Aalto University
School of Science

T-110.5111 Computer Networks II

Mobile networks

03.11.2014

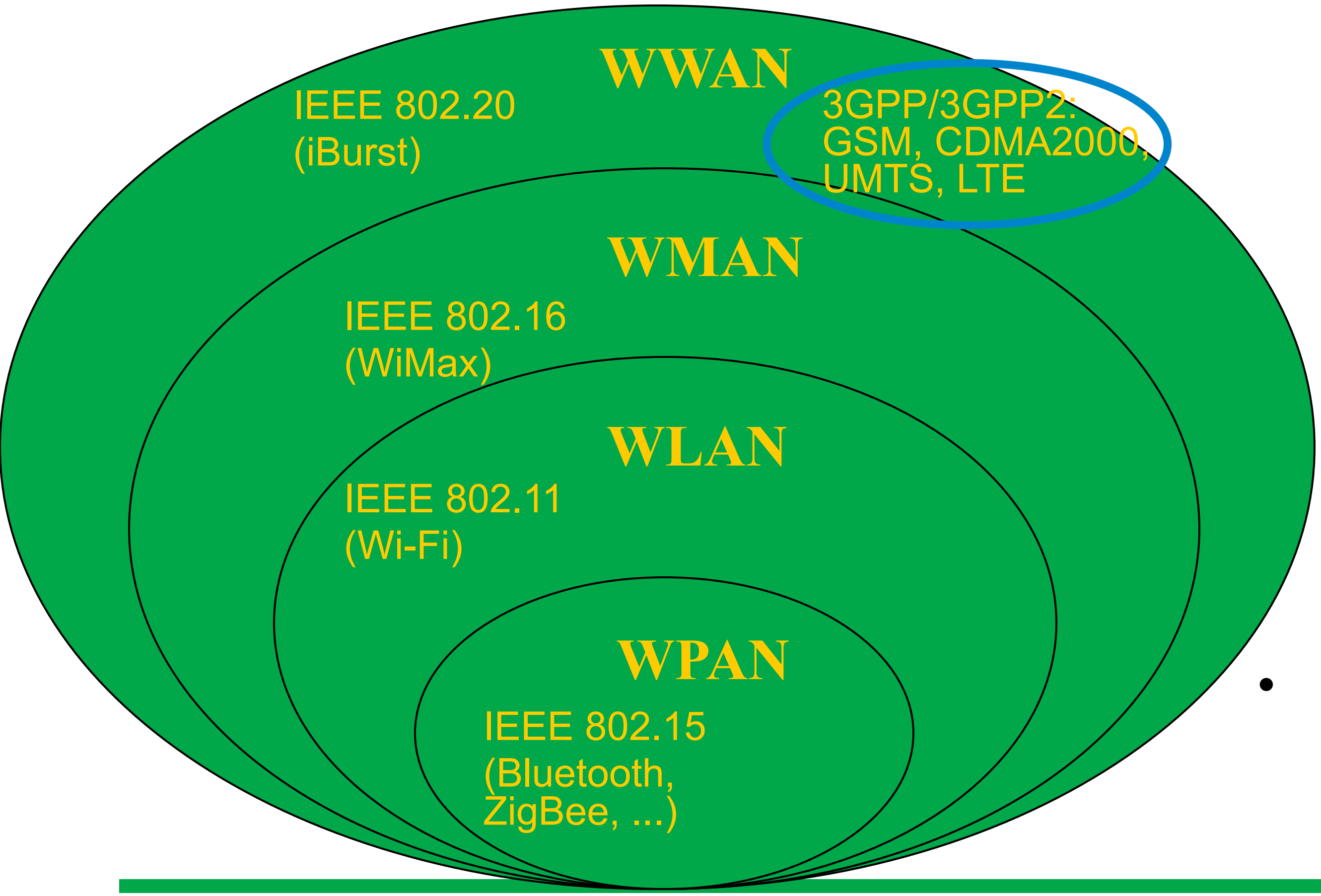
Matti Siekkinen

Sources:
- J. Kurose, K. Ross. *Computer Networking: A Top Down Approach.* 6th edition, Addison-Wesley, April 2009.
- A. Larmo et al: The LTE link layer design. IEEE Communications Mag. 2009.
- *Lecture 8 – Radio Resource Management in LTE System.* S-72.3260 Radio Resource Management Methods –course lecture. 2012. Aalto University
- J. Nurminen. *Mobile networks.* T-110.5121 Mobile Cloud Computing –course lecture. 2013
- L. E. Li. *Cellular Networks and Mobile Computing*. COMS 6998-10 –course lecture. 2013

Before we begin…

- Focus on cellular networks
  - They are the mobile networks in use today
  - Special emphasis on newer technologies, esp. LTE
- Goal: get an overall understanding of how they work
  - They are notoriously complex
  - Entire courses are taught on subjects I cover with half a slide…
- Difficult to find the right level of abstraction
  - We will look at some things in more detail too
  - Try not to get drowned in the soup of acronyms

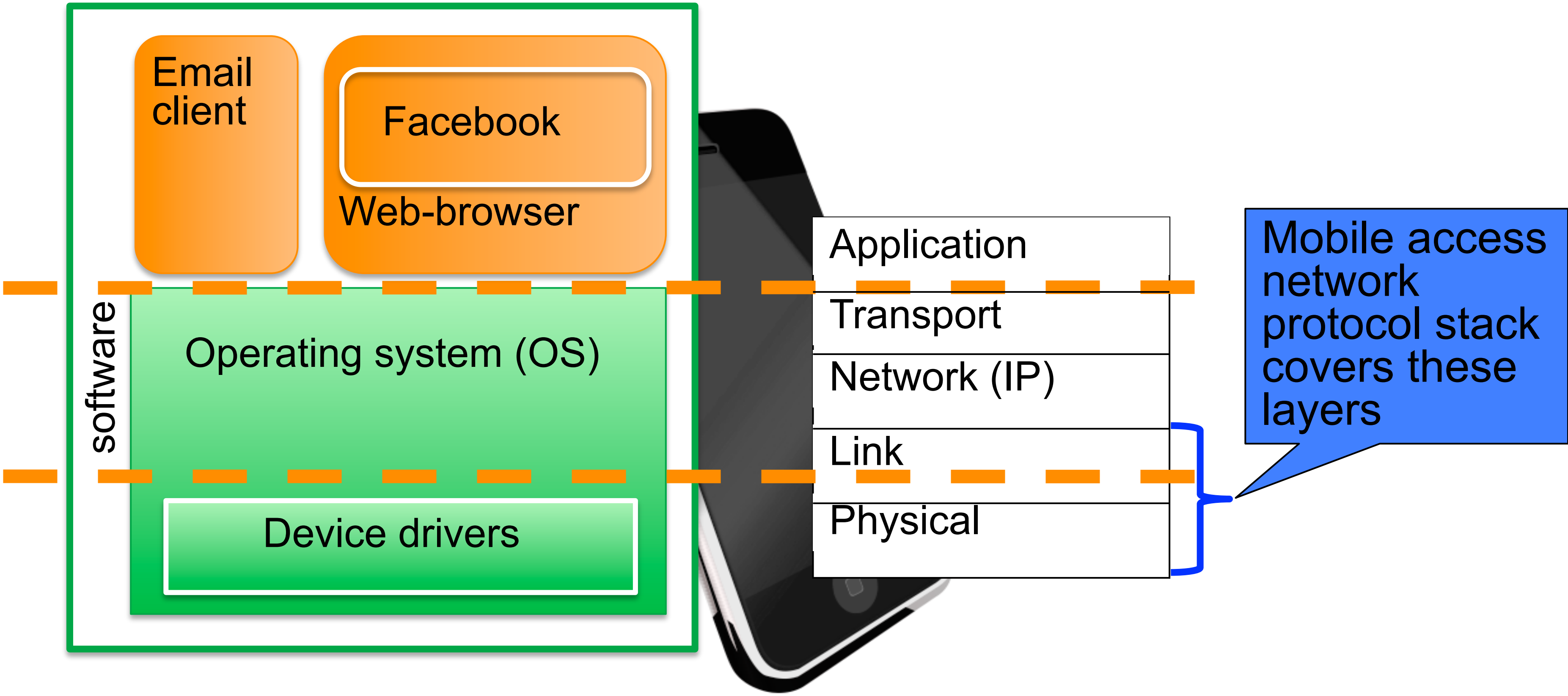
The big picture: Wireless networks, standards, technologies



- Technologies vary
  - Frequency bands
  - Modulation
    - BPSK, QAM...
  - Channel access
    - random access, CDMA, OFDMA, FHSS…
  - Error correction
    - FEC, ARQ
  - Smart antenna techniques
    - MIMO
  - Protocol stacks
    - Below IP or no IP at all
- Characteristics vary
  - Range
  - Data rates
  - Power efficiency

Our focus today is on cellular networks

What about the Internet protocol stack?



Outline

- Overview of cellular networks
  - Historical and future perspectives
  - Components of cellular networks
- Cellular network architecture
- Mobility
- Application-level performance
- Summary

History of cellular network technology

ARP NMT → GSM (2G) 1993 → GPRS (2.5G) 2001 → 3G 1999 → LTE 2009

Analog: ARP NMT

Digital: GSM (2G) through LTE

Faster data rates; towards global standards; smaller, lighter, smarter, …, terminals

Comparison of Generations 1G, 2G, 3G, 4G

Generation	Definition	Throughput	Technologies
1G	Analog	14.4 kbps (peak)	AMPS,NMT,TACS
2G	Digital (Narrow band Circuit Data)	9.6/14.4 kbps(peak)	TDMA, GSM, CDMA
2.5G	Packet Data	114/236.8 kbps(peak) 20-40 kbps	HSCSD, GPRS, EDGE
3G	Digital broadband packet data	3.1 mbps (peak) 500-700 kbps	UTMS, CDMA2000 1XRTT
3.5G	>2mbps	3.6/7.2/14.4 mbps(peak) 1-3 mbps	HSPA, CDMA2000 EV-DO
4G	Digital broadband packet based All IP (VOIP)	100 – 300 mbps (peak) 3-12 mbps	LTE Advanced WiMax Advanced HSPA+

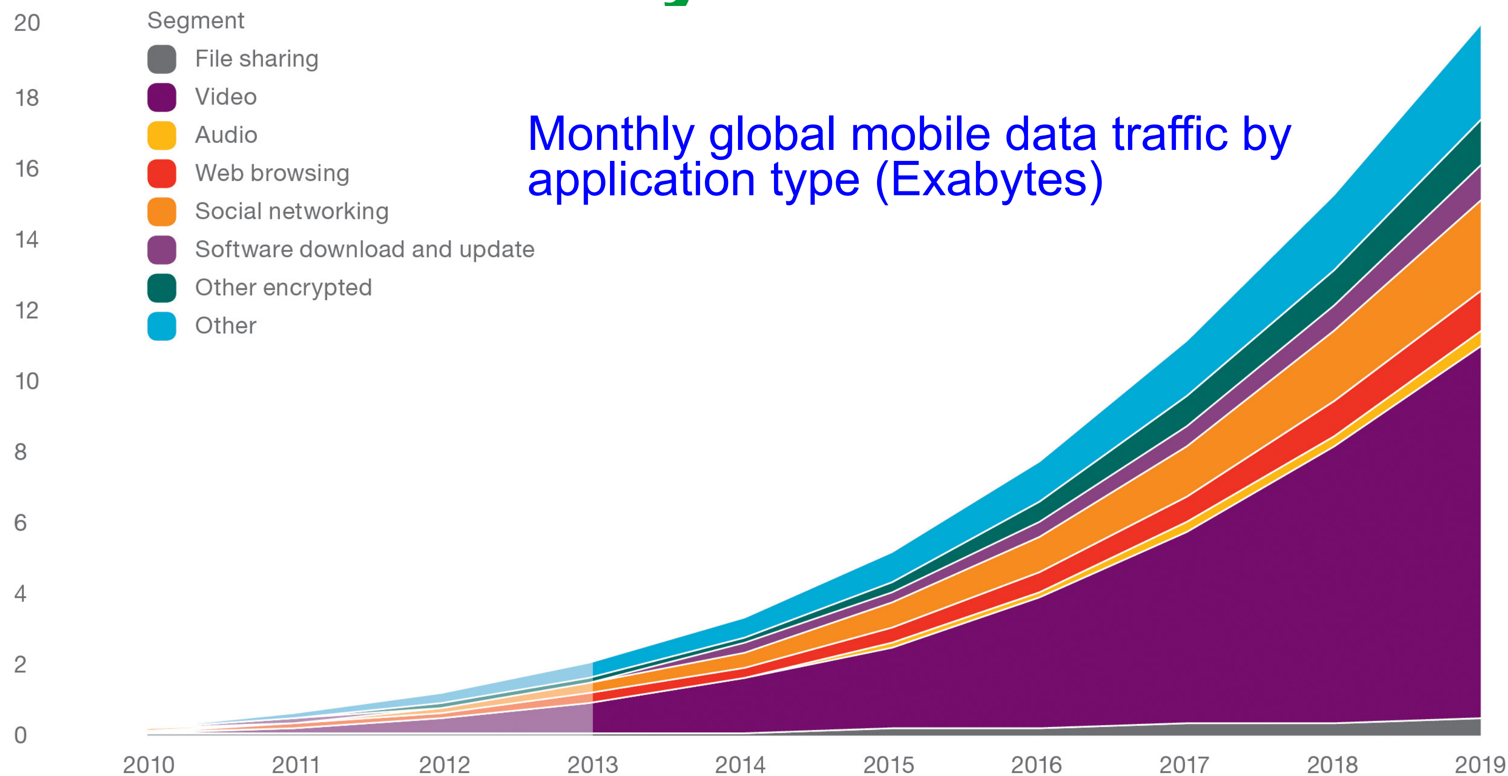
A

3GPP

A GLOBAL INITIATIVE

- 3rd Generation Partnership Program
  - Established in 1998 to define UMTS
  - Today also works on LTE and access-independent IMS
  - Still maintains GSM
  - All the major industrial players are members
- 3GPP standardizes systems
  - Architecture, protocols
- Works in releases
  - All specifications are consistent within a release
  - New release every 1-2 years
  - Currently finalizing Release-12, several categories of advances:
    - LTE small cell and heterogeneous networks
    - LTE multi-antennas (e.g., MIMO and beam forming)
    - LTE procedures for supporting diverse traffic types (further work on HSPA+ was also included)

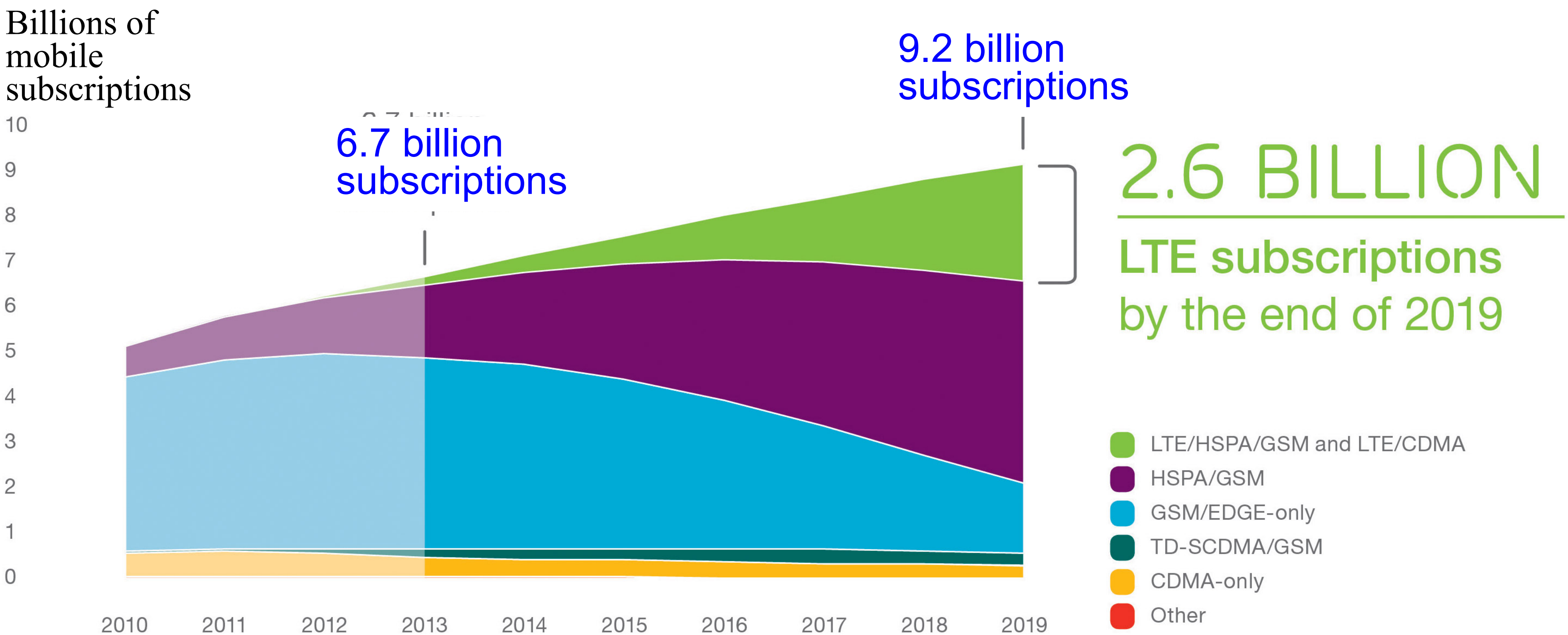
Data tsunami on the way…



- Ten fold increase in smartphone traffic 2013 → 2019
- Video driving the growth

Figure source: Ericsson mobility report (June 2014)

Transition from GSM to LTE through UMTS



- 2G still clearly the most used technology but no longer growing
- 3G (HSPA) still growing, expected to stick around for long time
- LTE relative growth (%) is very fast

Figure source: Ericsson mobility report (June 2014)

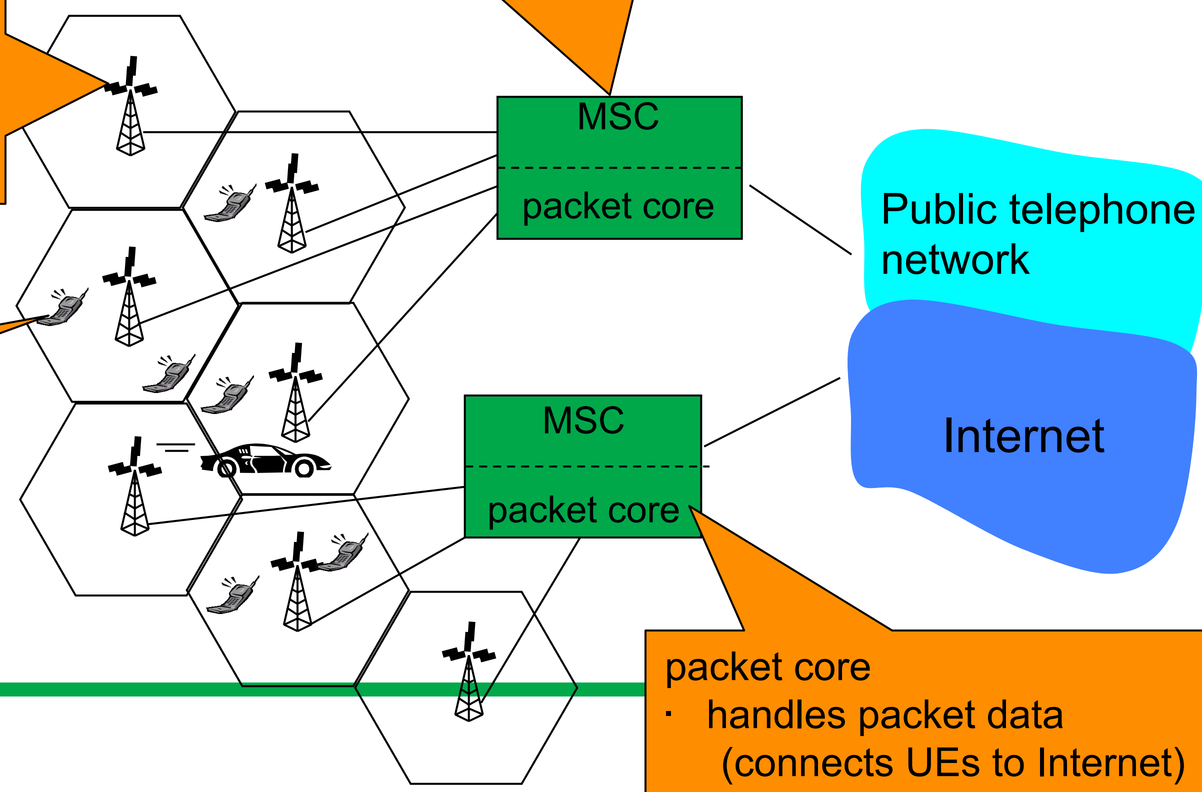
Outline

- Overview of cellular networks
  - Historical and future perspectives
  - → Components of cellular networks
- Cellular network architecture
- Mobility
- Application-level performance
- Summary

Components of cellular network architecture

Base station (BS)
- serves geographical region
- analogous to 802.11 AP
- mobile users attach to network through BS
- air-interface: physical and link layer protocol between mobile and BS

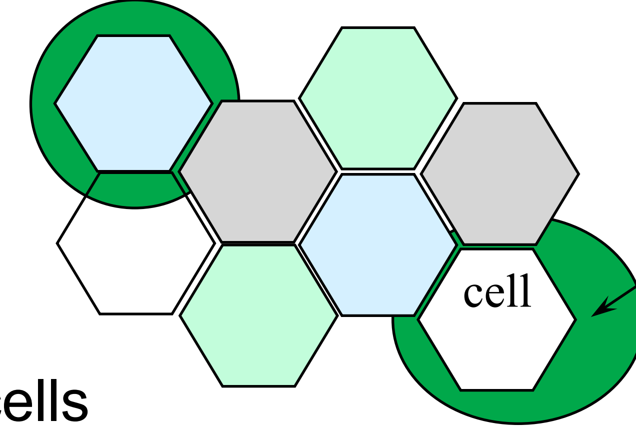
Mobile Switching Center (MSC)
- connects cells to wired tel. net.
- manages CS call setup
- handles mobility



User Equipment (UE)
- phone or other end user device

packet core
- handles packet data (connects UEs to Internet)
- manages VoIP calls (VoLTE)
- handles mobility (LTE)

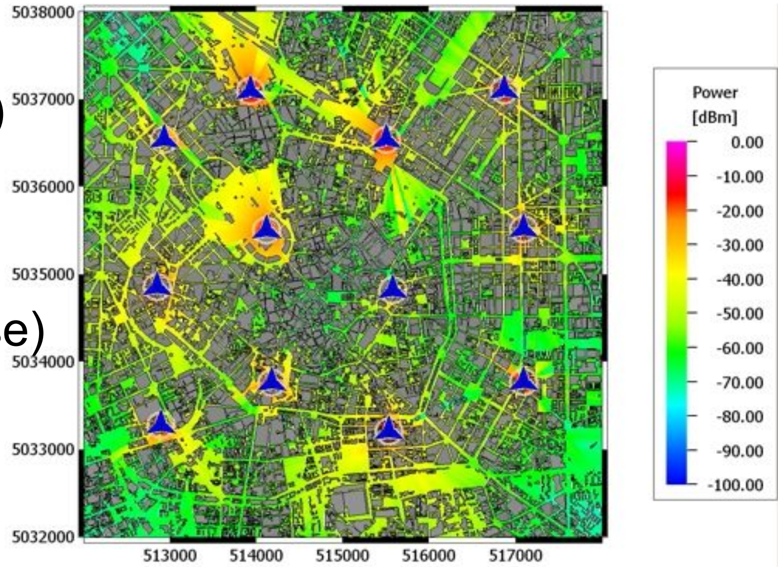
Cells



- Region is divided into cells
- Cells typically divided into sectors
  - Use directional antennas
  - E.g. multiple remote radio heads connected to single base station
- Frequencies are reused by different cells but not always
  - Must avoid co-channel interference between cells
  - Frequency reuse factor indicates how many cells cannot use same frequencies
  - E.g., assign adjacent cells with different frequency bands (fraction of whole licenced band)
  - LTE deployed even with factor = 1 (complete reuse)
    - Coordinated scheduling, inter-cell interference coordination (ICIC) mechanisms, etc.

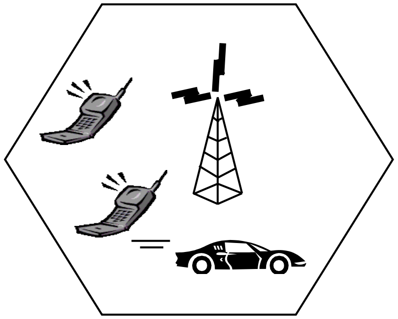
Cells

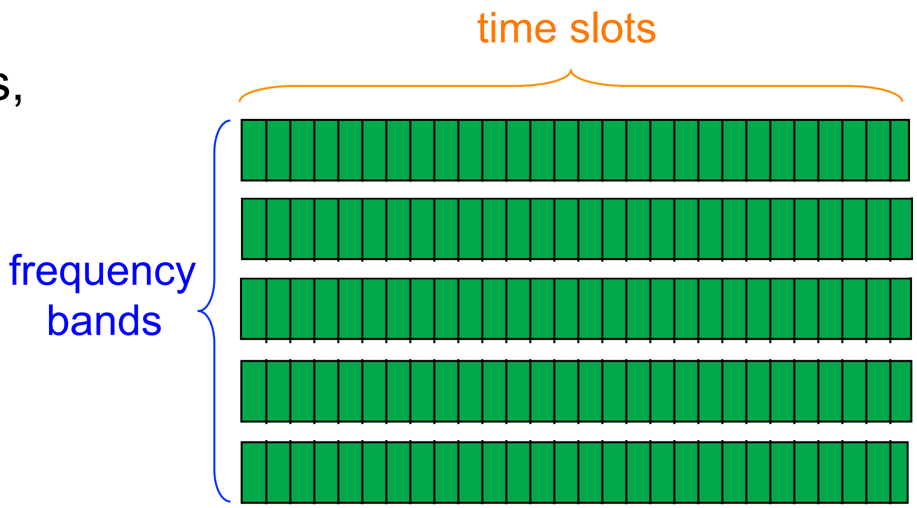
- Many different cell sizes possible
  - Macrocells (rural areas), microcells (urban), picocells (indoors and recently metropolitan outdoors), femtocells (indoors@home/small office, 10m range)
- Planning of cellular network is an optimization problem
  - Cover geographical area (rural areas)
  - Provide enough capacity (urban areas)
  - Minimize cost
    - Equipment purchase
    - Deployment cost (installation, land lease)
    - Operational cost (power, maintenance)
    - …



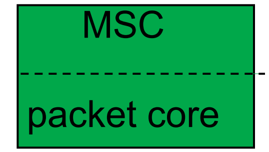
The first hop: Radio Access Network

- Provides radio access to UEs through base stations
  - Shared medium
- Two techniques for sharing mobile-to-BS radio spectrum
  - *combined FDMA/TDMA*: divide spectrum in frequency channels, divide each channel into time slots
    - GSM (2G) and LTE (4G)
  - *CDMA*: code division multiple access
    - UMTS (3G)





"Next hop": the core network



- Two types of operations
  - Circuit switching for voice calls (currently)
  - Packet switching for data
- MSC takes care of CS operations
  - Introduced to mobile networks with GSM (2G)
  - Still there today as most voice calls handled the same way
- Packet core takes care of packet switching
  - Takes care of data communication
  - Also (eventually) voice calls in 4G
  - GPRS Core Network (2G and 3G) → Evolved Packet Core (4G)

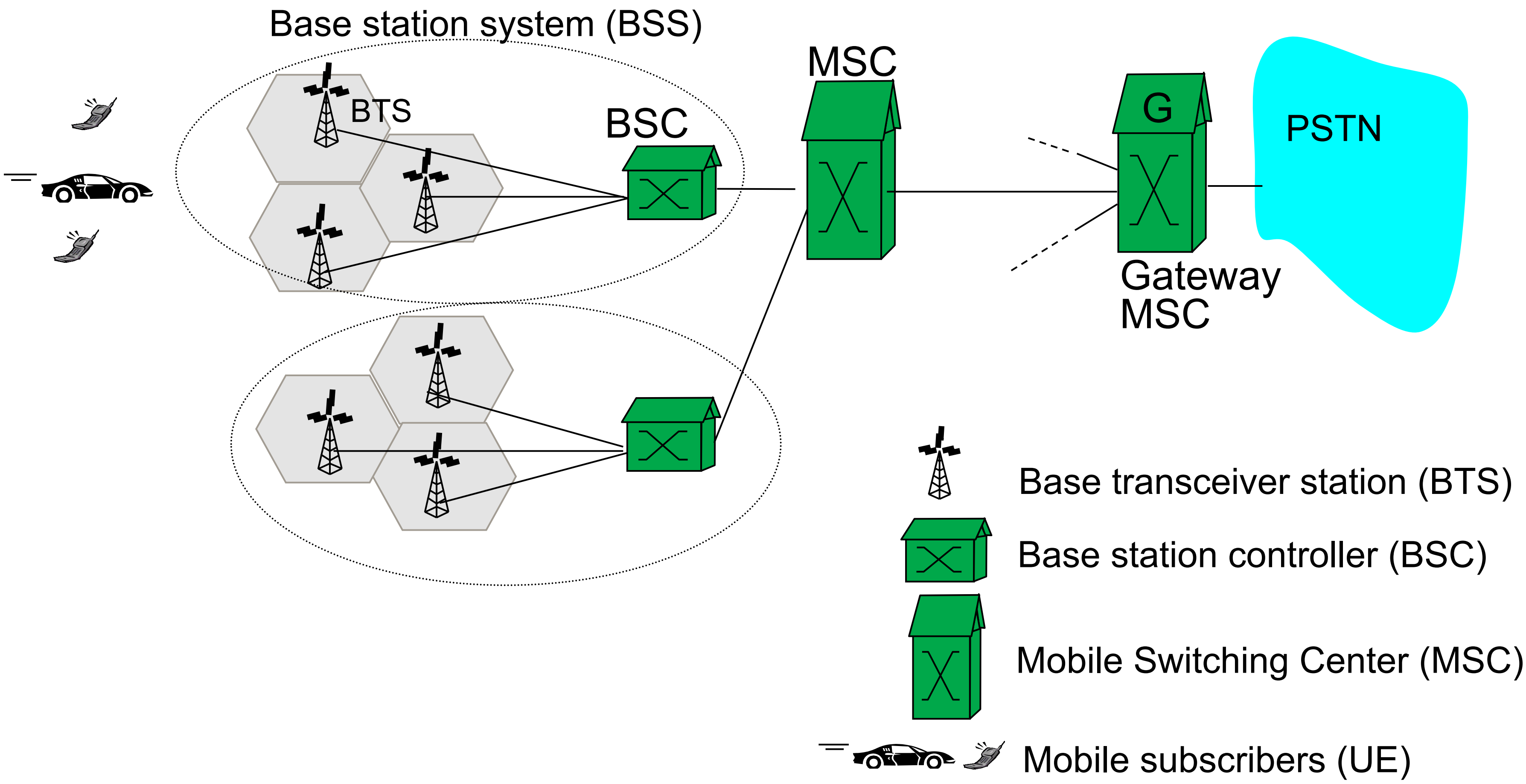
IP Multimedia Subsystem (IMS)

- Not standard part of the core network
  - Connected to it in one way or another
- Set of functions with standardized interfaces
  - Different manufacturers offer different kinds of solutions
- Used to handle e.g. VoIP (VoLTE in LTE) and video services
  - Note that these are the same as over-the-top (OTT) services like Skype

Outline

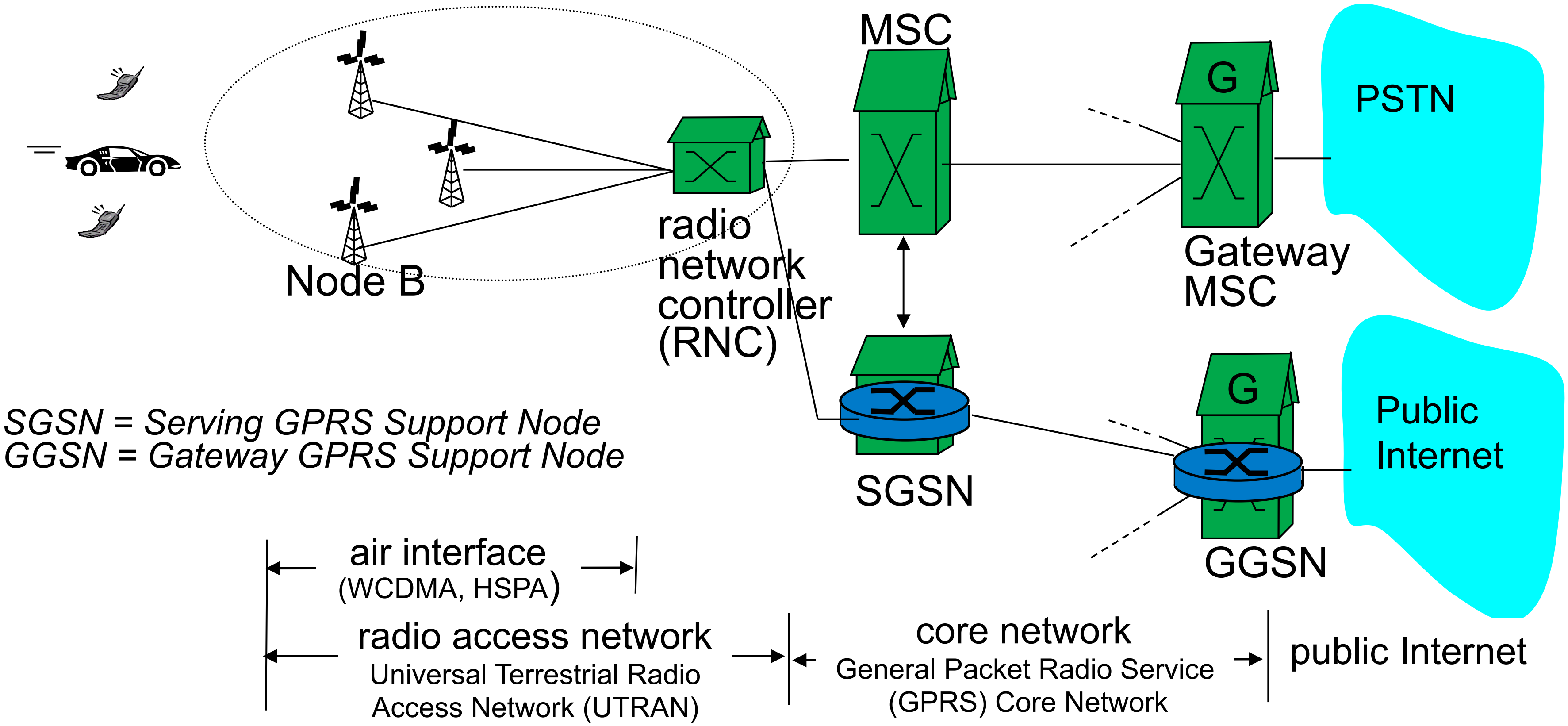
- Overview of cellular networks
- Cellular network architecture
  - → Overview
  - Radio Access Network (RAN)
  - Packet core
- Mobility
- Application-level performance
- Summary

2G (GSM) architecture

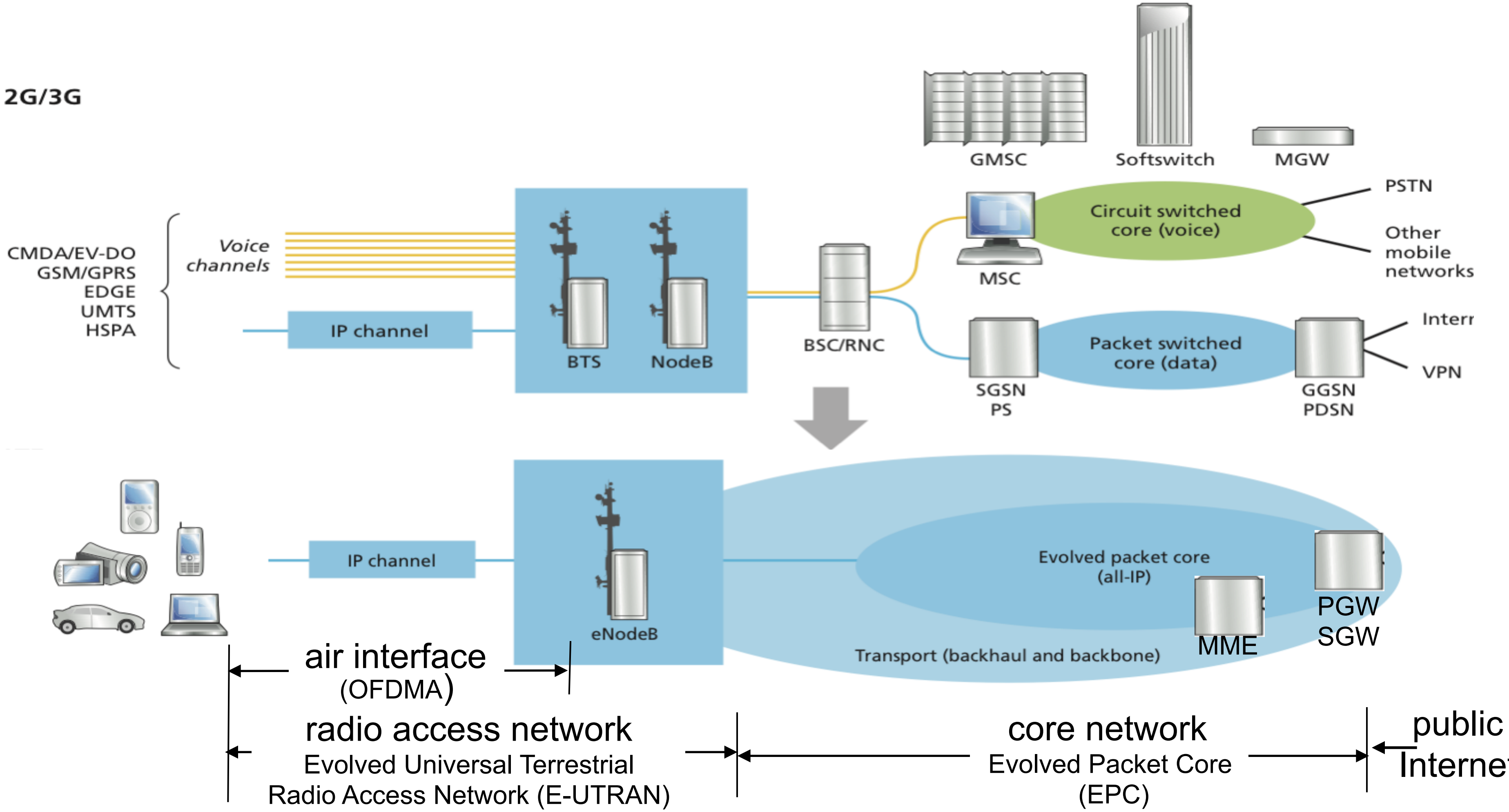


3G (UMTS) architecture

3G data network operates in *parallel* with voice network → voice network part can remain unchanged



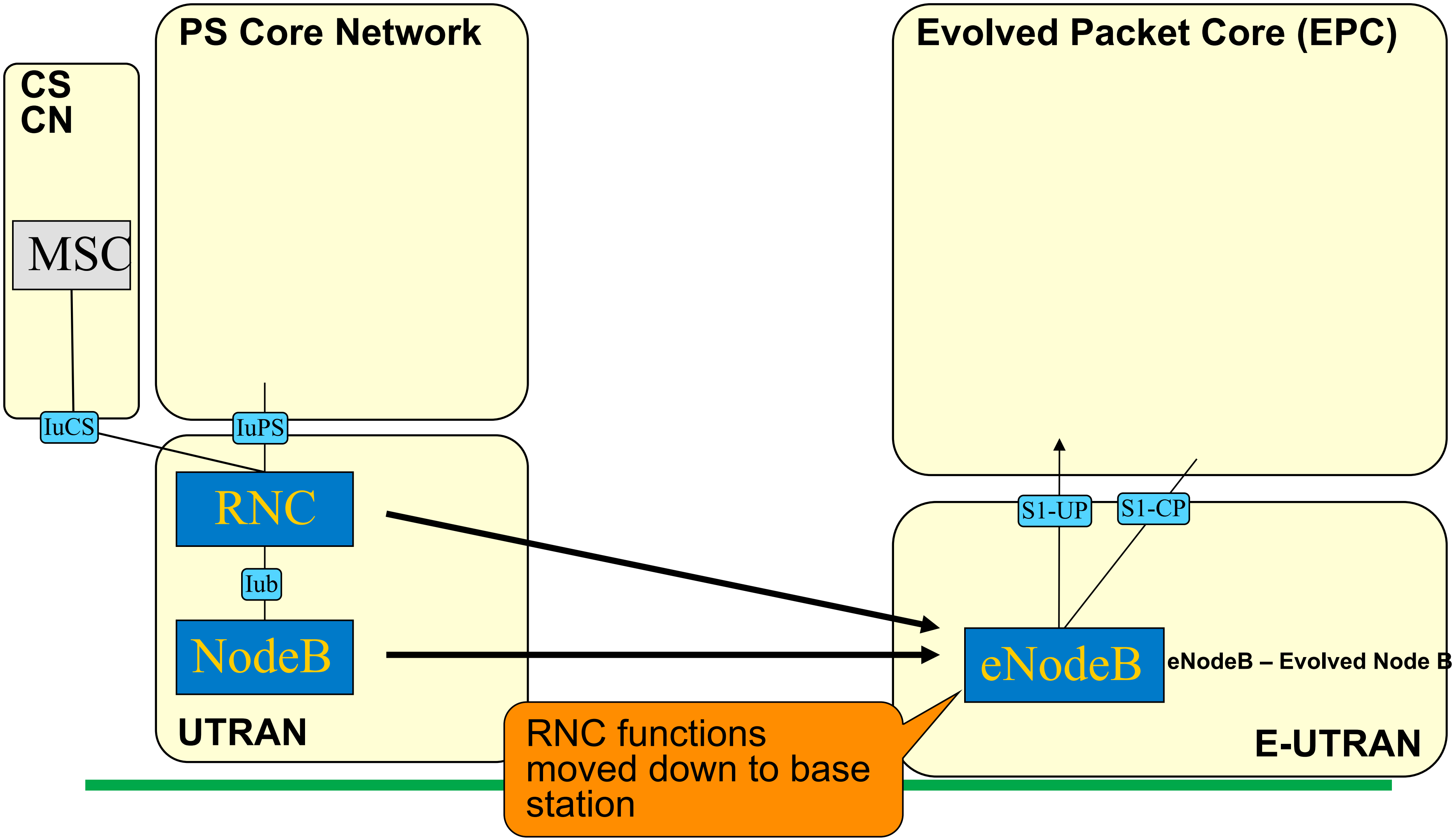
4G (LTE) architecture



Outline

- Overview of cellular networks
- Cellular network architecture
  - Overview
  - → Radio Access Network (RAN)
  - Packet core
- Mobility
- Application-level performance
- Summary

Architecture: UTRAN (3G) → E-UTRAN (4G)



Evolved NodeB (eNodeB)

- The only element in the LTE RAN
  - Base station
- Handles everything related to radio functionality in LTE
  - Both user plane (data transmission) and control plane (signaling)
  - Manages radio resources (scheduling transmissions to/from UEs)
- Provides UEs access to IP core
  - Performs as a layer 2 bridge
  - Encrypting and decrypting the user plane data over the radio link
- Important role in mobility management too
  - Decides when handover is required based on measurements sent by UE
  - Implements the handover

Air interface

- Air interface defines the way UE and base station communicate
- PHY layer radio access method
  - How to transmit bits into the shared channel
  - Such as OFDMA in LTE
- Link layer protocols
  - UE and base station need to exchange signaling messages all the time
  - Error control, multiple access, segmentation, security…

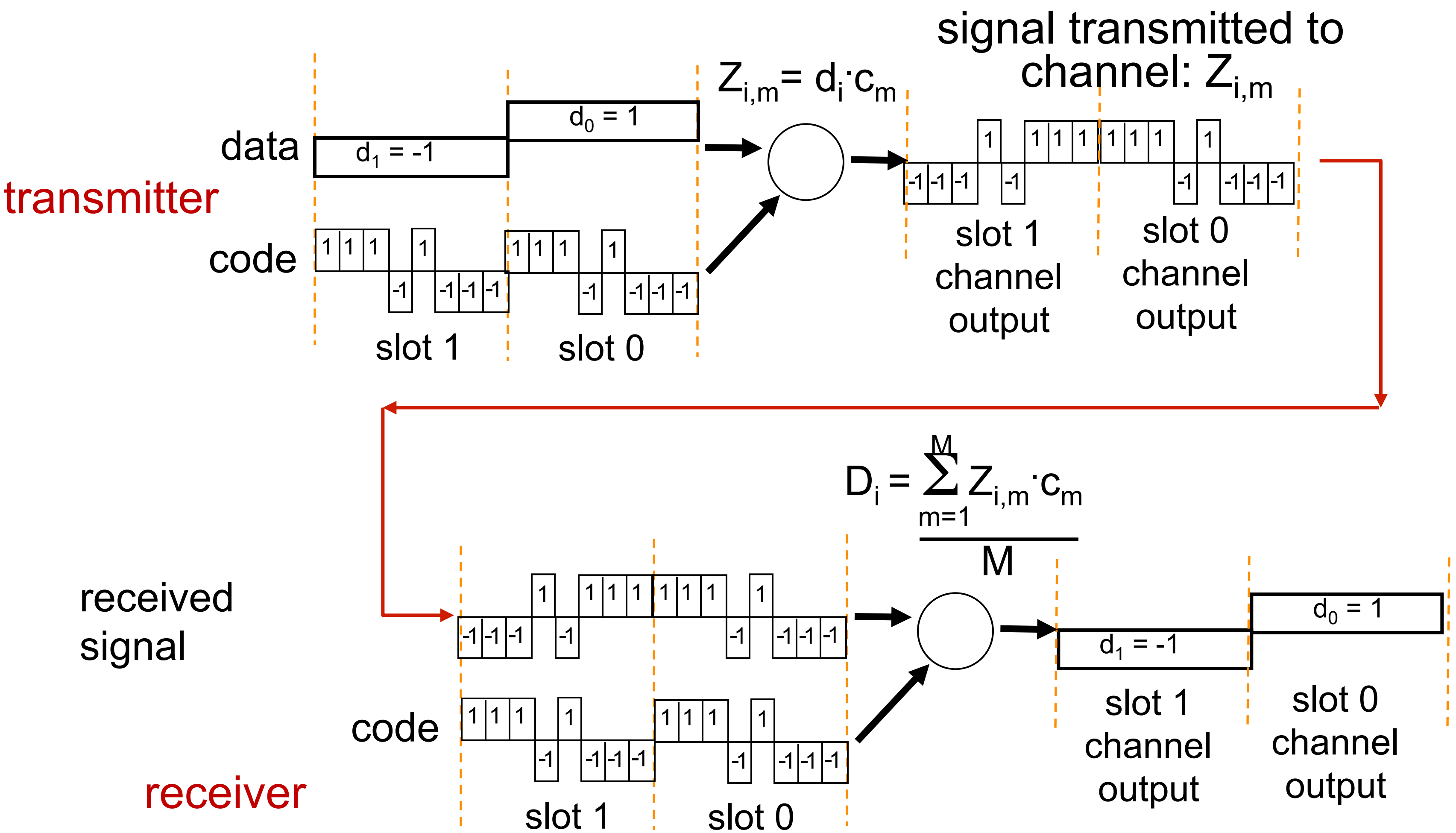
Radio access

- 3G uses CDMA (Code Division Multiple Access)
  - All base stations use the same frequency
  - Each UE's transmission encoded with a different code
    - Can transmit same time at the same frequency without co-channel interference
  - Several variants of CDMA used (e.g. W-CDMA)
- LTE radio access is based on OFDM (orthogonal frequency division multiplexing)
  - Specifically OFDMA: multi-user version of OFDM
    - Allocates subcarriers to different users
  - Also time division dimension

Code Division Multiple Access (CDMA)

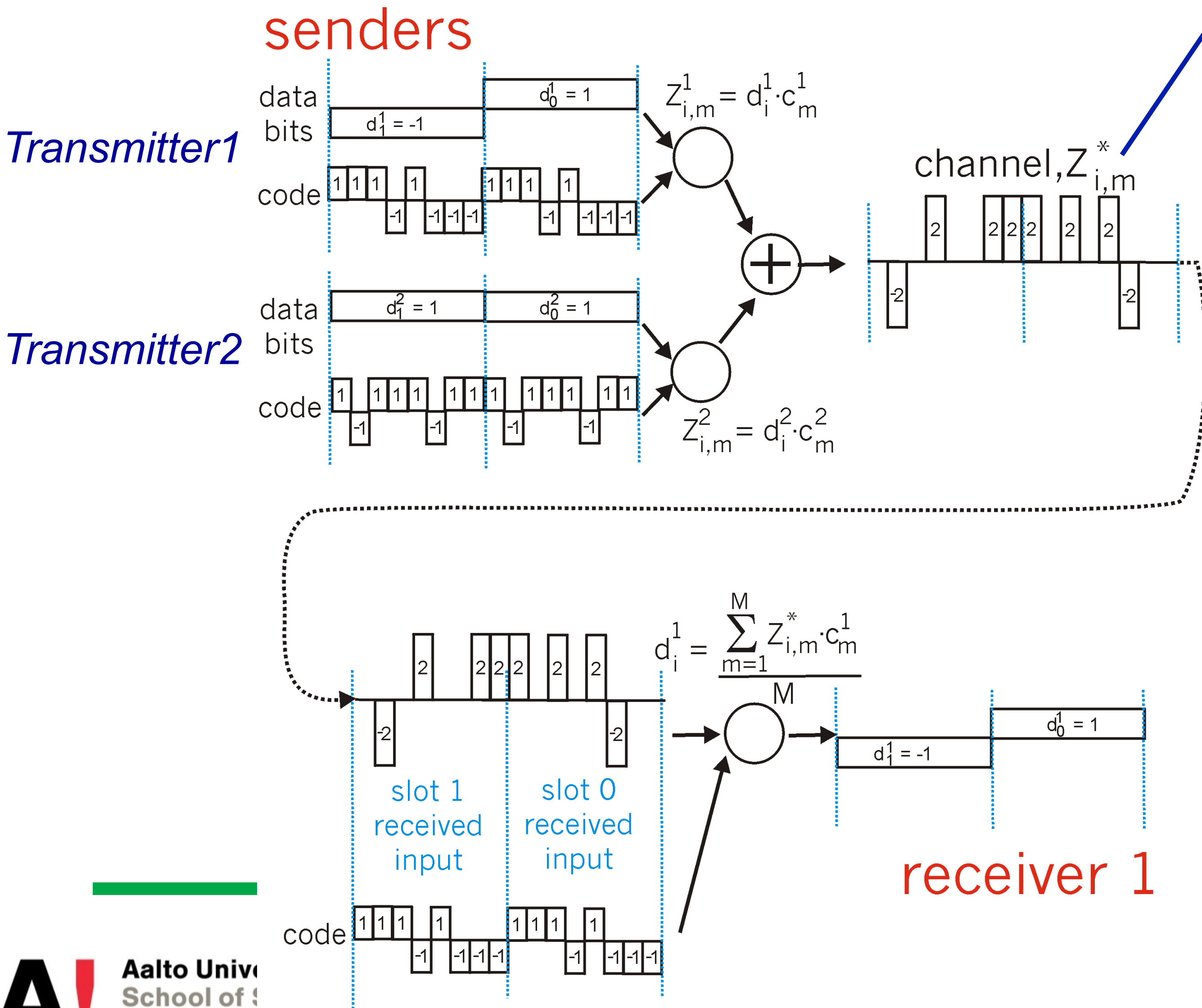
- Divide radio channel with codes:
  - Everyone transmits on the same frequency
  - Unique code to each transmitter
    - "chipping" sequence (i.e., code) used to encode bits to transmit
  - Several simultaneous transmissions possible without co-channel interference problems
- *encoded signal = (original data) X (chipping sequence)*
- *decoding*: compute inner product of received signal and chipping sequence divided by code length

CDMA encoding and decoding



CDMA: two transmitters

channel combines both transmissions



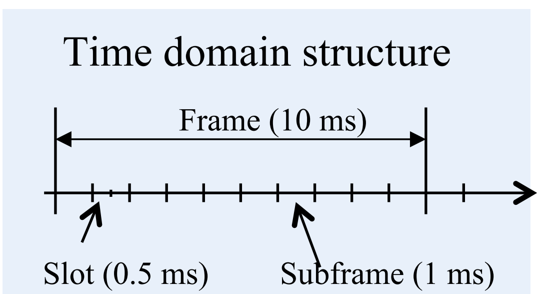
receiver can decode original data by specific transmitter using same code as transmitter

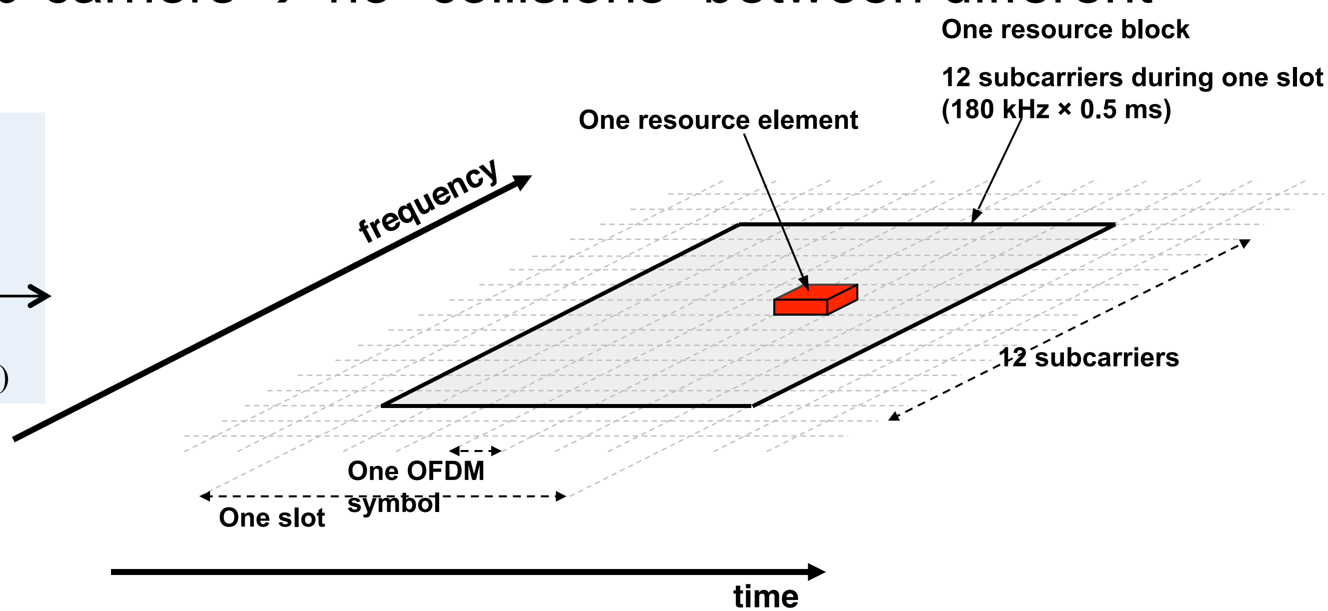
CDMA: tradeoff

- Codes must be carefully chosen
  - Orthogonal: inner product of two codes is zero
- Tradeoff
  - Must transmit several symbols per each bit of original data → reduces bitrate
  - Limited number of orthogonal codes of given length exist
    → imposes limits on simultaneous transmitters
  - Shorter code → higher bitrate but for fewer transmitters

LTE downlink: OFDMA-based radio access

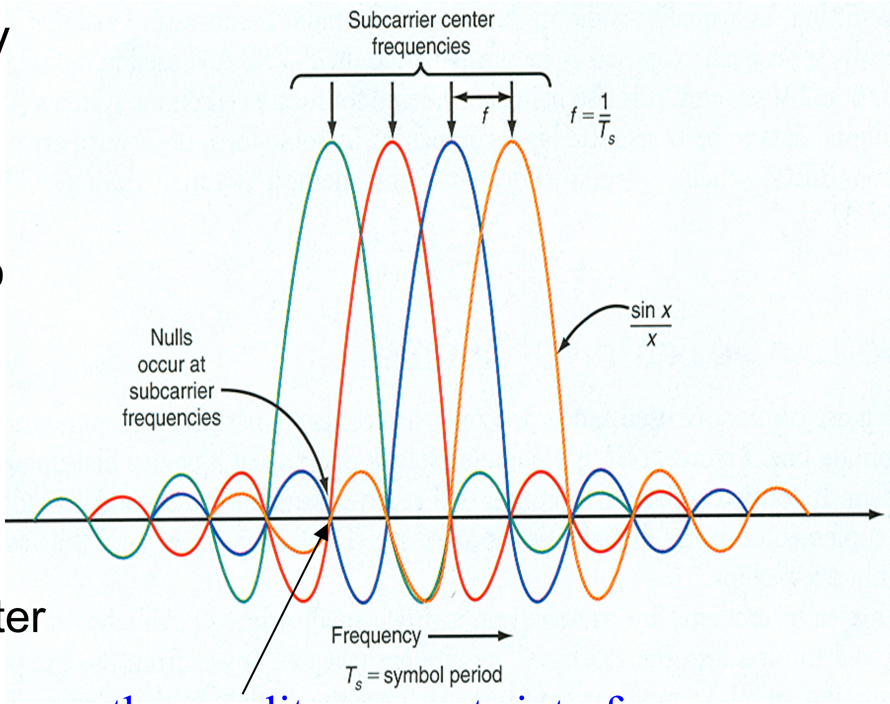
- 2D resource grid: frequency and time
- Narrowband channels: equal fading in a channel
  - Allows simpler signal processing implementations
- Orthogonal sub-carriers → no “collisions” between different transmitters





OFDM: Orthogonal frequency-division multiplexing

- Use multiple subcarriers
  - Each sub-carrier modulated separately → carries different symbols
- Advantages over wideband transmission:
  - Narrowband channels less sensitive to noise and fading than single wider bw one
- Difference to "regular" FDMA:
  - No guard bands, subcarriers overlap
  - Subcarriers must be **orthogonal**
    - Amplitude zero at other subcarrier center frequencies
  - OFDM much more bandwidth efficient

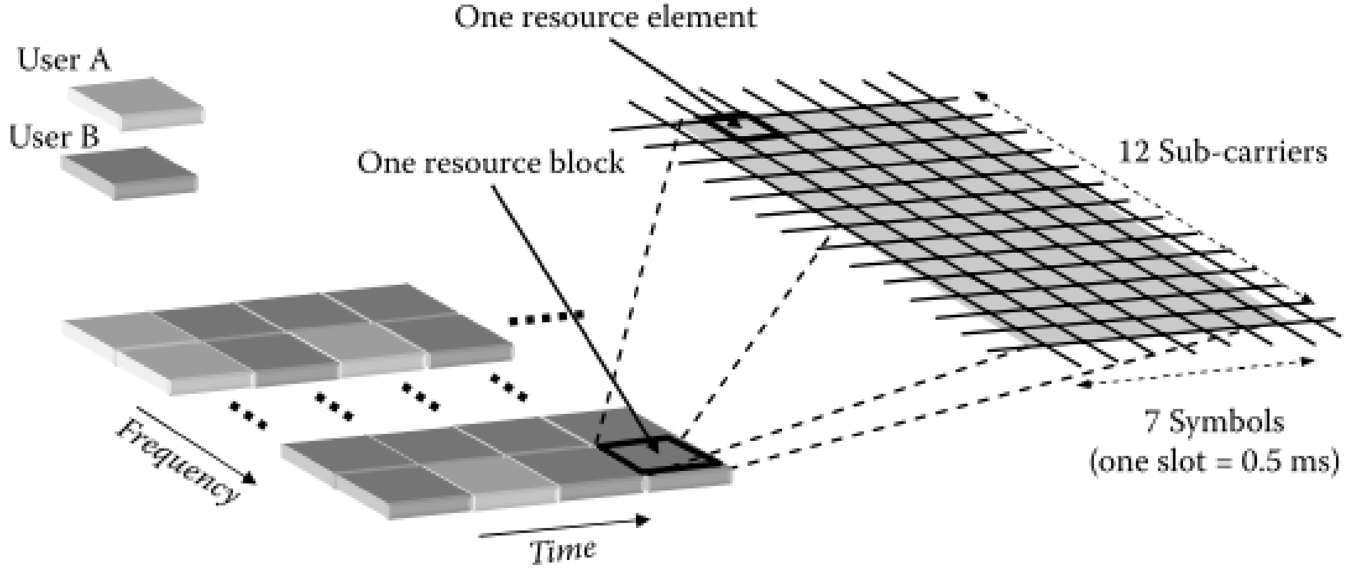


orthogonality prevents interference between subcarrier signals

Aalto University
School of Science

OFDMA: multiuser version of OFDM

- OFDMA assigns different users different subcarriers
  - Simultaneous transmissions without co-channel interference (collisions)
- Note: Wi-Fi uses single-user OFDM → single transmitter uses all subcarriers
  - Multiple access is simply random access (CSMA/CA)



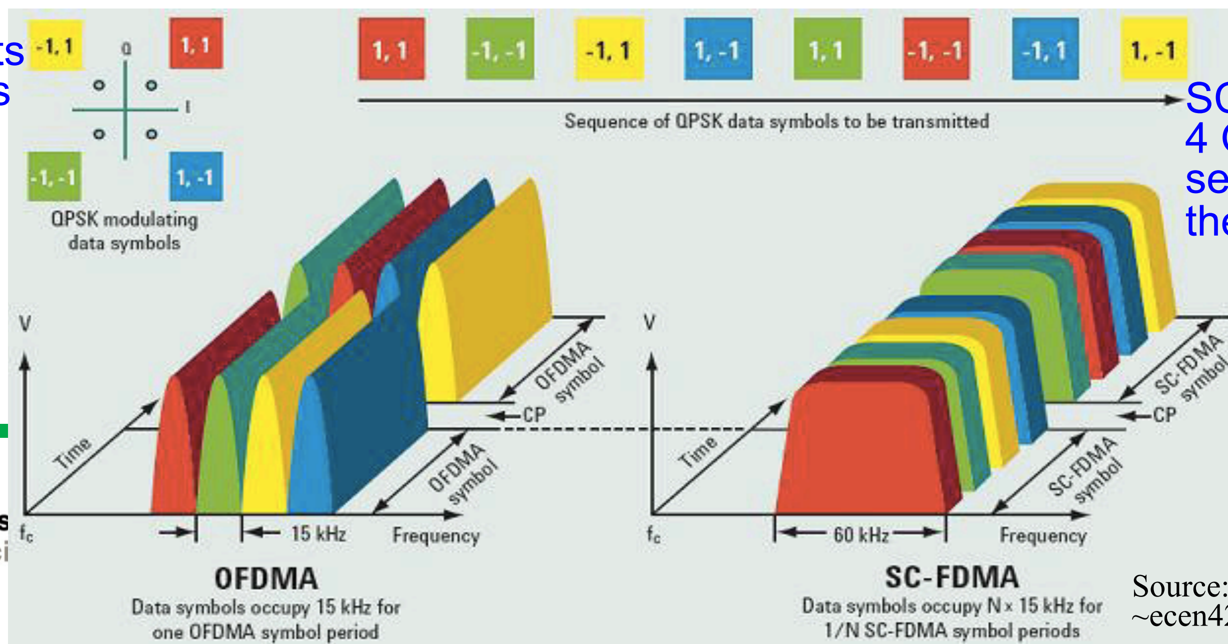
LTE uplink

- LTE uplink uses different radio access than downlink
- Single-Carrier FDMA (SC-FDMA) is used for cost and power efficiency
  – Transmitter design issues with OFDMA (peak-to-average power ratio)
- Using SC-FDMA somewhat complicates the scheduling
  – Cannot choose any set of resource blocks for single UE (should be consecutive or interleaved) as in OFDMA

SC-FDMA vs. OFDMA

- OFDMA: each subcarrier carries different group of bits
  - E.g. 64 QAM → each subcarrier carries 6 bits in one of the 64 possible symbols → 12 subcarriers will carry 12x6=72 bits for a duration of LTE Symbol (71.4 usec)
- SC-FDMA: whole group of 12 subcarriers modulated together as if they were a single carrier
  - E.g. 64 QAM → 12 subcarriers of the PRB (Physical Resource Block) will carry 1x6=6 bits but only for a duration of LTE Symbol divided by 12

OFDMA transmits 4 QPSK symbols in parallel (one per subcarrier)



SC-FDMA transmits 4 QPSK symbols in series at four times the rate

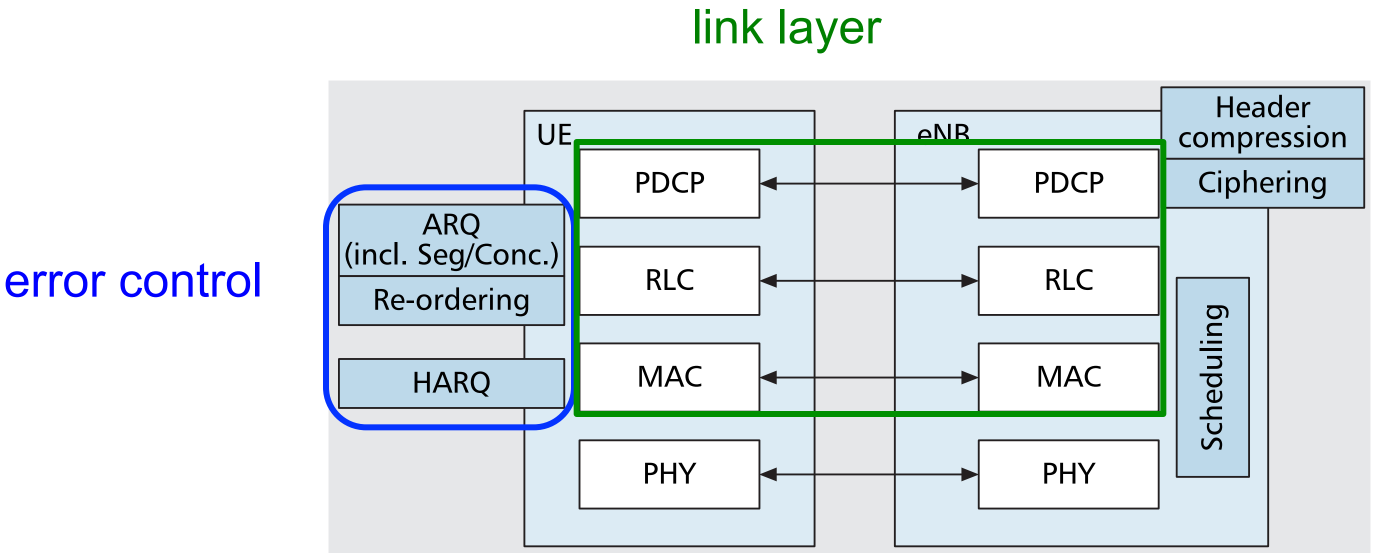
Source: http://ecee.colorado.edu/~ecen4242/LTE/radio.htm

LTE uplink and downlink

- Two versions of LTE exist: LTE TDD (TD-LTE) and LTE FDD (FDD-LTE)
- Difference lies in uplink and downlink multiplexing
  - No full duplex radios exist currently → must decide how to split whole channel between uplink and downlink
  - LTE FDD (frequency division duplex) uses paired frequencies to upload and download data
  - LTE TDD (time division duplex) uses a single frequency alternating between uploading and downloading data over time
- Different versions deployed in different parts of the world

LTE link layer

- We'll only take a brief look at some features of LTE's protocol stack



LTE error control

- Practically reliable transmission through two level error control
  - Both at MAC and RLC layers
- Hybrid Automatic Repeat Request (HARQ) is used at MAC layer
  - Combines forward error coding (FEC) and ARQ (error correction by retransmissions)
- HARQ uses multiple parallel stop-and-wait processes
  - Single bit ACK/NACK
  - Similar performance to window-based selective repeat but simpler to implement and less control overhead

LTE error control

- Single bit ACK/NACK scheme of HARQ causes false positive rate of about 10^{-4}-10^{-3}
  - Sender falsely interprets NACK as ACK
  - Missing packet eventually detected by receiving TCP → TCP sender retransmits it
  - Problem is that TCP sender may falsely conclude congestion and reduce rate unnecessarily
- Don't want to increase HARQ radio resource usage → second layer of error control at RLC
  - Sliding window based ARQ
  - Reordering detection required anyway in RLC because of multiple stop and wait processes by HARQ
  - ARQ reuses same sequence numbering → saves resources (compared to implementing at MAC layer)

Radio resource management

- Scheduling
  - Centralized control: eNodeB's responsibility in LTE
  - Decide how to allocate resources to UEs (both uplink and downlink)
    - Done per subframe level (i.e. each 1 ms) in LTE
    - UEs make Scheduling Requests to get uplink resources from eNodeB
  - Wi-Fi doesn't use centralized scheduling, only random access
    - RTS/CTS makes an exception
  - Scheduler is not standardized → manufacturers have developed proprietary schedulers
  - Typically use some form of proportional fair scheduling
    - Give resources to UEs in proportion to their link quality
    - Tradeoff between maximal system throughput and fairness per UE

Radio resource management (cont.)

- Link adaptation
  - Select modulation and coding scheme (MCS) and power allocation to schedule resources
  - Based on link quality reported by UE (downlink) and measured by eNodeB itself (uplink)
  - Goal is to optimize balance between data rate, bit error rate, and power usage (recall Wi-Fi lecture)
  - eNodeB can allocate different power to different subcarriers
- eNodeBs also perform Inter-Cell Interference Coordination (ICIC)
  - Optimization of resource usage between cells to curb the intercell interference

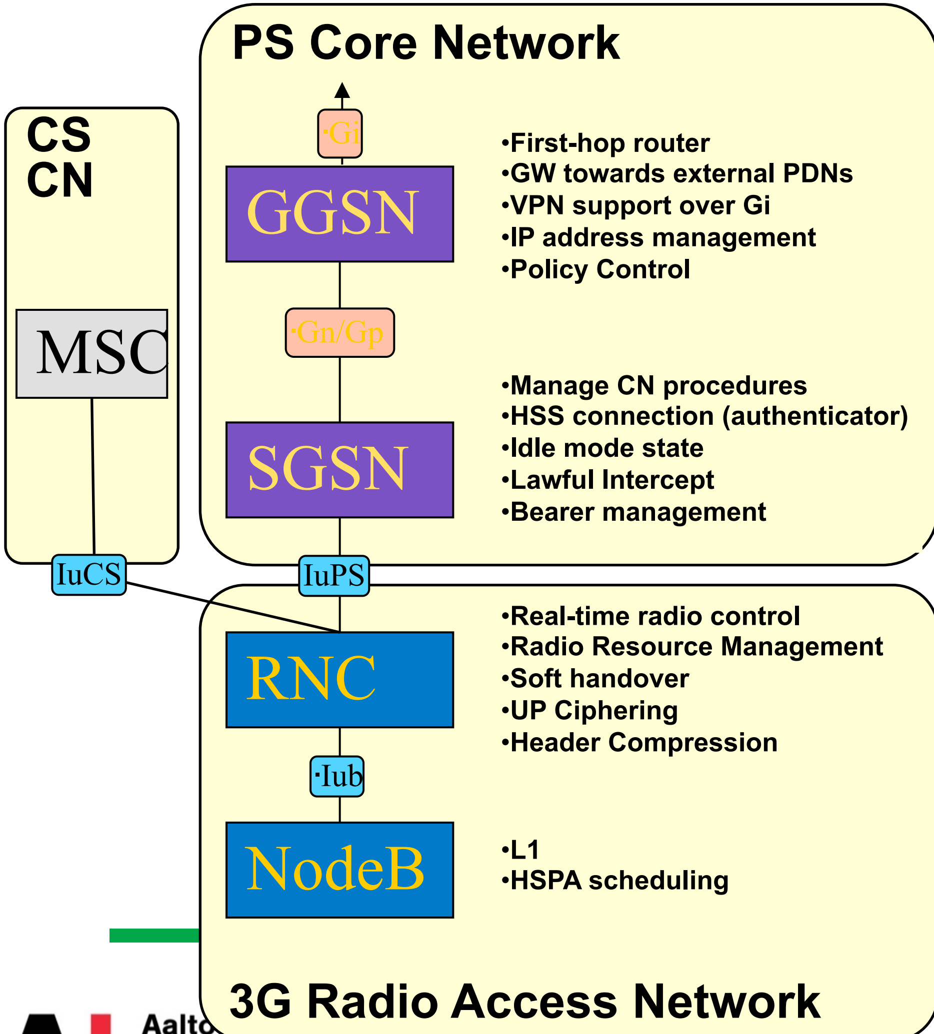
Radio resource management (cont.)

- MIMO configuration
  - Yet another dimension of resources managed by eNodeB
  - Spatial multiplexing: Different data streams are sent from different antennas → high data rate with high SINR
  - Diversity schemes: Exploit spatial diversity to improve SINR with it is poor
  - Beamforming: single symbol is multiplied by different weight factors and transmitted on different antenna elements → steer signal in receiver’s direction

Outline

- Overview of cellular networks
- Cellular network architecture
  - Overview
  - Radio Access Network (RAN)
  - → Packet core
- Mobility
- Application-level performance
- Summary

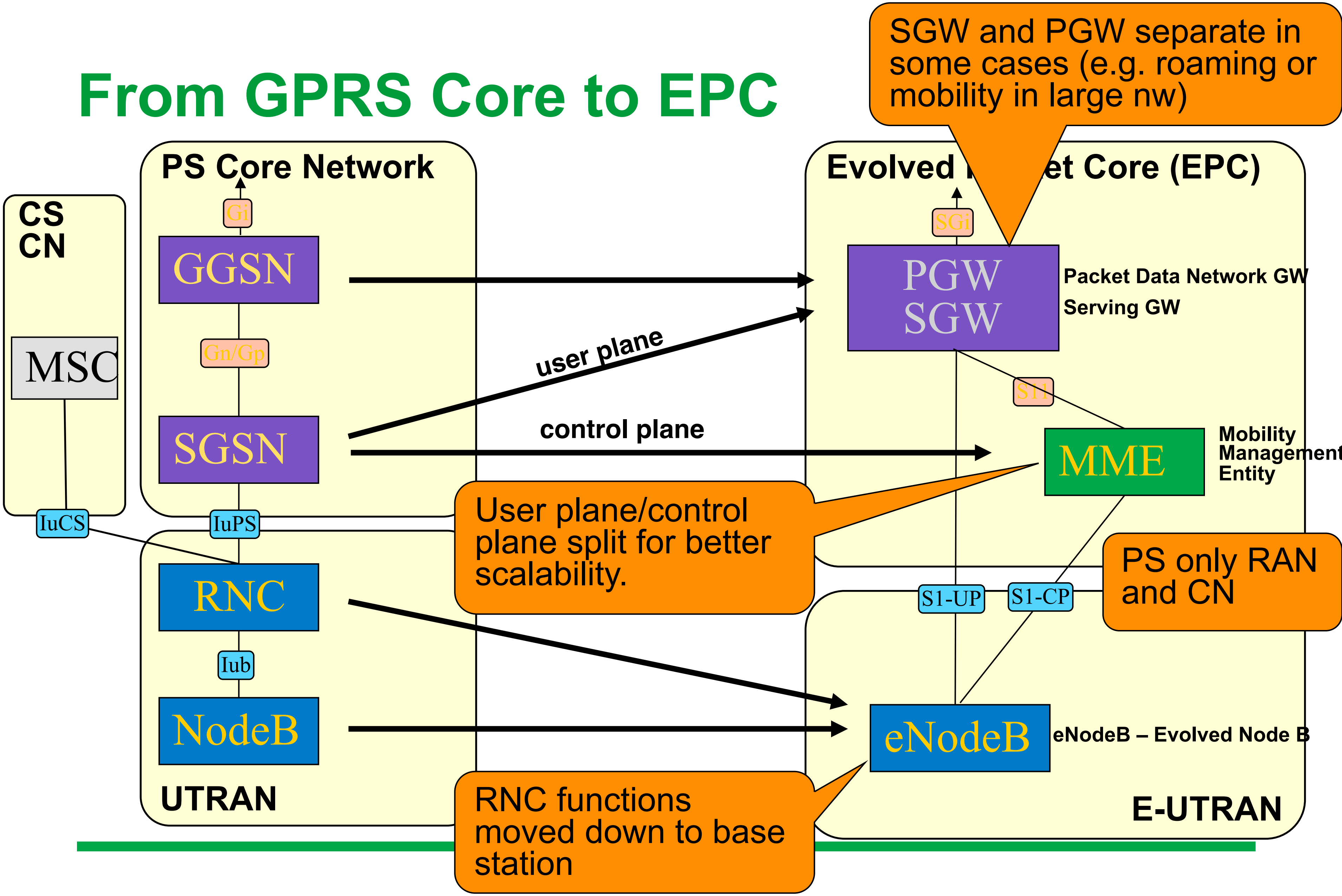
Pre-rel.8 Architecture



- Why separate RAN and CN?
  - Two CNs with same RAN
  - Multiple RANs with same CN
  - Modularization
  - Independent scaling, deployment and vendor selection

·GPRS – Generic Packet Radio Service
·GGSN – Gateway GPRS Support Node
·SGSN – Serving GPRS Support Node
·RNC – Radio Network Controller
·PDN – Packet Data Network
·CN – Core Network
·PS – Packet Switched
·CS – Circuit Switched
·MSC – Mobile Switching Center
·HSS – Home Subscriber Server

From GPRS Core to EPC



Evolved Packet Core

- PGW: Packet Data Network Gateway
  - Gateway to other IP networks (Internet but also e.g. IMS)
  - Maps incoming IP packets to correct bearers and forwards them
  - Performs accounting
- SGW: Serving Gateway
  - Manages user plane connections flowing through it
  - Switch packets to the correct elements in the network
- MME: Mobility Management Entity
  - Center of intelligence and control in the network (the only control plane element)
  - Tracks UE's location
  - Handovers: controls switch of the user plane path from SGW towards the new eNodeB
  - Authentication and authorization of UEs

Evolved Packet Core

- Home Subscriber Server (HSS) also exists
  - EPS equivalent of the Home Location Register (HLR) in legacy 3GPP networks
  - Holds subscribers' profile info such as allowed roaming areas
  - Tracks location of each UE with accuracy of an MME
  - Maintains master key for each subscription
    - All other security keys are derived from it
- Interworking with 3G core network is specified
  - Also with non-3GPP access networks
  - Anchor points during inter-system handovers: MME for signalling, SGW for user plane

Circuit switched (CS) fall back in LTE

- Most voice calls still handled through CS fall back
  - Use the good old solution from legacy 3GPP (GSM)
- LTE will eventually transition to all-IP
  - Voice calls as VoIP
  - VoLTE: Voice over LTE being deployed as we speak

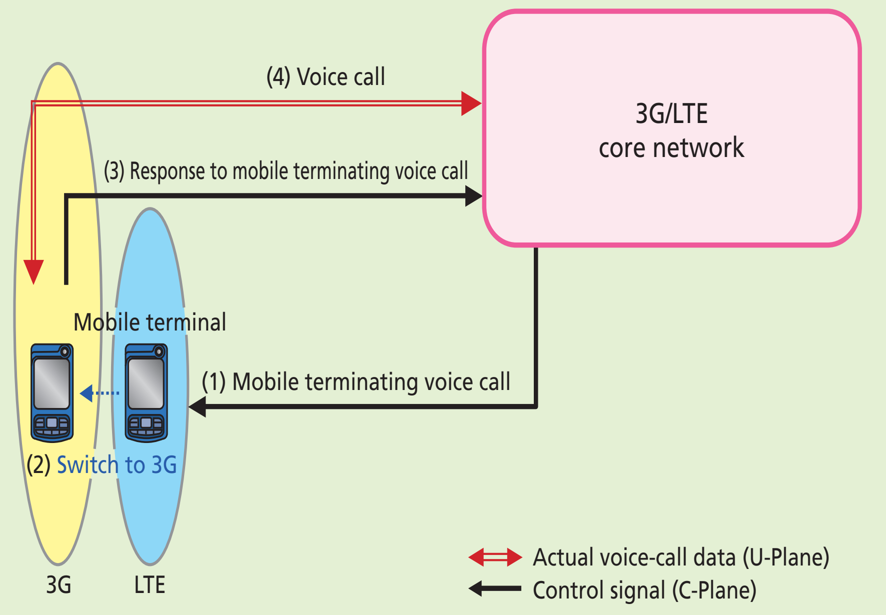


Figure 1 Overview of CS Fallback

Outline

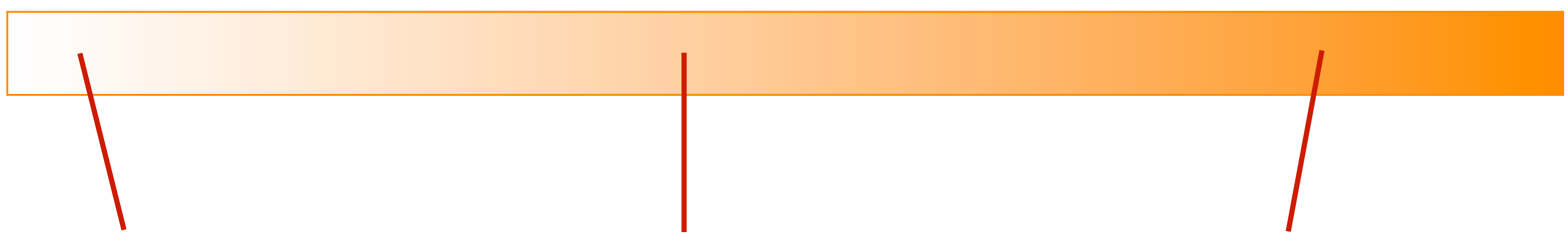
- Overview of cellular networks
- Cellular network architecture
- Mobility
- Application-level performance
- Summary

What is mobility?

- Spectrum of mobility, from the *network* perspective:

no mobility

high mobility



mobile wireless user, using same access point

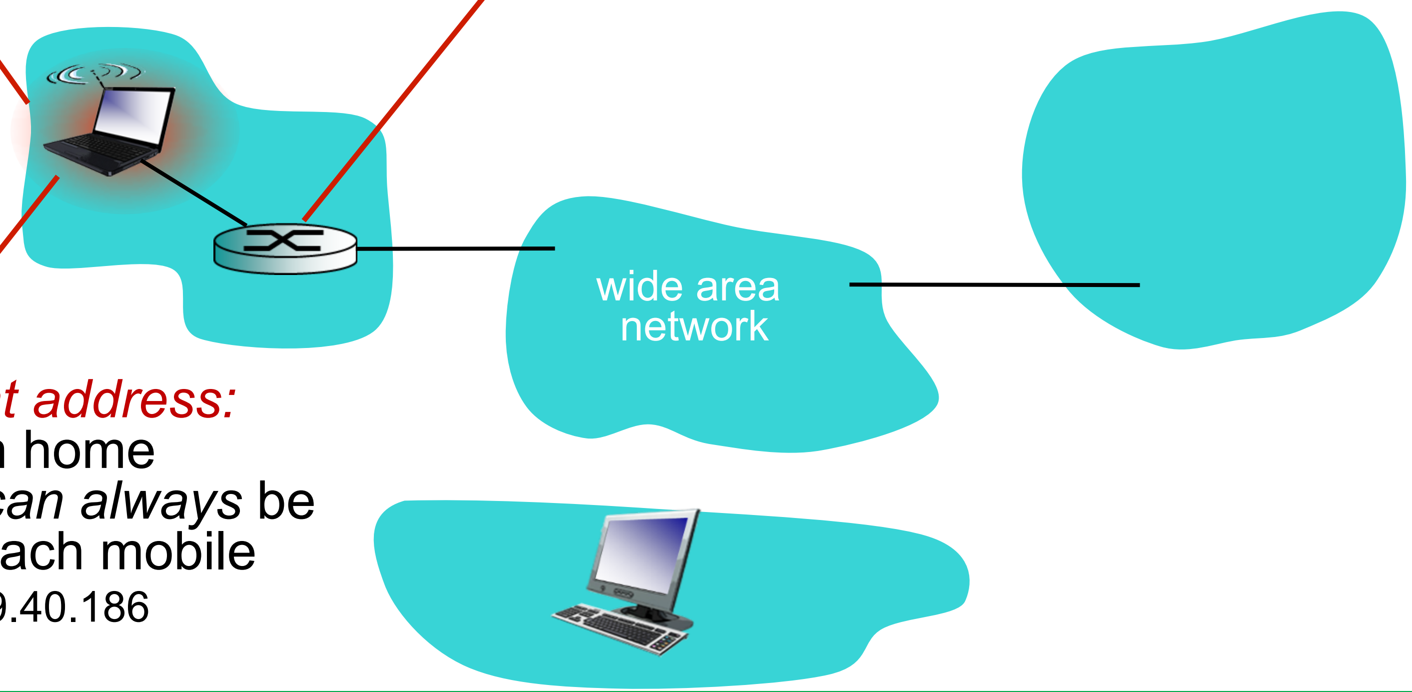
mobile user, connecting/ disconnecting from network using DHCP.

mobile user, passing through multiple access point while maintaining ongoing connections (like cell phone)

Mobility: vocabulary

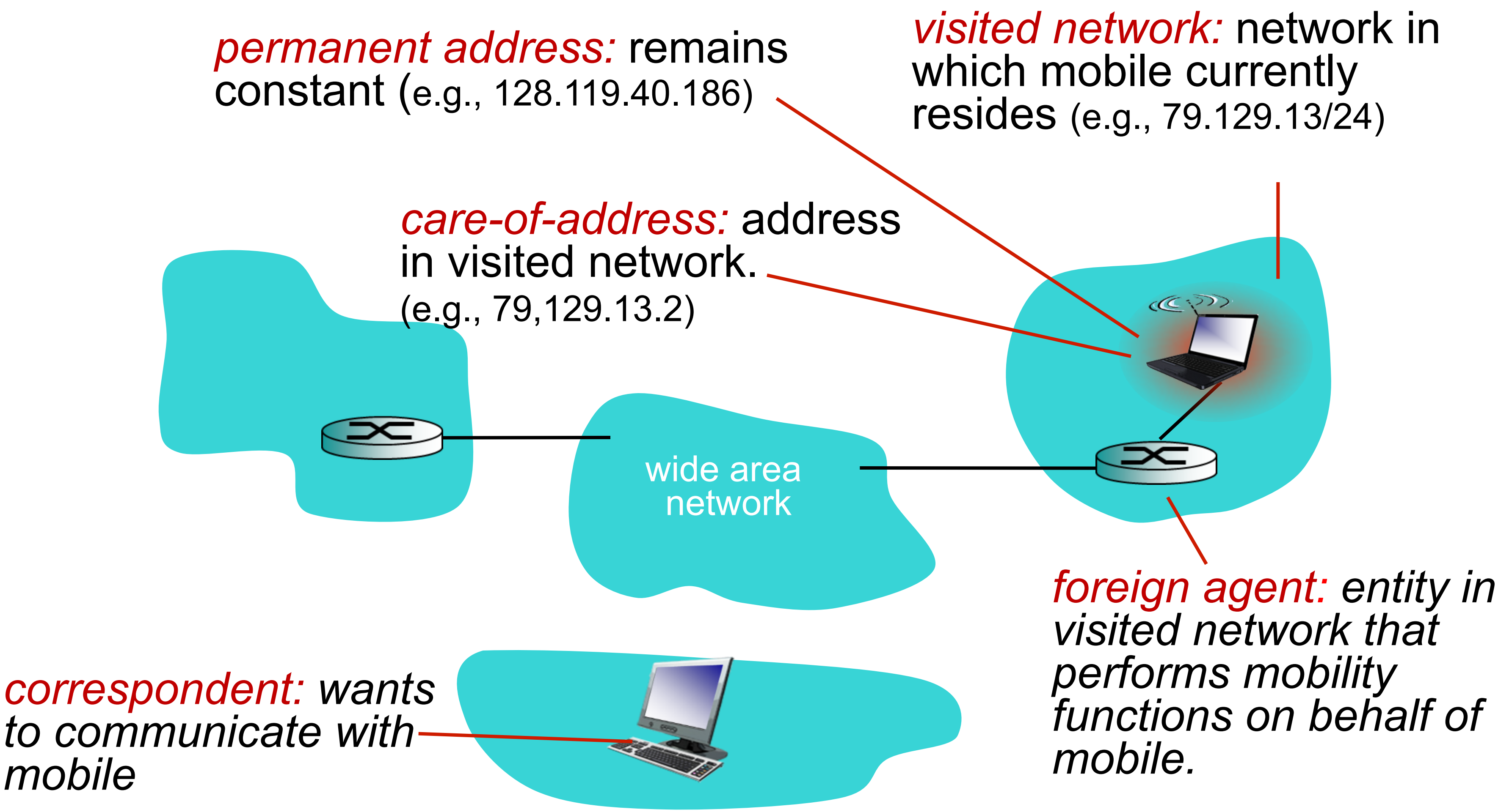
home network: permanent "home" of mobile
(e.g., 128.119.40/24)

home agent: entity that will perform mobility functions on behalf of mobile, when mobile is remote



permanent address:
address in home network, *can always* be used to reach mobile
e.g., 128.119.40.186

Mobility: more vocabulary



Approaches for mobility management

- let routing handle it
  - routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange
  - routing tables indicate where each mobile located
  - no changes to end-systems
- let end-systems handle it
  - *indirect routing*: communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing*: correspondent gets foreign address of mobile, sends directly to mobile

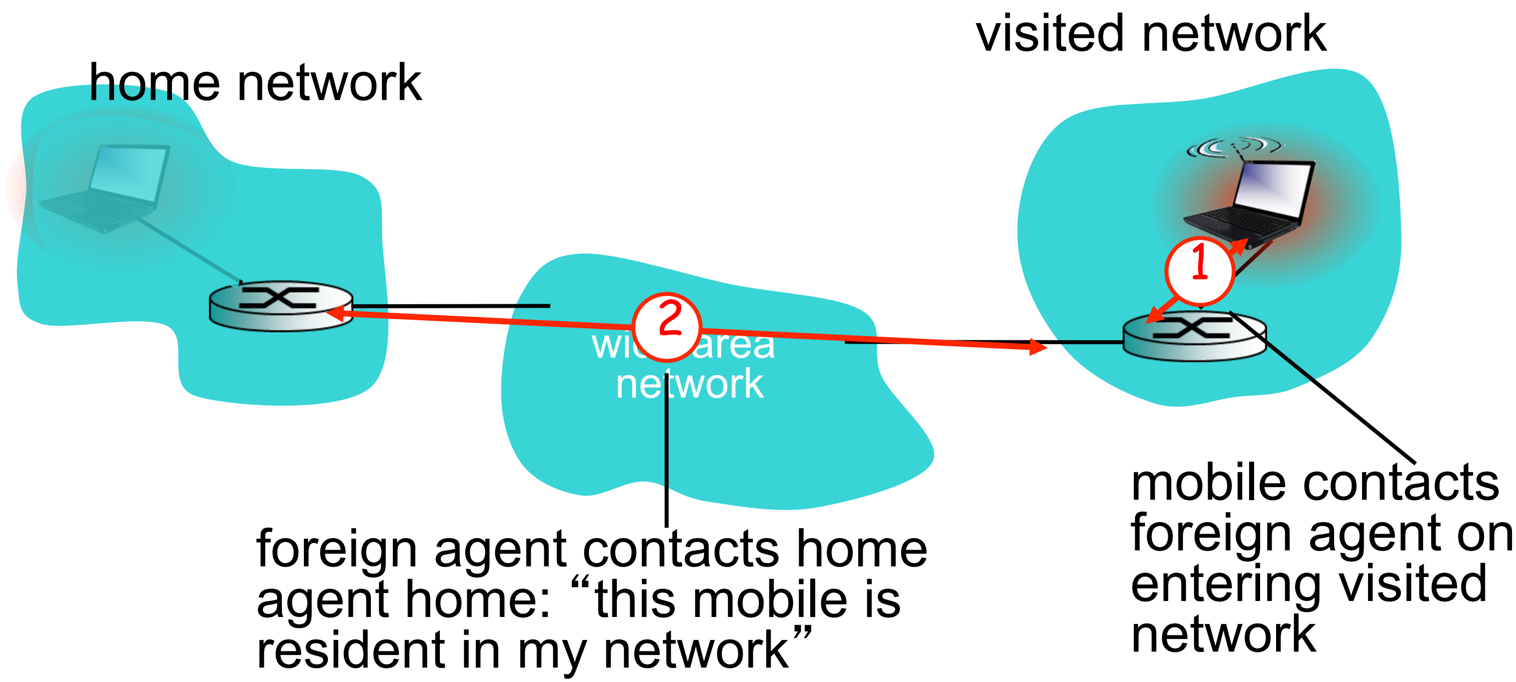
Approaches for mobility management

- let routing handle it
  - routers advertise … ress of mobile-nodes-in-residence via us … exchange.
  - routing tables inc … ch mobile located
  - no changes to end-…

not
scalable
to millions of
mobiles

- let end-systems handle it
  - *indirect routing*: communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing*: correspondent gets foreign address of mobile, sends directly to mobile

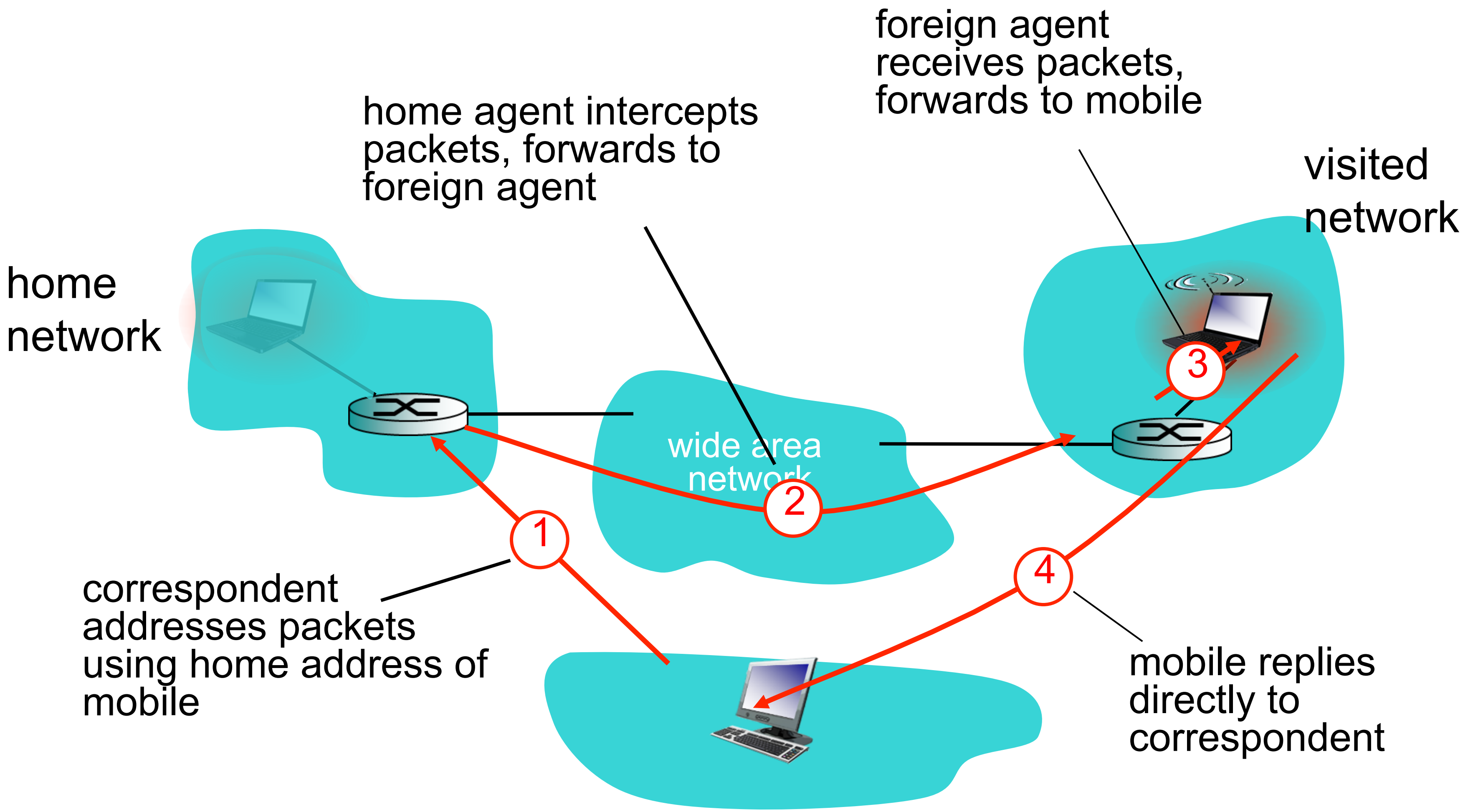
Mobility: registration



end result:

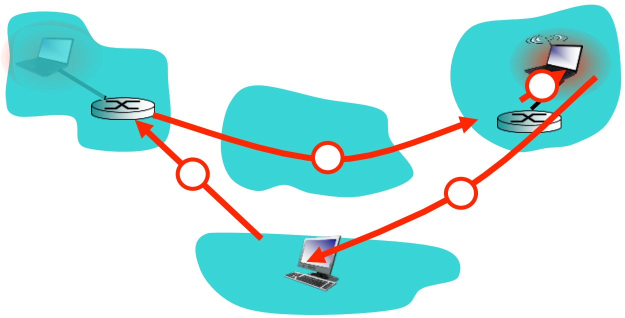
- foreign agent knows about mobile
- home agent knows location of mobile

Mobility via indirect routing



Indirect routing: comments

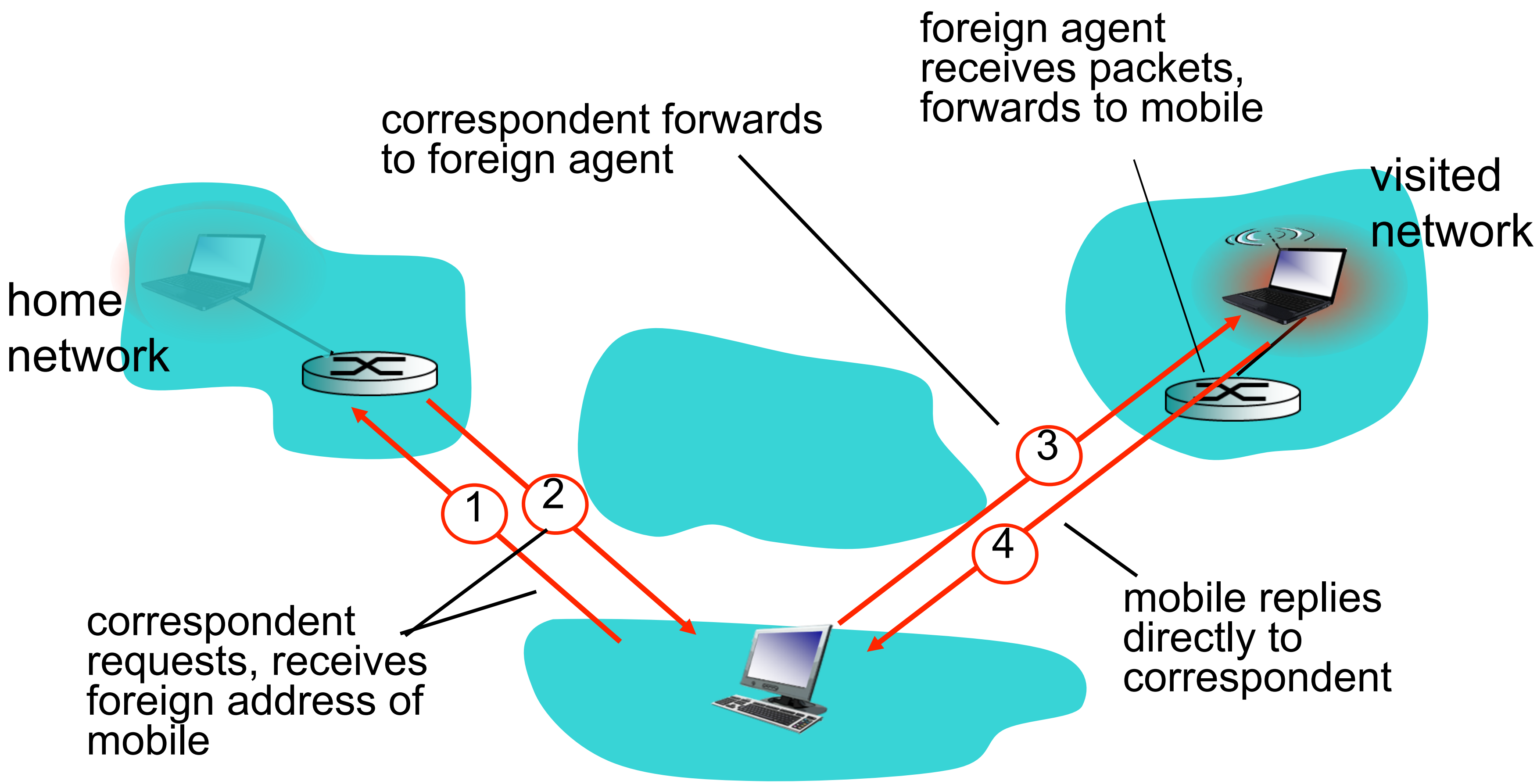
- mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- foreign agent functions may be done by mobile itself
- triangle routing: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network



Indirect routing: moving between networks

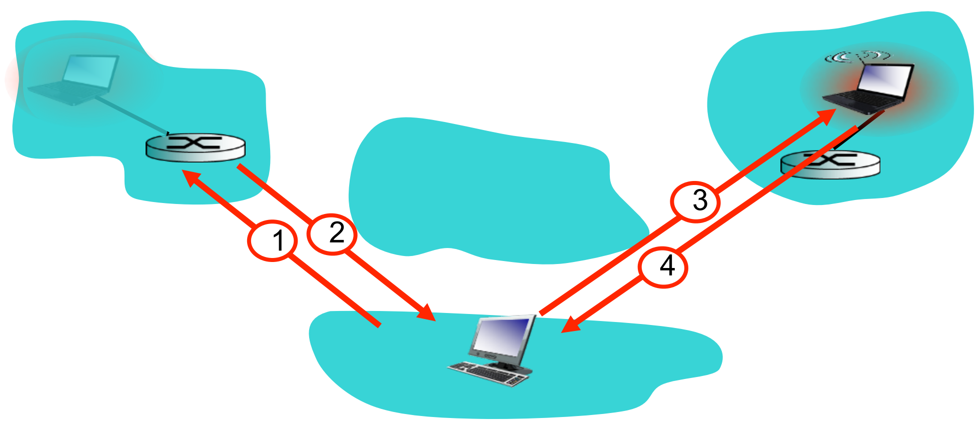
- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: on going connections can be maintained!

Mobility via direct routing



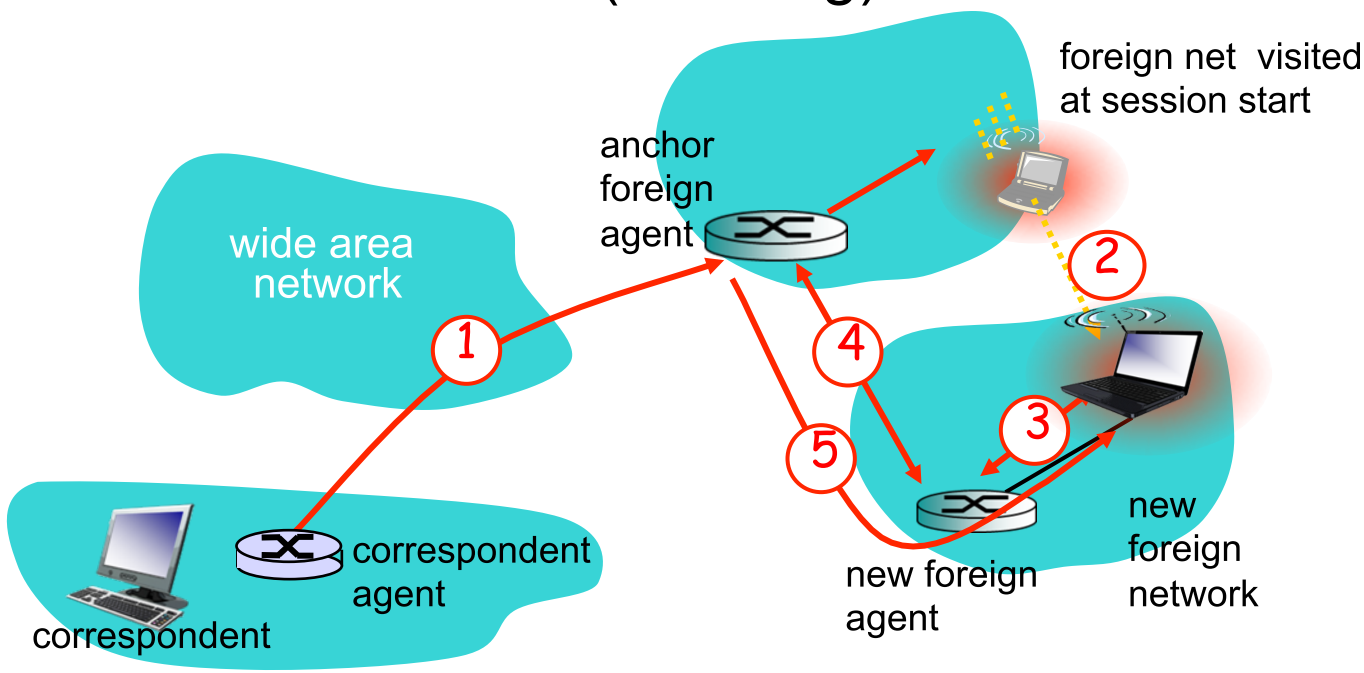
Mobility via direct routing: comments

- overcome triangle routing problem
- *non-transparent to correspondent:* correspondent must get care-of-address from home agent
  - what if mobile changes visited network?



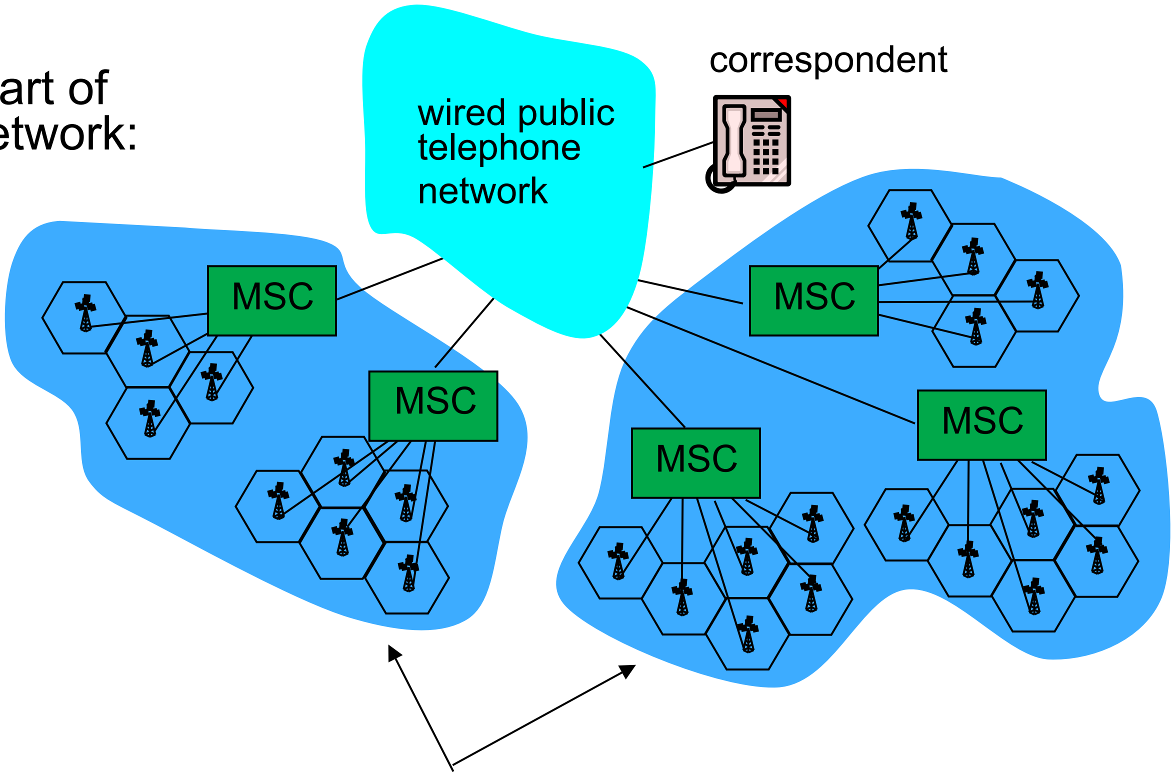
Accommodating mobility with direct routing

- anchor foreign agent: FA in first visited network
- data always routed first to anchor FA
- when mobile moves: new FA arranges to have data forwarded from old FA (chaining)



Handling mobility in cellular networks

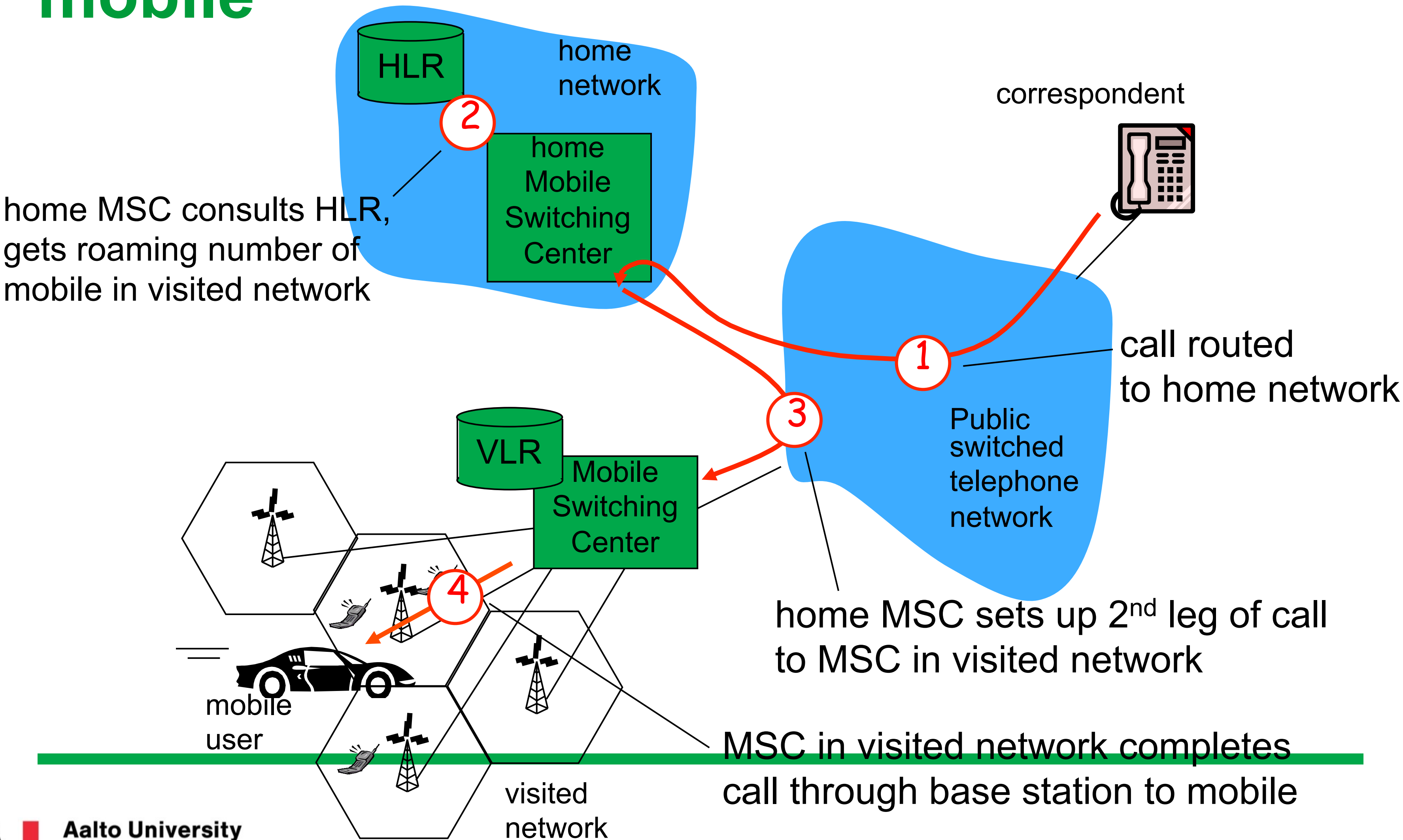
Recall the CS part of legacy 3GPP network:



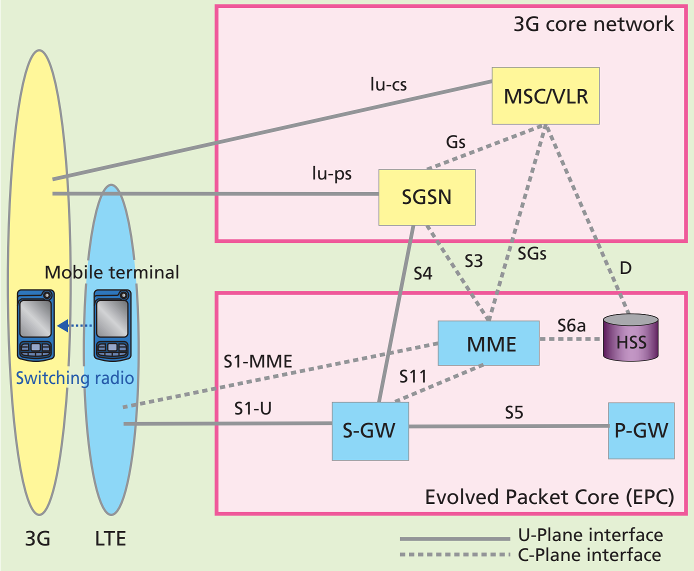
Handling mobility in cellular networks

- home network: network of cellular provider you subscribe to (e.g., Elisa, DNA)
  - *home location register (HLR):* database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)
- visited network: network in which mobile currently resides
  - *visitor location register (VLR):* database with entry for each user currently in network
  - could be home network

GSM (2G and 3G): indirect routing to mobile



LTE mobility management



- MME and HSS track UE location in LTE
  - MME does job of VLR (among other things)
  - HSS is the HLR equivalent in LTE
- Voice calls handled mainly through CS fallback
  - LTE EPC and legacy CS network need to collaborate
    - Combined mobility management
  - CS domain needs to know which LTE location area UE currently is
    - Needs to be able to send incoming CS call request to MME
    - EPC's MME must inform MSC/VLR that UE is present in location registration area

Handovers

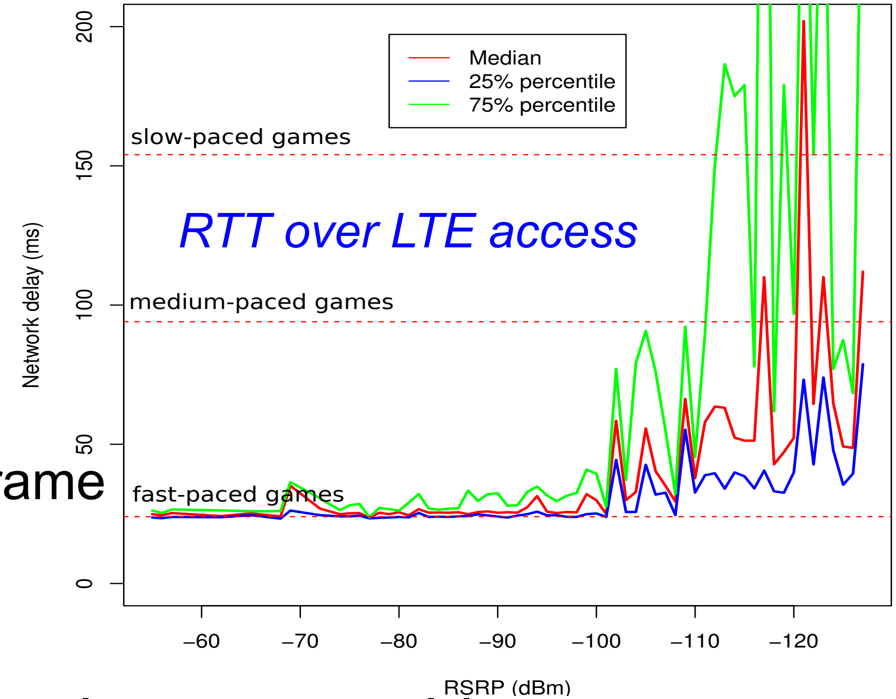
- Handovers are network controlled
  - eNodeB in LTE decides when to do it
  - RNC in legacy 3GPP
  - Note: client decides handovers in Wi-Fi
- UE assist network in decision making
  - UE measures link quality to nearby cells
  - UE sends measurement reports to network
- Handover types
  - legacy 3GPP has multiple types
    - Soft (make before break), softer, and hard (break before make)
  - LTE (currently) only supports hard handover

Outline

- Overview of cellular networks
- Cellular network architecture
- Mobility
- → Application-level performance
- Summary

Application-level performance: latency

- Latency shorter over LTE compared to 3G
  - LTE <50ms
  - 3G perhaps 50-100ms
  - Higher data rates and shorter frame size (1ms)

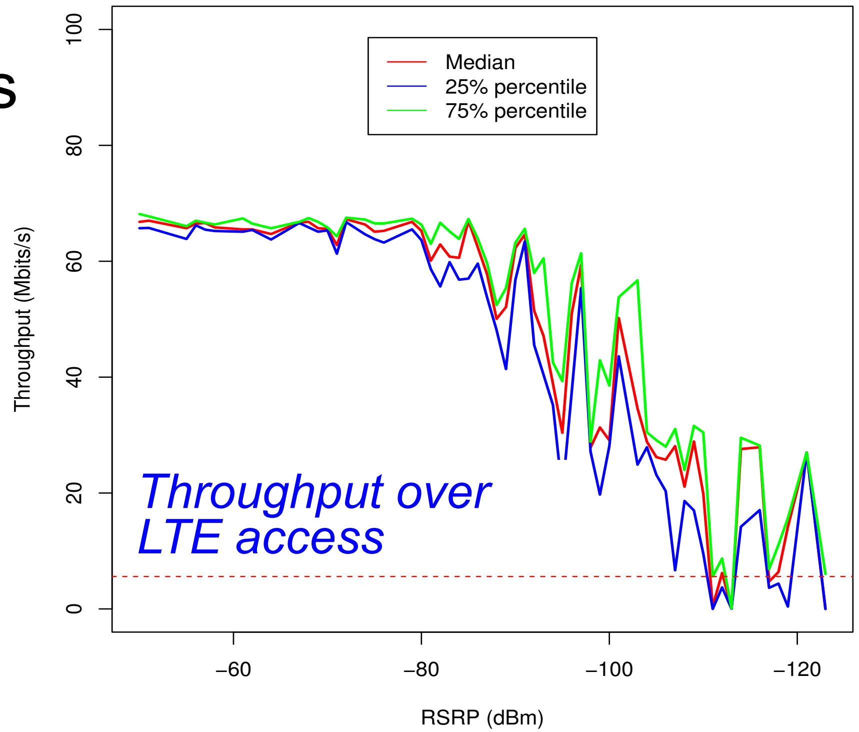


- End-to-end latency (RTT) depends on many things
  - Load in access network (radio and core)
  - Radio link quality
    - bit errors and retransmissions add to IP layer latency
  - Cross traffic in other networks besides the radio access network

Aalto University
School of Science

Application-level performance: throughput

- Data rates typically reported as peak rates
  - Assumes single user per cell/ sector and ideal link quality
- Peak rates depend on UE and network capabilities
  - LTE defines several categories (e.g. available MIMO configurations)



- Achieved throughput in practice may be far from peak rates
  - Same things cause reduced throughput than increased latency
  - In addition, bottleneck link may reside outside of mobile access nw

Aalto University
School of Science

Outline

- Overview of cellular networks
- Cellular network architecture
- Mobility
- Application-level performance
- Summary

Summary

- Mobile network usage is growing at an incredible pace
  - Technology tries to keep up
- Cellular networks are really complex systems
  - We just scratched the surface
- Architecture is split into RAN and core networks
  - UEs attach to RAN
  - Both parts have evolved over the generations
- Mobility management is integral part of cellular networks
  - Indirect routing of calls
  - Handover support
- Application-level performance is improving with each network generation
  - E2E performance depends on many things besides the air interface

Outlook

- The work towards 5G already started
  - Research in full steam
  - 5G Public-Private Partnership Association (5GPPP) formed
  - Standardization not yet started, expected around 2016-2019
- Industry targets: 1000x capacity, <1ms (RAN) latency by 2020
  - Very ambitious but theoretically possible…
- 5G will not be a single technology (s.a. 4G LTE)
  - Combination of evolved legacy technologies and new ones
  - More MIMO, small cell deployments (increase spectrum reuse)
  - Example of emerging technology: cm (3-30GHz) and mm wavelength (30-300GHz) radio access
    - Lots of unused spectrum available → much wider bandwidth → much higher datarates and shorter frame length (latency)

Next week: QoS/QoE

- What kind of quality of service Internet provides and how?
  - QoS mechanisms
- QoS vs. QoE?
  - Metrics
  - Application requirements
- Measuring and monitoring QoS/QoE
- Special focus on multimedia applications