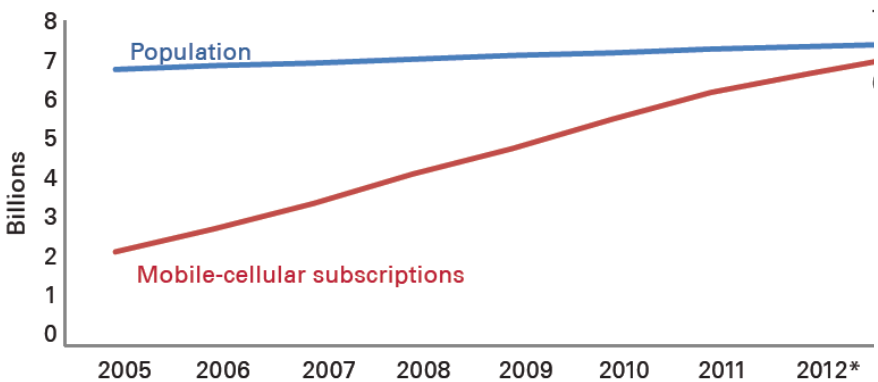
Wireless and Mobile Networks

Guest lecture by: Roger Piqueras Jover (AT&T Security R&D)

October 16th, 2014

Wireless and Mobile Networks



Source: ITU World Telecommunication /ICT Indicators database
Note: * Estimate

NUMBER OF MOBILE PHONES TO EXCEED WORLD POPULATION BY 2014

By **Joshua Pramis** — February 28, 2013

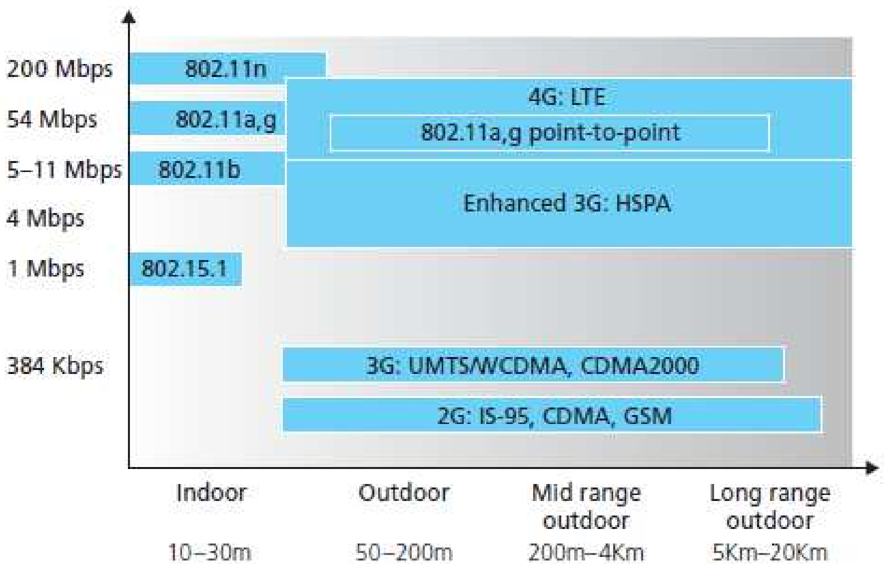
Lecture overview

- Overview and introduction to:
  - Wireless communications and wireless channel
  - Multiple access methods
    - TDMA, FDMA, CDMA, OFDMA
    - Contention-based methods
  - Cellular communications
  - Mobile networks
    - GSM, 3G (UMTS), “4G” (HSPA) and LTE

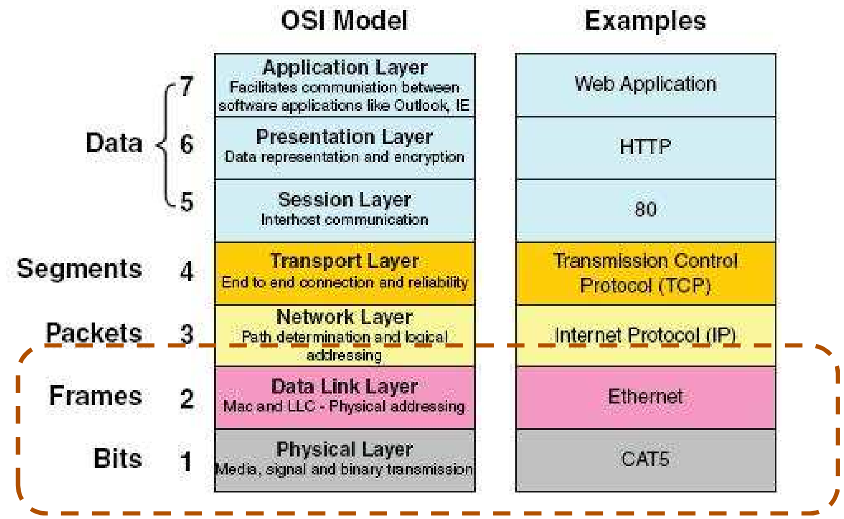
- I will be suggesting some readings and leaving some unanswered questions

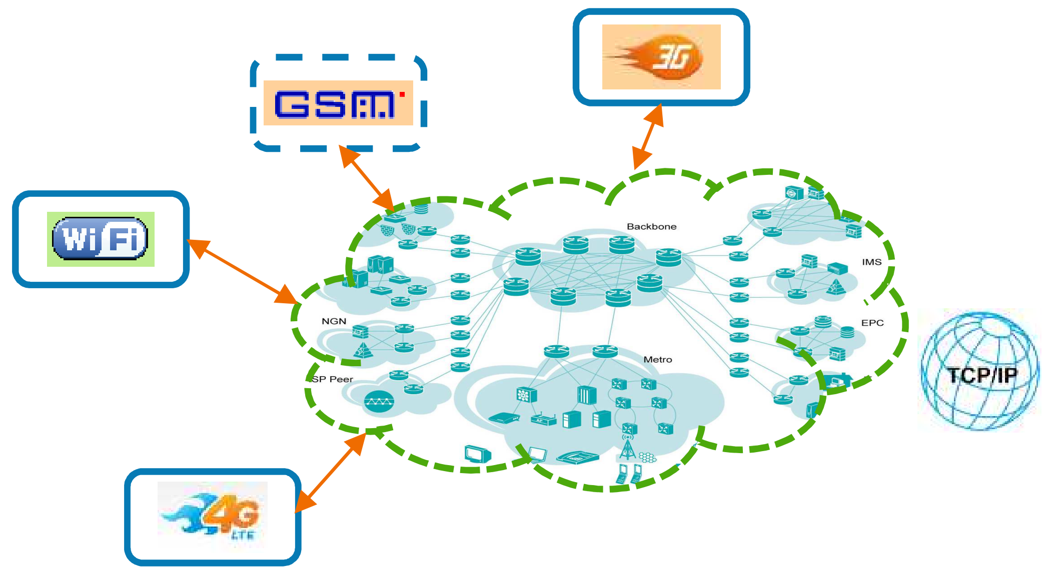
Lecture overview

- We will be focusing mostly on wireless access
  - Cellular, 802.11 and WiFi
  - PHY and MAC layers



From: Computer Networking – A top down approach. James Kurose, Keith Ross. Pearson.





Basics on wireless propagation and wireless channel

Wireless signal propagation

- Coverage area defined by
  - Propagation loss
  - Large scale fading (shadowing)
- Link/channel quality (error probability) defined by:
  - Small scale (fast) fading, multipath, etc

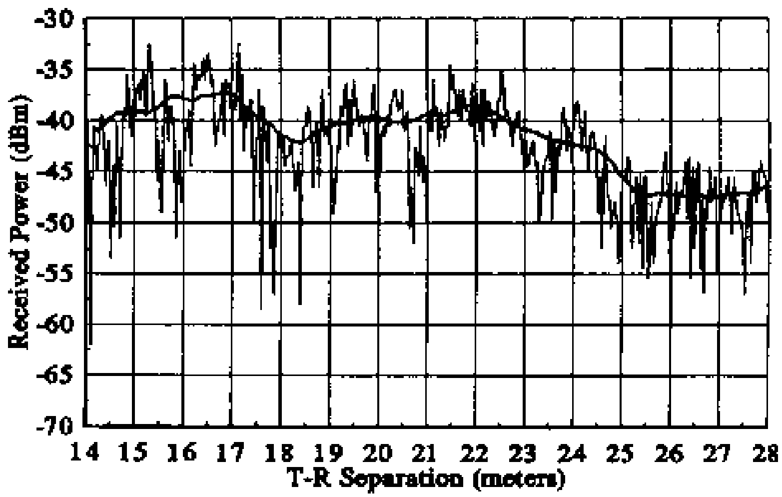


Figure 4.1 Small-scale and large-scale fading.

From: Wireless Communications: Principles and Practice (2nd Edition). Theodore Rappaport. Prentice Hall.

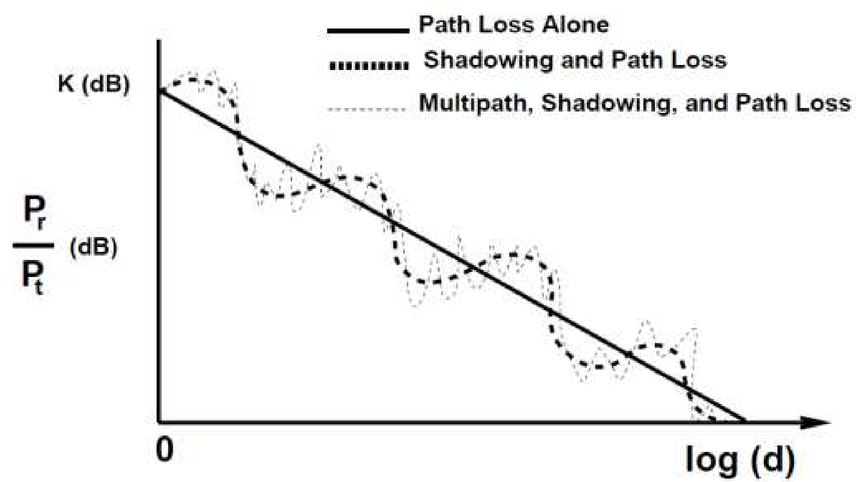


Figure 2.1: Path Loss, Shadowing and Multipath versus Distance.

From: Wireless Communications. Andrea Goldsmith. Cambridge University Press.

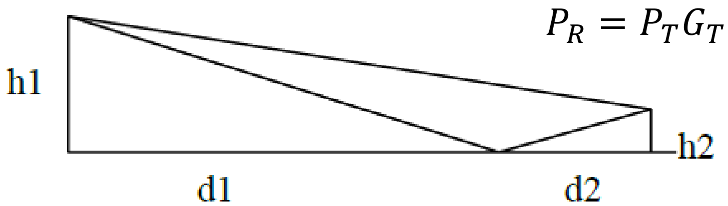
Propagation loss

- The power of a wireless signal decays proportionally to $1/d^{\alpha}$ (**path loss**)
  - α is the path-loss exponent
  - Different values of α for different environments
- Basic mathematical path loss models
  - Free-space

$$P_R = P_T G_T G_R \left(\frac{\lambda}{4\pi d} \right)^2$$

  - 2-ray ground bounce model

$$P_R = P_T G_T G_R \left(\frac{h_1 h_2}{d^2} \right)^2$$



- Empirical models (based on measurements)
  - Okomura-Hata, COST-231, etc
  - 5G mmWave path-loss models [1]

Table 4.2 Path Loss Exponents for Different Environments

Environment	Path Loss Exponent, *n*
Free space	2
Urban area cellular radio	2.7 to 3.5
Shadowed urban cellular radio	3 to 5
In building line-of-sight	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in factories	2 to 3

From: Wireless Communications: Principles and Practice (2nd Edition). Theodore Rappaport. Prentice Hall.

Large scale fading (shadow fading)

- As users move, their reception/transmission is obstructed by obstacles
  - Buildings, trees, vehicles, etc
- The duration of the fade is in the order of seconds
  - Time it takes to clear the obstacle
  - T=d/V=10 seconds, with d=100m and V=10m/s
- Shadowing modeled by a log-normal distribution

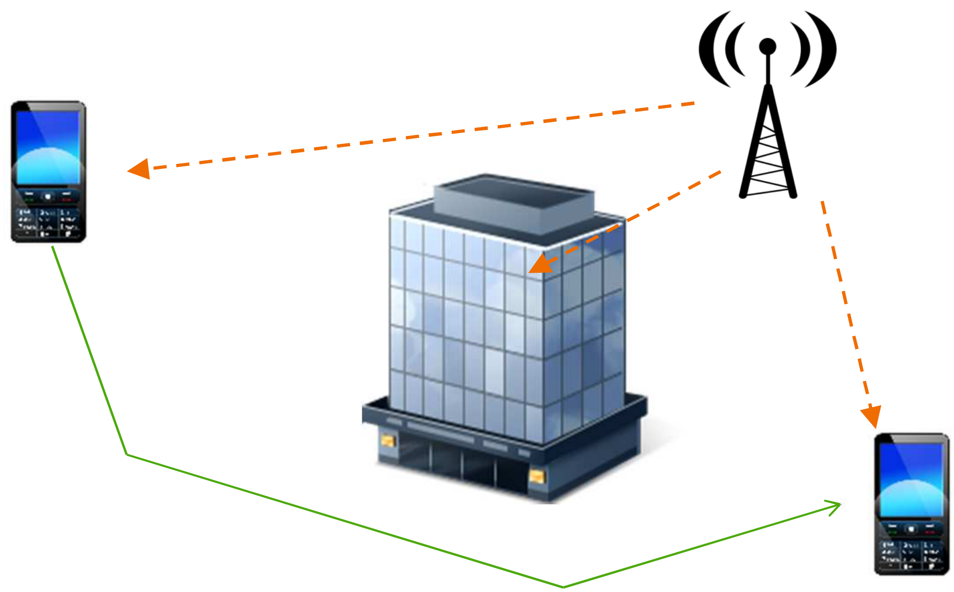
$$f(P) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(P-P_R)^2}{2\sigma^2}}$$

P: received power

P_R: average received power (path-loss)

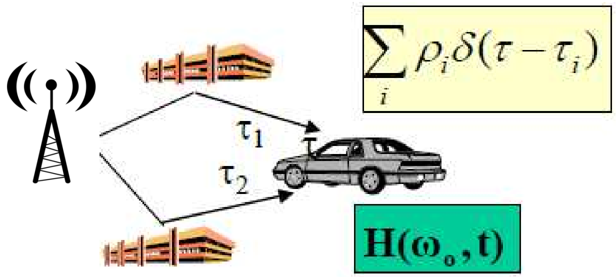
σ: shadowing coefficient

(The equation in in dBs)



Fast fading

- The received signal is a combination of multiple rays (multipath + scattering)



(Received signal)

$$\sum_i \rho_i \delta(\tau - \tau_i) \leftrightarrow H(w_0, t) = \sum_i \rho_i \exp(-j\frac{2\pi}{\lambda} c\tau_i) = \sum_i \rho_i \exp(-j\frac{2\pi}{\lambda}\Delta_i)$$

$\tau_i = \tau_i(t)$ $\quad \Delta_i$: Distance traveled by ray i

If Δ_i changes by fractions of λ the amplitude of r(t) can change substantially

- There is an infinite number of reflections (scattering)

$$H(\omega_O, t) = \mathrm{Re}\{H(\bullet)\} + j\,\mathrm{Im}\{H(\bullet)\} = x(t) + jy(t)$$

$$r(t) = |r(t)| \cos(\omega_o t + \phi(t))$$

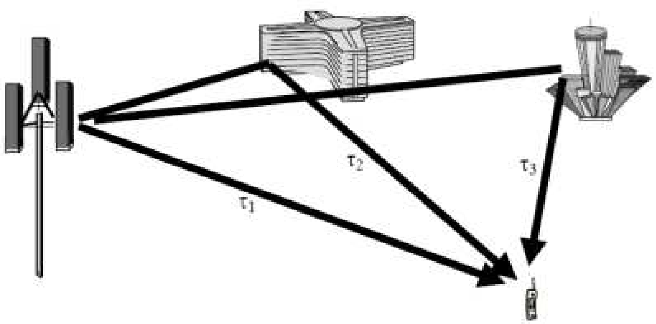
- $|r(t)|$ has Rayleigh (or Ricean) distribution
  - Fast fading

$$f_r(r) = \frac{r}{\sigma^2} e^{-r^2/2\sigma^2}$$

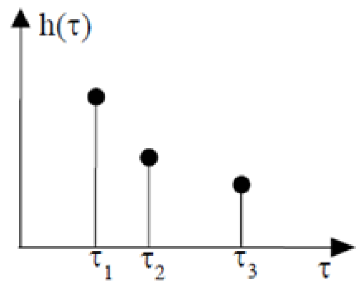
- $\varphi(t)$ has a uniform disribution
  - Phase and frequency variation

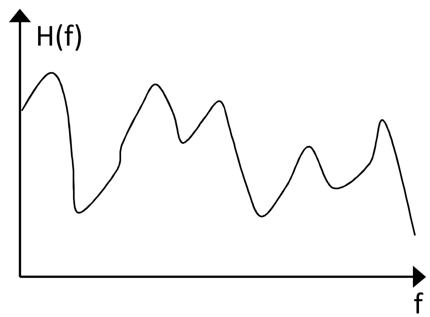
Multipath

- Multipath results in a frequency selective channel
  - Different fading attenuations at different frequencies
  - The frequency response of the channel is not flat

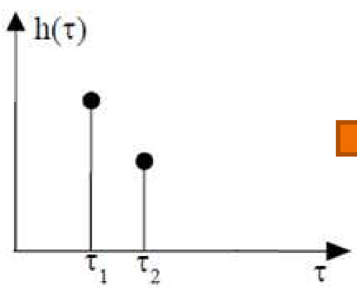


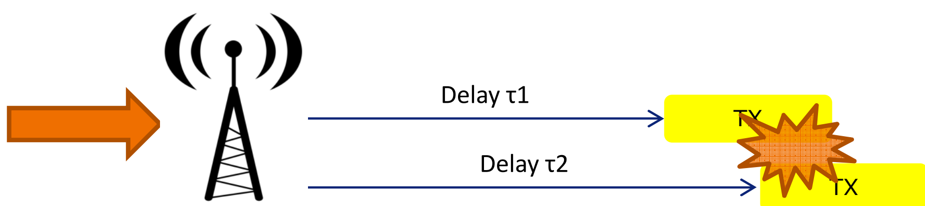
$$h(\tau) = \beta_1\delta(\tau - \tau_1) + \beta_2\delta(\tau - \tau_2) + \beta_3\delta(\tau - \tau_3)$$





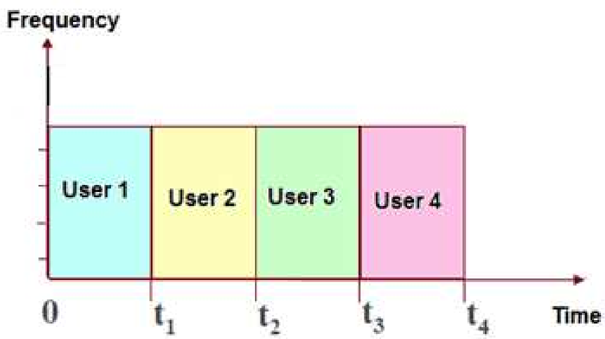
- Frequency selective channel results in signal distortion
  - Inter-symbol interference (ICI)



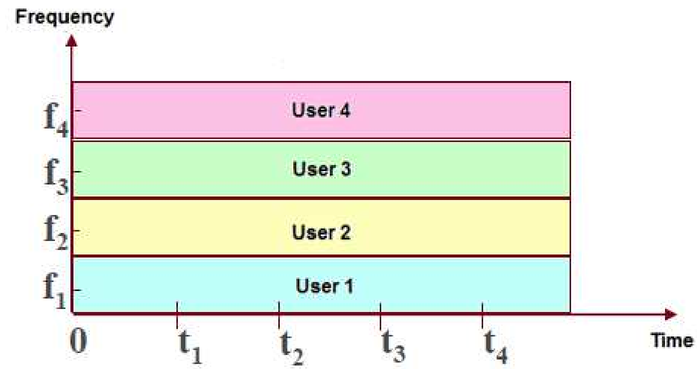


Multiple access methods

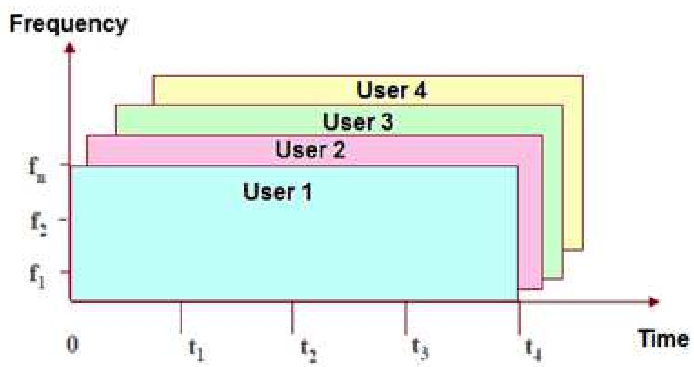
Multiple access methods



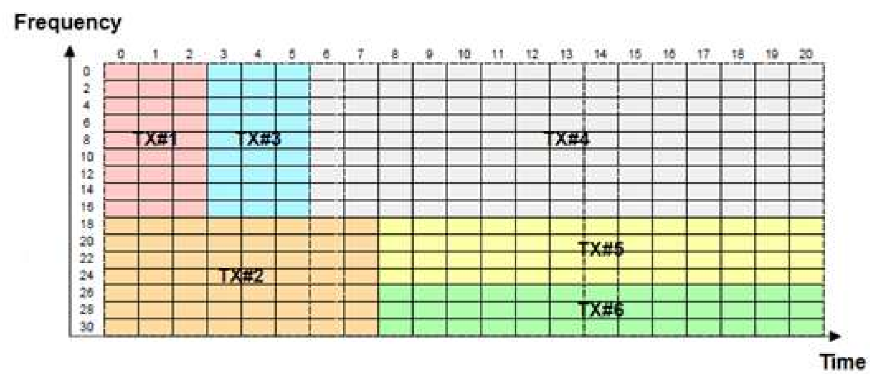
TDMA (GSM)



FDMA (AMPS)



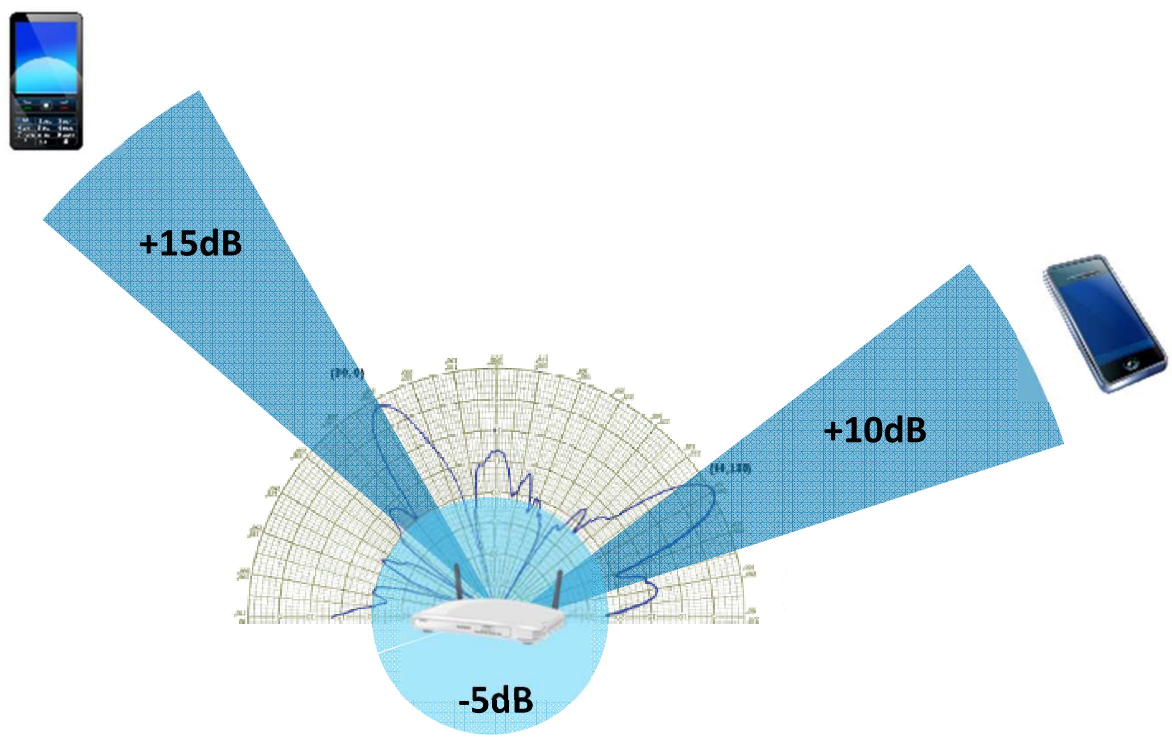
CDMA (3G - UMTS)



OFDMA (LTE)

Next-Gen multiple access methods – Spatial Division

- Multi-antenna (MIMO) arrays and beamforming
  - Transmit and receive to/from specific directions
  - Separate users spatially
- Theoretically feasible in 5G
  - mmWave
  - Massive MIMO arrays

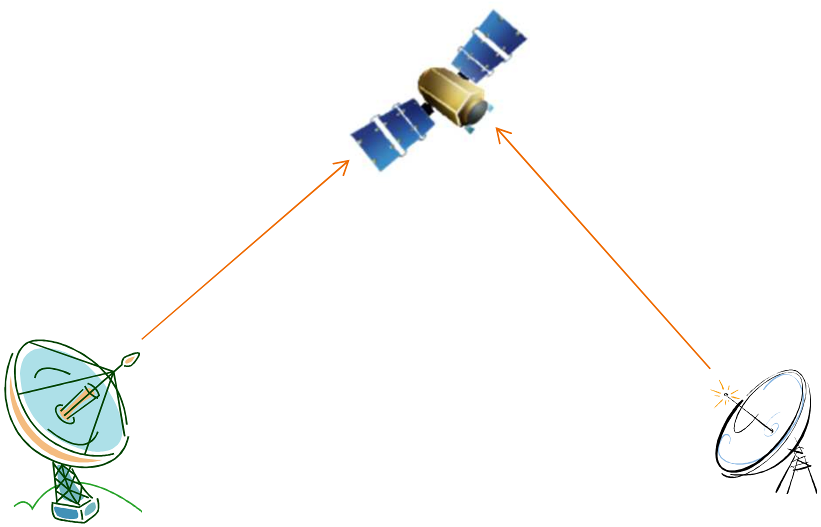


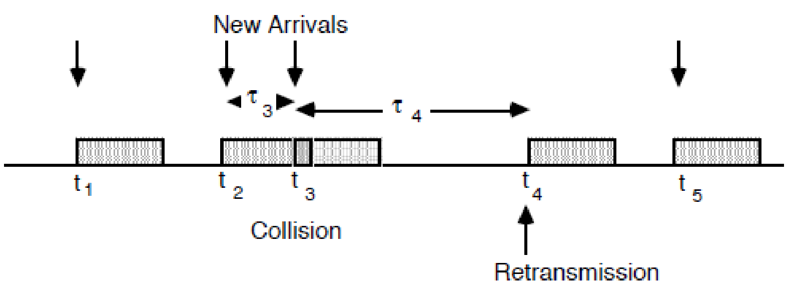
- Suggested reading [4]

Contention-based methods

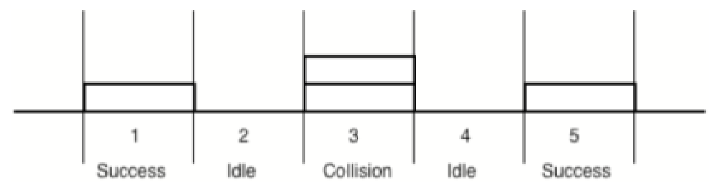
- All the users share the same medium (channel)
  - Collisions are possible
  - Different methods to detect, avoid and minimize collisions
- Examples
  - ALOHA and S-ALOHA
  - CSMA
  - Ethernet
  - 802.11

ALOHA and Slotted ALOHA

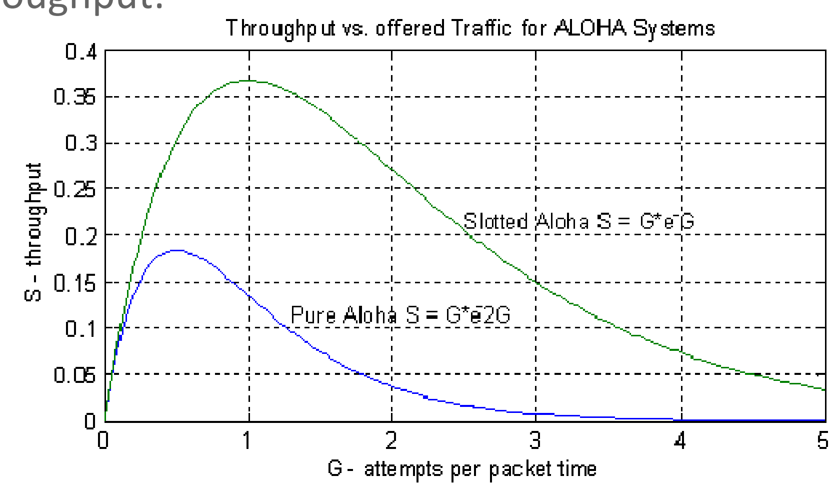




- Transmission from two or more nodes may collide
- No ACK received → Collision
  - Backoff for a random time
  - Try again
- S-ALOHA forces transmissions in pre-defined time “slots”



- Throughput:



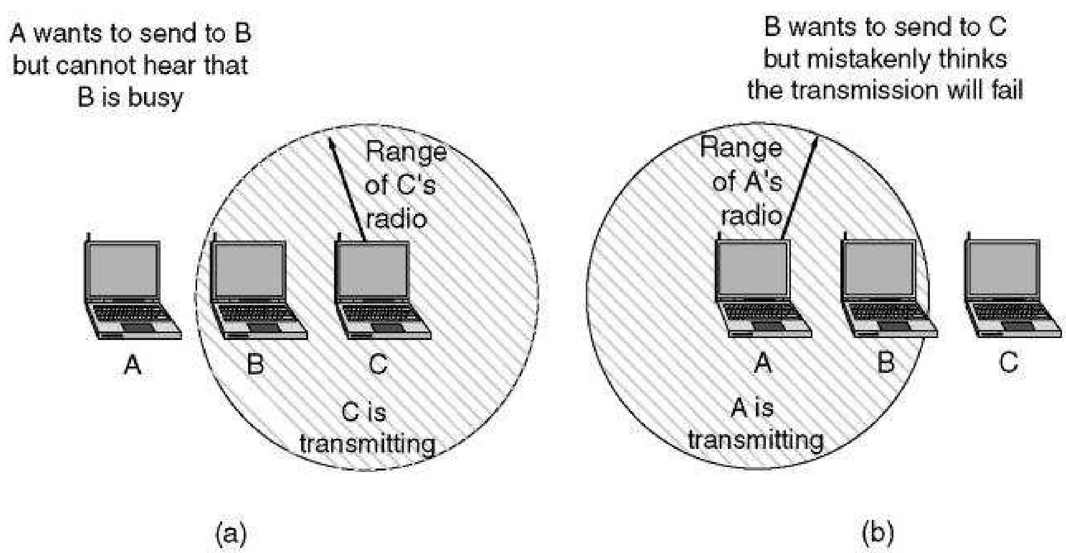
802.11

- IEEE 802.11 is the most pervasive technology for wireless LAN
- 2 different modes
  - Infrastructure (with AP)
  - Independent
- Based om CSMA-CA (Collision Sensing Multiple Access w Collision Avoidance)

- 802.11n
  - 2.4/5.0 GHz bands
  - OFDM modulation
  - MIMO
  - Up to hundreds of Mbps

802.11 – The hidden terminal and exposed terminal problems

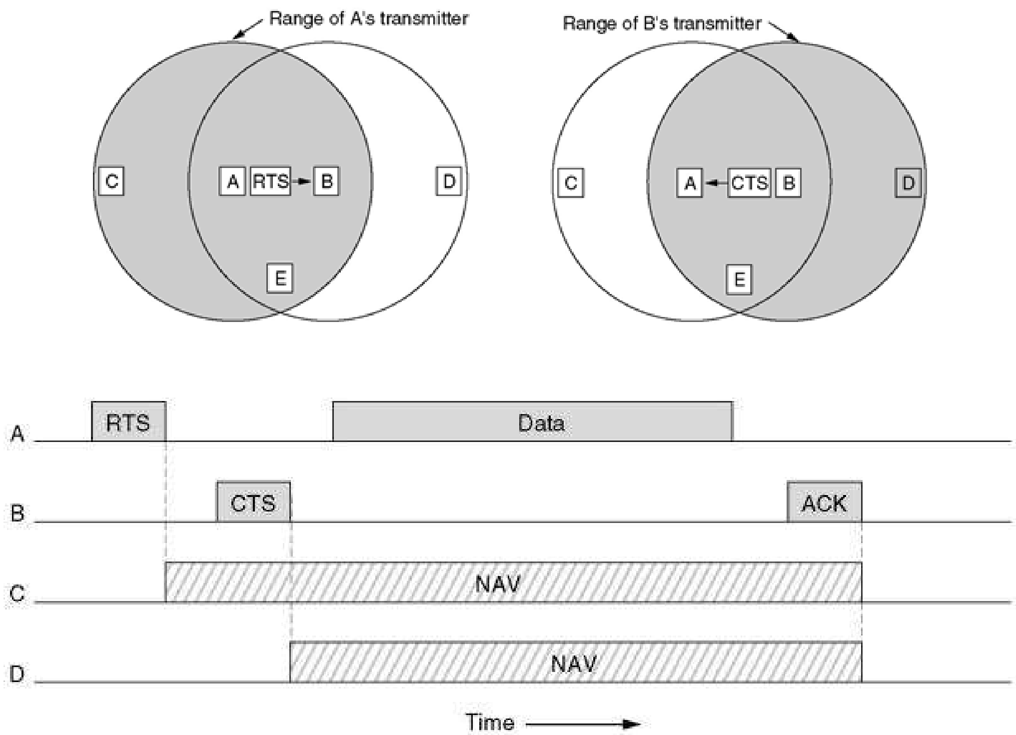
- Limited communication range of 802.11 nodes results in
  - Hidden terminal
  - Exposed terminal



(a) Hidden station problem. (b) Exposed station problem.

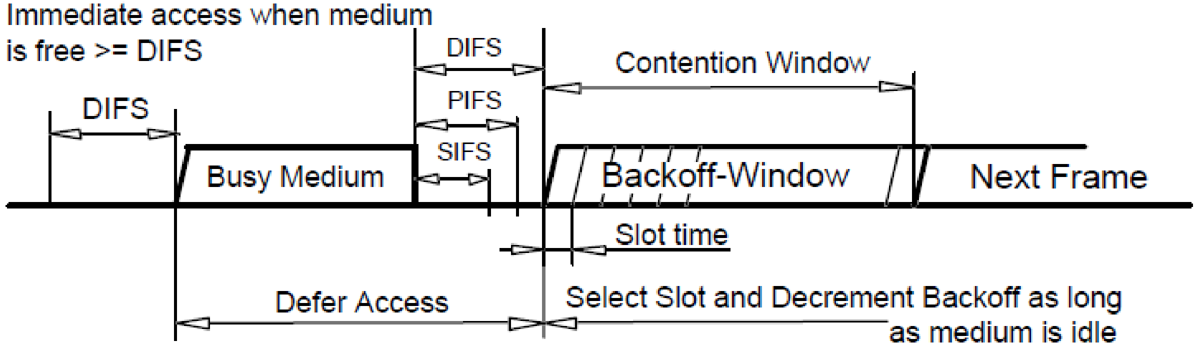
802.11 – The hidden terminal and exposed terminal problems

- Solution → RTS/CTS messages
  - RTS (Ready to Send) – Message sent to alert terminals within your coverage area that you are about to transmit
  - CTS (Clear to Send) – The receiving terminal ACKs you and alerts all terminals in its coverage area that it is about to start receiving



802.11 – Medium Access Control (MAC)

- The basic parameters are
  - Slot time – Basic unit of time for transmission and backoff delay
  - Short Inter-Frame Space (SIFS) – Time required to sense end of another transmission and transmit control frame
  - DCF Inter-Frame Space (DIFS) – Time to wait before starting to contend (SIFS + 2 slot times)
- Medium free for t=DIFS?
  - Yes – Start transmission
  - No – Start backoff
    - Wait for medium to be busy t=DIFS
    - Select random number k ~unif[1,CW] (CW: contention window size)
    - Wait for k slots (must be idle) and then transmit
    - If collision or busy medium again, increase CW and restart.



802.11 – MAC cheating

- The drivers and controllers for 802.11 cards are open source
  - **Food for thought**: What would happen if a user configured CW always to be 1?
- Suggested reading: Selfish MAC layer misbehavior in wireless networks [6].

802.11 – MAC + RTS/CTS

Food for thought: Why do we use SIFS instead of DIFS before ACKs and CTSs?

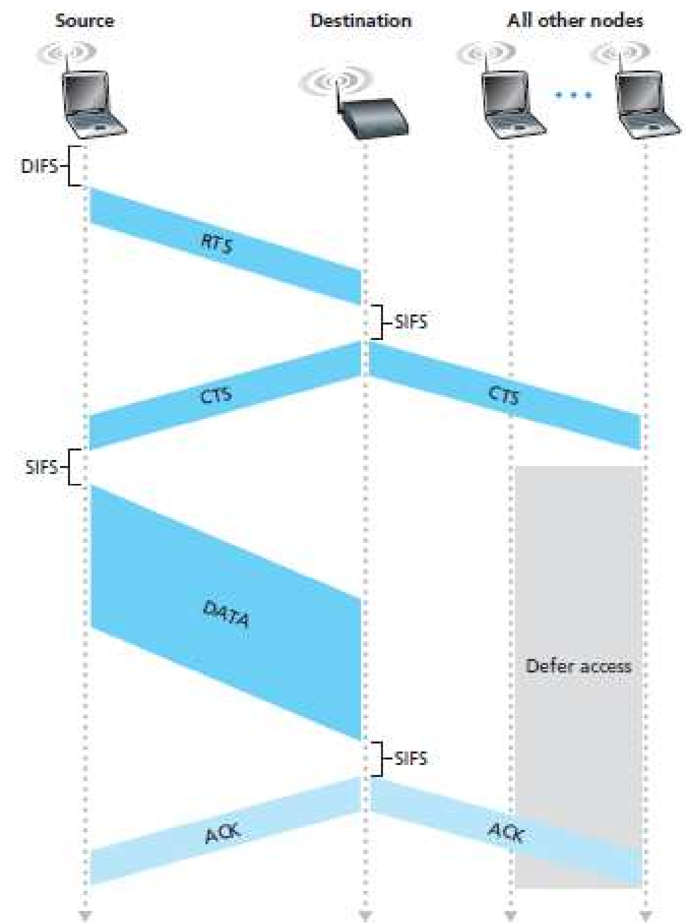
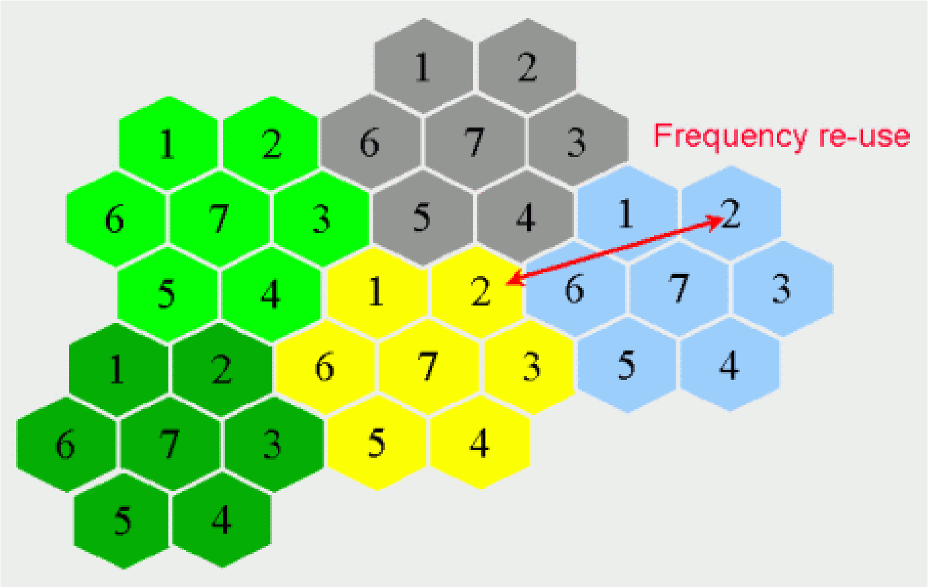


Figure 6.12 ♦ Collision avoidance using the RTS and CTS frames

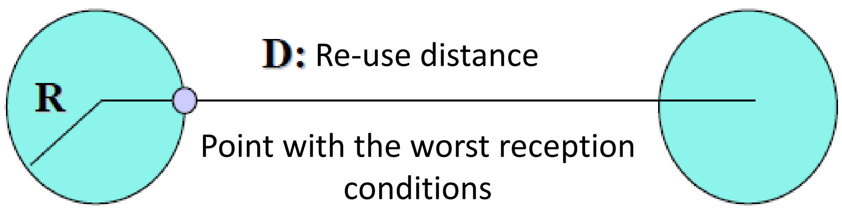
Basics on cellular communications

Cellular networks

- There are not enough wireless resources, so we reuse them
  - Area divided in cells
  - All available resources used in one cluster of K cells
- Network planning
  - If two phones using the same “resource” are very close to each other there is interference
  - The more cells in a cluster the less we reuse the resources (but the less interference we have)



Interference-limited system

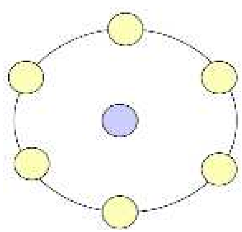


Signal to Interference Ratio

Path-loss coefficient

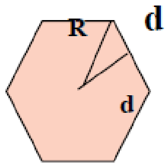
$$CIR = \frac{P_u}{P_I} = \frac{\beta \frac{1}{R^{\alpha}}}{\beta \frac{1}{(D-R)^{\alpha}}} = \left(\frac{D}{R} - 1\right)^{\alpha}$$

- Assuming hexagonal cells, the interference comes from 6 directions



$$CIR = \frac{P_u}{P_I} \approx \frac{1}{6}\left(\frac{D}{R} - 1\right)^{\alpha}$$

- Generalized for a cluster of size K

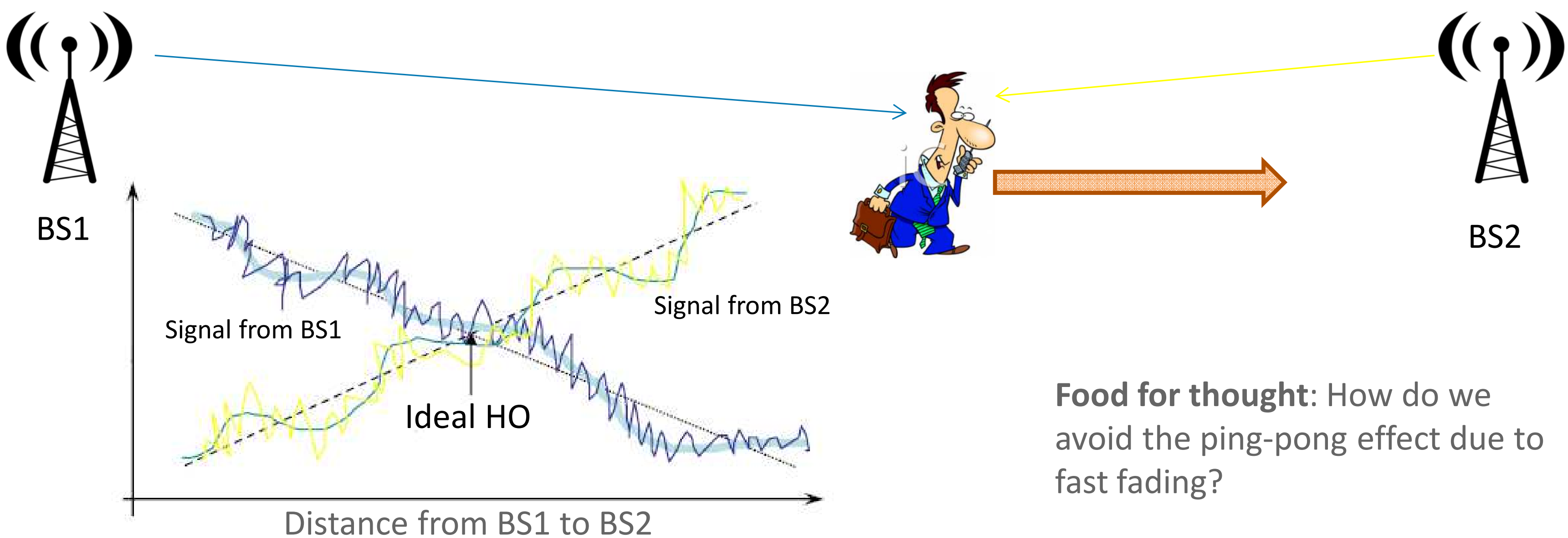


$$d = R\cos 30 = R\frac{\sqrt{3}}{2}$$

$$CIR = \frac{1}{6}\left(\frac{D}{R} - 1\right)^{\alpha} = \frac{1}{6}\left(\sqrt{3K} - 1\right)^{\alpha}$$

Handover

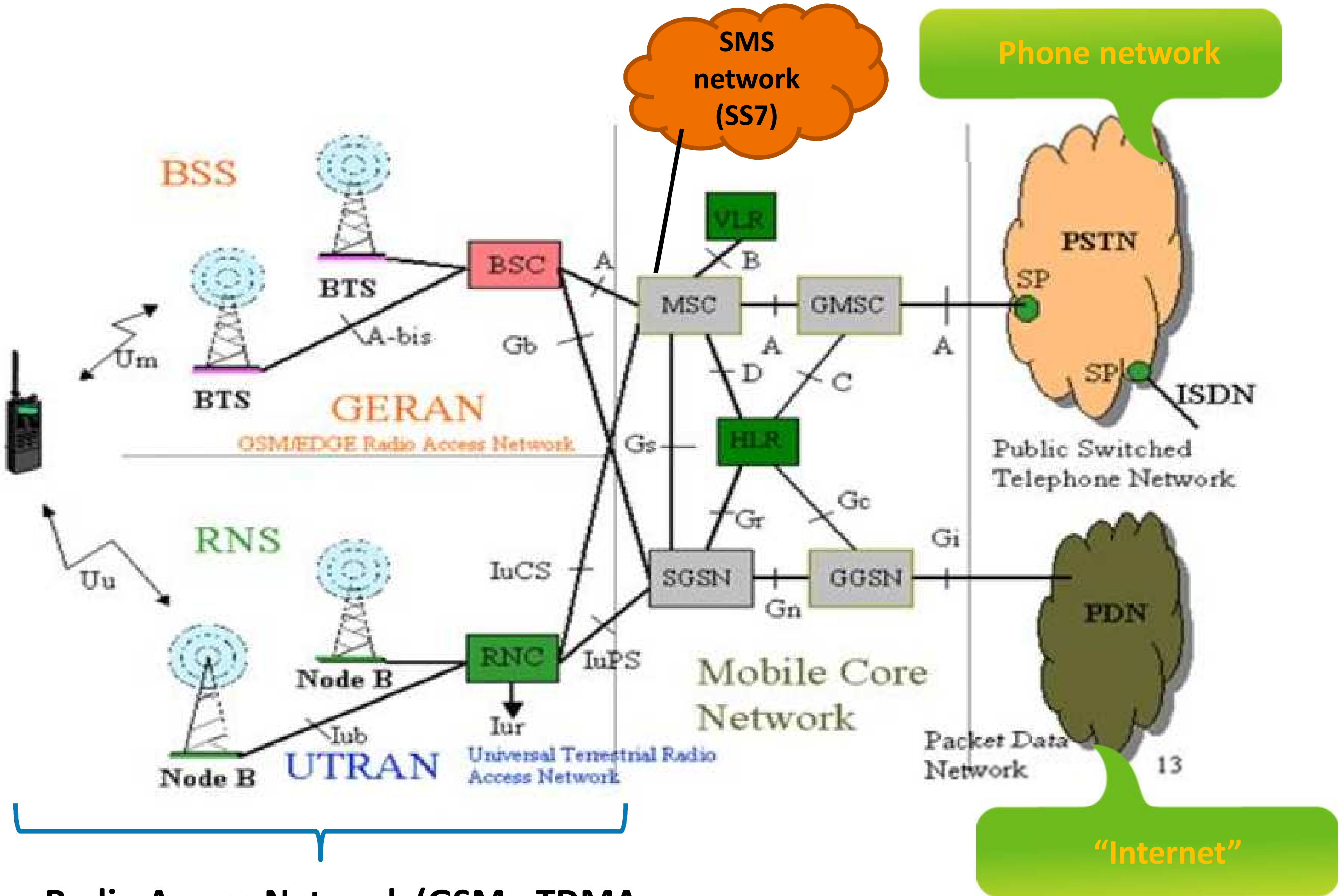
- When you move from one cell to another the phone does not disconnect
- This makes mobility in cellular networks possible
- Types of handover
  - Hard (GSM, LTE) – The phone disconnects from a tower and connects to a new one
  - Soft (3G UMTS) – The phone is always “connected” to N towers and just updates that list
    - Rake receiver



Food for thought: How do we avoid the ping-pong effect due to fast fading?

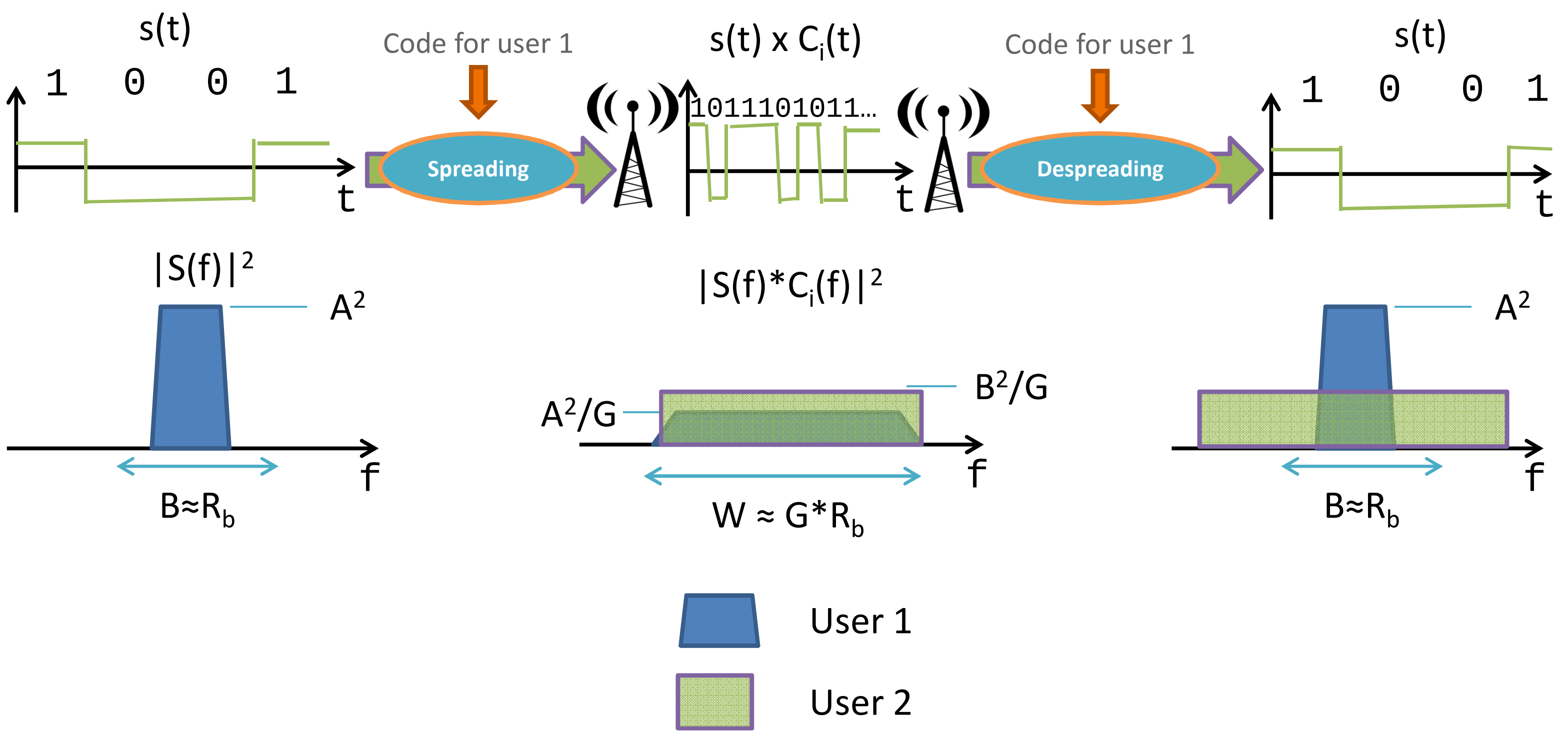
Mobile networks

2G and 3G mobile network architecture



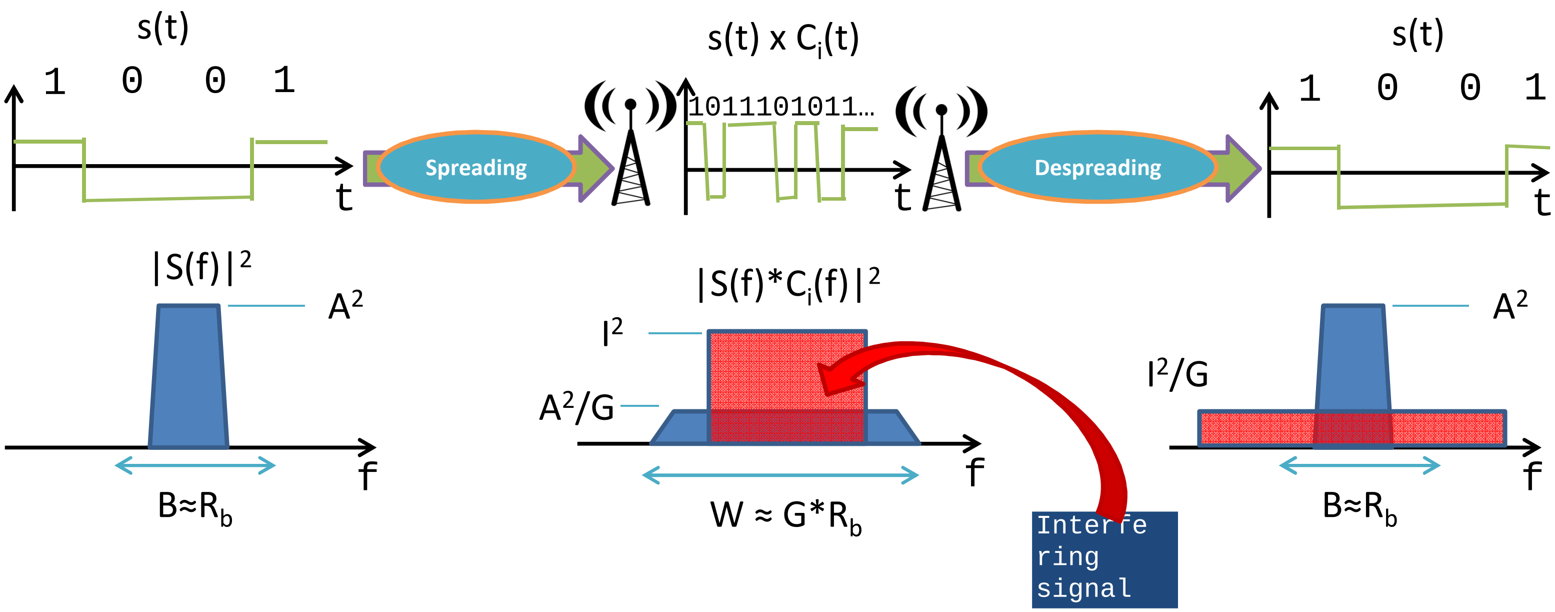
Radio Access Network (GSM - TDMA, 3G – WCDMA)

3G Radio Access Network - WCDMA



Resiliency of CDMA against adversarial interference

- CDMA was initially designed for military applications
  - The signal is transmitted hidden under the noise floor
  - Resiliency against adversarial interference



Mobile Core Network

- Routes and forwards each connection
  - **MSC**: Phone calls → PSTN (Public Switched Telephone Network)
  - **MSC+SMSC**: SMS → SS7 network
  - **GGSN/SGSN** (3G) or **S-GW** (LTE): Data → Internet
- Upon incoming call/SMS/connection, locates the recipient phone
  - **HLR** (Home Location Register)
  - Paging
- Controls and manages the Radio Access Network (RAN)

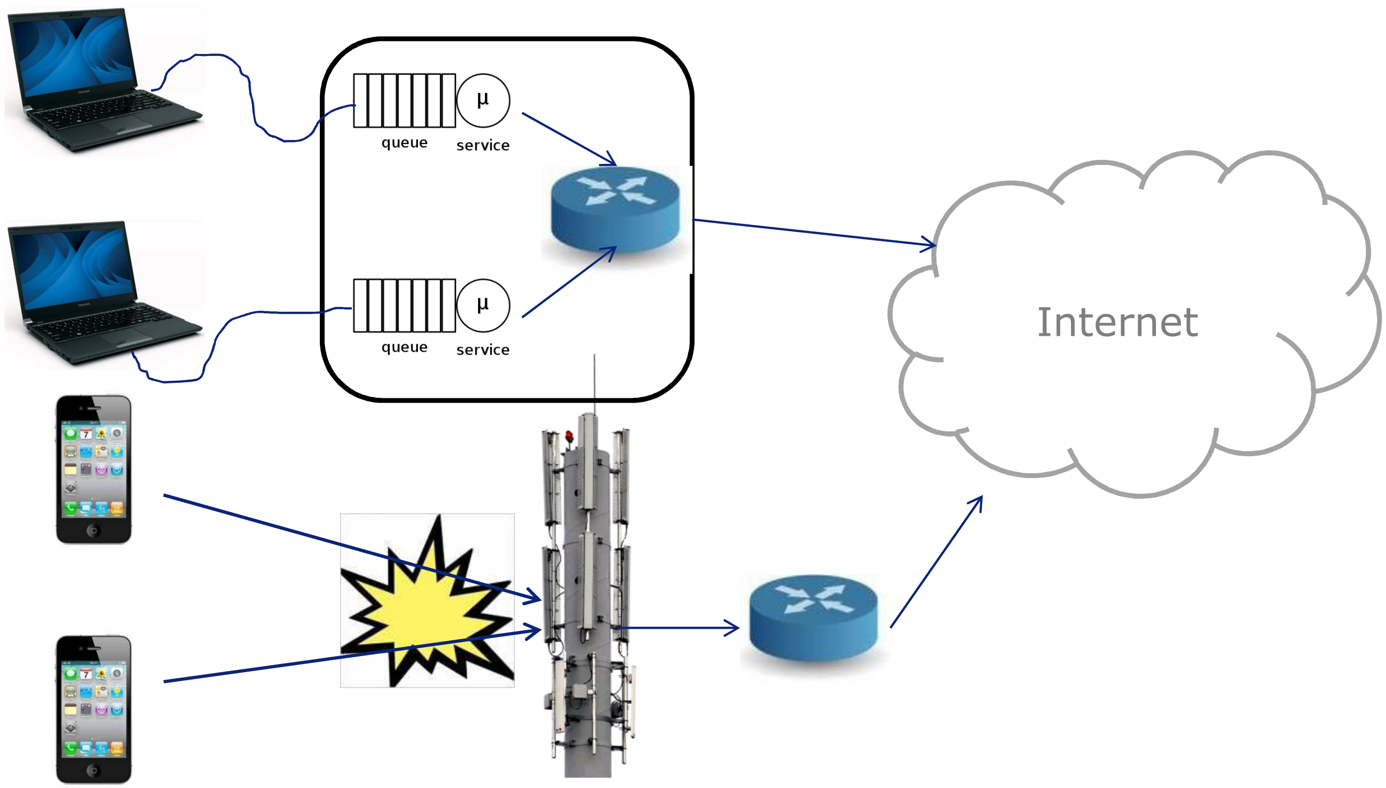
Paging

- When there is an incoming call/SMS, the network has to find the recipient
- A **paging** message is broadcasted
  - Broadcasting over every single cell in America sounds like an inefficient way to do it
  - The network (**HLR**) knows roughly the area where you were last seen (**Tracking Area**)
    - If a user moves → Tracking Area Update
  - Paging only broadcasted in your Location Area
  - If you move, the phone updates with the HLR your location (Location Area Update)
- When your phone receives the paging message replies to it
  - "Hey, I am here!"
  - Now the network knows in what specific cell you are

Food for thought: Why not keeping track of the cell where each user is instead of the Location Area?

Random Access Channel

- There is not enough “spectrum” for ever mobile device to be always connected (“channel” assigned)
  - Mobile devices are usually “disconnected”
  - When they need to “connect”, they request resources on a shared channel → RACH

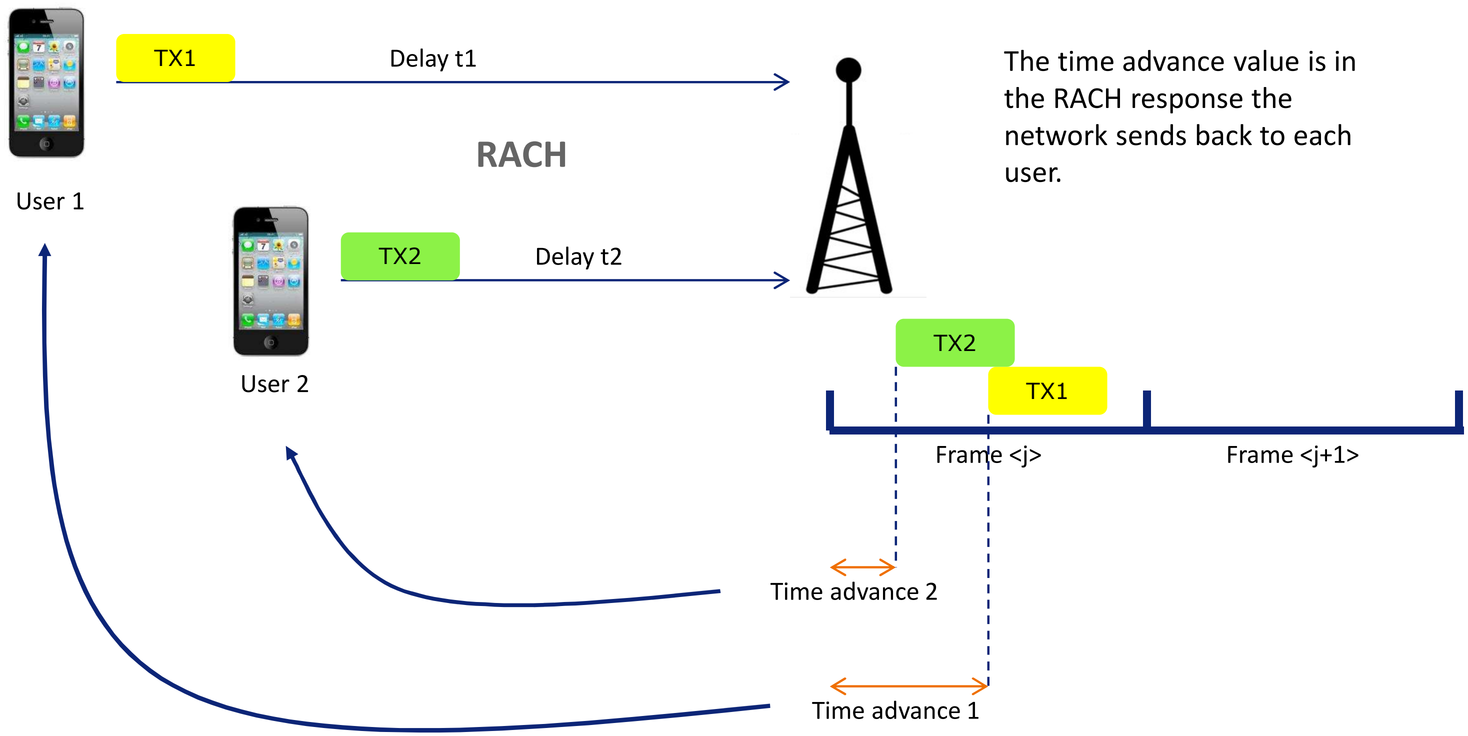


Random Access Channel

- The RACH is an important signaling channel in mobile networks
  - Used to initiate all transmissions
- Shared by all the users in a cell
  - Contention-based access
  - Method similar to S-ALOHA with random backoff delays, retransmissions

- Also used to acquire UL synchronization

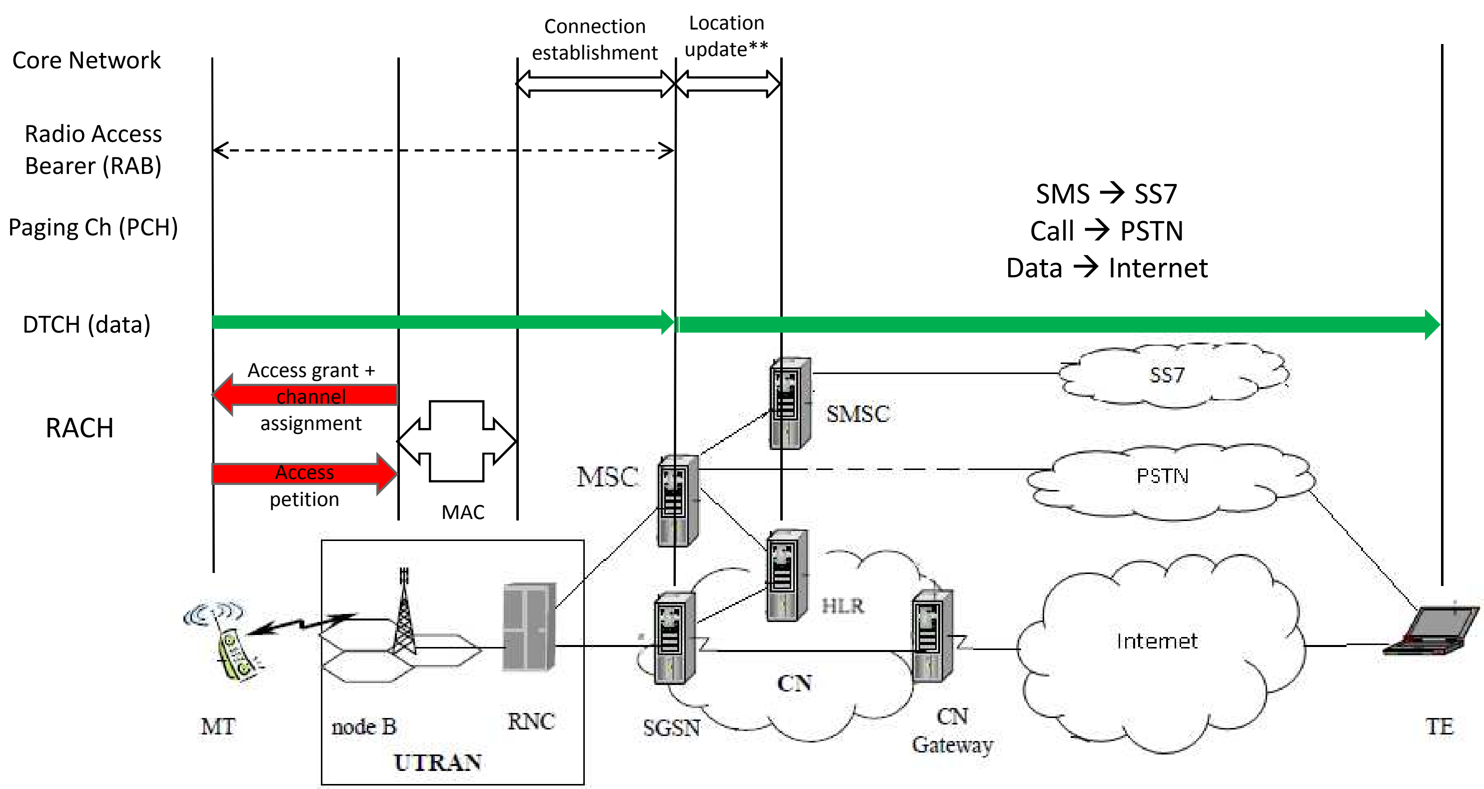
UL synchronization over the RACH



The time advance value is in the RACH response the network sends back to each user.

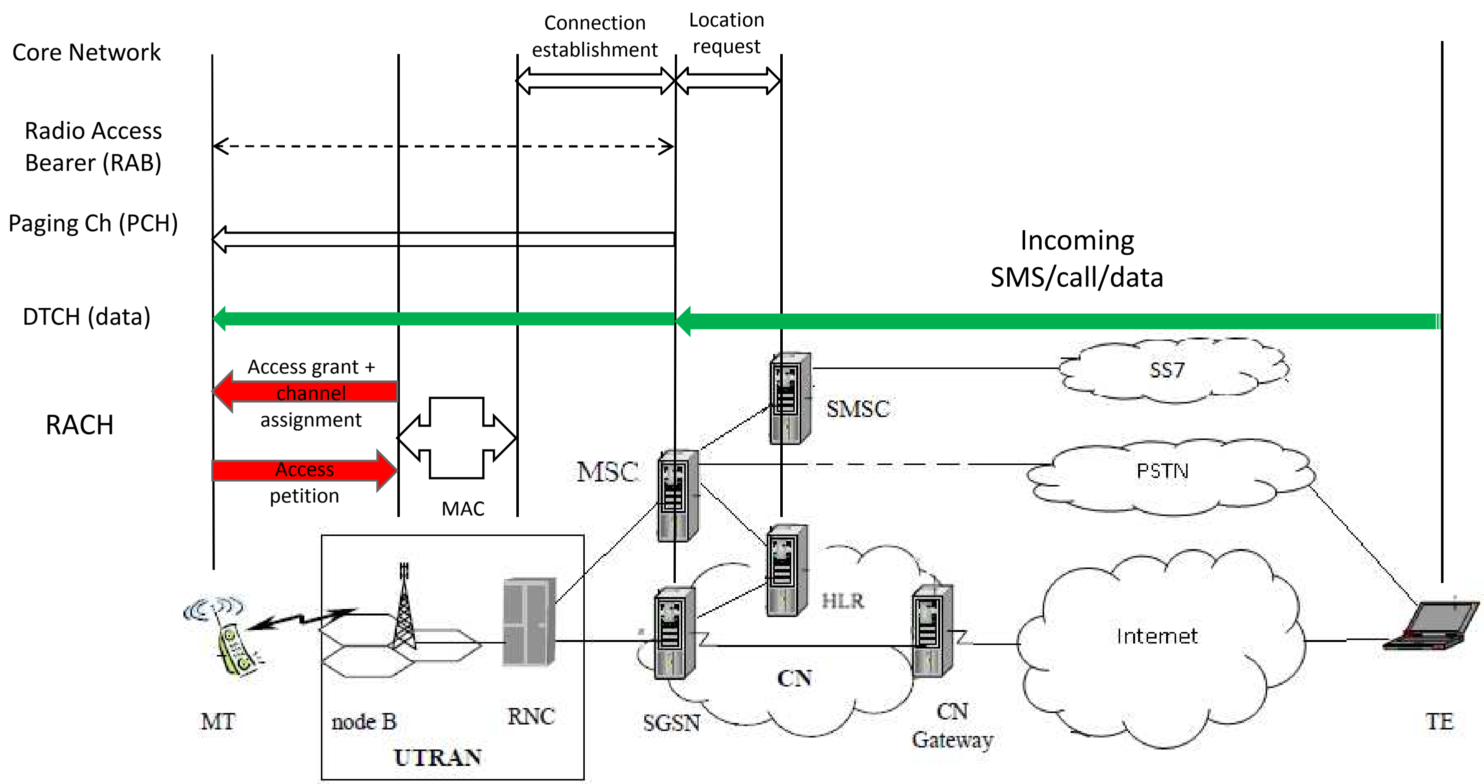
Connection establishment (2G/3G example)

Mobile initiated



Connection establishment (2G/3G example)

Mobile terminated



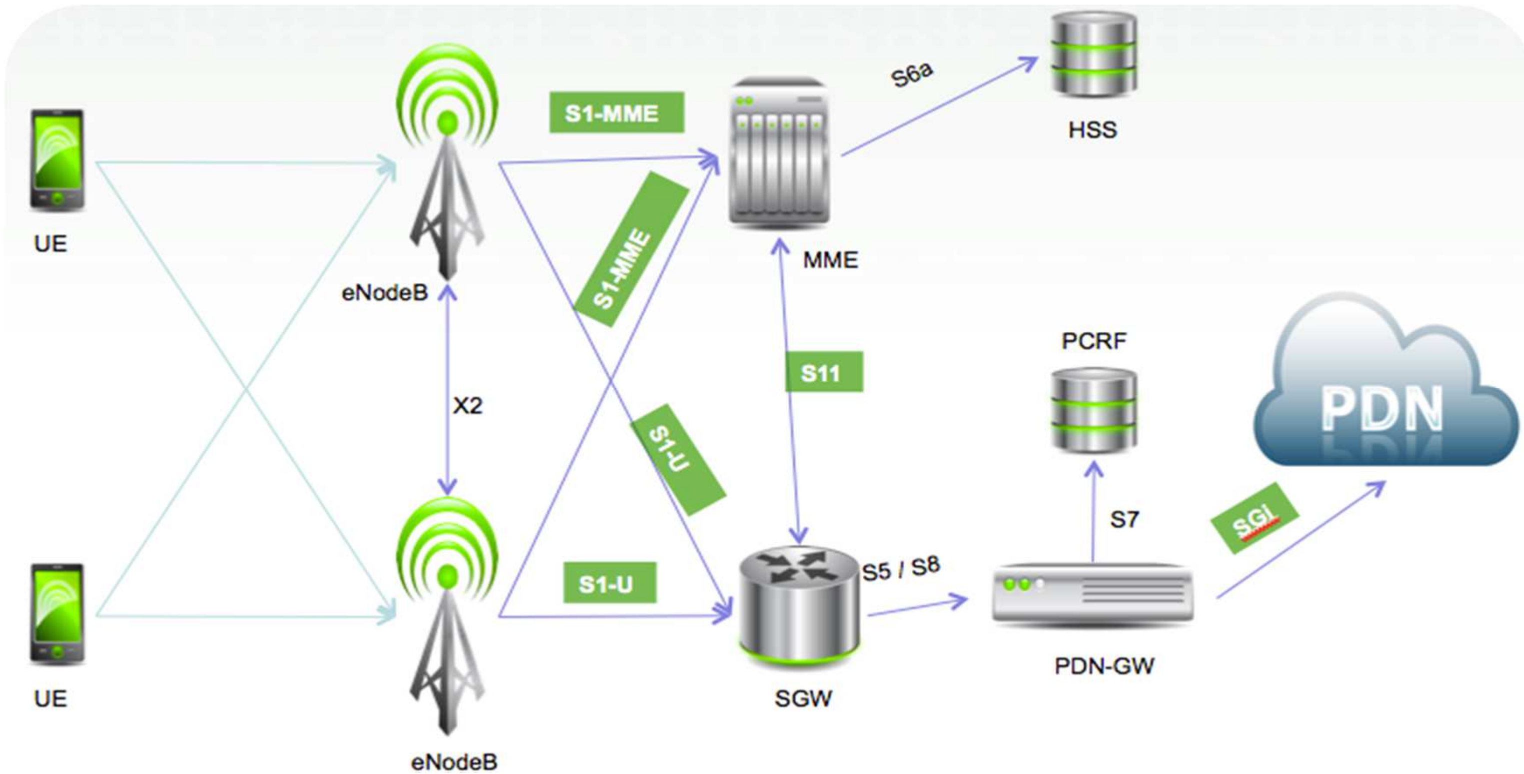
Long Term Evolution (LTE)

LTE mobile network architecture

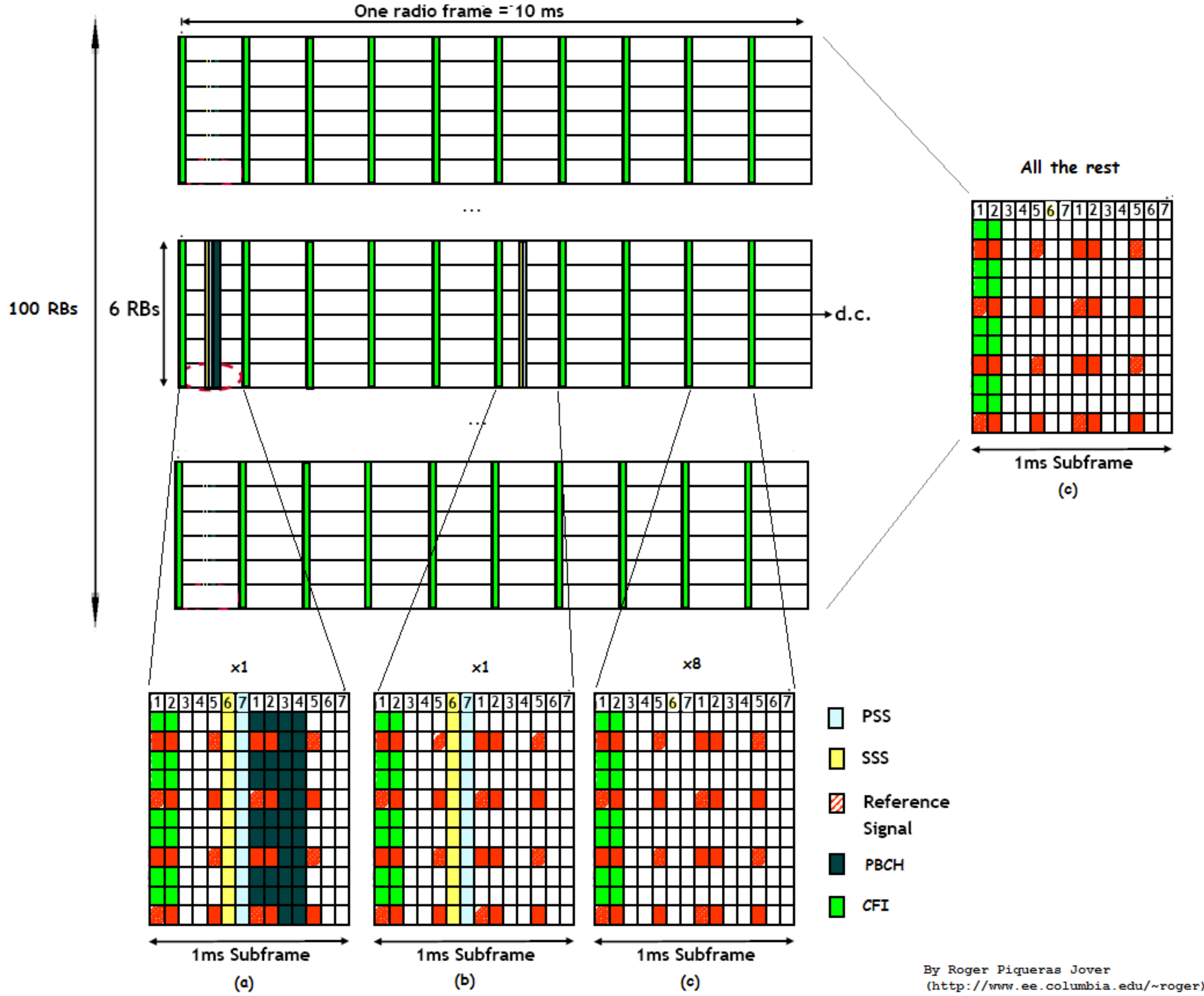
The Long Term Evolution (LTE)

- Latest evolution of 3GPP standards
  - Enhanced RAN → eUTRAN
    - OFDMA
    - MIMO
    - Robust performance in multipath environments
  - Enhanced Packet Core → EPC
    - Flat(er) “all-IP” architecture
    - Support and mobility between multiple heterogeneous access networks

LTE mobile network architecture

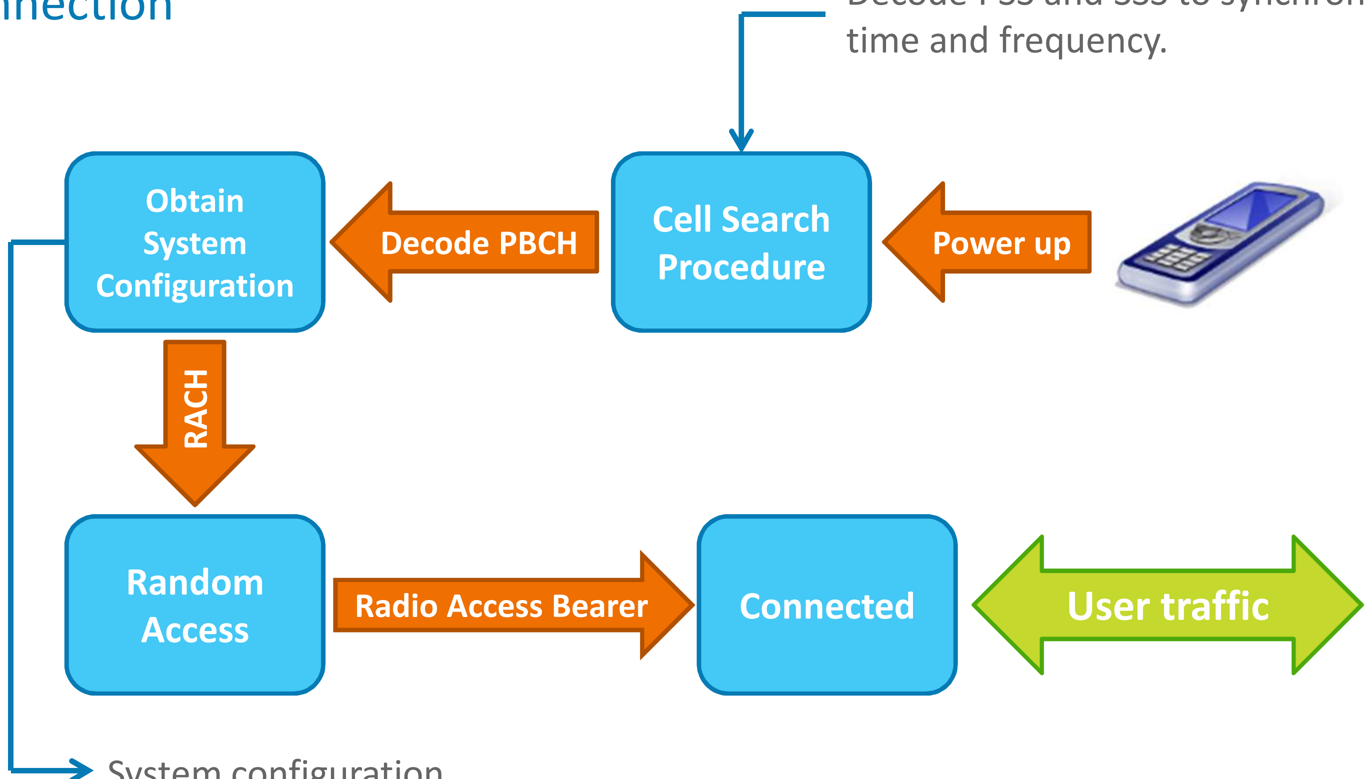


LTE RAN – Radio frame architecture



LTE connection

Decode PSS and SSS to synchronize in time and frequency.

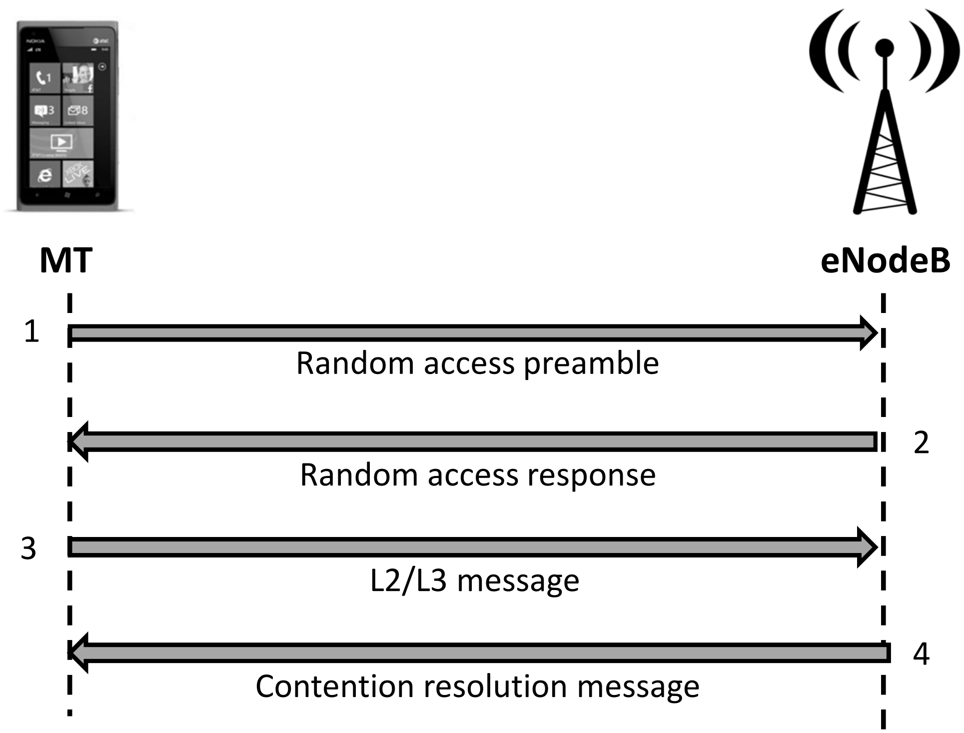


System configuration

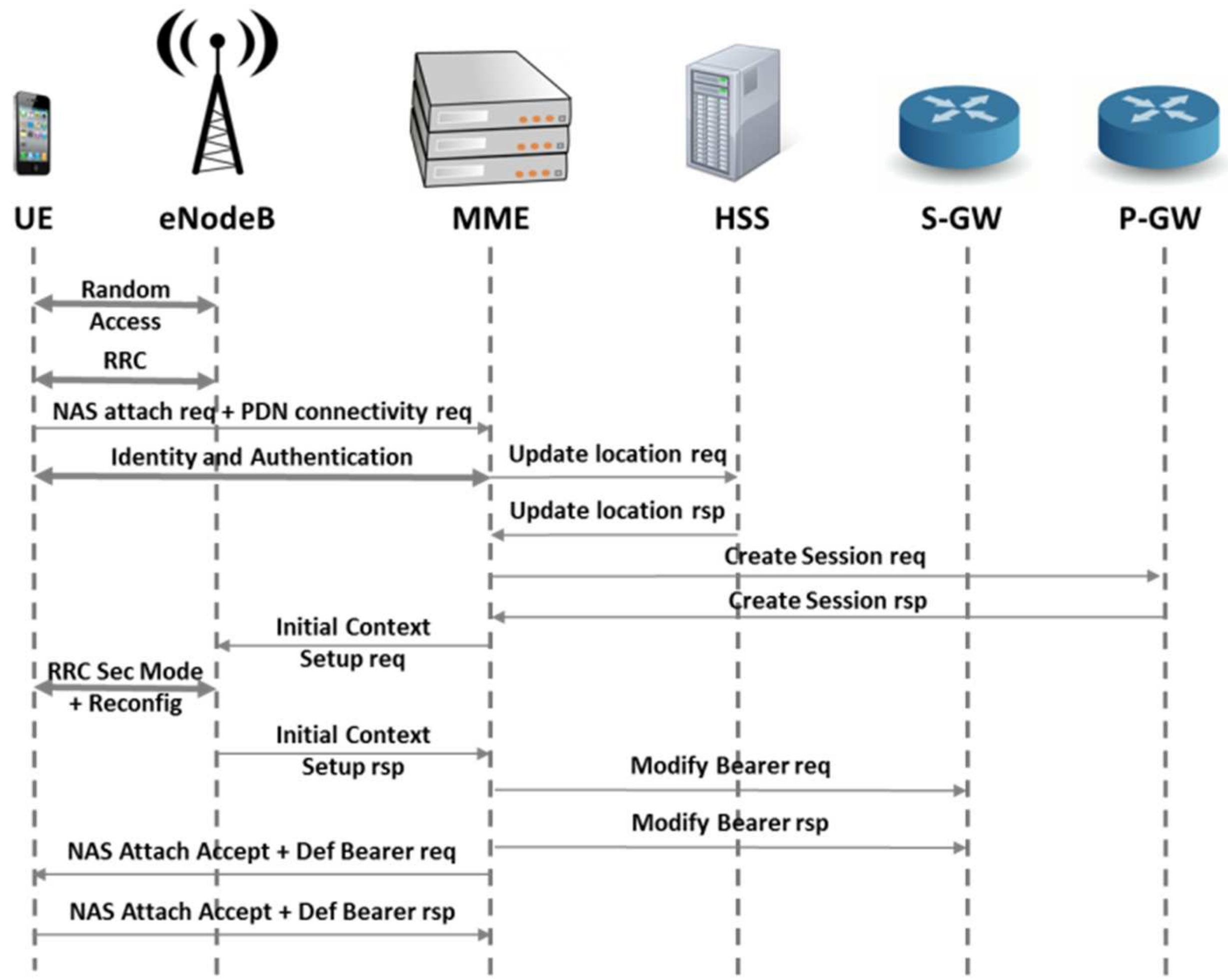
- Decode Master Information Block (MIB) from PBCH
- Decode System Information Blocks (SIBs) from PDSCH

LTE Random Access Channel

- Very similar procedure to 3G
  - Random access preamble – select a signature out of 64
  - Random Access Response – Time Advance command plus assignment of C-RNTI id



Radio Access Bearer setup



Radio Access Bearer setup - Real world example

Name	Start time	Dl/Ul	Cell	Cell ID	Frame	Subf	RCE	Power	Length	Errs	Retrans	Decr	Valid	Sf RSSI	SINR
RACH	01:32:03.954999	U	0	16	440	1	-16.64	-57.98	0						16.64
MAC Random Access Response	01:32:03.958999	D	0	16	440	5	-16.41	-45.73	7	OK				-39.20	16.41
RRCConnectionRequest	01:32:03.964999	U	0	16	441	1	-23.85	-51.14	6	OK					23.85
RRCConnectionSetup	01:32:03.979999	D	0	16	442	6	-15.11	-42.21	26	OK				-38.72	15.11
RRCConnectionSetupComplete	01:32:04.013999	U	0	16	446	0			56	OK					
Attach Request	01:32:04.013999	U	0	16	446	0	-25.25	-49.36	53	OK					25.25
PDN Connectivity Request	01:32:04.013999	U	0	16	446	0	-25.25	-49.36	36	OK					25.25
DLInformationTransfer	01:32:04.088999	D	0	16	453	5			39	OK					
Authentication Request	01:32:04.088999	D	0	16	453	5	-15.00	-41.33	36	OK				-38.44	15.00
ULInformationTransfer	01:32:04.225999	U	0	16	467	2			22	OK					
Authentication Response	01:32:04.225999	U	0	16	467	2	-20.80	-53.66	19	OK					20.80
DLInformationTransfer	01:32:04.267999	D	0	16	471	4			17	OK					
Security Protected NAS Message	01:32:04.267999	D	0	16	471	4	-15.52	-44.04	14	OK		Not...	No...	-39.22	15.52
Security Mode Command	01:32:04.267999	D	0	16	471	4	-15.52	-44.04	8	OK				-39.22	15.52
ULInformationTransfer	01:32:04.285999	U	0	16	473	2			22	OK					
Security Protected NAS Message	01:32:04.285999	U	0	16	473	2	-22.49	-52.16	19	OK		No...	No...		22.49
Unknown NAS	01:32:04.285999	U	0	16	473	2	-22.49	-52.16	13	OK					22.49
DLInformationTransfer	01:32:04.327999	D	0	16	477	4			12	OK					
Security Protected NAS Message	01:32:04.327999	D	0	16	477	4	-14.73	-45.68	9	OK		No...	No...	-39.27	14.73
Unknown NAS	01:32:04.327999	D	0	16	477	4	-14.73	-45.68	3	OK				-39.27	14.73
ULInformationTransfer	01:32:04.345999	U	0	16	479	2			24	OK					
Security Protected NAS Message	01:32:04.345999	U	0	16	479	2	-21.36	-53.39	21	OK		No...	No...		21.36
Unknown NAS	01:32:04.345999	U	0	16	479	2	-21.36	-53.39	15	OK					21.36
SecurityModeCommand	01:32:04.472999	D	0	16	491	9			3	OK					
Ciphered RRC	01:32:04.495999	U	0	16	494	2			2	OK		No...	No...		
Ciphered RRC	01:32:04.501999	D	0	16	494	8			3	OK		No...	No...		
Ciphered RRC	01:32:04.515999	U	0	16	496	2			18	OK		No...	No...		
Ciphered RRC	01:32:04.536999	D	0	16	498	3			165	OK		No...	No...		
Ciphered RRC	01:32:04.575999	U	0	16	502	2			2	OK		No...	No...		
Ciphered RRC	01:32:04.575999	U	0	16	502	2			16	OK		No...	No...		
Ciphered RRC	01:32:04.604999	D	0	16	505	1			30	OK		No...	No...		
Ciphered data	01:32:14.426997	U	0	16	463	3			96	OK		No...			
Ciphered data	01:32:14.475997	U	0	16	468	2			40	OK		No...			
Ciphered data	01:32:14.513997	U	0	16	472	0			96	OK		No...			

RACH handshake between UE and eNB

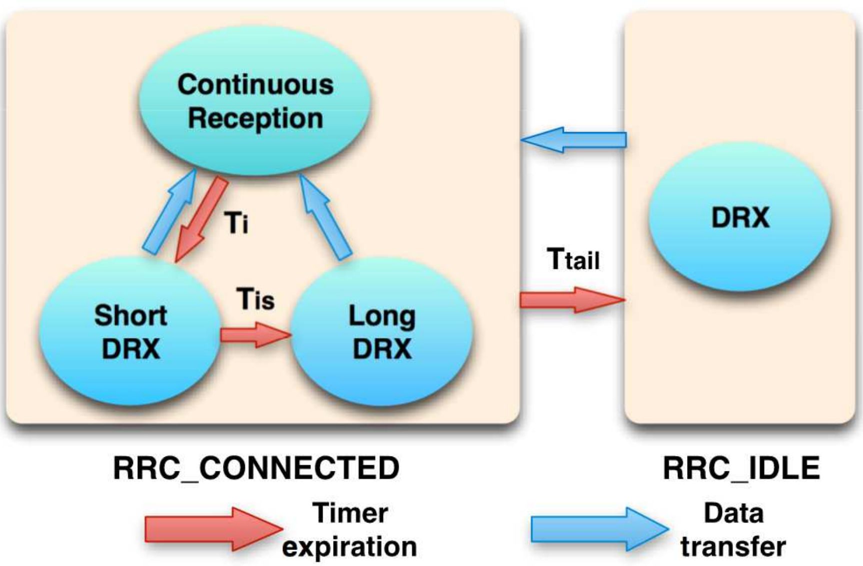
RRC handshake between UE and eNB

RAB setup (authentication, set-up of encryption, tunnel set-up, etc)

Encrypted traffic

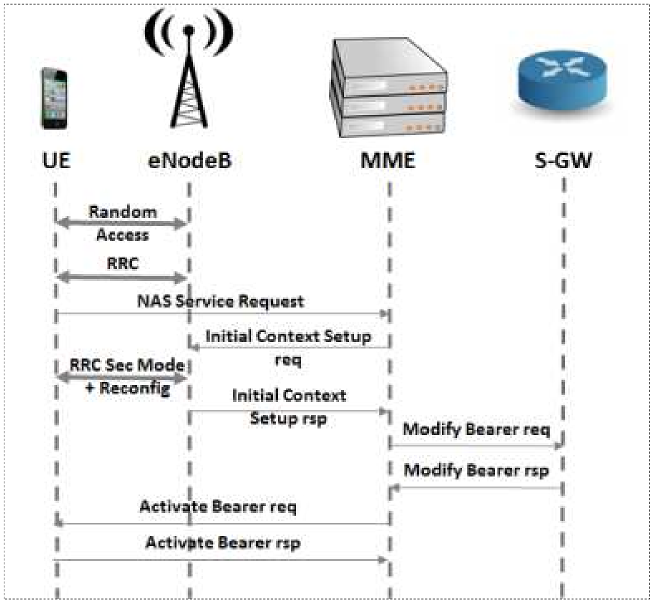
Radio Resource Control (RRC) and power management in LTE

- Motivation
  - RRC – Not enough radio resources for all users, they need to be reused when a user is idle
  - Power management – The radio of a mobile device burns a lot of battery, it is necessary to shut it down when the user is idle
- RRC state machine
  - Idle – low power usage, no active connection (no bearer with P-GW)
  - Connected – high battery usage, active bearer with P-GW

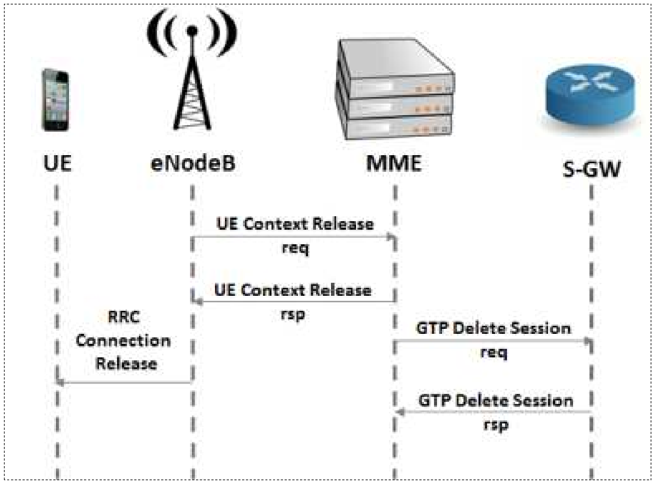


Radio Resource Control (RRC) and power management in LTE

- RRC state transitions



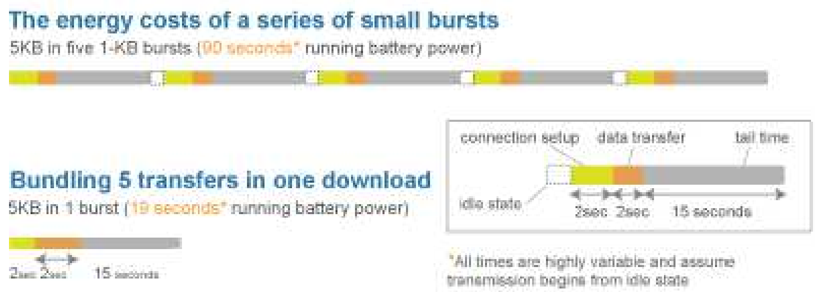
Idle to connected



Connected to idle

Radio Resource Control (RRC) and power management in LTE

- State demotions result in tail time
  - [RRC Connected → RRC Idle] transition occurs after the device has been idle for t seconds
  - The phone's radio is always on for t seconds after the device goes idle
- State promotions require a promotion delay
- State transitions result in signaling load at the core network



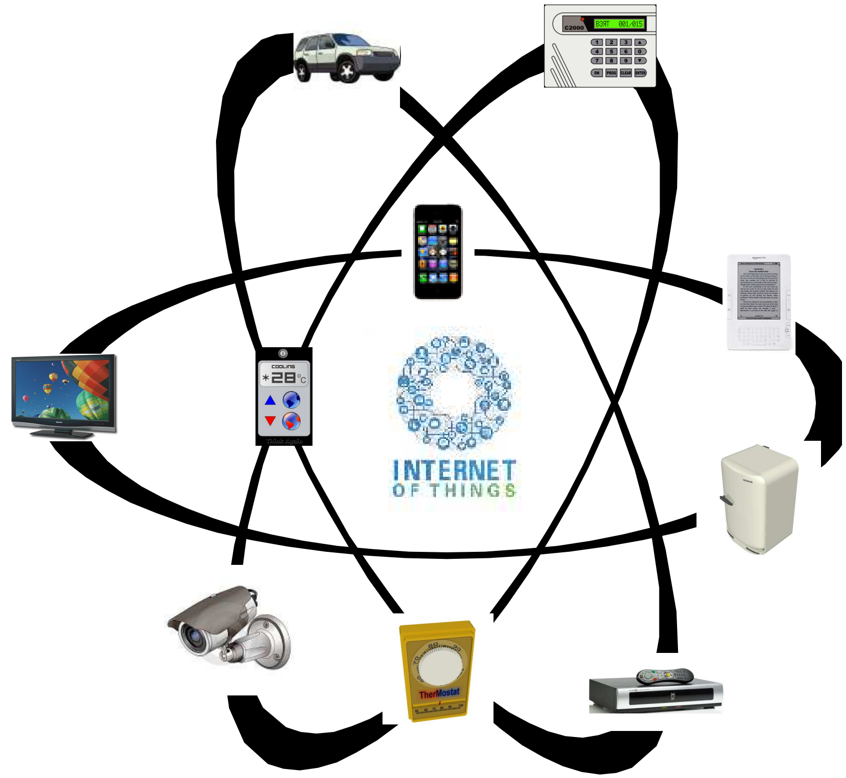
Because of the long tail time that holds the device in a power mode, transmitting data as a series of small data bursts takes much longer and requires much more battery power than it does to send a single bigger burst.

- Recommended reading: AT&T Research - A Call for More Energy-Efficient Apps [3]

The Internet of Things and M2M communications

IoT and M2M

- Already more “things” connected to the Internet than humans
  - Industry and standardization bodies talk about billions of connected devices by 2020
- Mobile networks are designed and optimized to handle {cell/smart}-phone traffic
  - Traffic characteristics of M2M devices very different than smart-phones
  - Different M2M devices have very different traffic characteristics than other M2M devices
- Current open research questions
  - Impact of IoT and M2M on cellular networks as we move to the connected world
  - Suggested reading [7]



Bluetooth

- Short-range, high-data-rate wireless link for personal devices
  - Originally designed to replace cables with a wireless link
  - Operates in the 2.4GHz ISM band
  - Note it's the same band as WiFi…
  - Range up to ~100m (usually less)

- Based on frequency hopping spread spectrum
  - 80 channels (1MHz per channel)
  - The transmitter and receiver "agree" on a pseudo-random frequency hop pattern
  - Time division duplexing
  - About 700kbps

- Master-slave communications
  - Piconet → Up to 7 slaves controlled by a master (3 bit addressing)

ZigBee

- Standard for low-power monitoring and control
  - Long battery life
  - Shorter range than Bluetooth (10m-75m)
  - ~200kbps
- IEEE 802.15.4
  - Defines PHY and MAC layers
  - ZigBee is the networking layer on top of 802.15.5
- PHY layer
  - 16 channels in the 2.4 GHz band (5 MHz per channel)
  - 10 channels in the 915 MHz band (2 MHz per channel)
  - 1 channel in the 868 MHz band
  - 2.4 GHz band uses Direct Sequence Spreading

Things to play with…

- The IoT is one of the hottest areas in communications right now
  - Lots of media attention, investment and technology developments

- Many easily available open-source and low cost tools to test cool stuff
  - Arduino: http://www.arduino.cc/
    - Arduino ZigBee: http://arduino.cc/en/Main/ArduinoXbeeShield
    - Arduino Bluetooth: http://arduino.cc/en/Main/ArduinoBoardBT?from=Main.ArduinoBoardBluetooth
  - Arduino + Android: http://www.mouser.com/new/arduino/arduinoandroid/
  - Raspberry Pi: http://www.raspberrypi.org/
  - Romo: http://www.romotive.com/

Suggested reading

[1] 5G wireless channel measurements: http://ieeexplore.ieee.org/iel7/6287639/6336544/06515173.pdf?arnumber=6515173

[2] Wireless Communications: Principles and Practice (2nd Edition). Theodore Rappaport. Prentice Hall.

[3] AT&T Research - A Call for More Energy-Efficient Apps:
http://www.research.att.com/articles/featured_stories/2011_03/201102_Energy_efficient?fbid=Vss1vjwl65X

[4] A. L. Swindlehurst, E. Ayanoglu, P. Heydari, and F Capolino, "Millimeter-Wave Massive MIMO: The Next Wireless Revolution?" IEEE Comm. Magazine, Vol. 52, No. 9, pp. 56-62, Sept. 2014.

[5] SESIA, S., BAKER, M., AND TOUFIK, I. LTE, The UMTS Long Term Evolution: From Theory to Practice. Wiley, 2009.

[6] P Kyasanur, NF Vaidya. Selfish MAC layer misbehavior in wireless networks. IEEE Transactions of Mobile Computing:
http://perso.prism.uvsq.fr/users/mogue/Biblio/Sensor/AUTRES/01492362.pdf

[7] F. Ghavimi, Hsiao-Hwa Chen. M2M Communications in 3GPP LTE/LTE-A Networks: Architectures, Service Requirements, Challenges and Applications. IEEE Comunication Surveys and Tutorials. 2014.
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6916986&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6916986

Technology directions for 5G:

[8] F. Boccardi, et. al. Five Disruptive Technology Directions for 5G. IEEE Communications Magazine. 2014. http://arxiv.org/pdf/1312.0229

Mobile network security:

[9] R. Piqueras Jover. Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions. IEEE Global Wireless Summit 2013. http://web2.research.att.com/techdocs/TD_101153.pdf