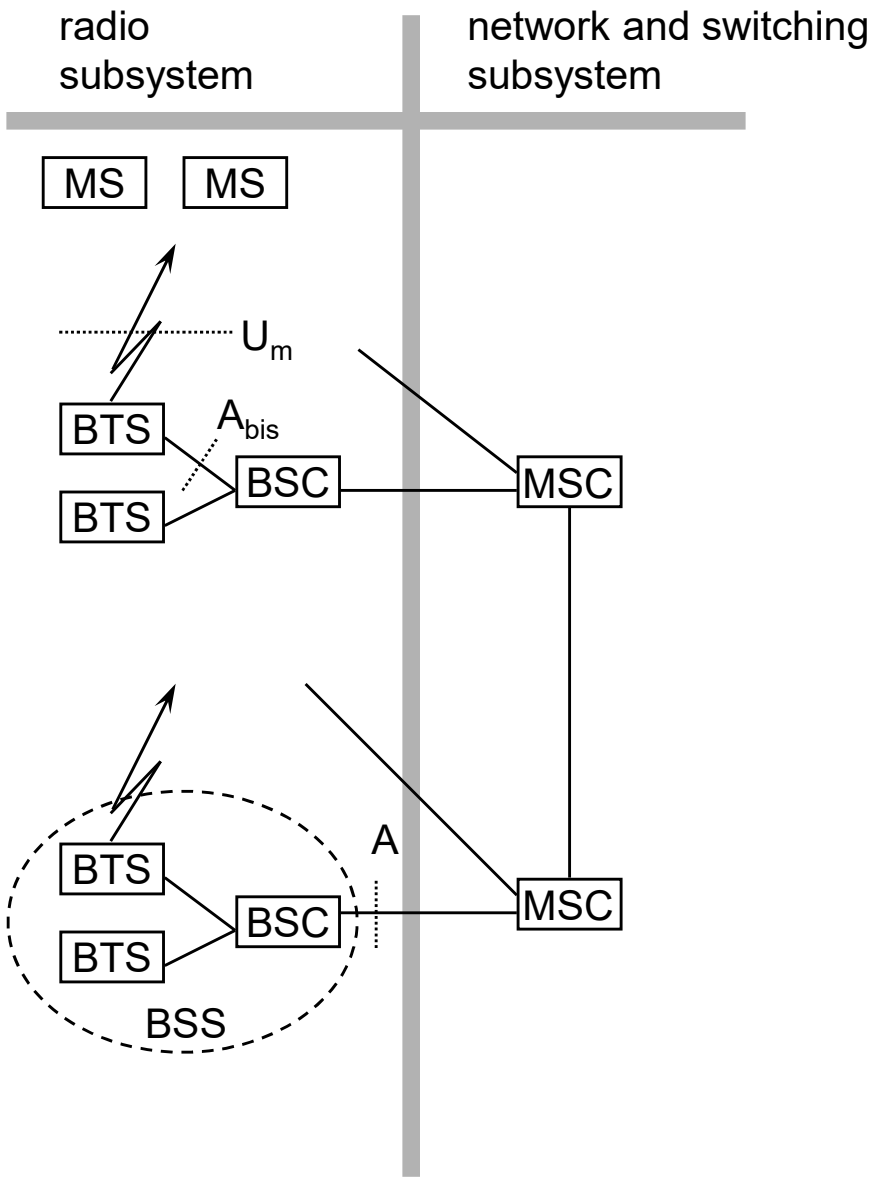
GSM: elements and interfaces



GSM: system architecture



System architecture: radio subsystem



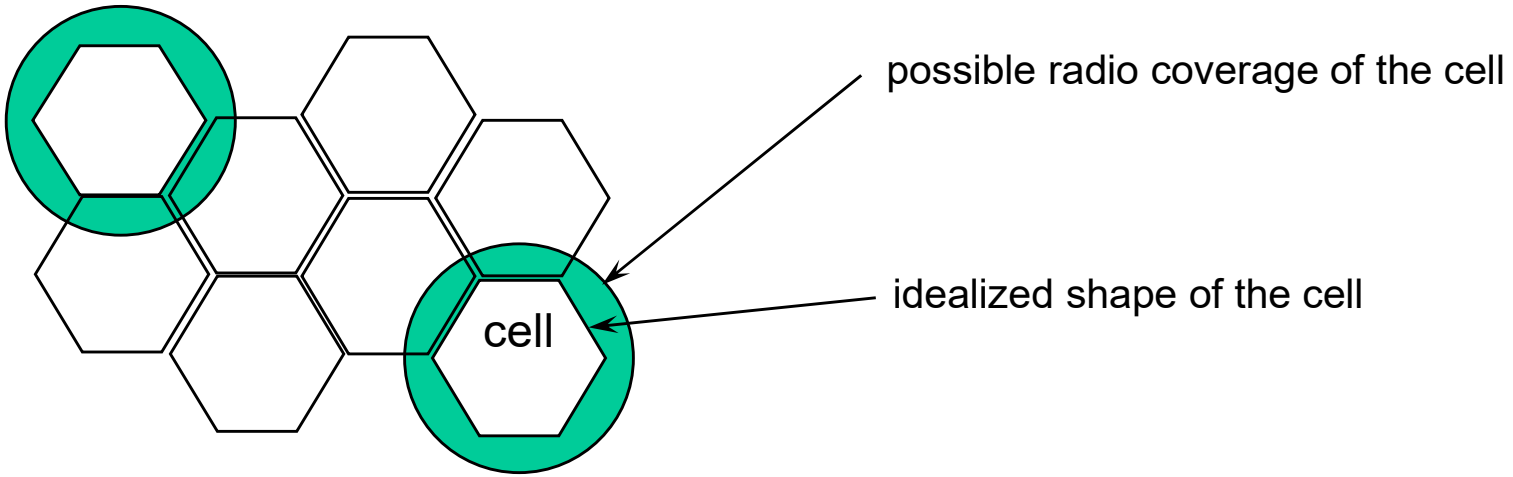
- Components
  - *MS* (Mobile Station)
  - *BSS* (Base Station Subsystem): consisting of
    - *BTS* (Base Transceiver Station): sender and receiver
    - *BSC* (Base Station Controller): controlling several transceivers
- Interfaces
  - U_m : radio interface
  - A_{bis} : standardized, open interface with 16 kbit/s user channels
  - *A*: standardized, open interface with 64 kbit/s user channels

Radio subsystem

- The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers
- Components
  - Base Station Subsystem (BSS):
    - Base Transceiver Station (BTS): radio components including sender, receiver, antenna - if directed antennas are used one BTS can cover several cells
    - Base Station Controller (BSC): switching between BTSs, controlling BTSs, managing of network resources, mapping of radio channels (U_m) onto terrestrial channels (A interface)
    - BSS = BSC + sum(BTS) + interconnection
  - Mobile Stations (MS)

GSM: cellular network

segmentation of the area into cells

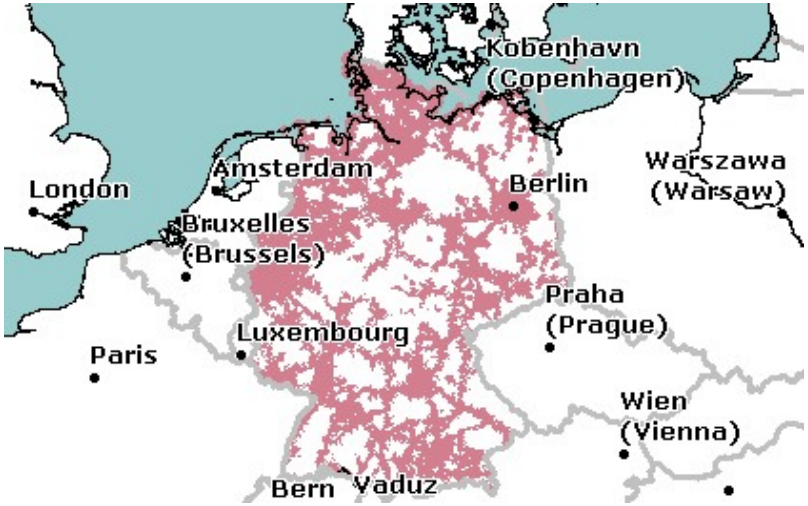


- use of several carrier frequencies
- not the same frequency in adjoining cells
- cell sizes vary from some 100 m up to 35 km depending on user density, geography, transceiver power etc.
- hexagonal shape of cells is idealized (cells overlap, shapes depend on geography)
- if a mobile user changes cells
  - handover of the connection to the neighbor cell

Example coverage of GSM networks (www.gsmworld.com)

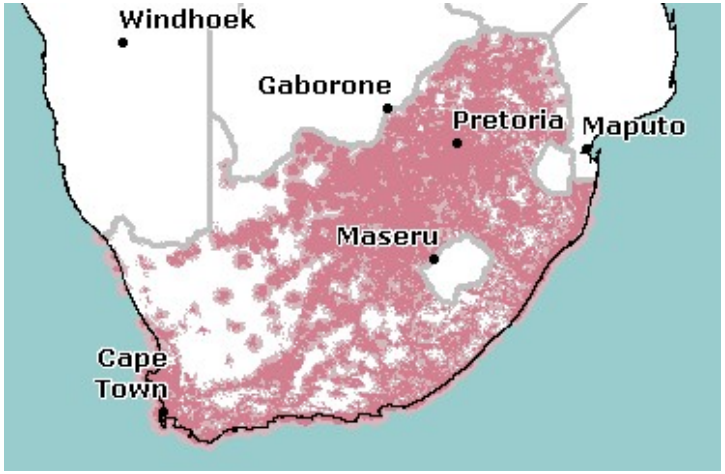
T-Mobile (GSM-900/1800) Germany

O_2 (GSM-1800) Germany



AT&T (GSM-850/1900) USA

Vodacom (GSM-900) South Africa



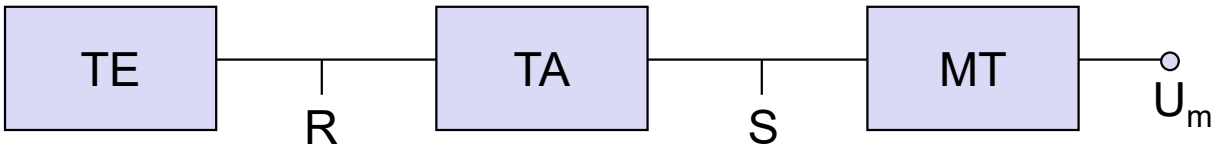
Base Transceiver Station and Base Station Controller

- Tasks of a BSS are distributed over BSC and BTS
- BTS comprises radio specific functions
- BSC is the switching center for radio channels

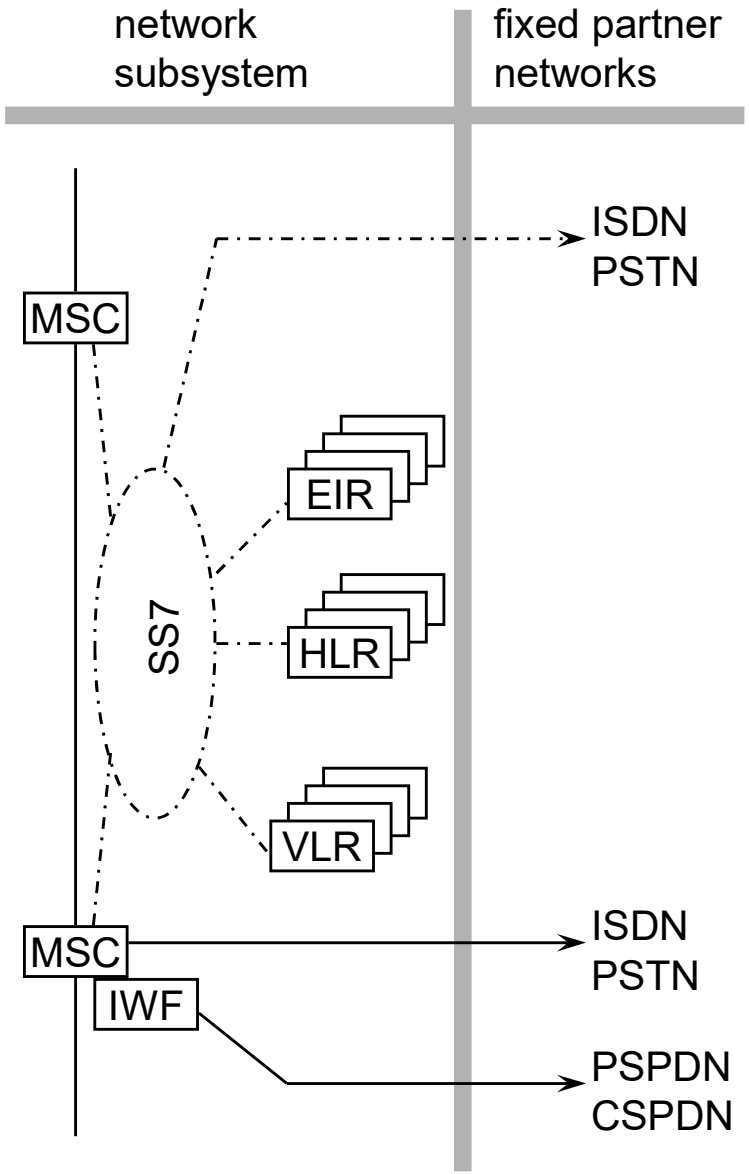
Functions	BTS	BSC
Management of radio channels		X
Frequency hopping (FH)	X	X
Management of terrestrial channels		X
Mapping of terrestrial onto radio channels		X
Channel coding and decoding	X	
Rate adaptation	X	
Encryption and decryption	X	X
Paging	X	X
Uplink signal measurements	X	
Traffic measurement		X
Authentication		X
Location registry, location update		X
Handover management		X

Mobile station

- Terminal for the use of GSM services
- A mobile station (MS) comprises several functional groups
  - MT (Mobile Terminal):
    - offers common functions used by all services the MS offers
    - corresponds to the network termination (NT) of an ISDN access
    - end-point of the radio interface (U_m)
  - TA (Terminal Adapter):
    - terminal adaptation, hides radio specific characteristics
  - TE (Terminal Equipment):
    - peripheral device of the MS, offers services to a user
    - does not contain GSM specific functions
  - SIM (Subscriber Identity Module):
    - personalization of the mobile terminal, stores user parameters



System architecture: network and switching subsystem



Components

- *MSC* (Mobile Services Switching Center):
- *IWF* (Interworking Functions)

- *ISDN* (Integrated Services Digital Network)
- *PSTN* (Public Switched Telephone Network)
- *PSPDN* (Packet Switched Public Data Net.)
- *CSPDN* (Circuit Switched Public Data Net.)

Databases

- *HLR* (Home Location *R*egister)
- *VLR* (Visitor Location *R*egister)
- *EIR* (Equipment Identity Register)

Network and switching subsystem

- NSS is the main component of the public mobile network GSM
  - switching, mobility management, interconnection to other networks, system control
- Components
  - Mobile Services Switching Center (MSC)
    controls all connections via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC
  - Databases (important: scalability, high capacity, low delay)
    - Home Location Register (HLR)
      central master database containing user data, permanent and semi-permanent data of all subscribers assigned to the HLR (one provider can have several HLRs)
    - Visitor Location Register (VLR)
      local database for a subset of user data, including data about all user currently in the domain of the VLR

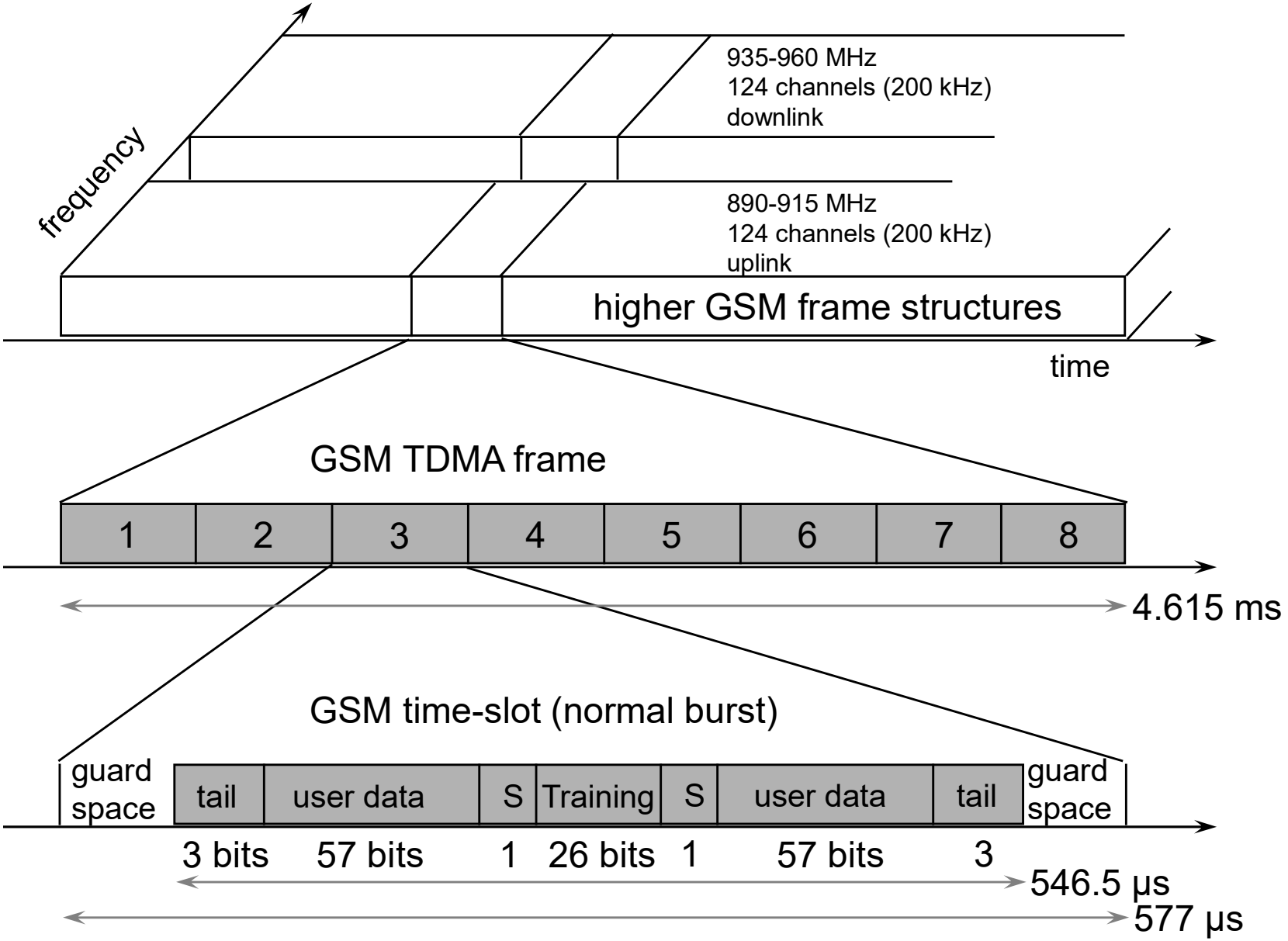
Mobile Services Switching Center

- The MSC (mobile switching center) plays a central role in GSM
  - switching functions
  - additional functions for mobility support
  - management of network resources
  - interworking functions via Gateway MSC (GMSC)
  - integration of several databases
- Functions of a MSC
  - specific functions for paging and call forwarding
  - termination of SS7 (signaling system no. 7)
  - mobility specific signaling
  - location registration and forwarding of location information
  - provision of new services (fax, data calls)
  - support of short message service (SMS)
  - generation and forwarding of accounting and billing information

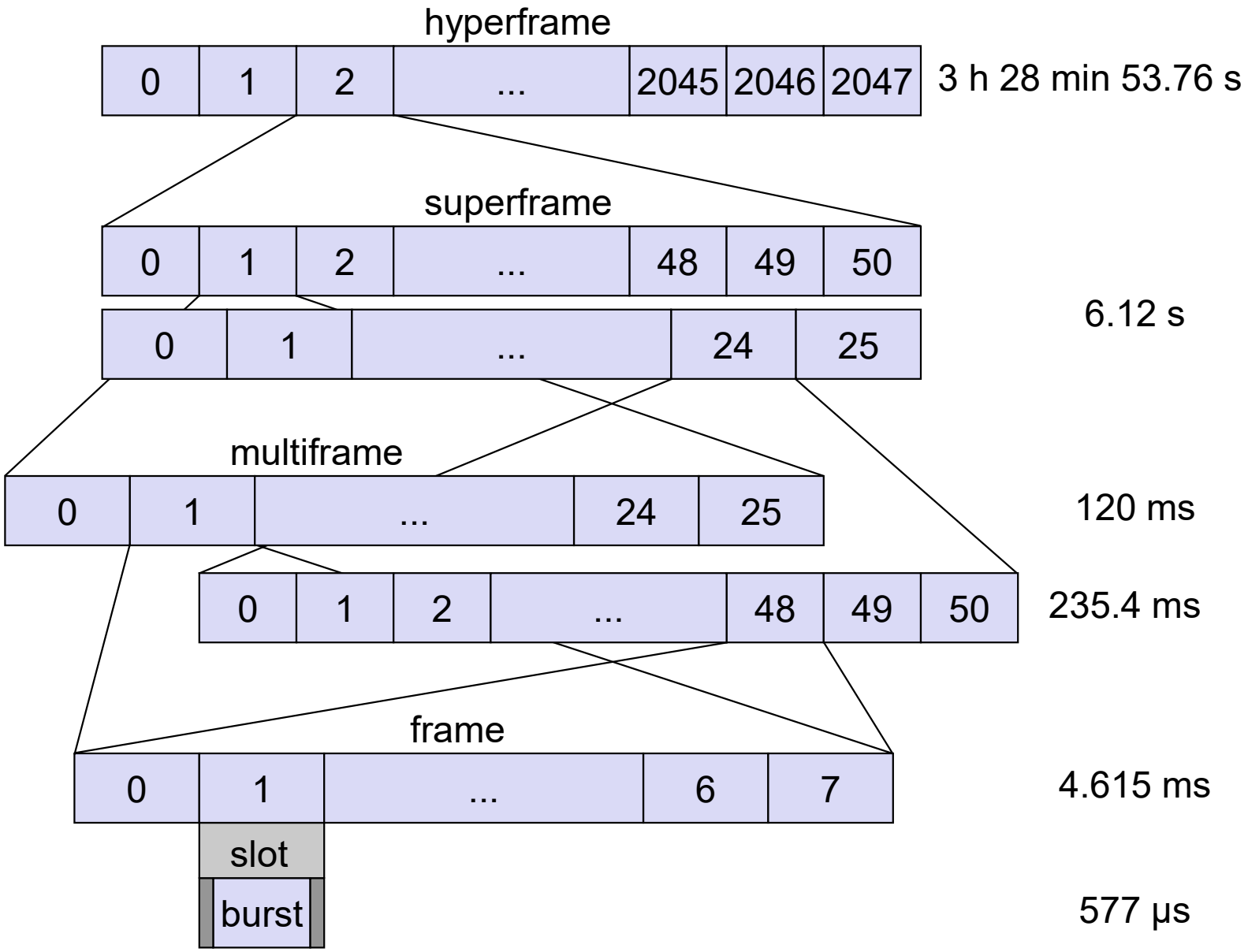
Operation subsystem

- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems
- Components
  - Authentication Center (AUC)
    - generates user specific authentication parameters on request of a VLR
    - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
  - Equipment Identity Register (EIR)
    - registers GSM mobile stations and user rights
    - stolen or malfunctioning mobile stations can be locked and sometimes even localized
  - Operation and Maintenance Center (OMC)
    - different control capabilities for the radio subsystem and the network subsystem

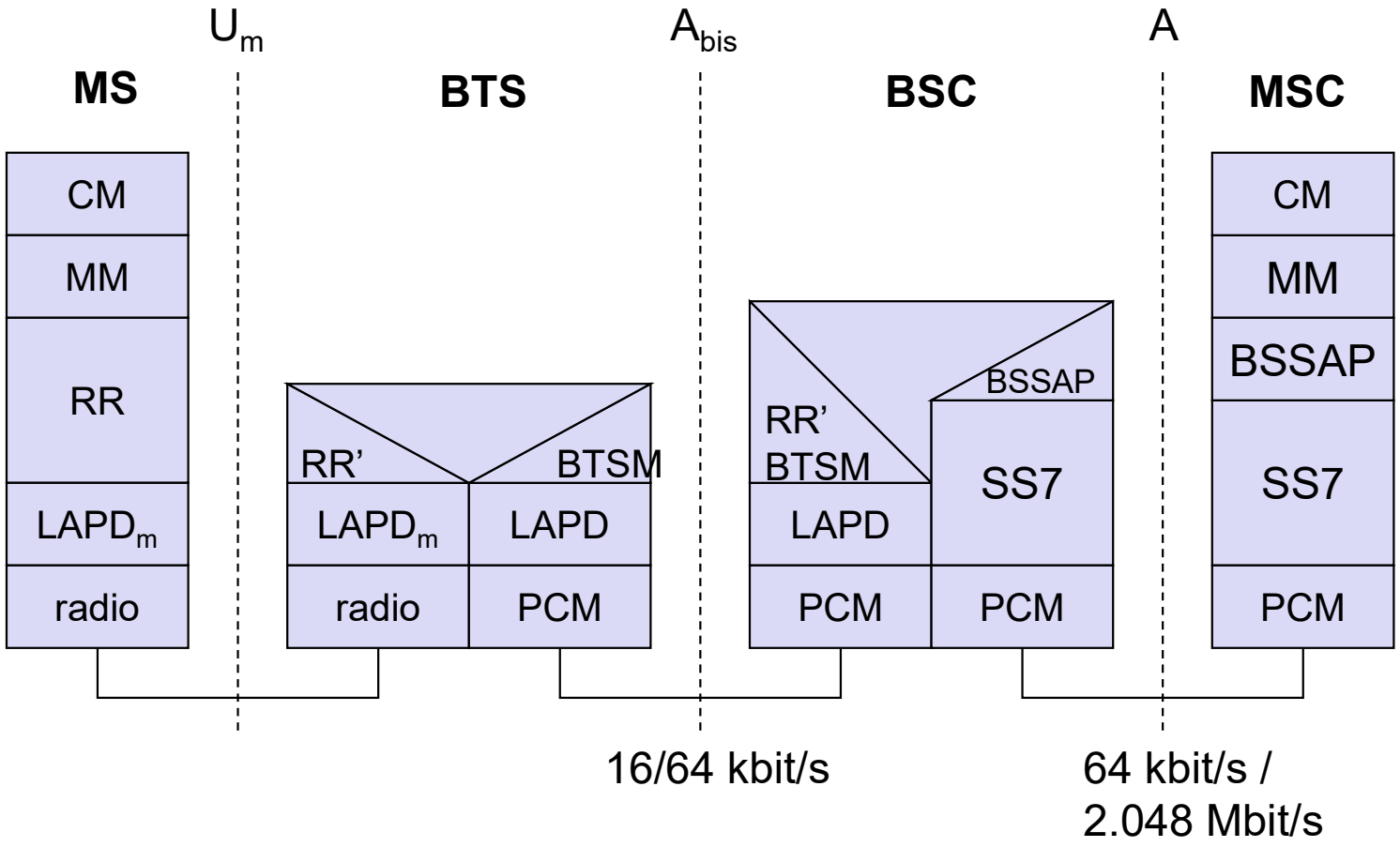
GSM - TDMA/FDMA



GSM hierarchy of frames

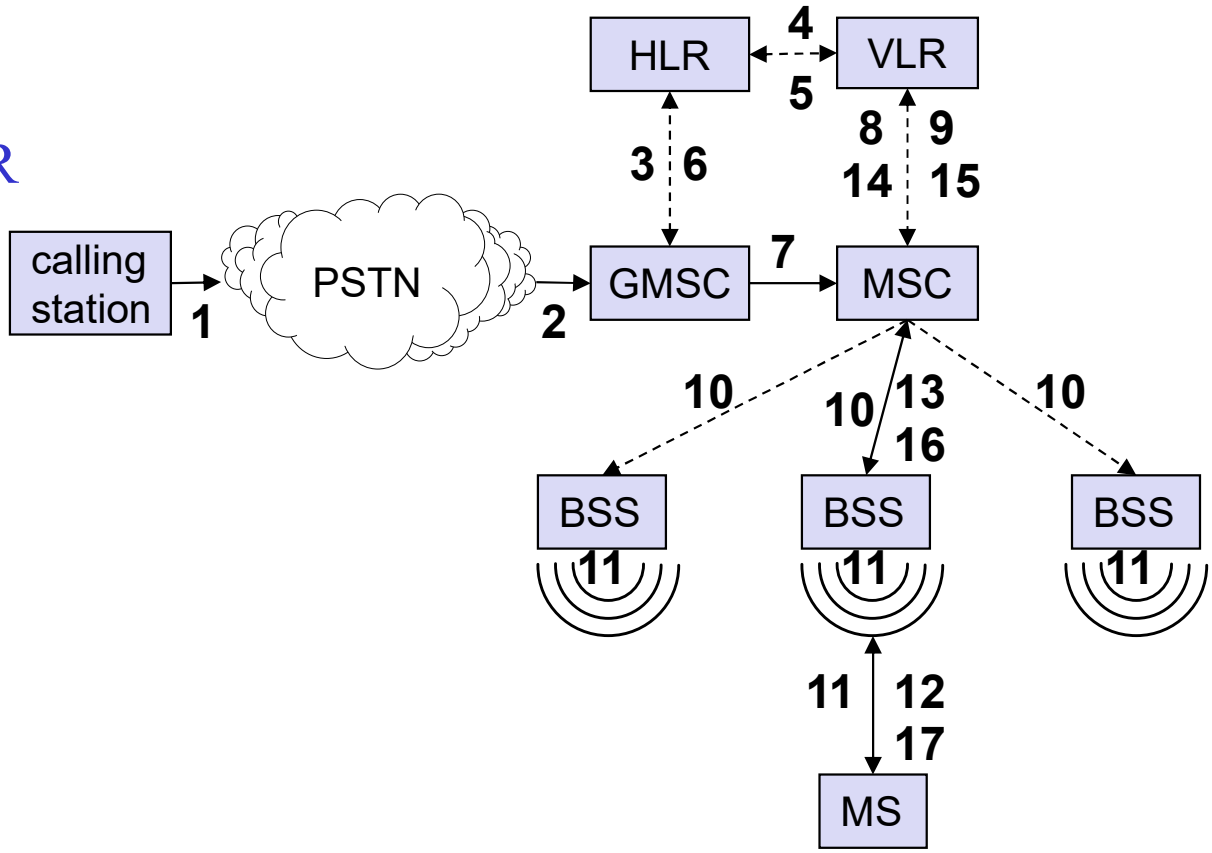


GSM protocol layers for signaling



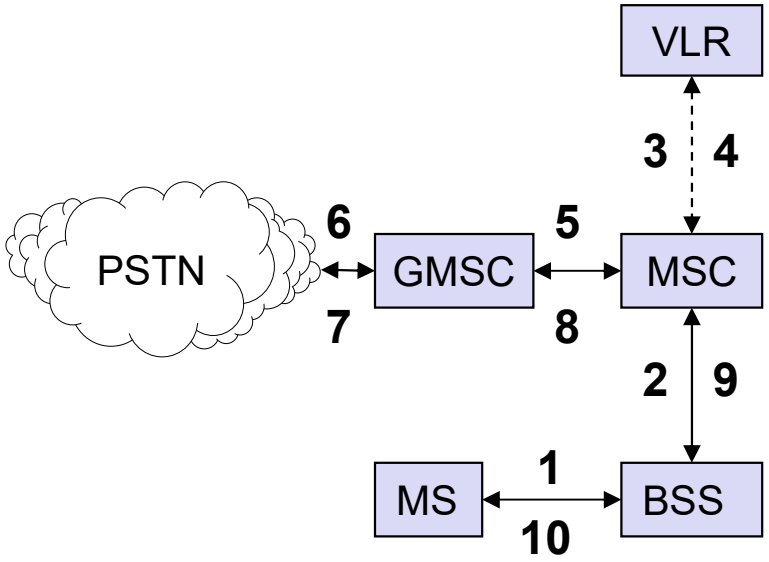
Mobile Terminated Call

- 1: calling a GSM subscriber
- 2: forwarding call to GMSC
- 3: signal call setup to HLR
- 4, 5: request MSRN from VLR
- 6: forward responsible MSC to GMSC
- 7: forward call to
- current MSC
- 8, 9: get current status of MS
- 10, 11: paging of MS
- 12, 13: MS answers
- 14, 15: security checks
- 16, 17: set up connection

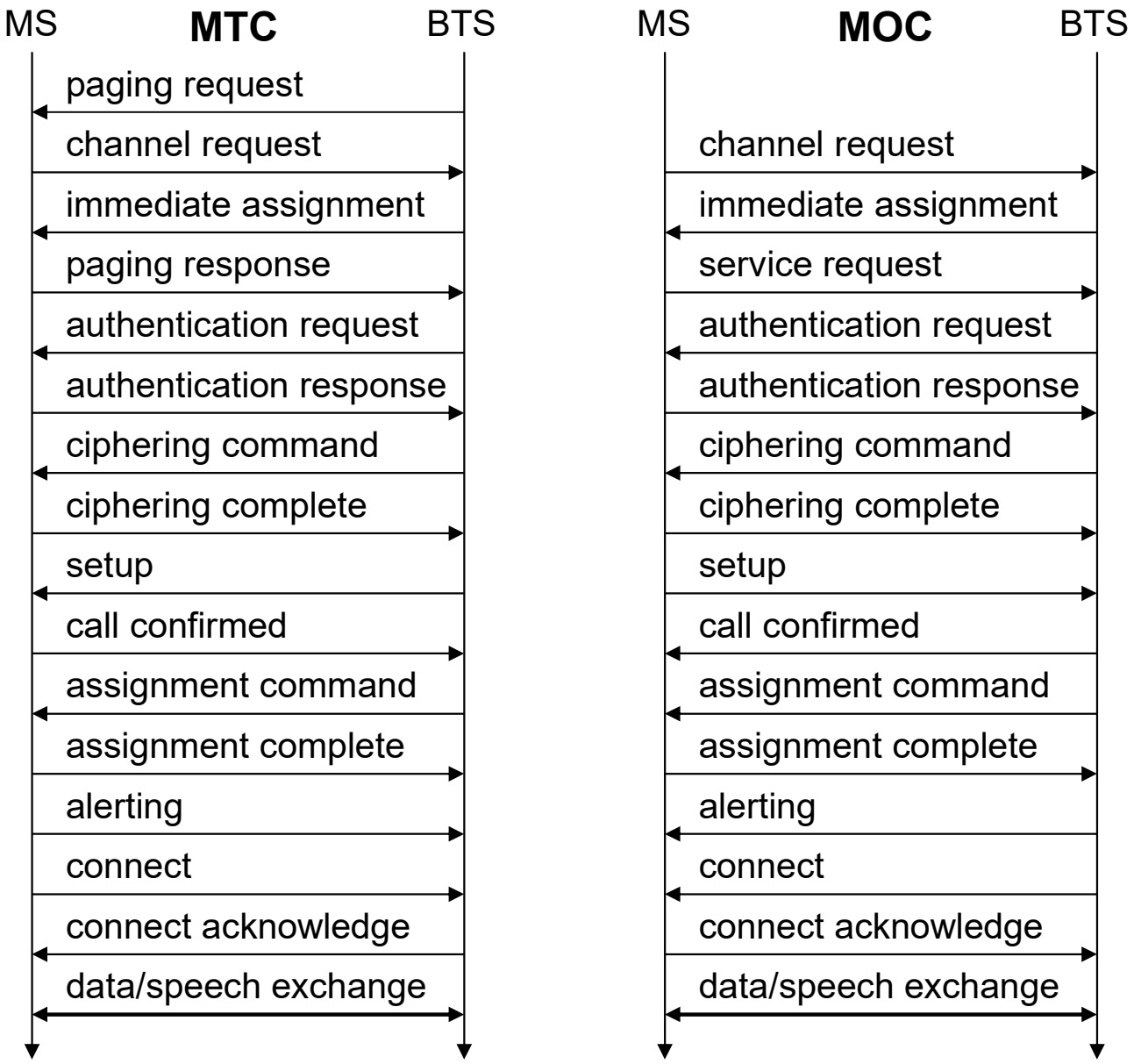


Mobile Originated Call

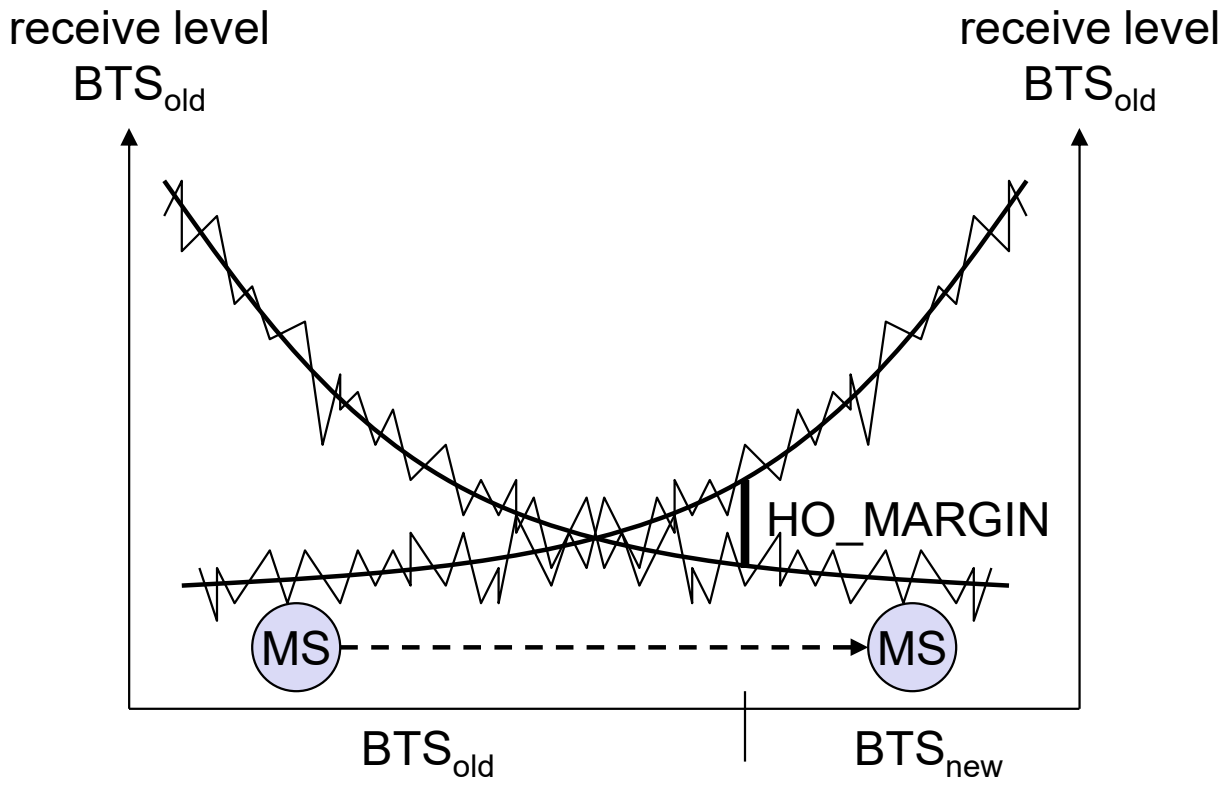
- 1, 2: connection request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call



MTC/MOC


MS
MTC
BTS
paging request
channel request
immediate assignment
paging response
authentication request
authentication response
ciphering command
ciphering complete
setup
call confirmed
assignment command
assignment complete
alerting
connect
connect acknowledge
data/speech exchange
MS
MOC
BTS
channel request
immediate assignment
service request
authentication request
authentication response
ciphering command
ciphering complete
setup
call confirmed
assignment command
assignment complete
alerting
connect
connect acknowledge
data/speech exchange

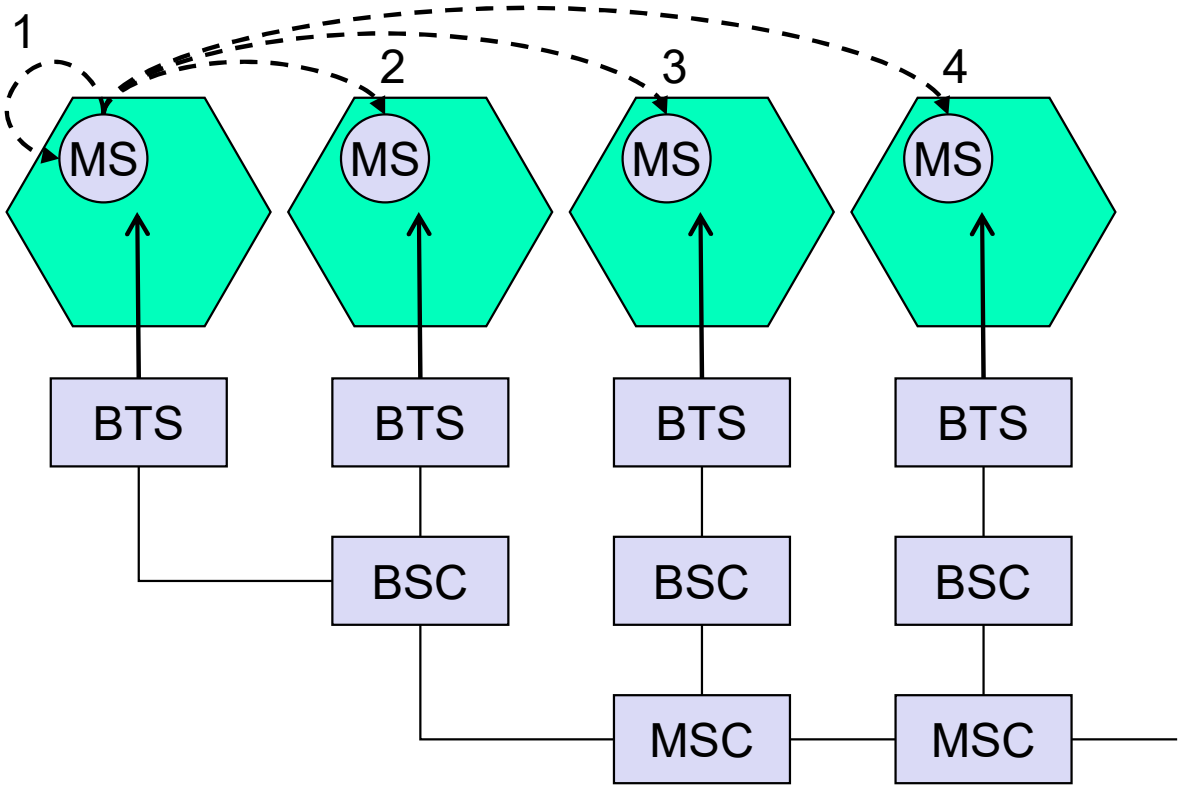
Handover decision



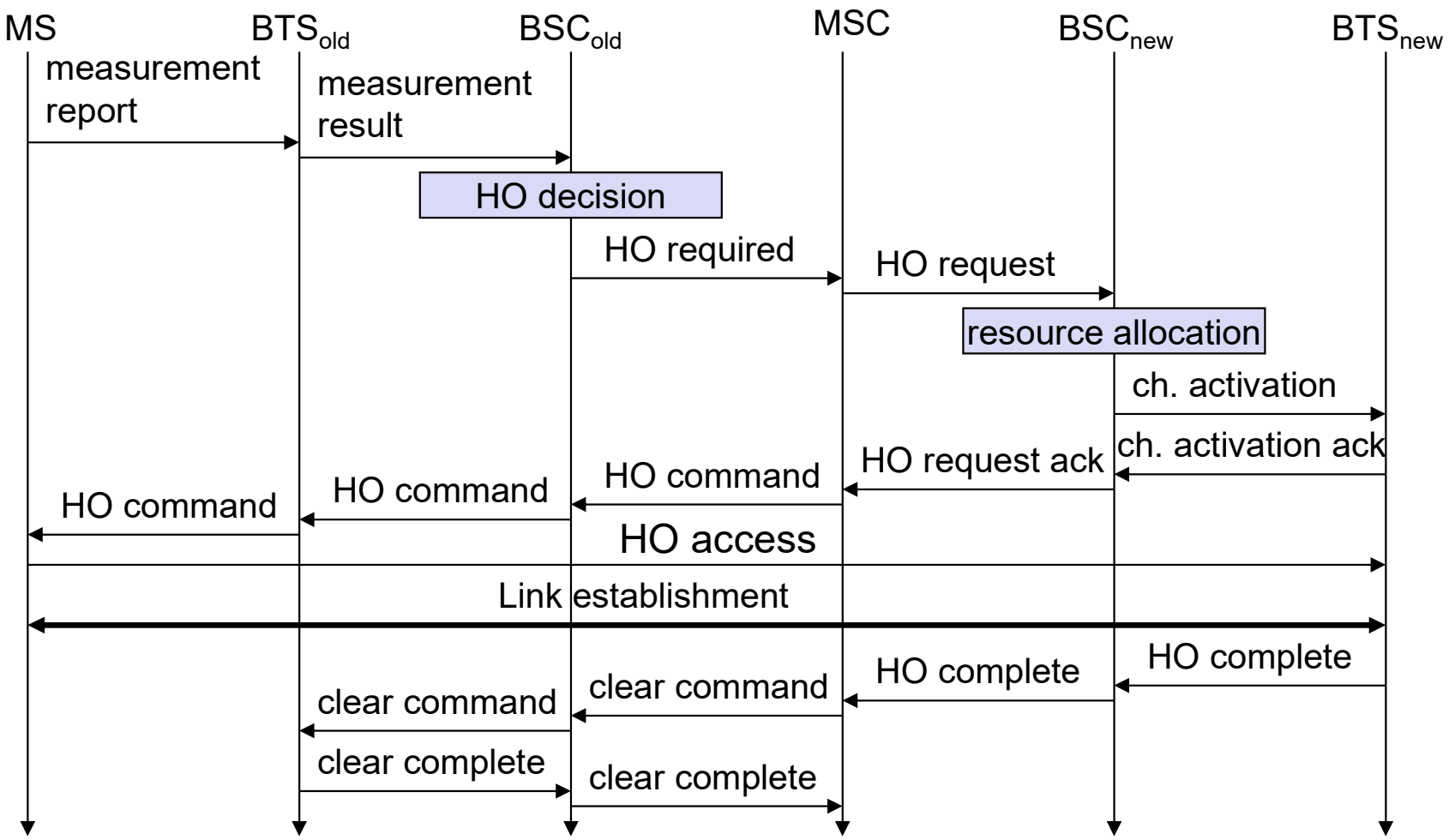
Handover

- Reasons for handover
  - Moving out of range
  - Load balancing
- Handover scenarios
  - Intra-cell handover (e.g., change frequency due to narrowband interference)
  - Inter-cell, intra-BSC handover (e.g., movement across cells)
  - Inter-BSC, intra-MSC handover (e.g., movement across BSC)
  - Inter MSC handover (e.g., movement across MSC)

4 types of handover



Handover procedure

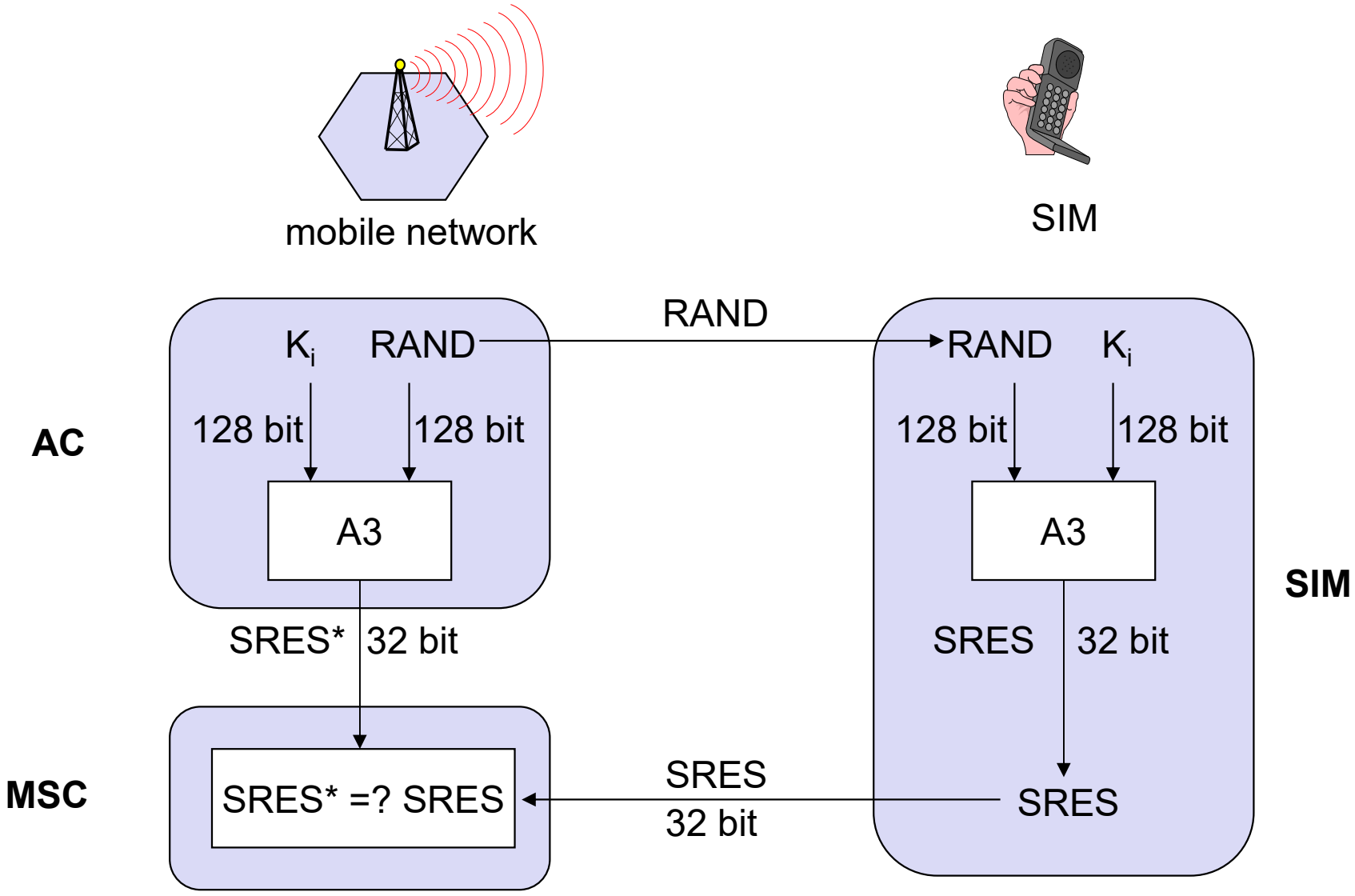


Security in GSM

- 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)

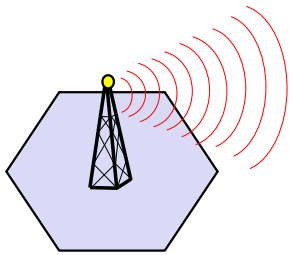
"secret":
• A3 and A8 available via the Internet
• network providers can use stronger mechanisms

GSM - authentication



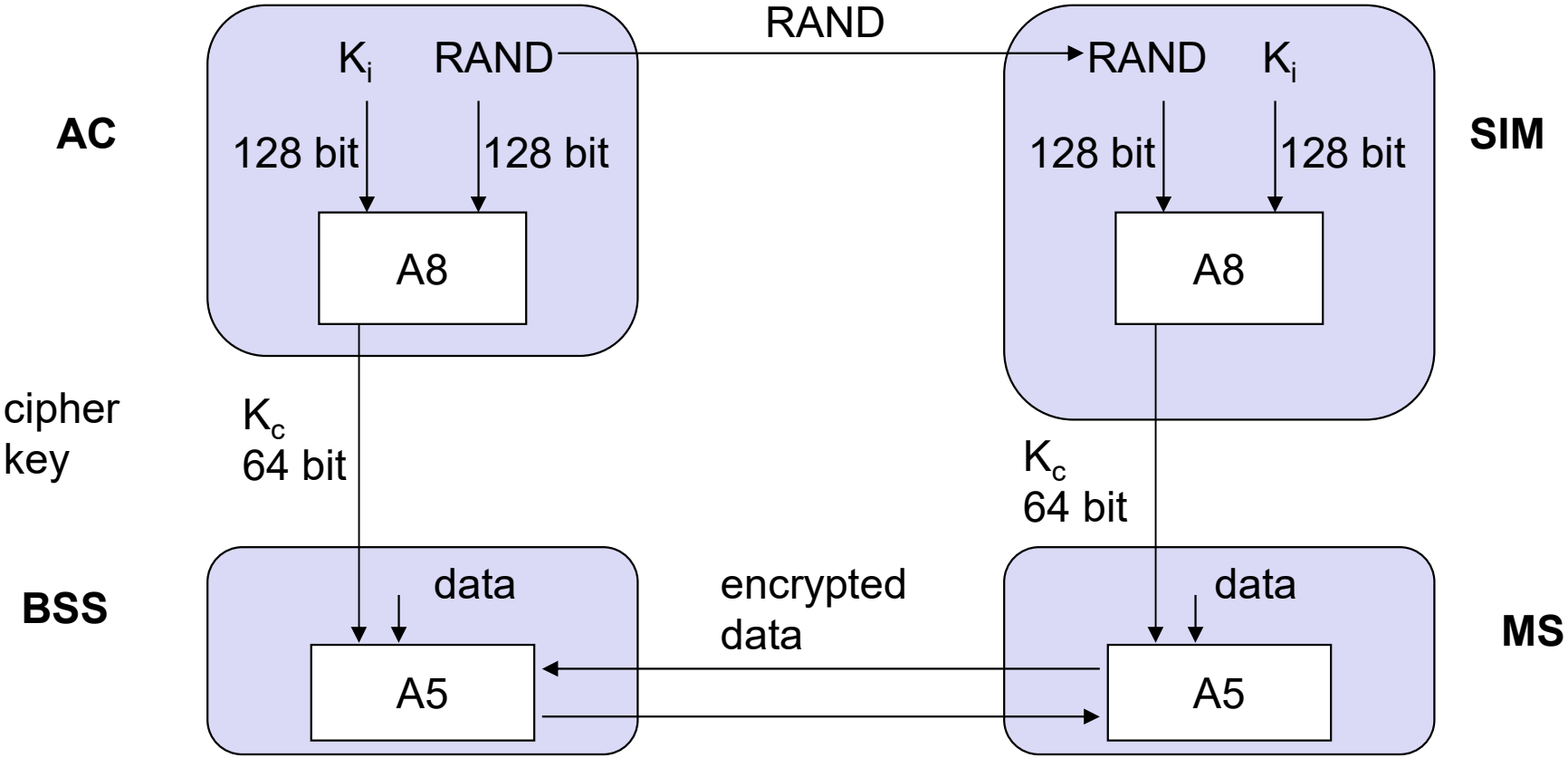
K_i: individual subscriber authentication key SRES: signed response

GSM - key generation and encryption



mobile network (BTS)

MS with SIM



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 each)
  - 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

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			

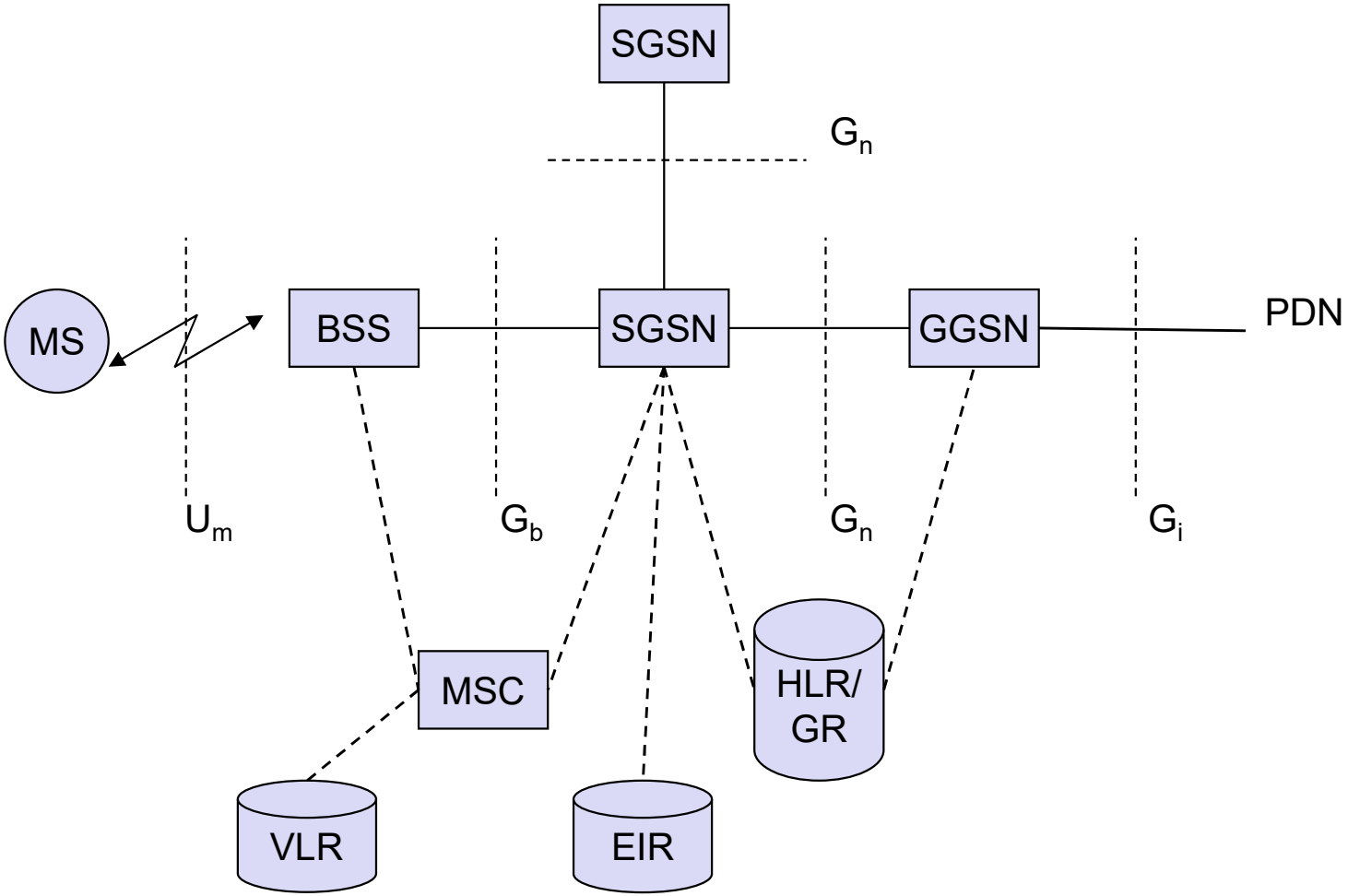
Examples for GPRS device classes

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

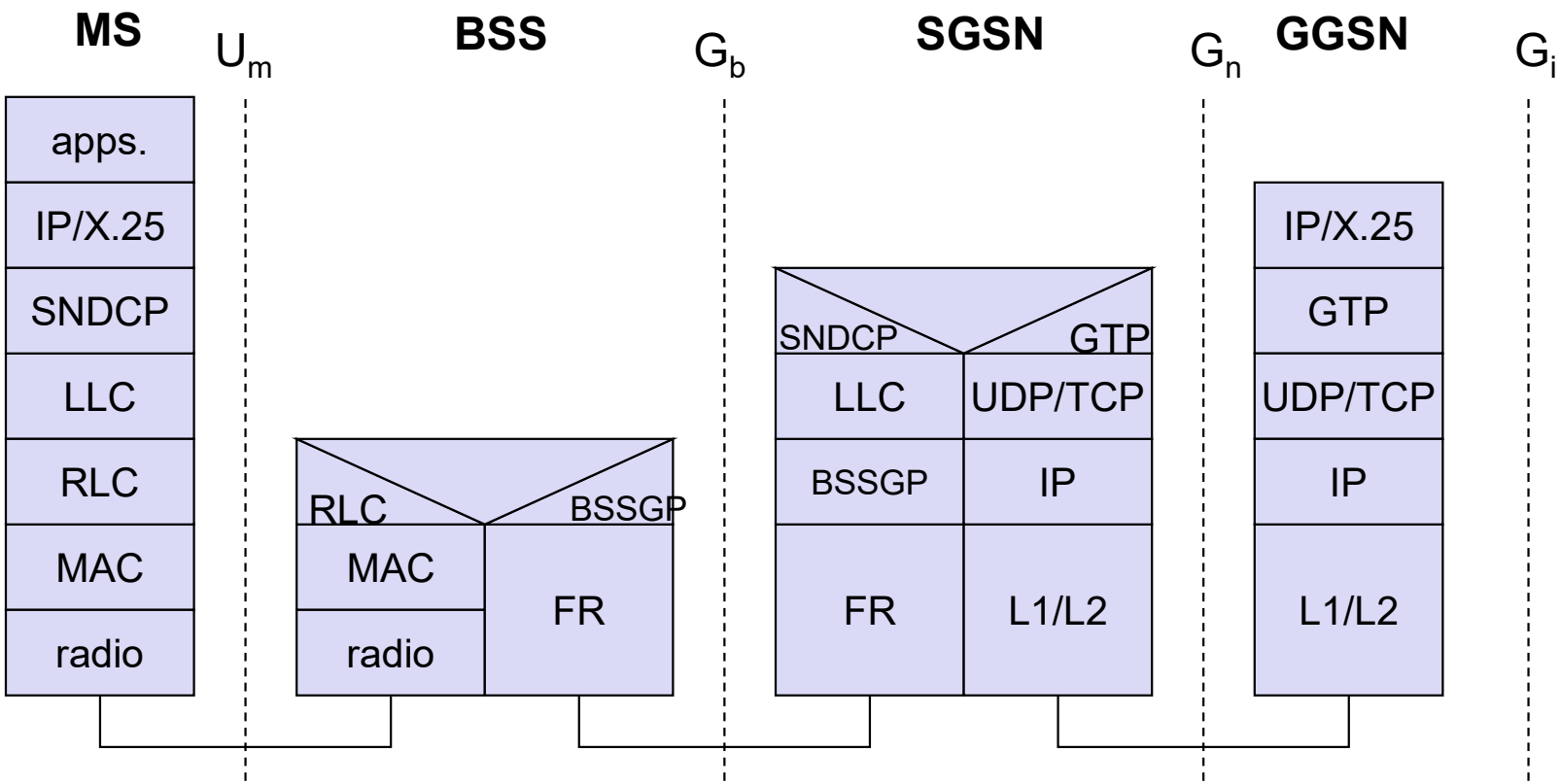
GPRS user data rates in kbit/s

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



Recap

- Introduction
- Frequency reuse
  - a cluster has N cells with unique and disjoint channel
  - # physical channels S = kN
  - Cluster repeated M times in a system
  - Capacity C = MkN = MS
- Channel assignment strategies: fixed vs. dynamic

Recap (Cont.)

- Little's Theorem
  - # users in system = arrival rate * service time
- M/M/c/c queue
  - Blocking probability = $(\alpha^c/c!)/\sum_{i=0..c}(\alpha^i/i!)$ where α is Offered load
  - Learn how to lookup Erlang-B table that relates offered load, # channels, and blocking probability

Offloading Cellular Traffic

- Explosive growth of cellular traffic
- Highly dynamic traffic and large peak-to-average traffic ratio
- Too costly to provision based on peak load

Offloading Cellular Traffic

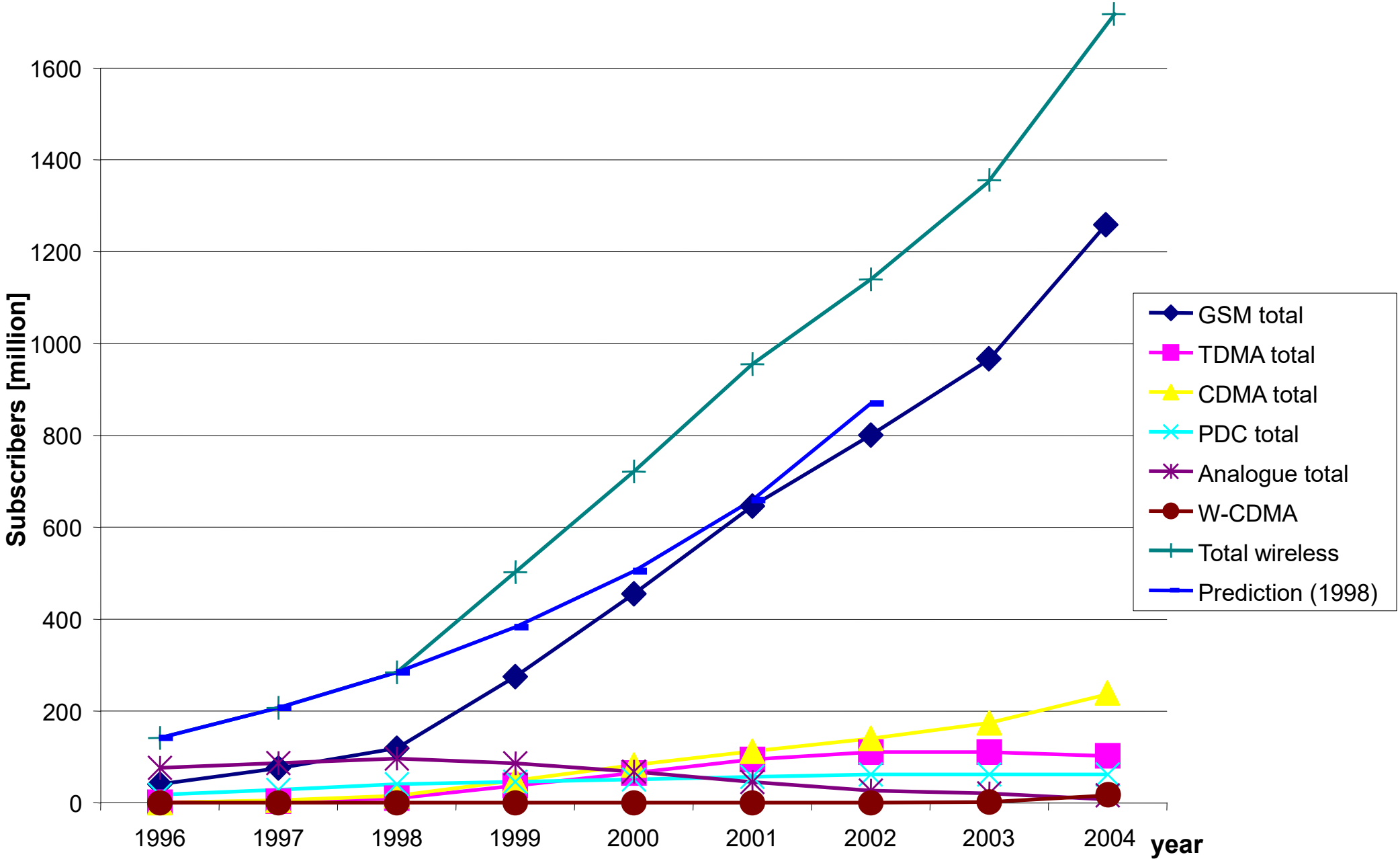
- Cellular provider purchases bandwidth on demand from 3rd party resources
  - Wi-Fi, femtocells, or other cellular resources
- Win-win solution
  - Cellular service provider achieves significant savings
  - 3rd party resource owners gain additional revenue
  - Overall user experience is also improved
- Need an incentive framework to foster collaboration

Dynamic Spectrum Auction

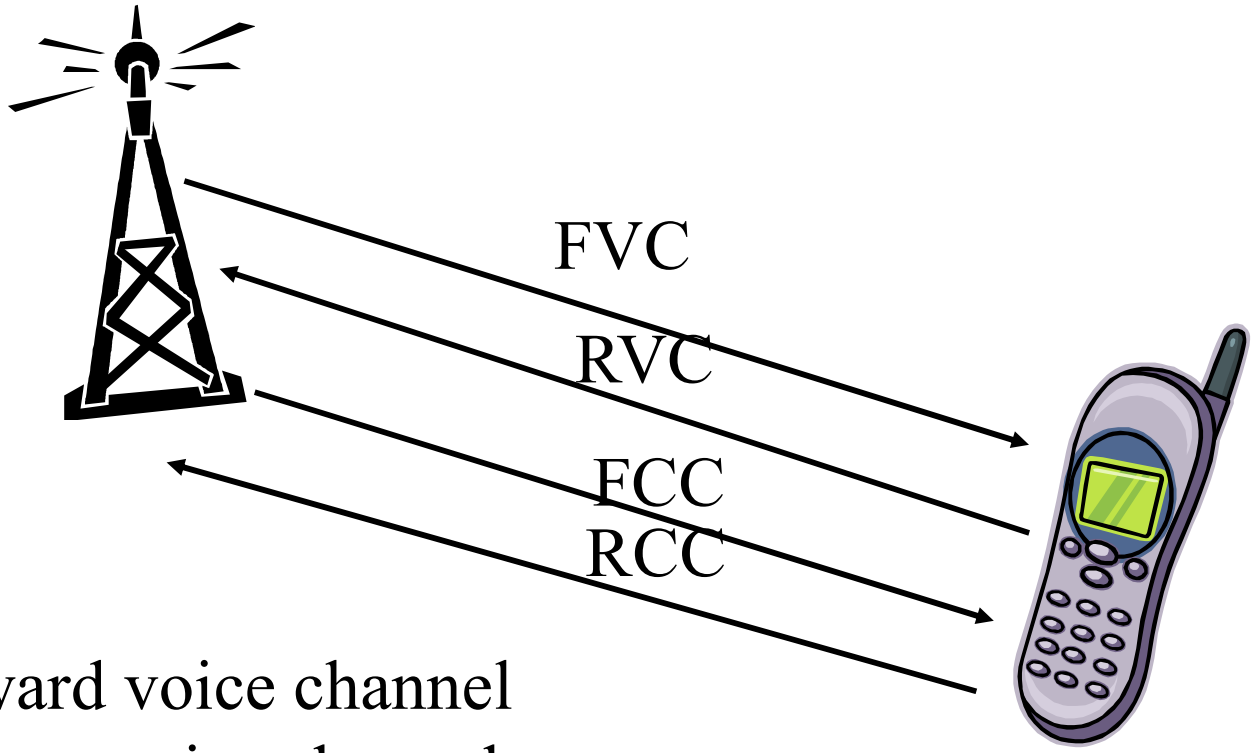
- Buy and sell spectrum among cellular providers

- Spectrum auction
  - Fundamentally different from traditional auction
  - Spectrum can be reused and competition is complicated due to wireless interference

Mobile phone subscribers worldwide



Base Station



Forward voice channel
Reverse voice channel
Forward control channel
Reverse control channel