Computer Networks

Ch.4 Wireless and Mobile Networks

(bruno.quoitin@umons.ac.be)

Important note: These slides are based on the instructors material provided by **J.F. Kurose** and **K.W. Ross** (c) 1996-2009.

Chapter 6: Wireless and Mobile Networks

Background

- # wireless (mobile) phone subscribers now exceed wired phone subscribers ! (since ~2003)[1]
- computer nets : laptops, smartphones, Internet-enabled phones promise anytime untethered Internet access

Two important (but different) challenges

- *Wireless* : communication over wireless link
- *Mobility* : handling the mobile user who changes point of attachment to network

(1) **MOBILE OVERTAKES FIXED: IMPLICATIONS FOR POLICY AND REGULATION**, International Telecommunication Union (ITU), 2003.

Chapter 6 outline

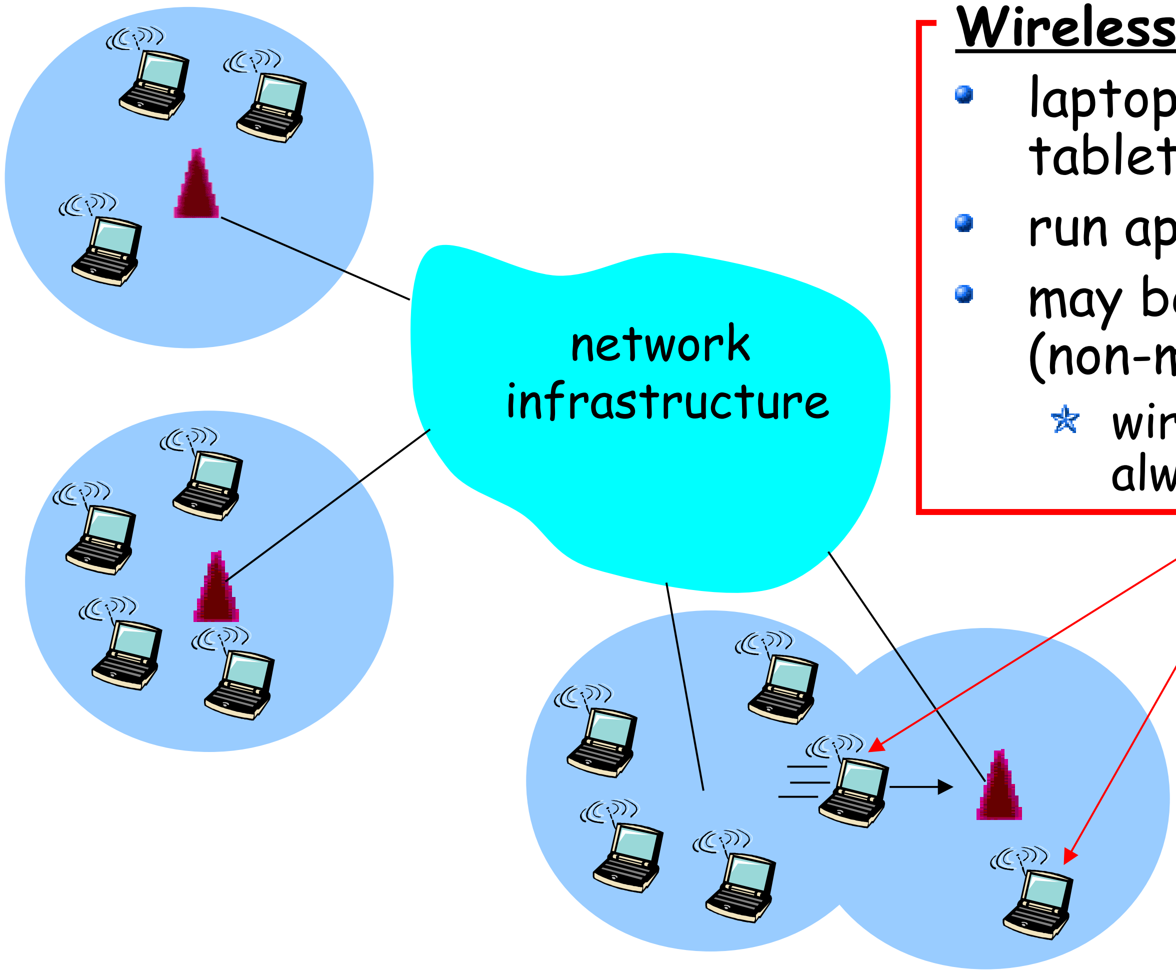
6.1 Introduction

Wireless
- 6.2 Wireless links, characteristics
  - Spread spectrum
- 6.3 IEEE 802.11 wireless LANs ("wi-fi")
- 6.4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Mobility
- 6.5 Principles: addressing and routing to mobile users
- 6.6 Mobile IP
- 6.7 Handling mobility in cellular networks
- 6.8 Mobility and higher-layer protocols

6.9 Summary

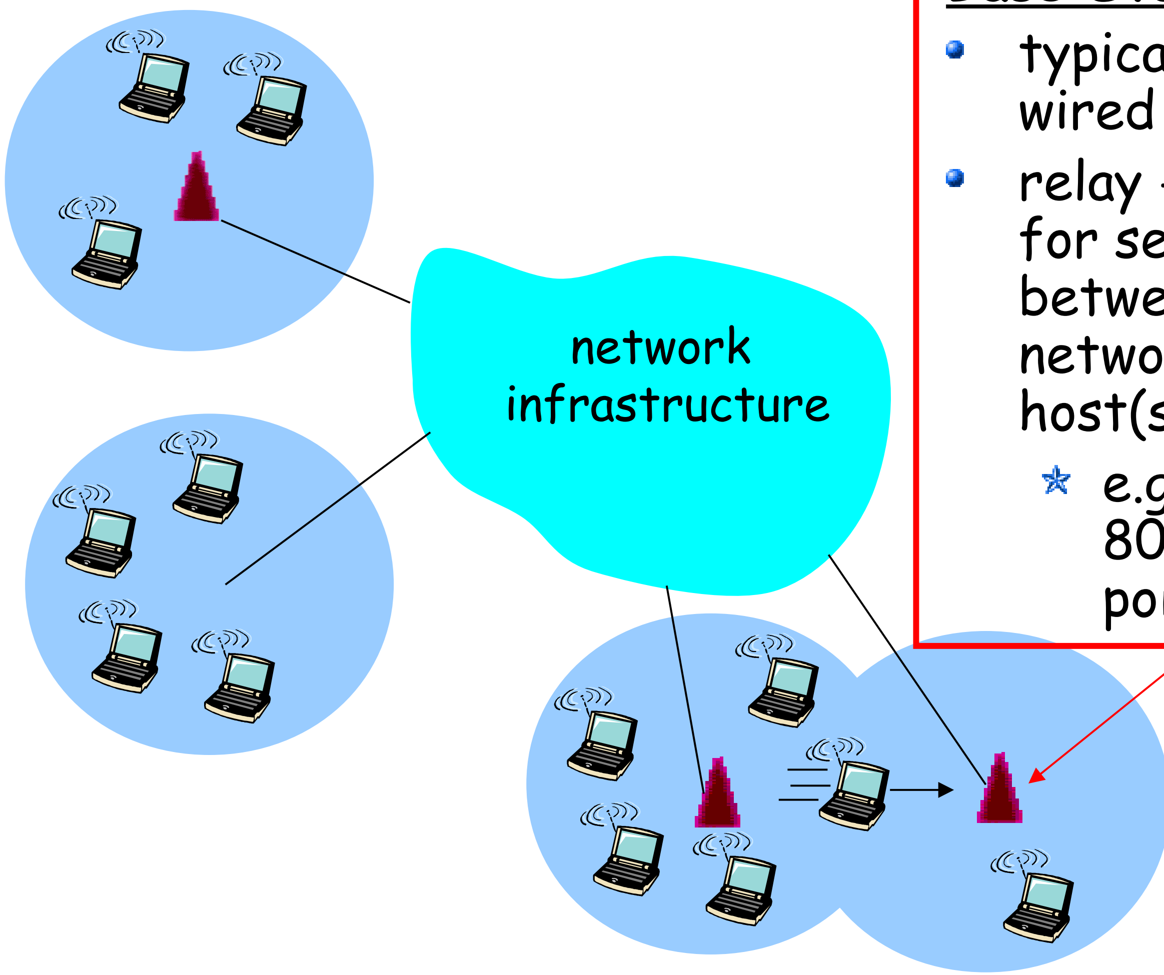
Elements of a wireless network (1/5)



Wireless Hosts

- laptop, smartphone, tablet
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

Elements of a wireless network (2/5)



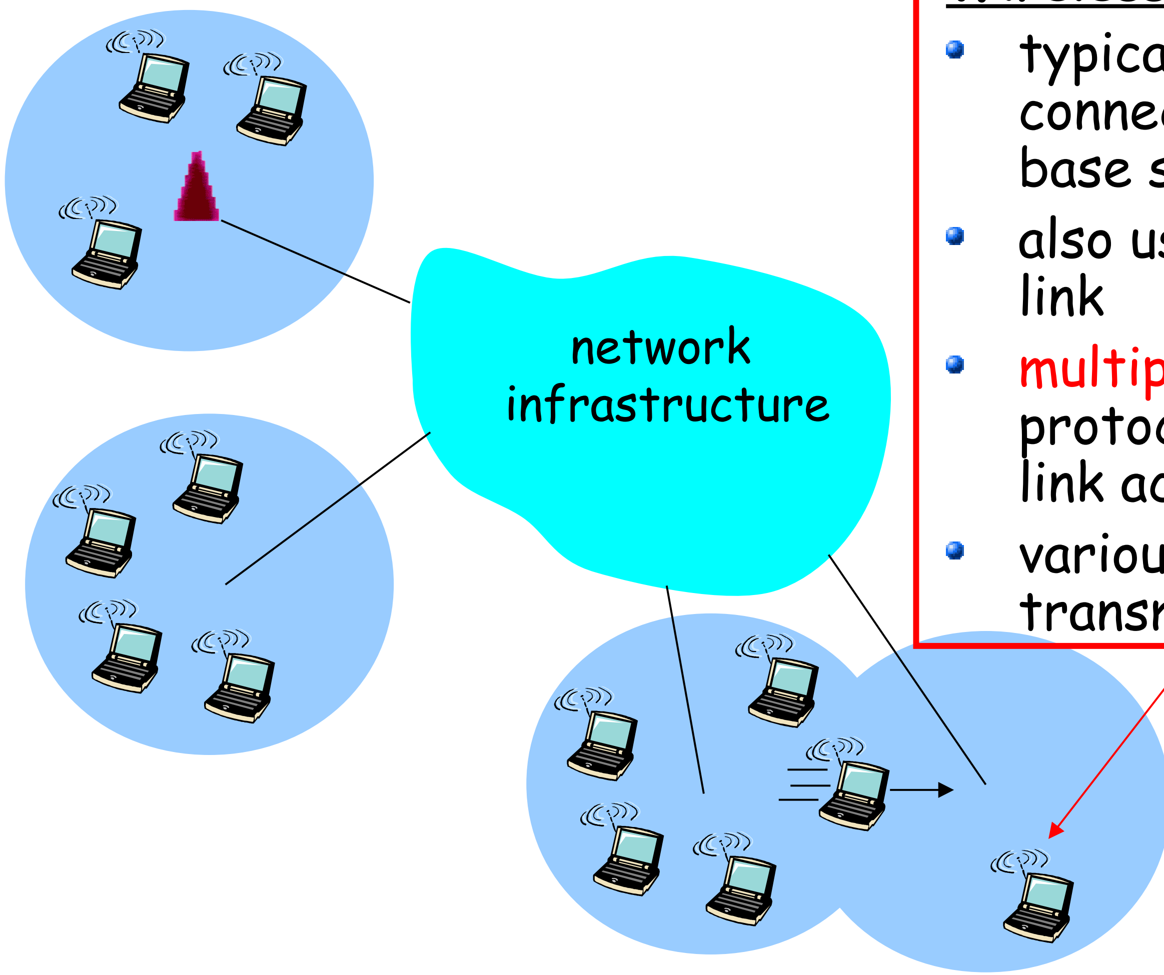
Base Station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

Ne sais pas utiliser CSMA/CD (=> revoir !) car Ne sais pas détecter de collision.

CSMA/CA utiliser pour éviter les collisions !

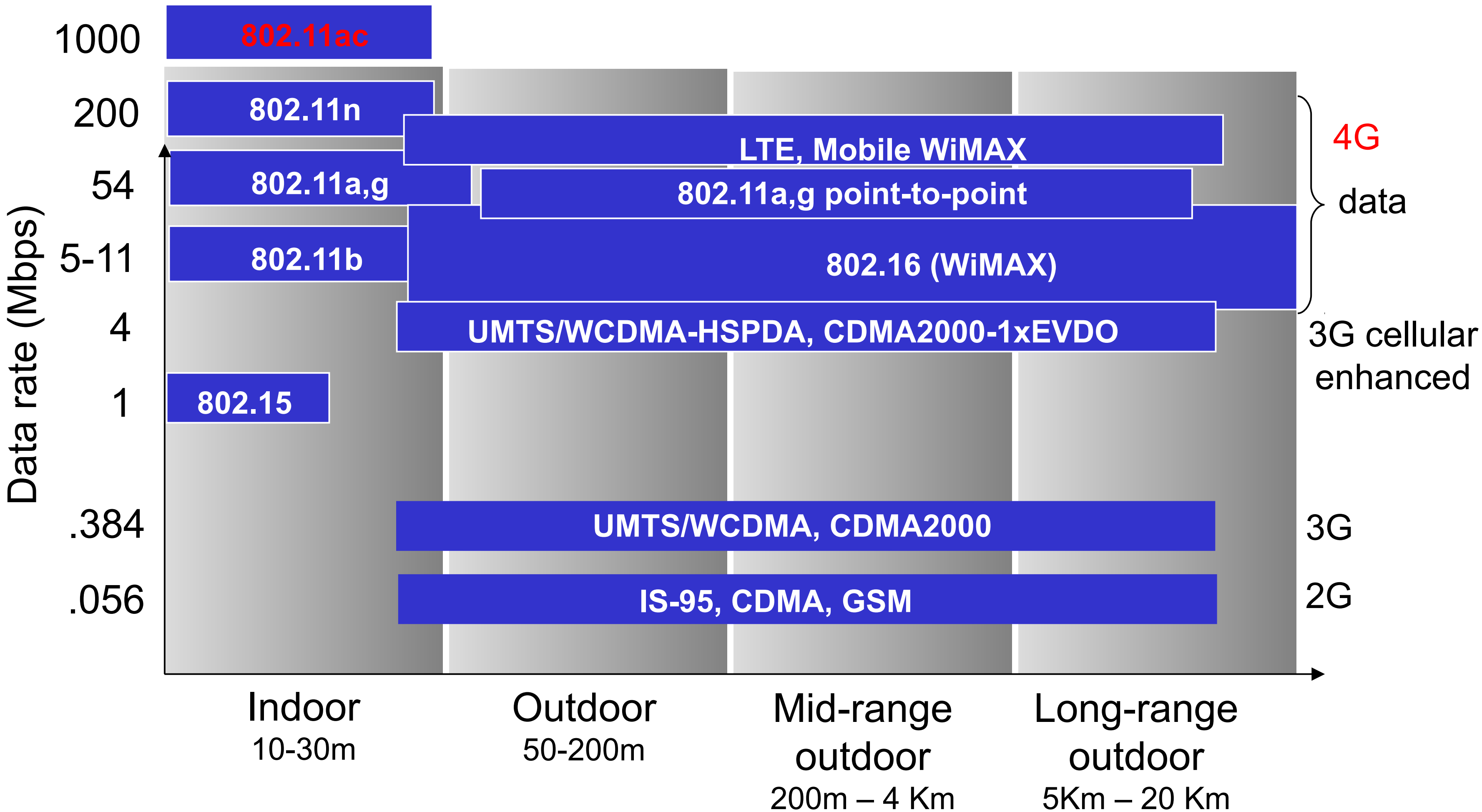
Elements of a wireless network (3/5)



Wireless Link

- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access control protocol coordinates link access
- various data rates, transmission distance

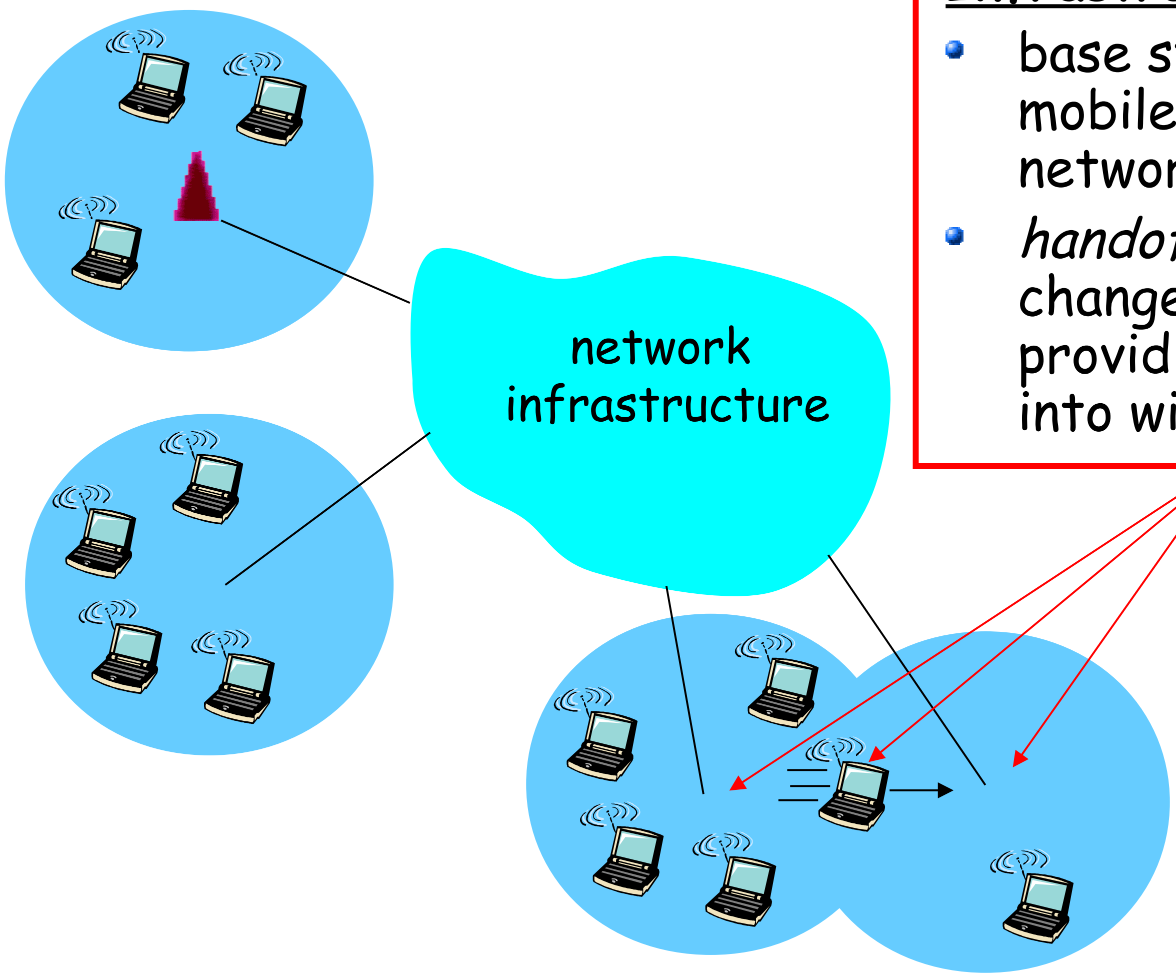
Various data rates and transmission distances of selected wireless link standards



<u>Note</u> : 2G, 3G, 4G, ... are requirerments defined by the ITU (International Telecommunications Union)

handoff : passage d'une station à une autre: court moment ou la communication est interrompue.

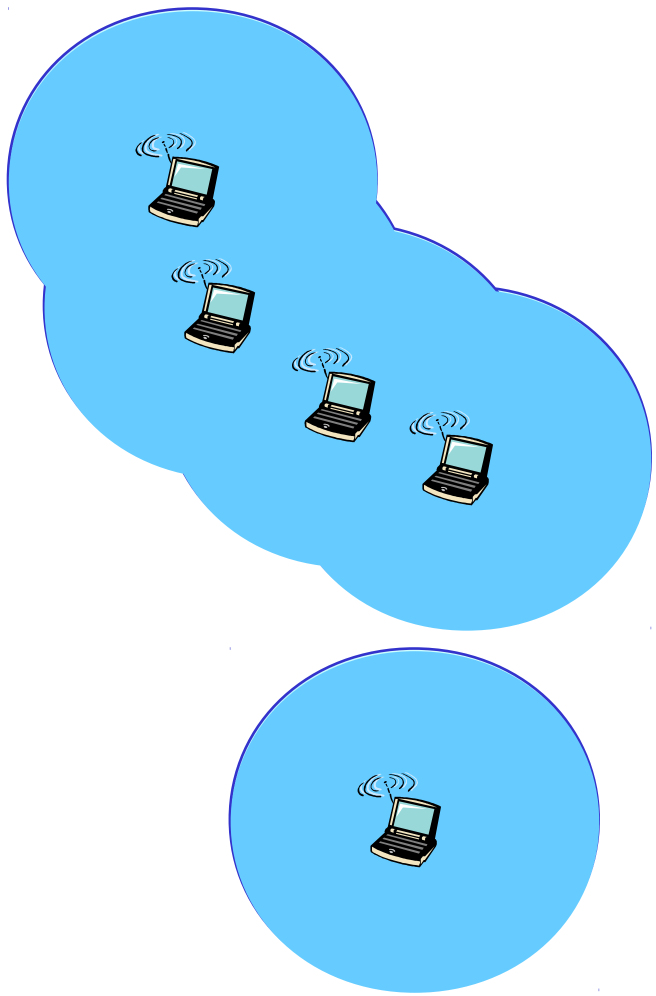
Elements of a wireless network (4/5)



Infrastructure Mode

- base station connects mobiles into wired network
- *handoff* : mobile changes base station providing connection into wired network

Elements of a wireless network (5/5)



Ad hoc Mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves (*mesh routing*)

Wireless network taxonomy

	Single hop	Multiple hops
Infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
No infrastructure (Ad-Hoc)	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach another wireless node MANET, VANET

MANET : *Mobile Ad hoc NETwork*
VANET : *Vehicular Ad hoc NETwork*

Radiofrequency (RF) communications

Basic principles

- ElectroMagnetic (EM) wave
- Radio frequencies span from 3kHz to 300GHz
- Propagation speed = speed of light c (~3.10^8 m/s) in vacuum[(1)]
- Wavelength λ = length of one period of the signal

$$\lambda = c\,T = \frac{c}{f}$$

where T is the period (s) and f is the frequency (Hz)

(1) In other mediums, propagation speed is smaller, depending on the index of refraction of the medium (e.g. ~1.0003 for air)

Radiofrequency (RF) communications

Radio spectrum classification[1]

- Different frequencies → different propagation properties. In particular, VHF band and up, propagation ~ line-of-sight[2]

Abbreviation	Frequencies	Wavelength
VLF (*Very Low Frequencies*)	3-30kHz	10-100km
LF (*Low Frequencies*)	30-300kHz	1-10km
MF (*Medium Frequencies*)	0.3-3MHz	0.1-1km
HF (*High Frequencies*)	3-30MHz	10-100m
VHF (*Very High Frequencies*)	30-300MHz	1-10m
UHF (*Ultra High Frequencies*)	0.3-3GHz	0.1-1m
SHF (*Super High Frequencies*)	3-30GHz	1-10cm
EHF (*Extremely High Frequencies*)	30-300GHz	1-10mm

(1) Source : The ARRL Handbook of Radio Communications, 2011
(2) Source : ES310, Introduction to Naval Weapons Engineering, 1998

Radiofrequency (RF) communications

Radio spectrum regulation

- The whole radio spectrum cannot be used freely. It is a *finite resource* shared by users worldwide.
- Parts allocated to specific users (e.g. military) or services (e.g. FM radio, television, aicraft control, ...)
- Some bands can be used freely provided power is within limits.
  - *Industrial, Scientific and Medical* (ISM) bands.
  - Some of then used for Wi-Fi (e.g. bands around 2.4 and 5 GHz)
- See regulation authorities for exact allocation
  - *European Telecommunications Standards Institute* (ETSI) and *European Conference on Postal and Telecommunications Administration* (CEPT)
  - *Belgian Institutes for Postal services and Telecommunications* (BIPT/IBPT)

Wireless Link Characteristics (1/12)

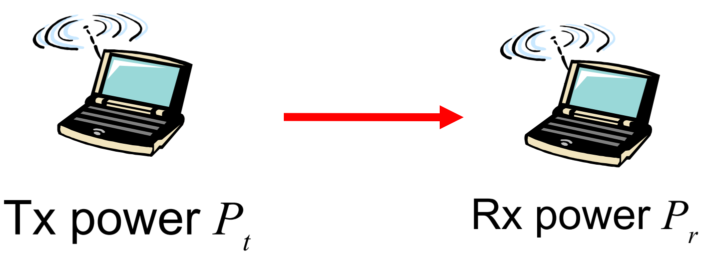
Differences from wired link ….

- Decreased signal strength
  - radio signal attenuates as it propagates through matter (path loss)
- Interference from other sources
  - standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- Multipath propagation
  - radio signal reflects off objects ground, arriving at destination at slightly different times

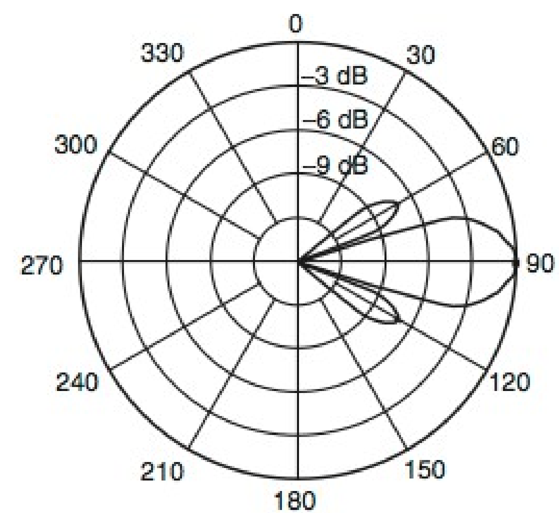
…. make communication across (even a point to point) wireless link much more "difficult"

Wireless Link Characteristics (2/12)

- **Wireless transmission range - factors**
  - Transmission power : Measured in Watts or in dBm.
  - Receiver sensitivity : Minimum received power (in Watts or dBm) that allows reception with a reasonable BER[1].



  - Antenna gain : antenna does not radiate EM power uniformly in every direction (see e.g. radiation pattern of YAGI antenna)



Radiation pattern of a YAGI antenna

Note : there are regulatory limits on Tx power (e.g. ETSI limits the Tx power to 100mW or 20dBm in Europe for the 2.4GHz ISM band)

(1) BER : Bit Error Rate

huh ? deciBels, you said ???

- **Introduction to deciBels (dB)**
  - Used to express a ratio logarithmically
  - ratio of amplitudes, powers, currents, ...
  - Bel : unit used in acoustics that represents a ratio of 10
  - deciBel = 1/10th of a Bel
  - Different versions for power/amplitude[(1)]
    - Power ratio in dB $= 10 \log(P_1/P_2)$
    - Amplitude ratio in dB $= 20 \log(A_1/A_2)$
  - Why use logarithmic ratios ?
    - smaller numbers for large ratios
    - logarithmic ratios can be added : $\log(a.b) = \log(a) + \log(b)$
  - Absolute powers in dBm
    - $10\ log_{10}$(power in milliWatts)

(1) power ~ square of amplitude

deciBels (dB)

- **Examples - Ratios between two powers**
  - What are the ratios of powers $P_1 = 100$ W and $P_2 = 10$ W expressed in dB ?
    - $P_1 / P_2 = 10 \;\rightarrow\; \text{Ratio}_{\text{dB}} = 10 \log_{10}(P_1 / P_2) = 10 \log_{10}(10) = 10 \text{ dB}$
    - $P_2 / P_1 = 0.1 \;\rightarrow\; \text{Ratio}_{\text{dB}} = 10 \log_{10}(P_2 / P_1) = 10 \log_{10}(0.1) = -10 \text{ dB}$
  - What is the gain G of an antenna rated 6 dBi[(1)] ?
    - $\text{G}_{\text{dB}} = 6 \text{ dBi} = 10 \log_{10}(\text{G})$
    - $\text{G} = 10^{6/10} = 3.98$

6 = 10 log(G)

(1) Note : **dBi** stands for gain in comparison to an *isotropic* antenna (which radiates uniformly in every direction)

deciBels (dB)

Power ratios

P_2 / P_1	dB
10	10
4	6
2	3
1	0
0.5	-3
0.25	-6
0.1	-10

Amplitude ratios

A_2 / A_1	dB
10	20
4	12
2	6
1.414	3
1	0
0.707	-3
0.5	-6
0.25	-12
0.1	-20

deciBels (dB)

- **Examples – Powers in dBm**
  - If a receiver sensitivity is equal to -80 dBM, what is the minimum power in Watts that it must receive ?
    - $-80 \text{ dBm} = 10 \log_{10}(P \text{ in mW })$
    - $P = 10^{(-80/10)} \text{ mW} = 10^{-11} \text{ W}$
  - Express a power of 0.05 mW in dBm
    - $10 \log_{10}(0.05) = -13 \text{ dBm}$

Wireless Link Characteristics (3/12)

- **Free space transmission equation**
  - Question : given transmitted power P_t , what is the amount of power P_r received?
  - Friis transmission equation

$$P_r = G_t G_r P_t \cdot \left(\frac{\lambda}{4 \pi d} \right)^2$$

  - where
    - G_t and G_r are the transmitter and receiver antenna gains, respectively
    - λ is the signal wavelength
    - d is the distance between the transmitter and receiver antennas

Wireless Link Characteristics (4/12)

- **Free space transmission equation**
  - Explanation for Friis equation. Two reasons.

(1) Spreading of signal

- Omnidirectional point source antenna (*isotropic antenna*) → radio signal propagates uniformly in all directions
- Power at distance d from source is equal to power at source divided by area of sphere of radius d

La puissance reçue baisse de manière quadratique avec l'augmentation de la distance

$$S = P_t \cdot \frac{1}{4\pi d^2}$$

- Non-isotropic antennas can radiate energy non uniformly → gain G_t of antenna in a specific direction

Wireless Link Characteristics (5/12)

- **Free space transmission equation**
  - Explanation for Friis equation. Two reasons.

  (2) Antenna aperture
    - Area that captures electromagnetic signal energy (similar to a camera aperture). Indication of how well an antenna will "pick up" received signal.
    - Depends on the signal's wavelength (λ)

Ne pas connaître la formule

$$P_r = S \cdot \frac{\lambda^2}{4\pi} = S \cdot \frac{c^2}{4\pi f^2}$$

- Non isotropic antenna can do better
  $\rightarrow$ receiving gain G_r

Wireless Link Characteristics (6/12)

- **Free space path loss equation**
  - Friis equation often expressed as path loss equation.
  - Expresses attenuation/loss factor of signal power with distance
    - assuming unity antennae gains ($G_t = G_r = 1$)

$$L = \frac{P_t}{P_r} = \frac{1}{\left(\frac{\lambda}{4\pi d}\right)^2} = \left(\frac{4\pi d}{\lambda}\right)^2$$

  - As the wavelength is related to frequency by $\lambda = \frac{c}{f}$, it can also be written

$$L = \left(\frac{4\pi d f}{c}\right)^2$$

  - Pass loss (L) often expressed in deciBels...

Wireless Link Characteristics (7/12)

- **Free space path loss equation**
  - The path loss equation

$$L = \left(\frac{4 \pi d f}{c} \right)^2$$

can be rewritten in a logarithmic form (in dB)

$$L_{dB} = 10.\log_{10}\left(\frac{P_t}{P_r}\right) = 10.\log_{10}\left(\left(\frac{4 \pi d f}{c}\right)^2\right)$$

$$= 20 \log_{10}(d) + 20 \log_{10}(f) + C_1$$

constant

$$= 20 \log_{10}(d) + C_2$$

if fixed frequency

Wireless Link Characteristics (8/12)

- **Example**
  - Frequency 2.4 GHz
  - Distances 10 m and 100 m
  - What are the attenuations in dB ?

  - For convenience, frequency is often expressed in MHz and distance in kilometers. In this case, the path loss can be obtained with

$$L_{dB} = 20\log_{10}(d) + 20\log_{10}(f) + 32.45\,dB$$

  - $L(10\text{ m}) = 60\text{ dB}$
  - $L(100\text{ m}) = 80\text{ dB}$

$$32.45\,dB = 10.\log_{10}\left(\left(10^{9}.\frac{4.\pi}{c}\right)^{2}\right)$$

where factor 10^9 comes from the conversions from km and MHz

Wireless Link Characteristics (9/12)

Free space path loss equation

- A generalized version of the path loss equation is used for non-free space propagation (to take into account fading)

$$L_{dB} = 10.\gamma.\log_{10}(d) + C$$

- The value of γ (*loss factor*) depends on the environment. It usually ranges from 2 to 6.

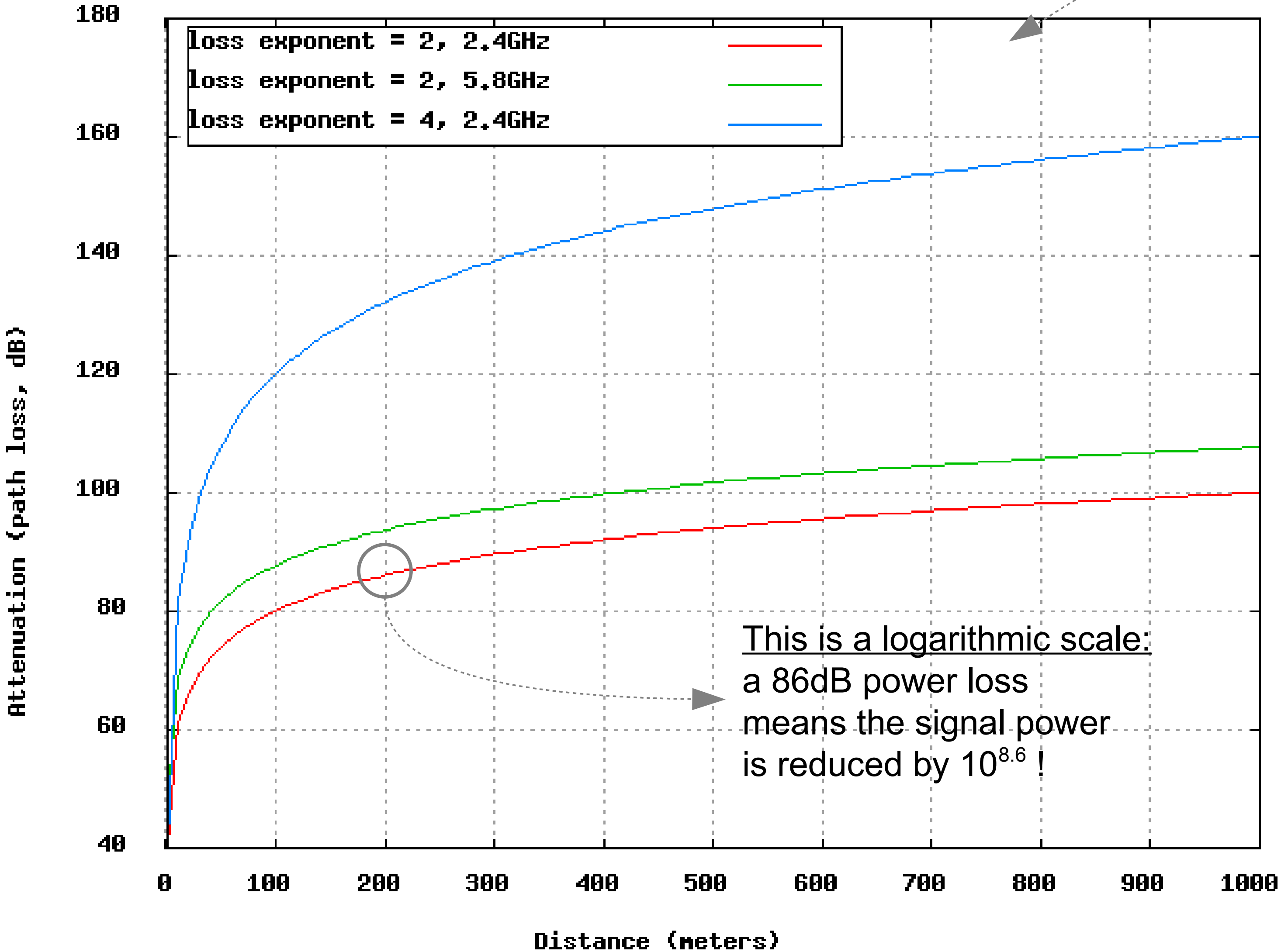
Environment	Path loss exponent (γ)
Free space	2
Urban area	2.7 to 3.5
Suburban area	3 to 5
Indoor (line-of-sight)	1.6 to 1.8

car signal rebondis contre les murs proches

Source : EE4367 Telecom. Switching and Transmission, M. Torlak (University of Texas, Dallas)

Simple Path Loss Model

$$L_{dB} = 10\,\gamma \log_{10}(d) + C$$



This is a logarithmic scale:
a 86dB power loss
means the signal power
is reduced by $10^{8.6}$!

Note : here, $C = 10\log_{10}\left(\left(\frac{4\,pi\,f}{c}\right)^2\right)$

Wireless Link Characteristics (10/12)

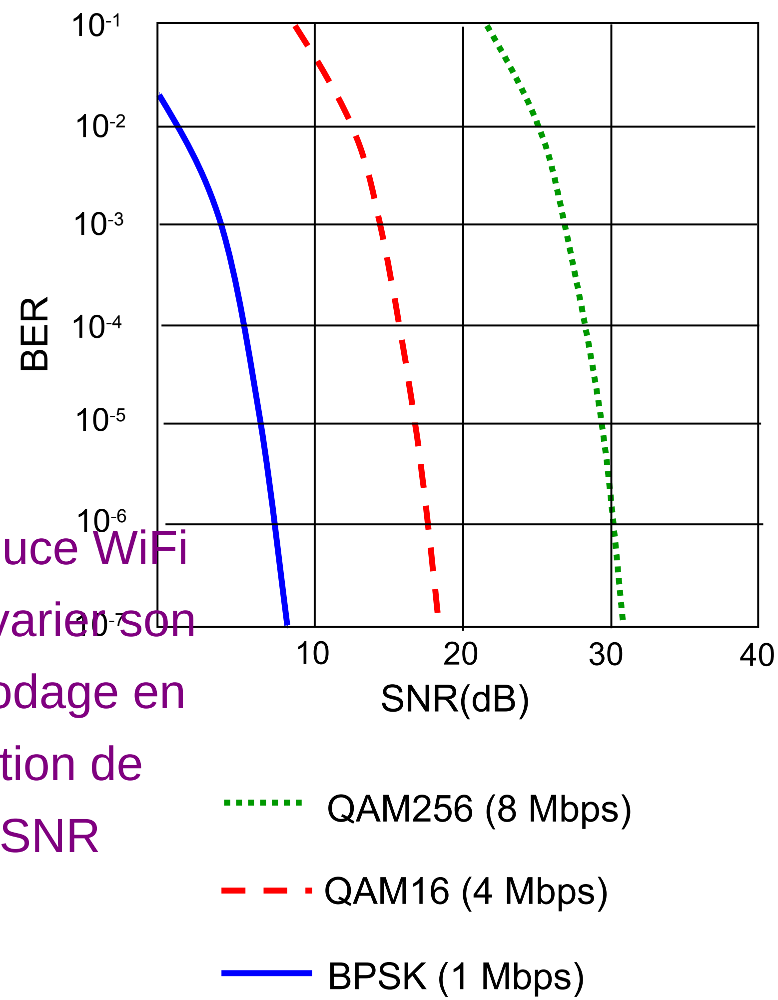
SNR : signal-to-noise ratio

- larger SNR – easier to extract signal from noise (a "good thing")

SNR versus BER tradeoffs

- *given physical layer :* increase power → increase SNR → decrease BER
- *given SNR :* choose physical layer that meets BER requirement, giving highest throughput
  - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)

La puce WiFi fait varier son encodage en fonction de son SNR

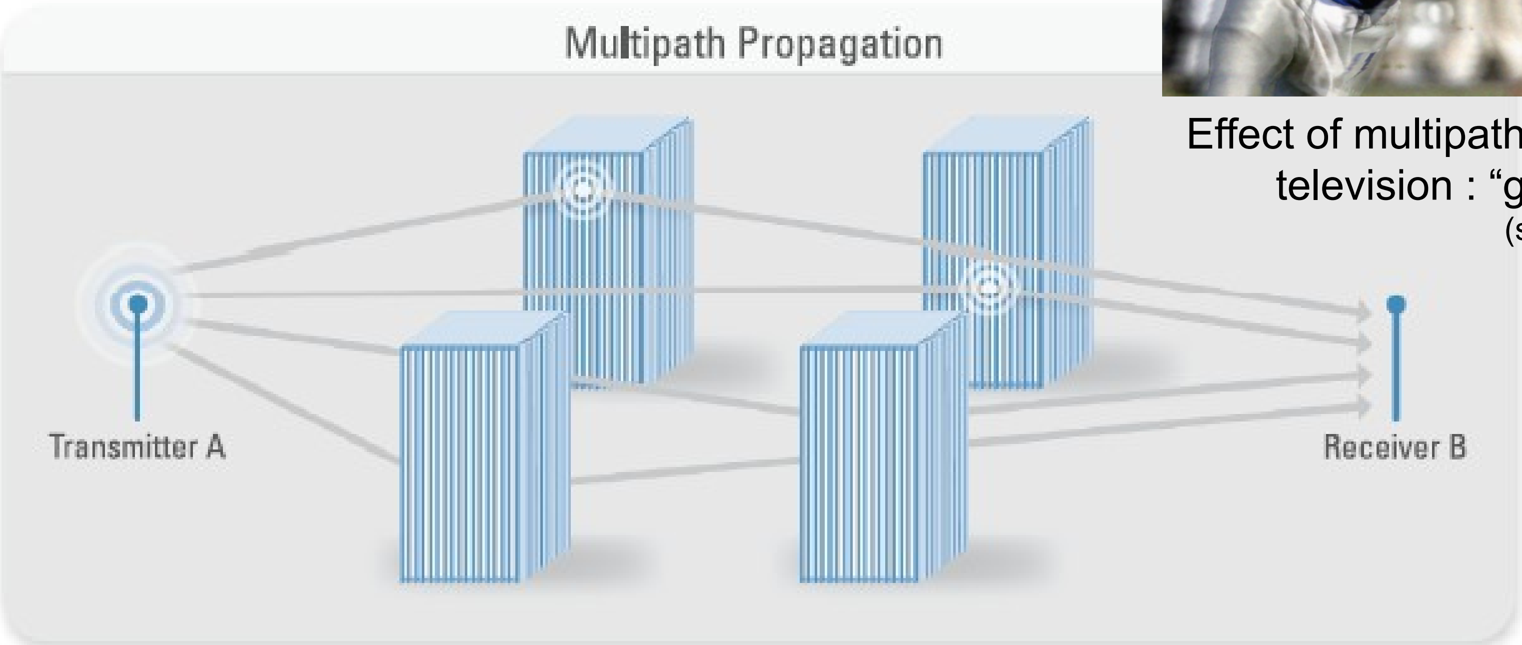


Ne pas savoir, compétence Télécom...

Wireless Link Characteristics (11/12)

Multi-path propagation

- Receiver gets signal composed of direct path signal + reflected components



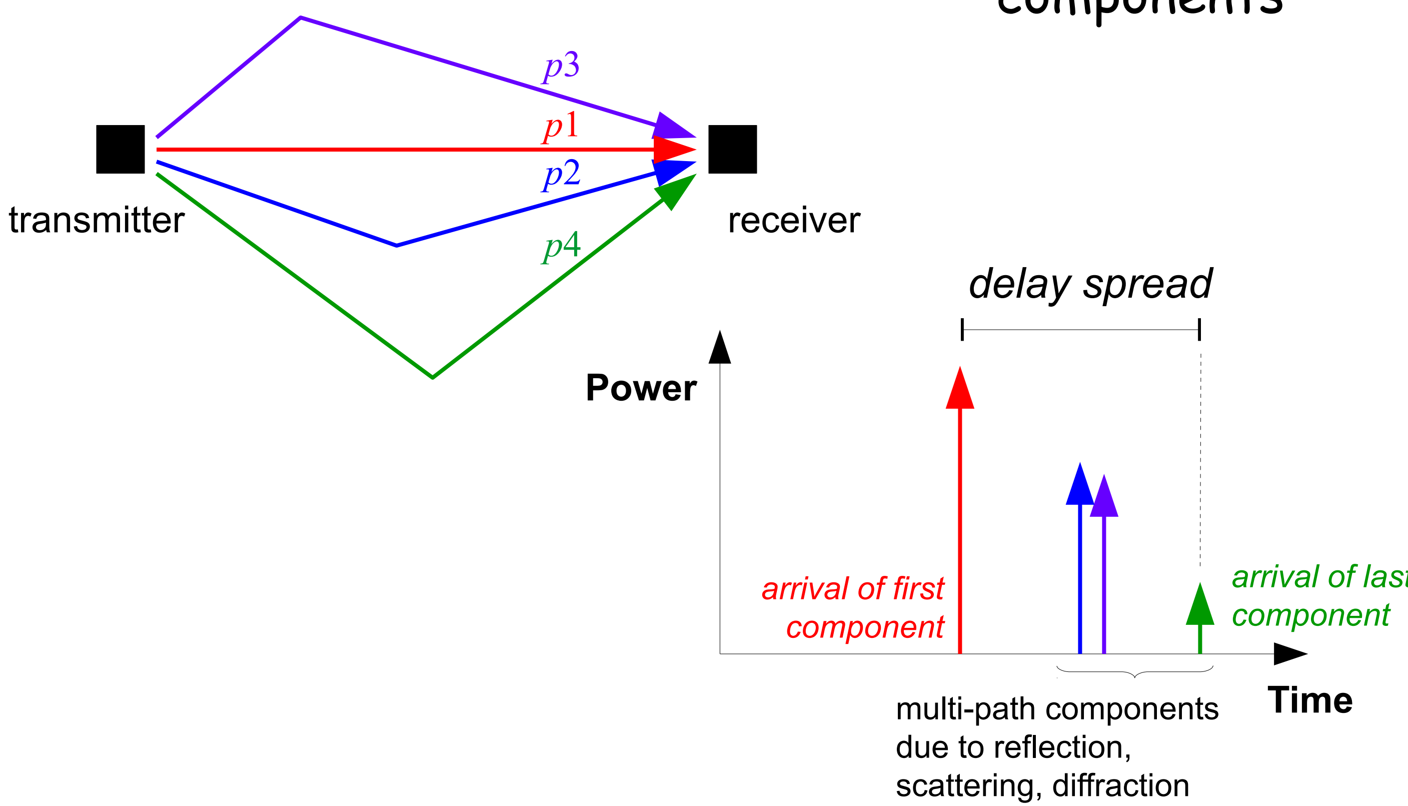
Effect of multipath in broadcast television : “ghost images”
(source: wikipedia)

Source: National Instruments, Testing Wireless Receivers with Recorded RF Spectrum
http://zone.ni.com/devzone/cda/pub/p/id/197

Wireless Link Characteristics (12/12)

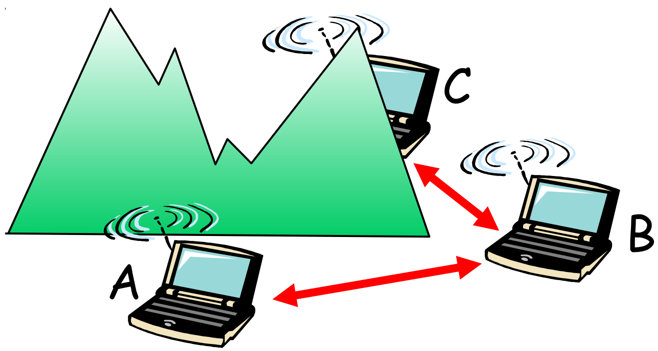
Multi-path propagation

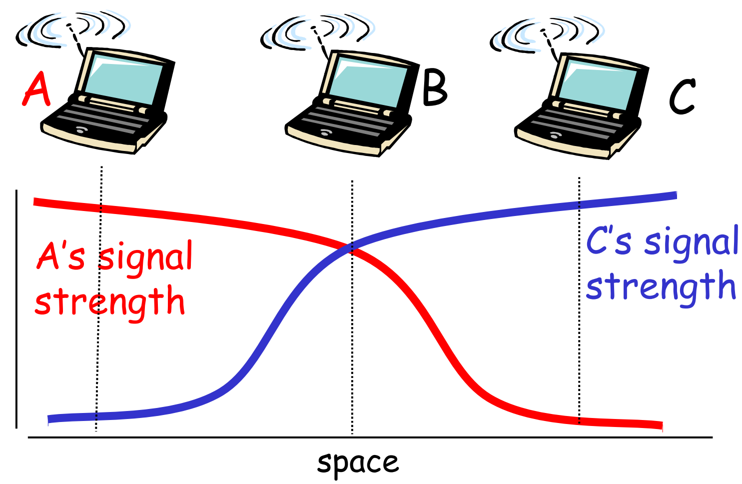
- *delay spread* : delay between arrival of first and last components



Wireless network characteristics (1/2)

Multiple wireless senders and receivers create additional problems (beyond multiple access):





Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other

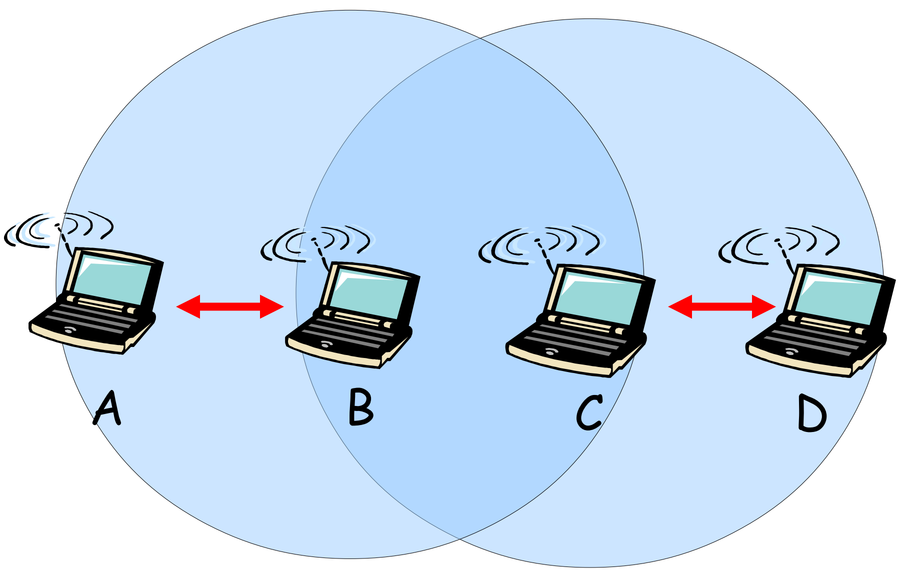
means A, C unaware of their interference at B

Signal attenuation

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

Wireless network characteristics (2/2)

Multiple wireless senders and receivers create additional problems (beyond multiple access):



Exposed terminal problem

- B and C hear each other
- A can't hear C
- D can't hear B
- B and C not willing to send simultaneously to A and D respectively (due so CSMA)

Chapter 6 outline

6.1 Introduction

Wireless

- 6.2 Wireless links, characteristics
  - Spread spectrum
- 6.3 IEEE 802.11 wireless LANs (“wi-fi”)
- 6.4 cellular Internet access
  - architecture
  - standards (e.g., GSM)

Mobility

- 6.5 Principles: addressing and routing to mobile users
- 6.6 Mobile IP
- 6.7 Handling mobility in cellular networks
- 6.8 Mobility and higher-layer protocols

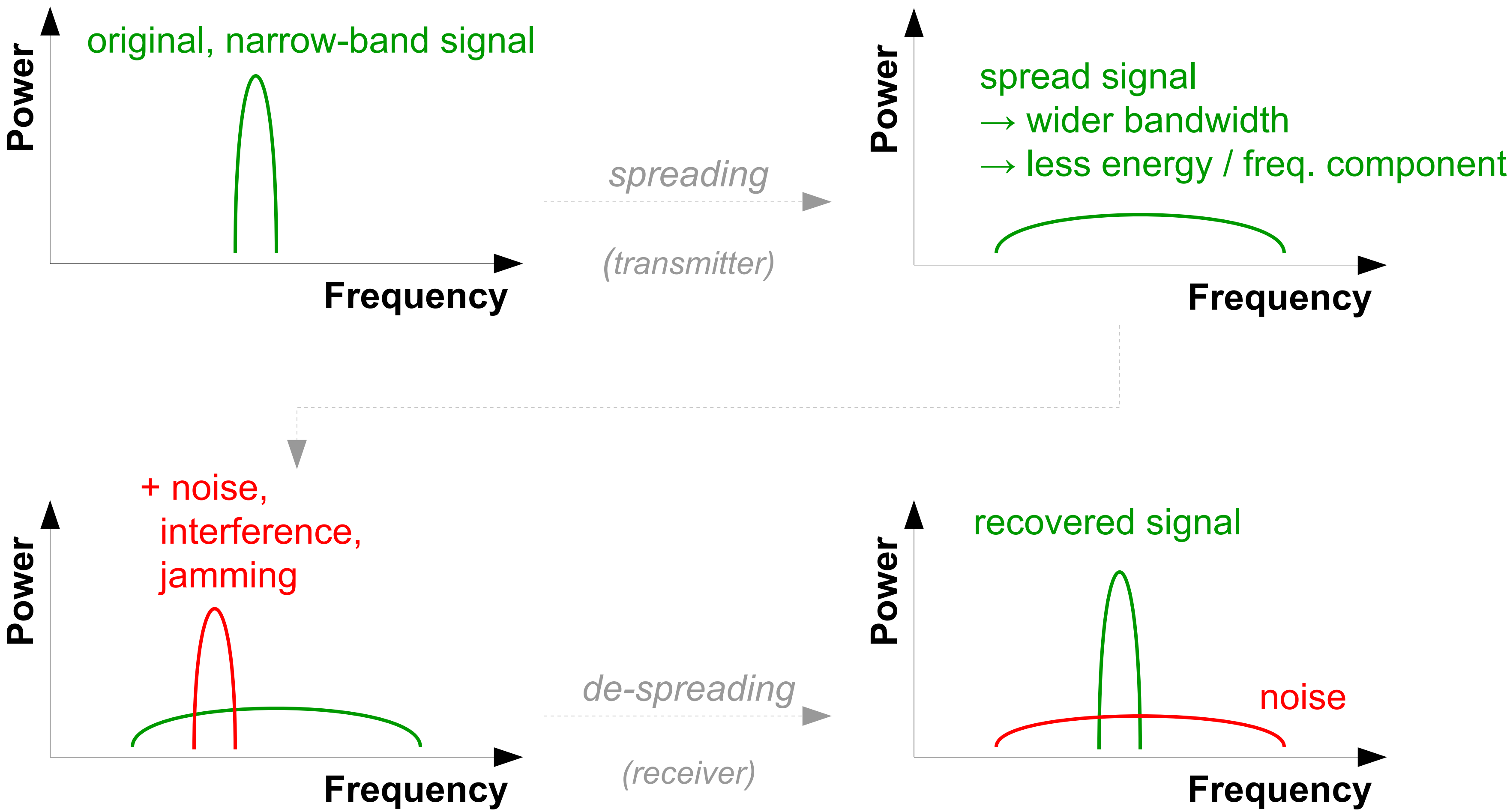
6.9 Summary

Spread Spectrum

Introduction

- Initially developped for "military and intelligence requirements" [Stallings 2011]
- Spread signal over larger bandwidth thanks to spreading code (usually pseudorandom)
  - jamming and interference more complex
  - hiding signal : receiver must know spreading code
  - multiplex several communications (CDMA)
- Different techniques
  - *Frequency-Hopping Spread Spectrum* (FHSS)
  - *Direct Sequence Spread Spectrum* (DSSS)
- Today, used in several wireless broadcast channels standards (cellular, satellite, etc)

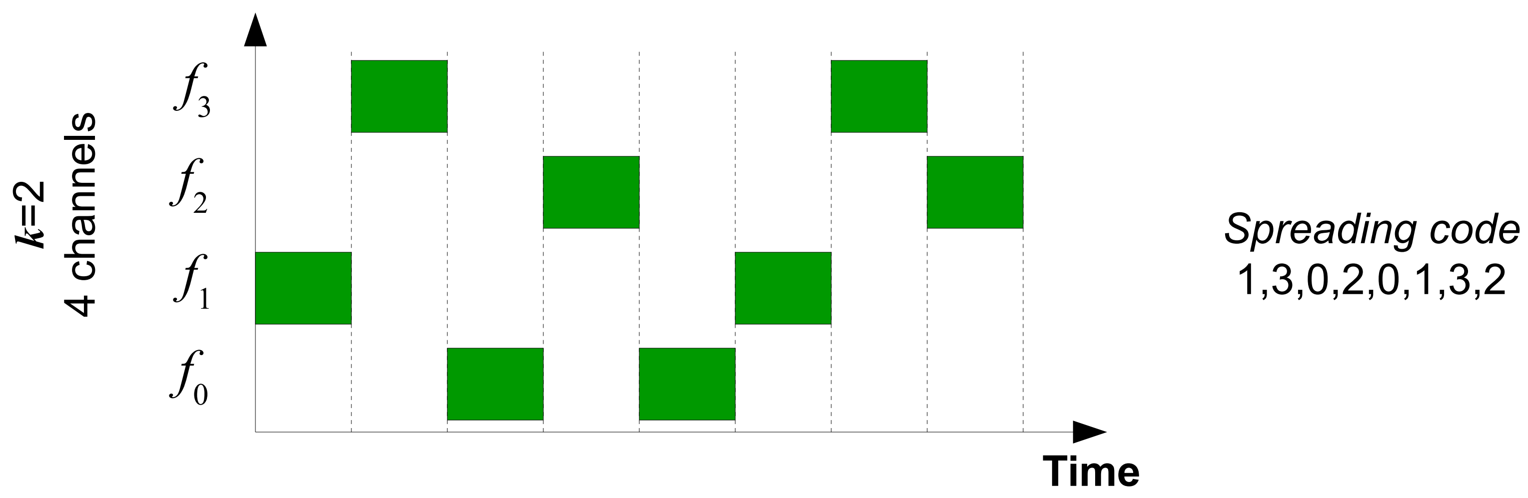
Spread Spectrum



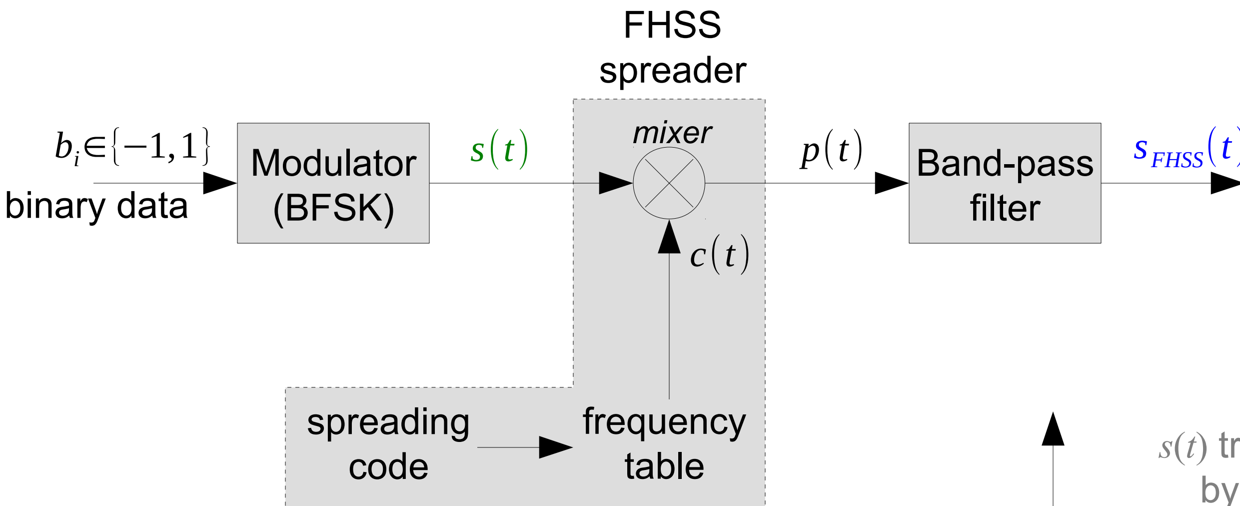
Frequency-Hopping Spread Spectrum (FHSS)

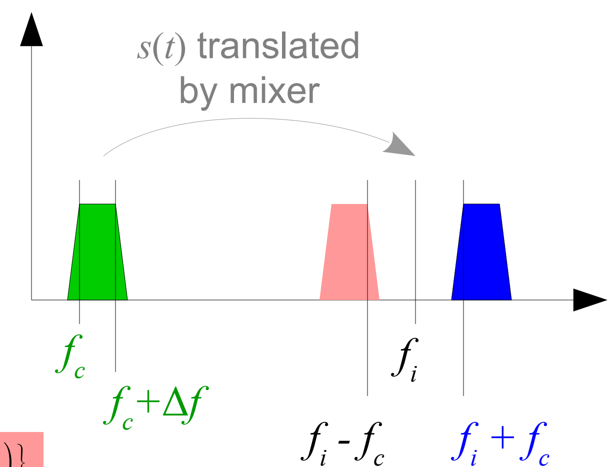
Principle

- 2^k channels of different frequencies allocated
  (bandwidth of each channel = bandwidth of signal to send)
- one channel used at a time for a fixed duration
- current channel dictated by spreading code (receiver must use same channel sequence)



Frequency-Hopping Spread Spectrum (FHSS)





$$s(t) = A\cos(2\pi(f_c + 0.5(1+b_i)\Delta f)t)$$

$$c(t) = A\cos(2\pi f_i t)$$

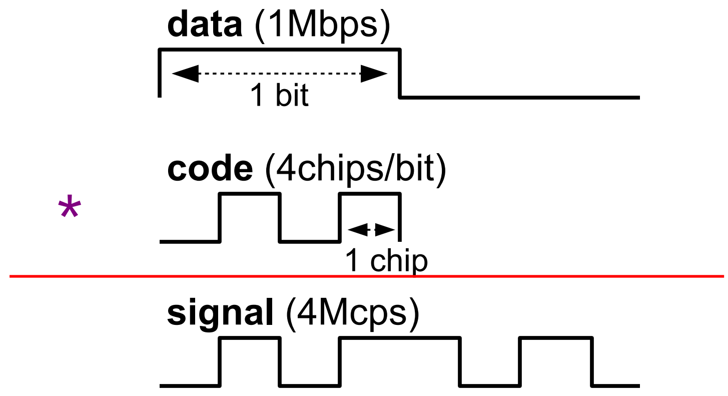
$$\begin{aligned} p(t) &= c(t).s(t) \\ &= A\cos(2\pi(f_c + 0.5(1+b_i)\Delta f)t)\cos(2\pi f_i t) \\ &= \frac{A}{2}\{\cos(2\pi(f_c + 0.5(1+b_i) + f_i)t) + \underbrace{\cos(2\pi(f_c + 0.5(1+b_i) - f_i)t)\}}_{\text{removed by band-pass filter}} \end{aligned}$$

$$s_{FHSS}(t) = \frac{A}{2}\cos(2\pi(f_c + 0.5(1+b_i) + f_i)t)$$

Direct Sequence Spread Spectrum (DSSS)

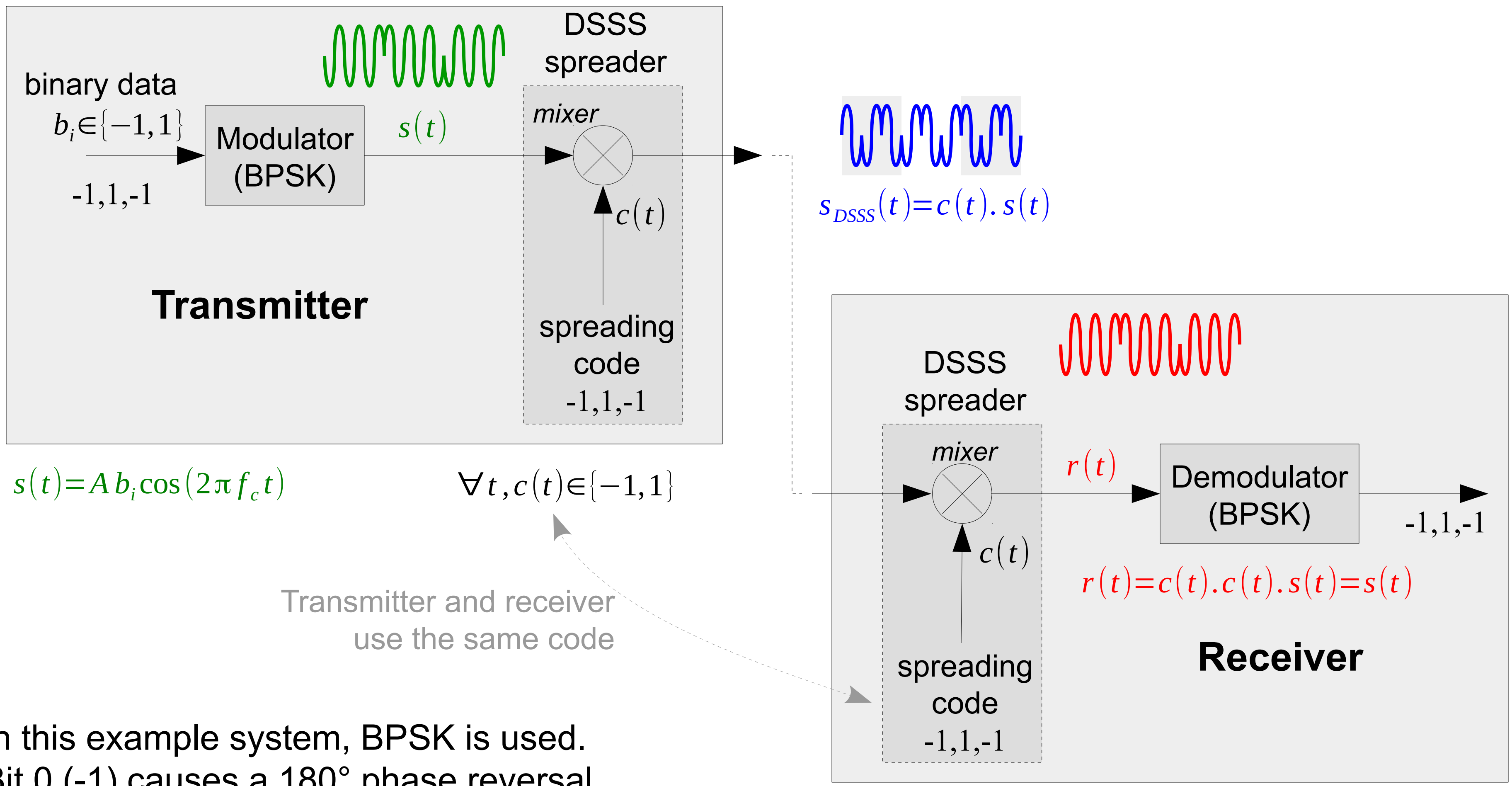
Principle

- each bit b_i in input data represented by sequence of N bits in translated signal, using a spreading code
- combination of input signal and spreading code usually done with XOR
- consequence : bandwidth of transmitted signal N times larger than input signal (spreading)



- Encoding : signal = data bit stream encoded with chipping sequence
- Decoding : dot-product of signal and chipping sequence

Direct Sequence Spread Spectrum (DSSS)



In this example system, BPSK is used.
Bit 0 (-1) causes a 180° phase reversal.
The spreading code causes additional phase shifts.

Code Division Multiple Access (CDMA)

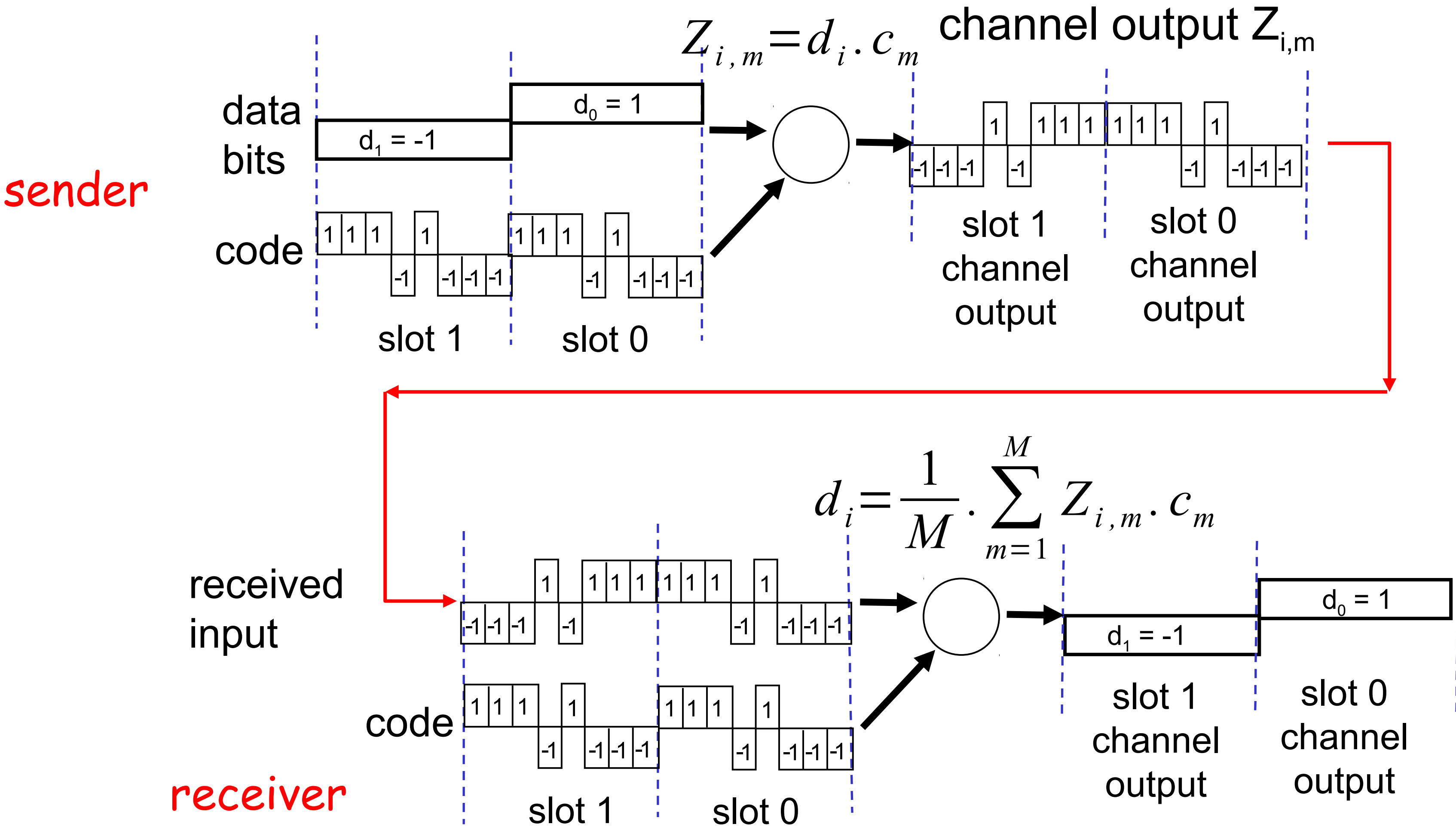
Introduction

- Same principle as DSSS... but used to multiplex several communications on the same channel
- Each user assigned a unique N-bits code (or chipping sequence)
- Codes orthogonal[(1)] to each other, i.e. their dot product is null

- Example : a and b are orthogonal codes
  - $a = 1,1,1,\text{-}1,1,\text{-}1,\text{-}1,\text{-}1$
  - $b = 1,\text{-}1,1,1,1,\text{-}1,1,1$

$$
\begin{aligned}
a \cdot b &= \sum_{i=1}^{M} a_i b_i \\
&= 1 + (-1) + 1 + (-1) + 1 + 1 + (-1) + (-1) \\
&= 0
\end{aligned}
$$

CDMA - Example



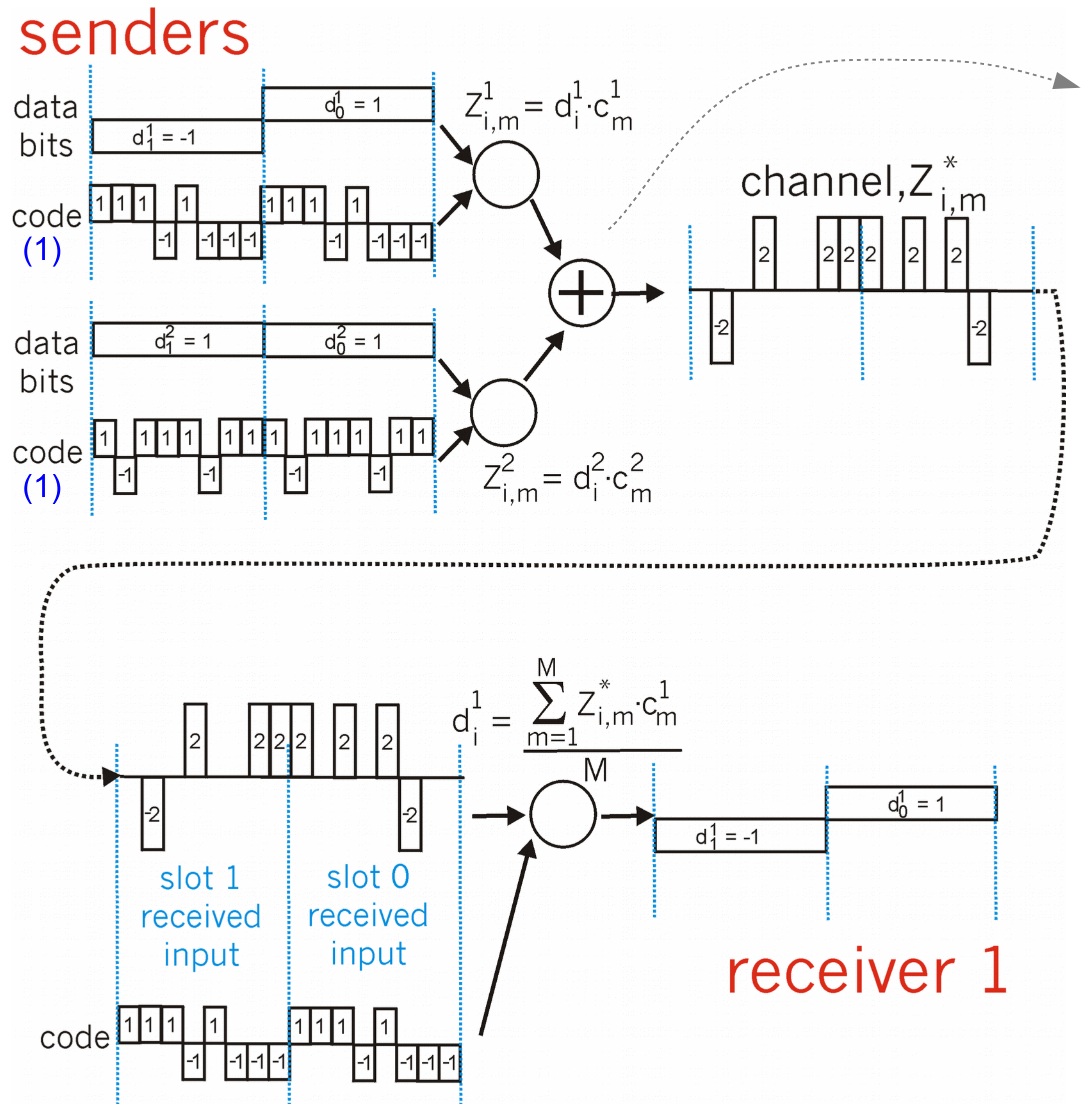
Addition de produits divisé par le nombre de chips

Note: data bit 0 = -1 ; data bit 1 = 1 ; no data = 0

CDMA - Example

sent signal = sum
of all senders' signals

$$Z^*_{i,m} = \sum_{s=1}^{N} Z^s_{i,m}$$



Les chips impliquent une fréquence supérieure ! (0 et 1 = une période normale; avec les chips, c'est le nombre de chips * le 0 et le nombre de chips * 1 qui va définir la période)
Dans ce cas : fréquence max = 8 fois celle des 0 et 1 "normaux"

(1) Note : you can check that those codes are orthogonal (their dot product is null).

Generating orthogonal codes

Walsh codes

- generated using *Hadamard matrices, defined recursively as*

$$W_1 = (1) \qquad W_{2n} = \begin{pmatrix} W_n & W_n \\ W_n & \overline{W_n} \end{pmatrix}$$

- leading to

$$W_1 = (1) \qquad W_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad W_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \qquad \ldots$$

- Check that rows in W_4 are orthogonal

$$(1,1,1,1) \cdot (1,-1,1,-1) = 1 + (-1) + 1 + (-1) = 0$$

$$(1,1,1,1) \cdot (1,1,-1,-1) = 1 + 1 + (-1) + (-1) = 0$$

$$\ldots$$

Orthogonal Frequency Division Multiplexing (OFDM)

Principles

- multi-carrier modulation
- similar to FDM... but all channels used by the same source
- some of the bits send on each channel
- better bandwidth usage than traditional FDM as channels are more tightly packed
- bitrate on each channel = $1/N$ of total bitrate (if N channels) $\rightarrow$ more robust to multi-path propagation and inter-symbol interference (ISI)

- orthogonality in the OFDM context has a different meaning : it is related to proper channel frequency spacing.

Chapter 6 outline

6.1 Introduction

Wireless

- 6.2 Wireless links, characteristics
  - Spread spectrum
- 6.3 IEEE 802.11 wireless LANs ("wi-fi")
- 6.4 cellular Internet access
  - architecture
  - standards (e.g., GSM)

Mobility

- 6.5 Principles: addressing and routing to mobile users
- 6.6 Mobile IP
- 6.7 Handling mobility in cellular networks
- 6.8 Mobility and higher-layer protocols

6.9 Summary

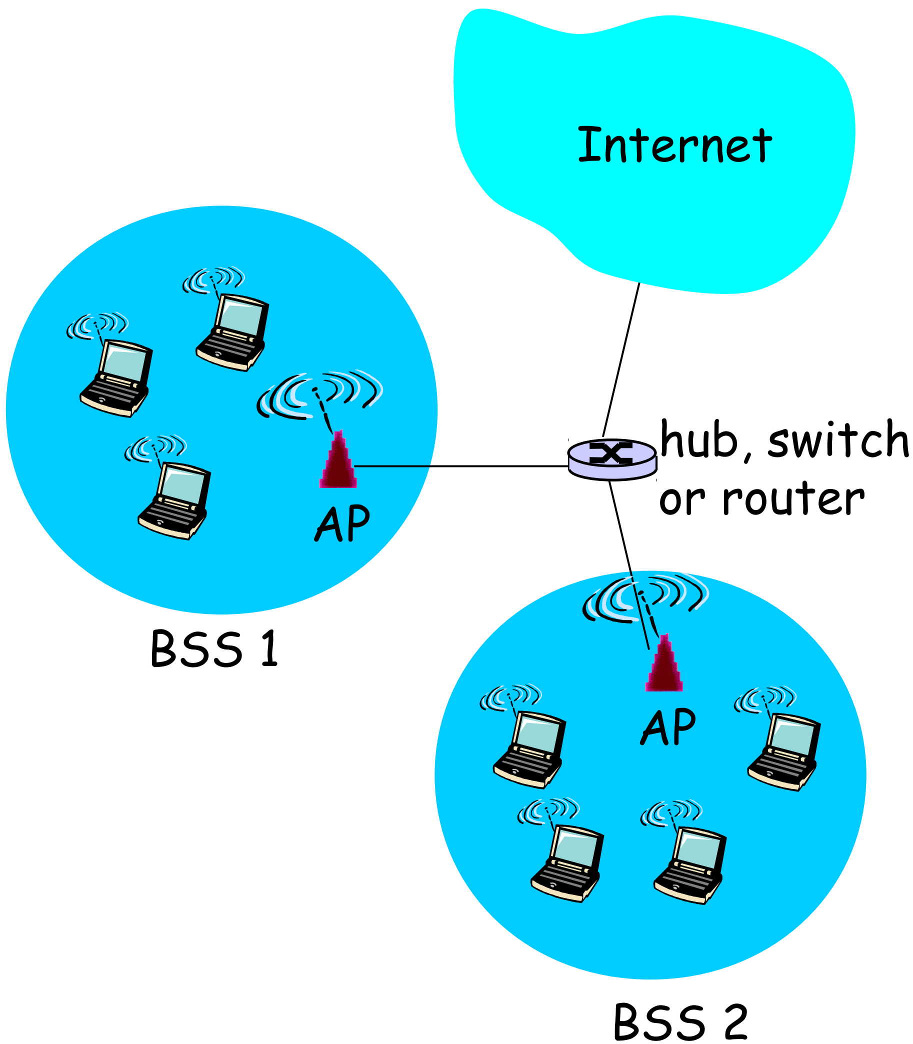
IEEE 802.11 (Wireless LAN)

Version	Year	PHY	Frequency range (GHz)	Peak rate (Mbps)
802.11 (legacy)	1997	FHSS[1]/DSSS	2.4-2.485	2
802.11b	1999	DSSS	2.4-2.485	11
802.11a	1999	OFDM[2]	5.1-5.8	54
802.11g	2003	OFDM	2.4-2.485	54
802.11n	2009	OFDM	2.4-2.485 5.1-5.8	600
802.11ac	2013	OFDM	5.1-5.8	~7000
...				

- all use CSMA/CA for multiple access
- all have infrastructure and ad-hoc network versions

(1) FHSS : *Frequency Hopping Spread Spectrum*
(2) OFDM : *Orthogonal Frequency Division Multiplexing*

802.11 LAN architecture



- Wireless host communicates with base station
  - base station = access point (AP)

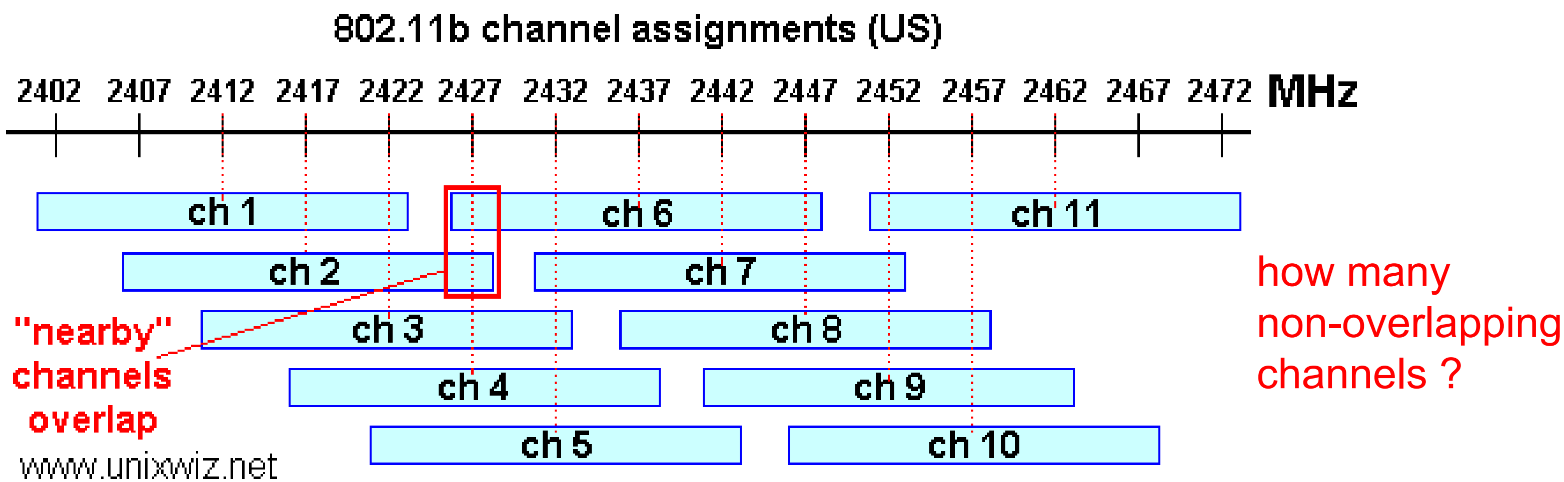
AP + stations connectées = BSS

- Basic Service Set (BSS) (aka "cell")
  - in <u>infrastructure mode</u>, contains wireless hosts and access point
  - in <u>ad hoc mode</u> (IBSS – Independent BSS), contains hosts only

802.11 Channels

802.11b

- **2.4GHz-2.485GHz** spectrum divided into **11 22MHz** channels at different frequencies (13 channels allowed in Europe)

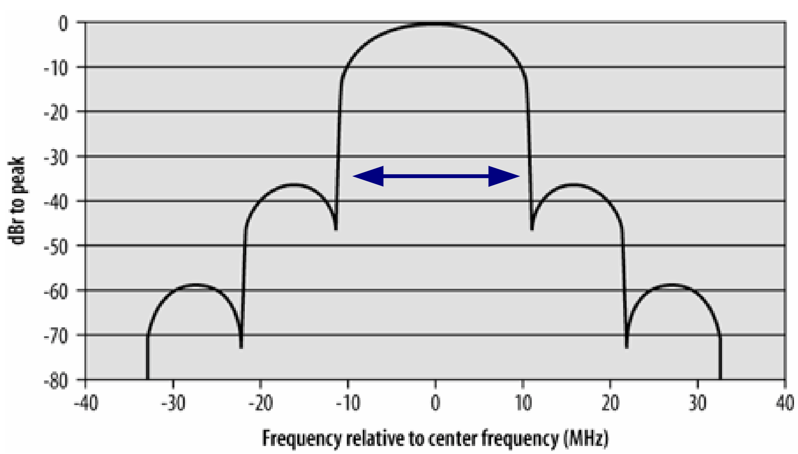


- AP admin must choose
  - frequency (channel) for AP
  - interference possible: channel can be same as or overlap with that chosen by neighboring AP !

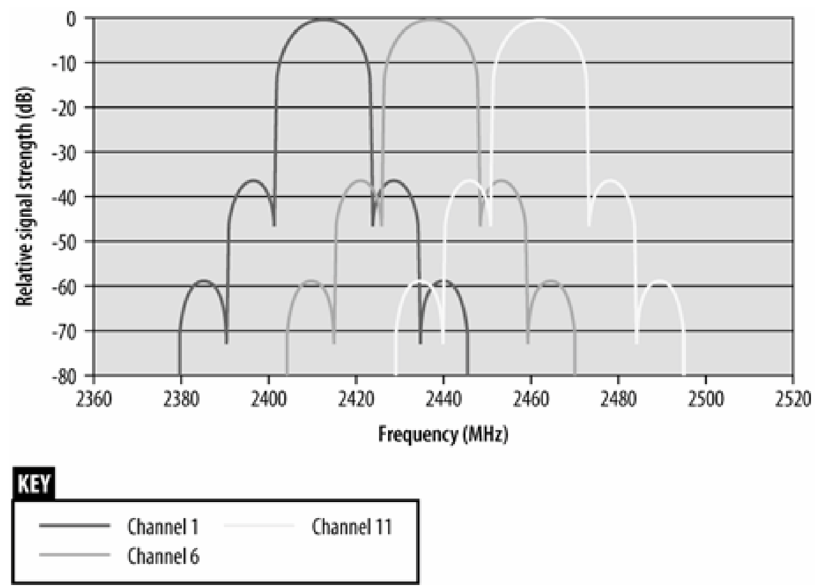
802.11 Channels

802.11b

- **2.4GHz-2.485GHz** spectrum divided into **11 22MHz** channels at different frequencies (13 channels allowed in Europe)



main lobe has ~22MHz bandwidth



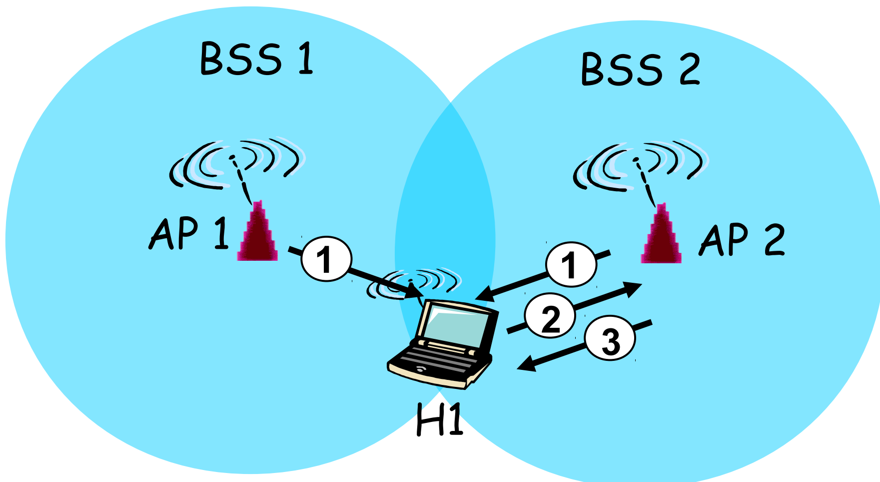
Interference exists even between the less overlapping channels

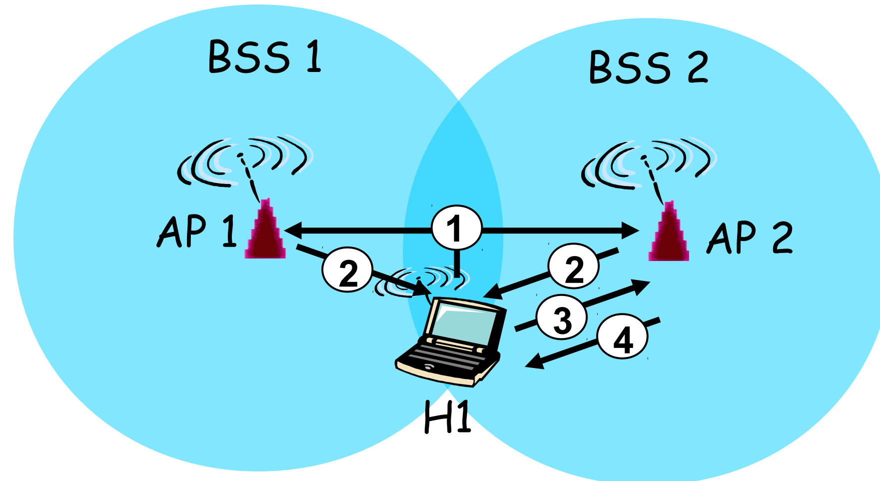
802.11 Association

Wifi jungle

- Several APs available at a single location
- Each AP should have a unique *Service Set Identifier* (SSID) assigned by AP admin
- Host's NIC must *associate* with a single AP, i.e. create a *"virtual wire"* with AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication
  - Host will then typically run DHCP to get IP address in AP's subnet

802.11 : passive/active scanning





Passive Scanning

(1) Beacon frames periodically sent from APs (contains SSID + MAC address)

(2) Association Request frame sent: H1 to selected AP

(3) Association Response frame sent: selected AP to H1

Active Scanning

(1) Probe Request frame broadcast from H1

(2) Probe Response frames sent from APs

(3) Association Request frame sent: H1 to selected AP

(4) Association Response frame sent: selected AP to H1

```
IEEE 802.11 Beacon frame
    Type/Subtype: Beacon frame (0x08)
    [...]
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: 5c:33:8e:17:dd:39 (5c:33:8e:17:dd:39)
    BSS Id: 5c:33:8e:17:dd:39 (5c:33:8e:17:dd:39)
    Frame check sequence: 0x4fb89df2 [correct]
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x000000C3695C3181
        Beacon Interval: 0.102400 [Seconds]
        Capability Information: 0x0431
        [...]
    Tagged parameters (117 bytes)
        SSID parameter set
            Tag Number: 0 (SSID parameter set)
            Tag length: 6
            Tag interpretation:
                VBNET2: "VBNET2"
        Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) 6.0 9.0 12.0 18.0
            Tag Number: 1 (Supported Rates)
            Tag length: 8
            Tag interpretation:
                Supported rates:
                    1.0(B) 2.0(B) 5.5(B) 11.0(B) 6.0 9.0 12.0 18.0  [Mbit/sec]
        Extended Supported Rates: 24.0 36.0 48.0 54.0
            Tag Number: 50 (Extended Supported Rates)
            Tag length: 4
            Tag interpretation:
                Supported rates:
                    24.0 36.0 48.0 54.0  [Mbit/sec]
        [...]
```

Set of Basic Rates
Thoses rates are mandatory
for joining this BSS

802.11 : passive/active scanning

Which AP to select ?

- Selection algorithm not specified in 802.11 standard
  - left to the implementor

- Some possible hints
  - NIC provides indication of *Received Signal Strength* (RSS) that can be used to pick the strongest AP
  - Some APs might need authentication (not open)
  - Some APs might be more loaded than others
  - Several APs might be using the same channel (leading to interference and reduced bandwidth)

802.11 Multiple Access

Challenges for the MAC

- **RF Link Quality**
  - On a wired network, it was reasonable to assume a transmitted frame will be received. Not true for wireless links → use of positive ACKs
- **Collision detection impossible**
  - CSMA/CD cannot be applied : an RF transceiver is either in transmit or receive state (half-duplex), not both at the same time → *avoid collisions :* CSMA/CA (*Collision Avoidance*)
- **Hidden node problem**
  - Reservation mechanism to prevent collisions → use of special RTS/CTS frames (resp. *Request/Clear To Send*)

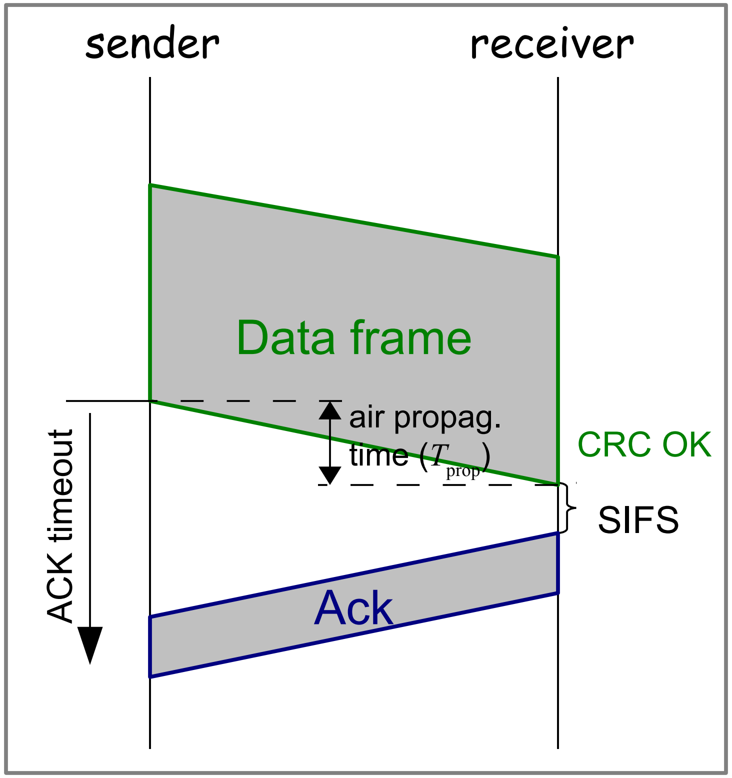
802.11 ACK frames & retransmissions

Positive ACKs

- Sender operation
  - send frame
  - wait for ACK
  - **if** (no ACK within timeout) **then** retransmit frame
- Receiver operation
  - **if** (CRC of received frame = OK) **then** wait SIFS
    send ACK frame

ACK timeout value

- depends on PHY layer
- timeout ≈ SIFS + 2 * T_{prop}



SIFS (*Single InterFrame Space*)
16us for 802.11a
10us for 802.11b/g
10/16us for 802.11n 2.4/5GHz
$2T_{prop}$ ≤ 1us

Pas connaître

SIFS : temps pour passerdu mode Tx à Rx

802.11 ACK frames & retransmissions

Duplicate frames

- It is possible that the same frame is received more than once due to retransmissions (e.g. due to lost ACKs)
- To filter duplicate frames, a 12-bits Sequence Control field is incorporated in the frame header.

802.11 Multiple Access

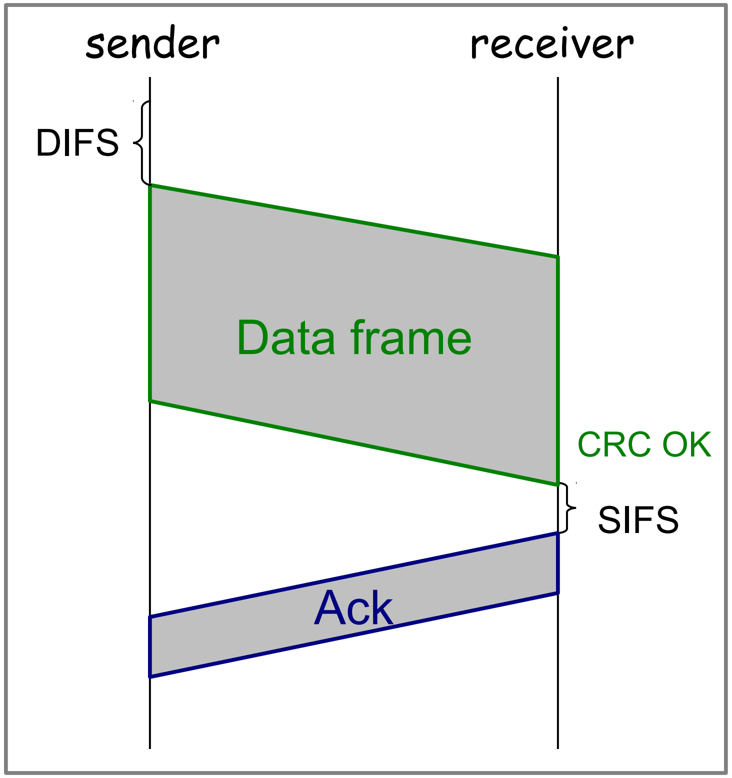
Access Modes

- **Distributed Coordination Function (DCF)**
  - Basic CSMA/CA mechanism : check link is clear before transmitting (CSMA). To avoid collisions, stations use a random backoff after each frame. Can optionally rely on RTS/CTS exchanges.
- **Point Coordination Function (PCF)**
  - Contention-free service, only available in infrastructure mode (AP = coordinator). Use of PIFS to gain priority channel access.
- **Hybrid Coordination Function (HCF)**
  - Half-way between DCF and PCF for applications that need better than best-effort but not with the constraints of PCF.

802.11 MAC Protocol: DCF (1/4)

Sender operation

1. if sense channel idle[1] for **DIFS** then
   - transmit entire frame (no collision detection)
2. if sense channel busy then
   - defer frame transmission
   - wait random time : start random backoff timer
   - timer counts down while channel idle (frozen when channel busy)
   - transmit when timer expires
   - if no ACK, increase random backoff window, repeat step 2



DIFS (*Distributed InterFrame Space*)
34us for 802.11a
50us for 802.11b
28us for 802.11g
28/34us for 802.11n 2.4/5GHz

(1) channel sensing = *Clear Channel Assessment* (CCA)

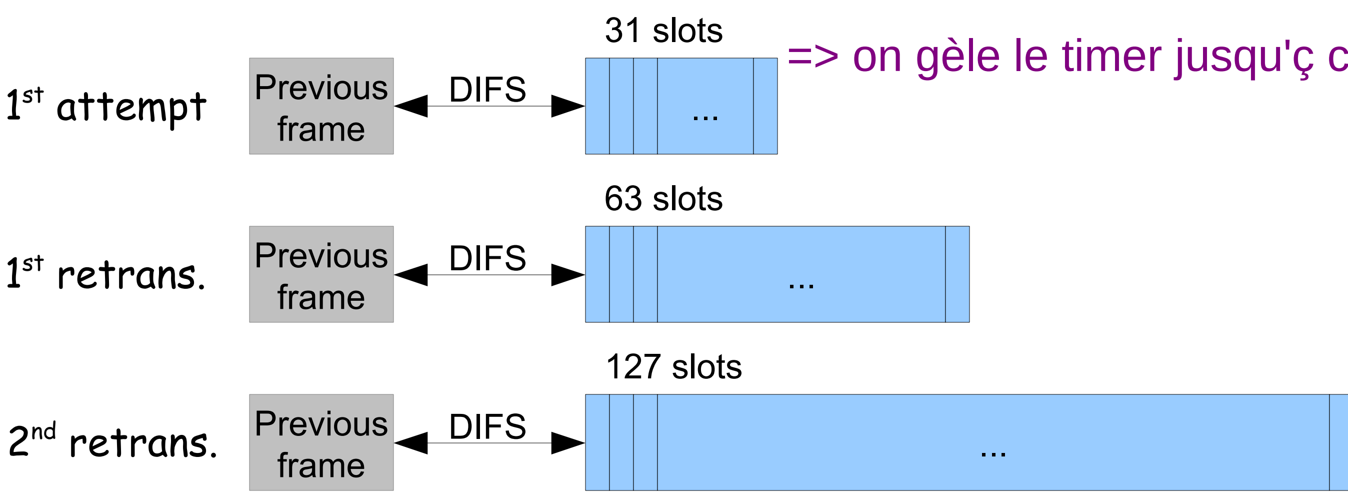
802.11 MAC Protocol: DCF (2/4)

Exponential backoff

- Principle : after DIFS, transmission slot is picked randomly within a contention window (CW). The size of CW increases exponentially (doubles) with the number of retransmissions.
- Default CW size = 31 slots of 20us (802.11b). Can go up to 1023 slots.

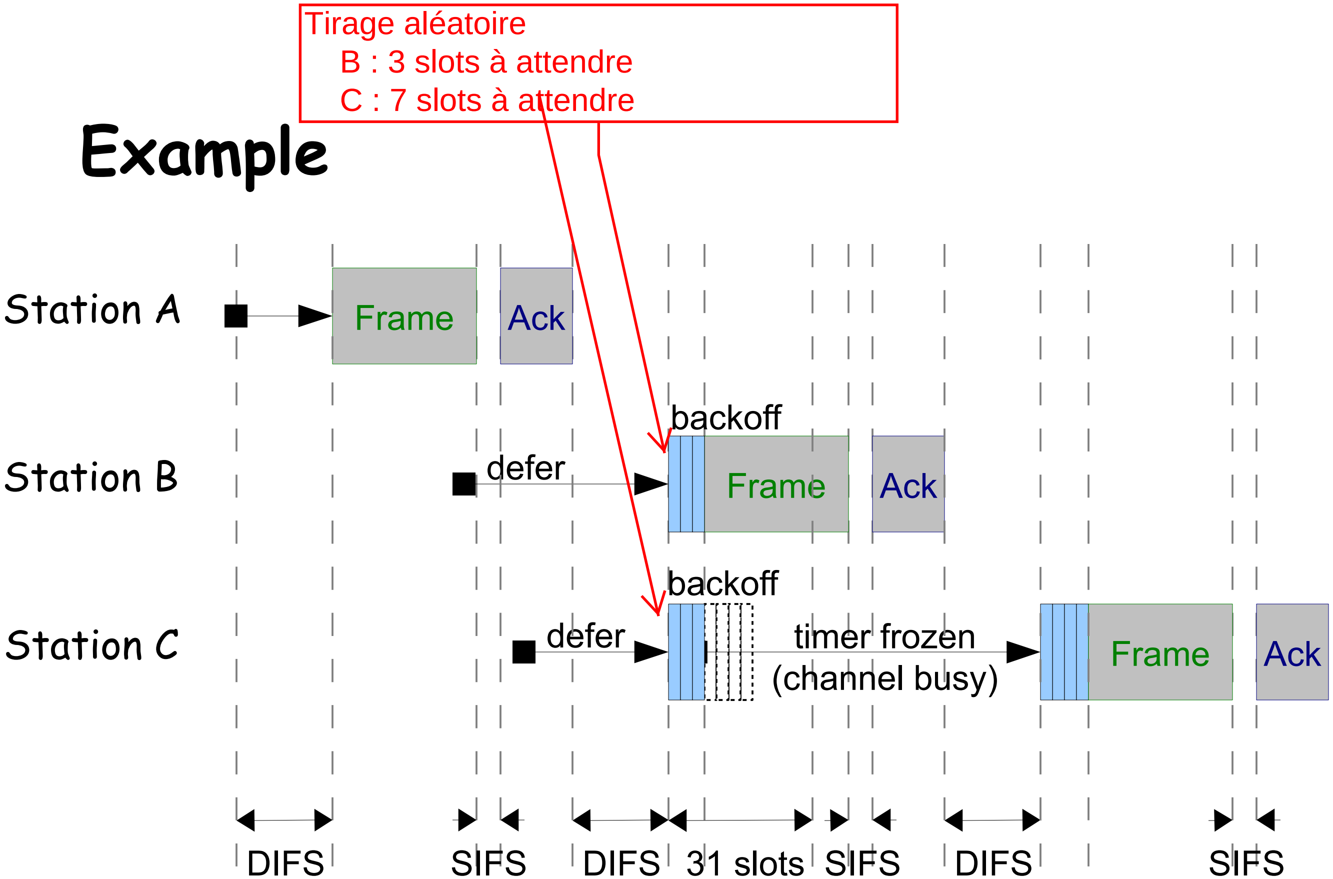
Lorsqu'on a un slot libre, on le "réserve"

=> on gèle le timer jusqu'ç ce que le canal soit libre



802.11 MAC Protocol: DCF (3/4)

Example

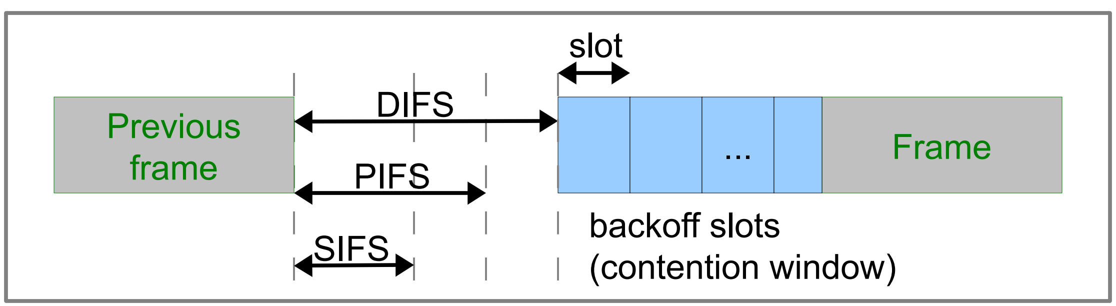


Note : in the above illustration, the boundaries of the SIFS, DIFS and backoff slots are perfectly aligned. However, in practice, due to the propagation delay, they are not : nodes do not sense the channel idle at the same time.

802.11 MAC Protocol: DCF (4/4)

Different Inter-Frame Spaces (IFS)

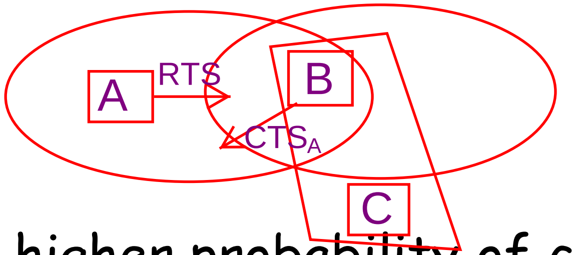
- **SIFS** (Short IFS)
  - mainly time to change the transceiver state from Rx to Tx[1].
- **DIFS** (Distributed IFS)[2]
  - > SIFS to prioritize shorter frames (ACK, CTS).
  - DIFS = SIFS + 2*slotTime
- **PIFS** (PCF IFS)
  - defined such as SIFS < PIFS < DIFS
  - PIFS = SIFS + slotTime



Slot time
- 9us for 802.11a
- 20us for 802.11b
- 9/20us for 802.11g
- 9/20us for 802.11n

(1) aRxTxTurnaroundTime, typically 2-5us, depending on PHY
(2) A longer EIFS replaces DIFS after a transmission error.

802.11 RTS / CTS mechanism (1/3)



Si pas de CTS, C ne pourrait ne pas être au courant que A a demandé RTS

Observation

- long frames = higher probability of collision in presence of hidden terminals

Idea : allow sender to "*reserve*" channel rather than random access of data frames → avoid collisions of long data frames

1. Sender first transmits *Request-To-Send* (RTS) frame using CSMA. RTS frames may collide with each other (but they're short)
2. BS broadcasts *Clear-To-Send* (CTS) in response to RTS frame. CTS frame heard by all nodes in BSS. Other stations defer transmissions
3. Sender transmits data frame
4. Receiver Acks data frame

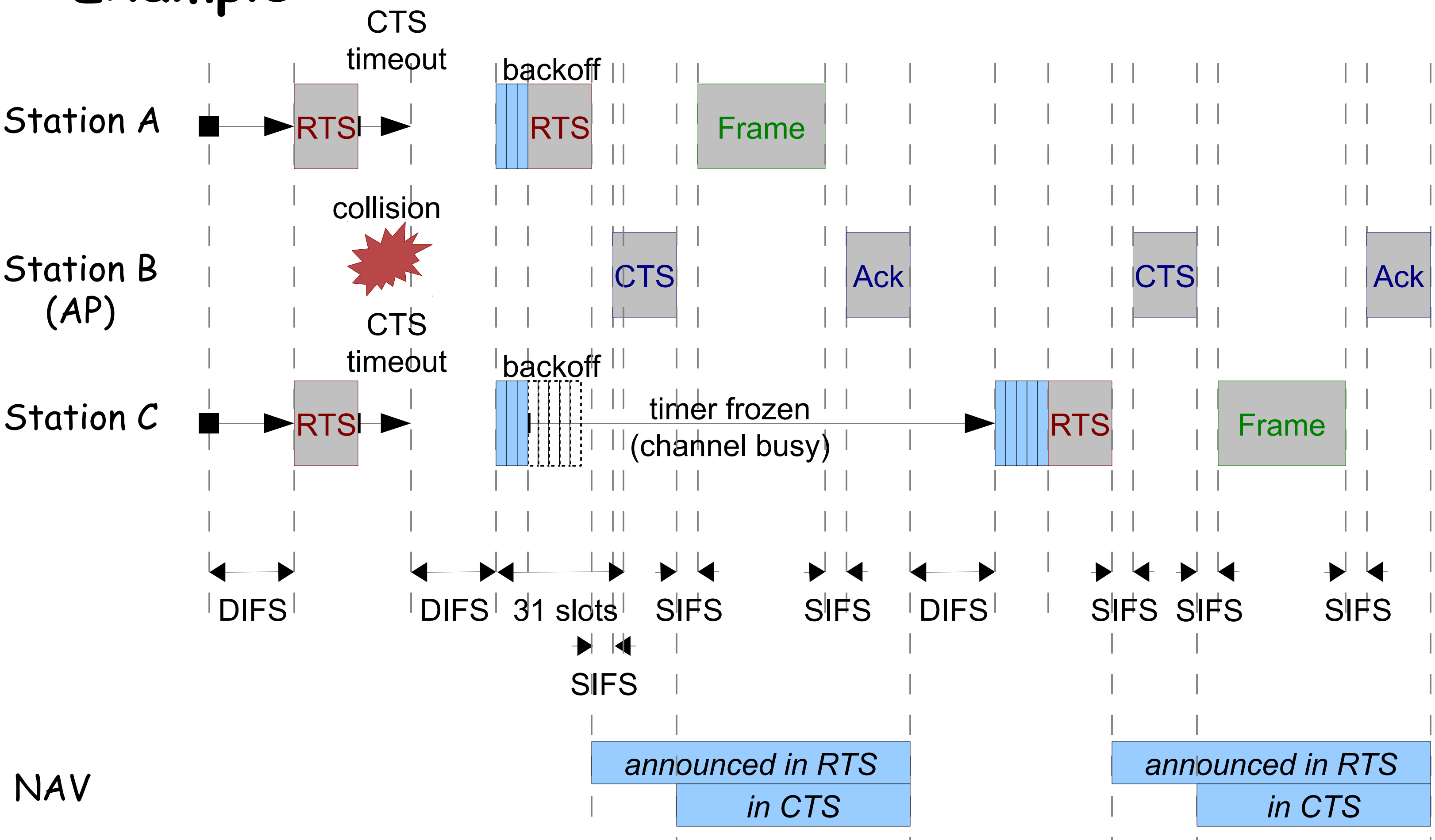
802.11 RTS / CTS mechanism (2/3)

Network Allocation Vector (NAV)

- Carrier sensing (CCA) can be performed by listening to the physical medium. However, CCA cannot detect when the channel is busy due to a hidden node.
- A virtual carrier-sensing mechanism is added : *Network Allocation Vector* explicitly transmitted within frames. Defines how long the channel will be busy for the current operation.
- NAV announced in RTS frames and repeated in CTS frames → hidden terminals can learn how long the channel will be busy.

802.11 RTS / CTS mechanism (3/3)

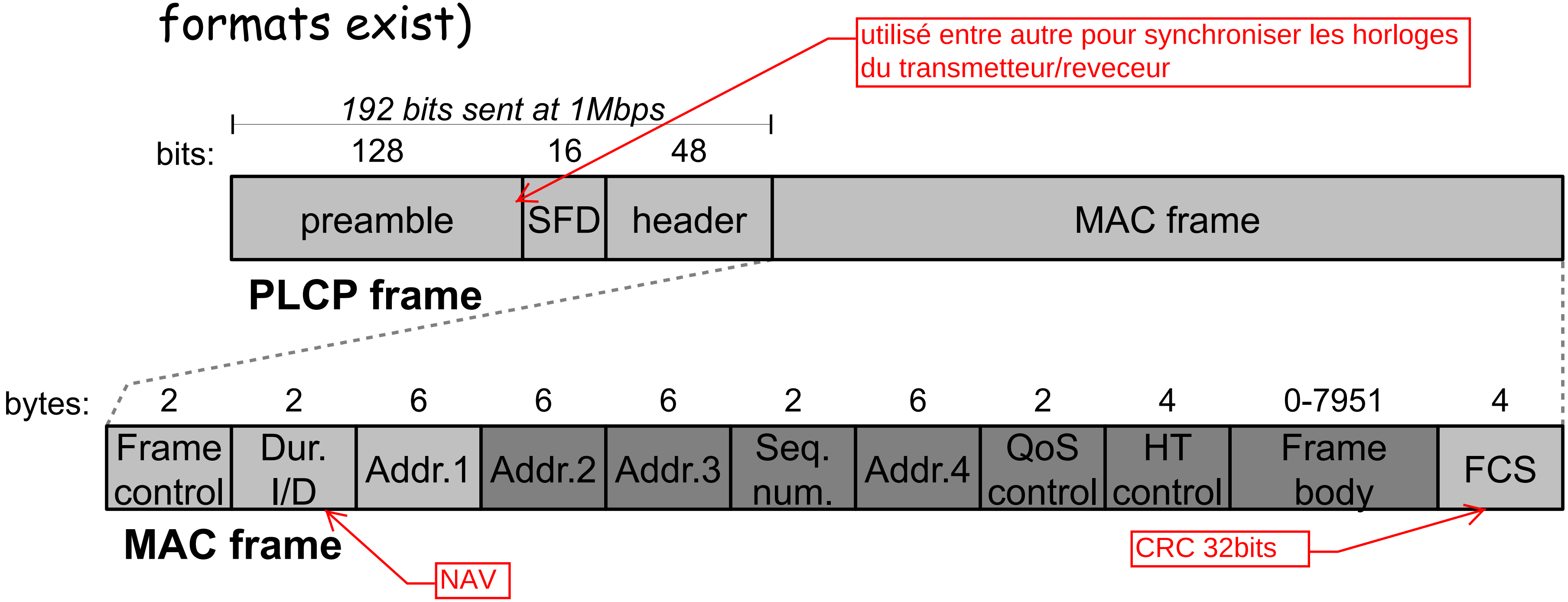
Example



802.11 General frame format (1/3)

Principle

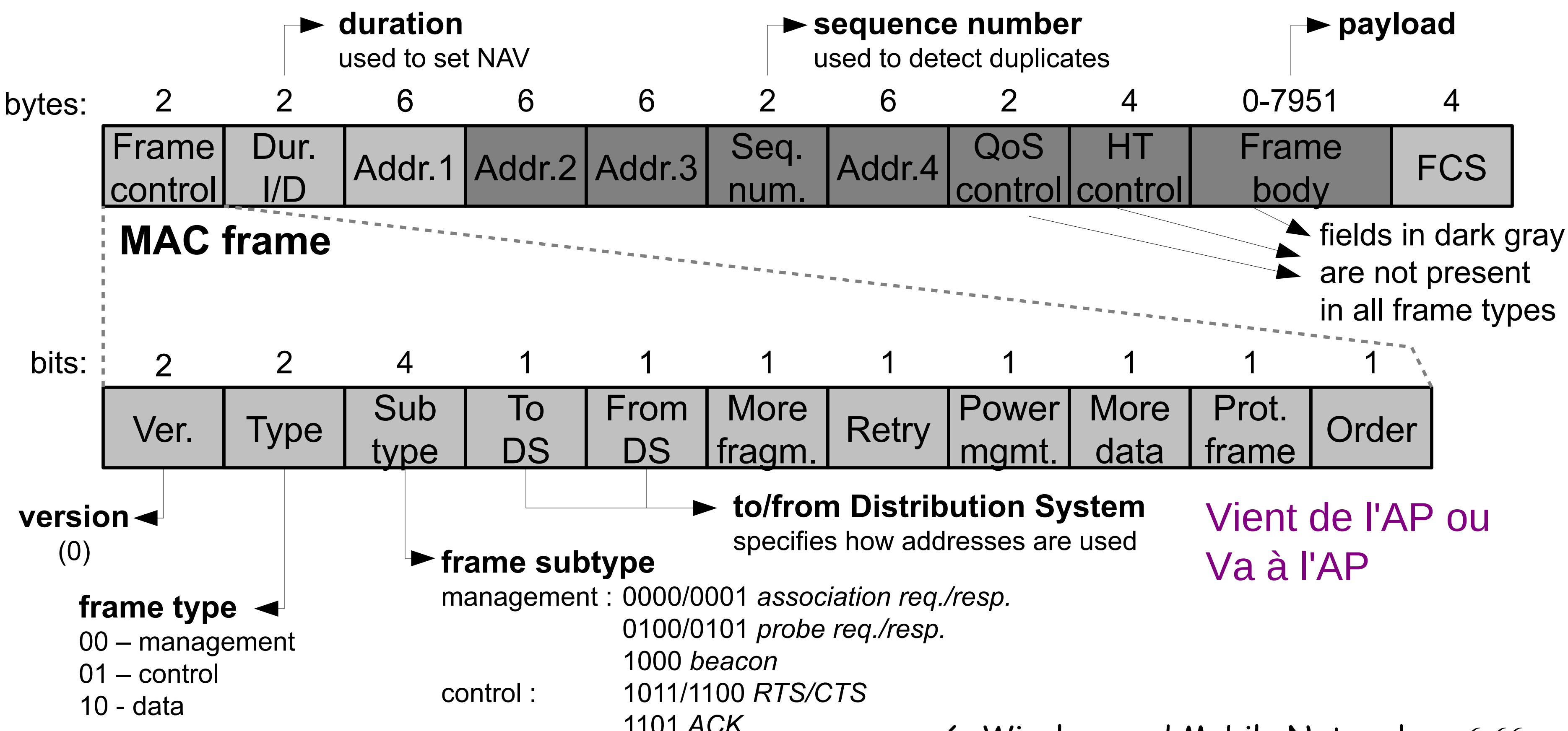
- PLCP(1) sublayer used to synchronize receiver + allow for compatibility with older versions (specify e.g. MAC frame rate)
- PLCP frame format shown for 802.11b with long preamble (other formats exist)



(1) PLCP = Physical Layer Convergence Protocol

802.11 General frame format (2/3)

Principle



802.11 General frame format (3/3)

Addressing

- A frame can contain up to 4 addresses !

Frame control	Dur. I/D	Addr.1	Addr.2	Addr.3	Seq. num.	Addr.4	QoS control	HT control	Frame body	FCS

- The meaning and use of addresses varies among the MAC frame types.

Frame control	Dur. I/D	Addr.1	FCS

MAC ACK frame

Frame control	Dur. I/D	Addr.1	Addr.2	Addr.3	Seq. num.	Addr.4	QoS control	HT control	Frame body	FCS

MAC DATA frame

802.11 DATA frame format

Addressing

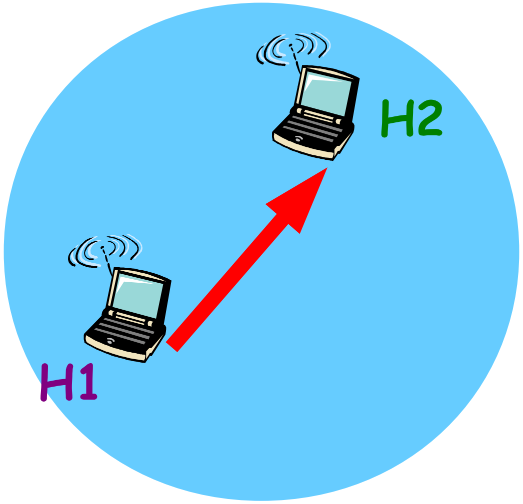
- Depending on the ToDS and FromDS flags in the Frame Control field, the following uses are possible

	ToDS	FromDS	Addr.1	Addr.2	Addr.3	Addr.4
Ad-hoc	0	0	RA=DA	TA=SA	BSSID(2)	N/A
Infrastructure	1	0	RA=BSSID	TA=SA	DA	N/A
	0	1	RA=DA	TA=BSSID	SA	N/A
WDS(1)	1	1	RA	TA	DA	SA

- where the addresses are as follows
  - TA / RA = station that physically transmits / receives
  - SA/DA = initial source / final destination
  - BSSID = identifier of BSS (Access Point)

(1) WDS = *Wireless Distribution System*
(2) For the ad-hoc mode, the BSSID has been generated randomly.

802.11 Frame: addressing (1/5)



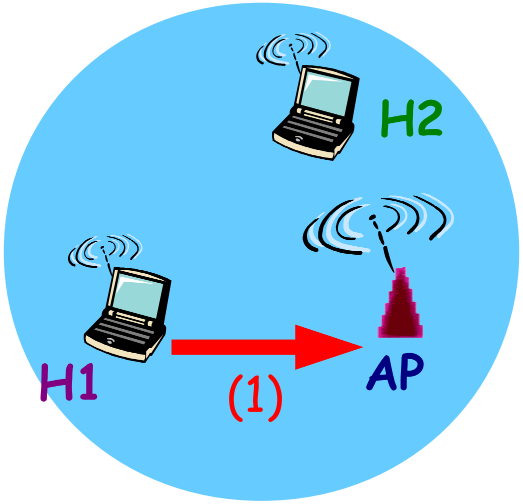
H1 → H2
Ad-hoc mode
(no Access Point)

802.11 frame

FC.ToDS=0
FC.FromDS=0
Address 1 (receiver) = **H2**
Address 2 (transmitter) = **H1**
Address 3 = **BSSID**(1)
Address 4 not used

(1) In ad-hoc mode, the BSSID has been generated randomly.

802.11 Frame: addressing (2/5)

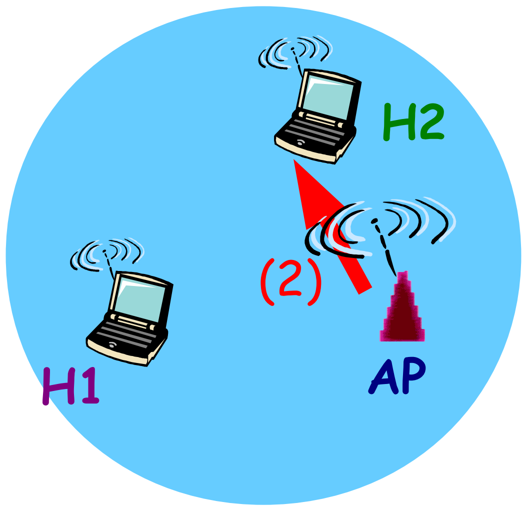


H1 → H2
infrastructure mode

802.11 frame

FC.ToDS=1
FC.FromDS=0
Address 1 (receiver) = **AP** (BSSID)
Address 2 (transmitter) = **H1**
Address 3 = **H2**
Address 4 not used

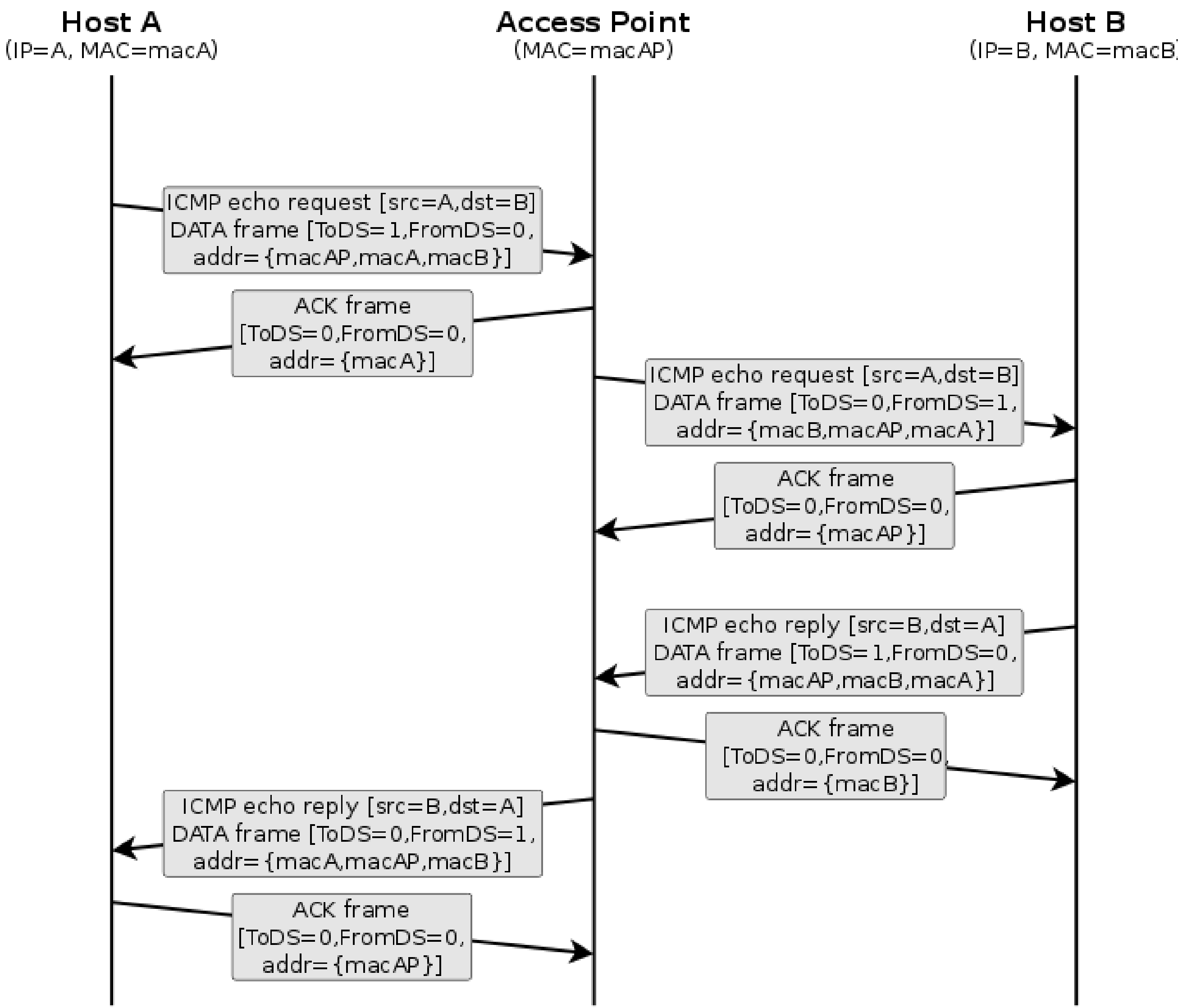
802.11 Frame: addressing (3/5)



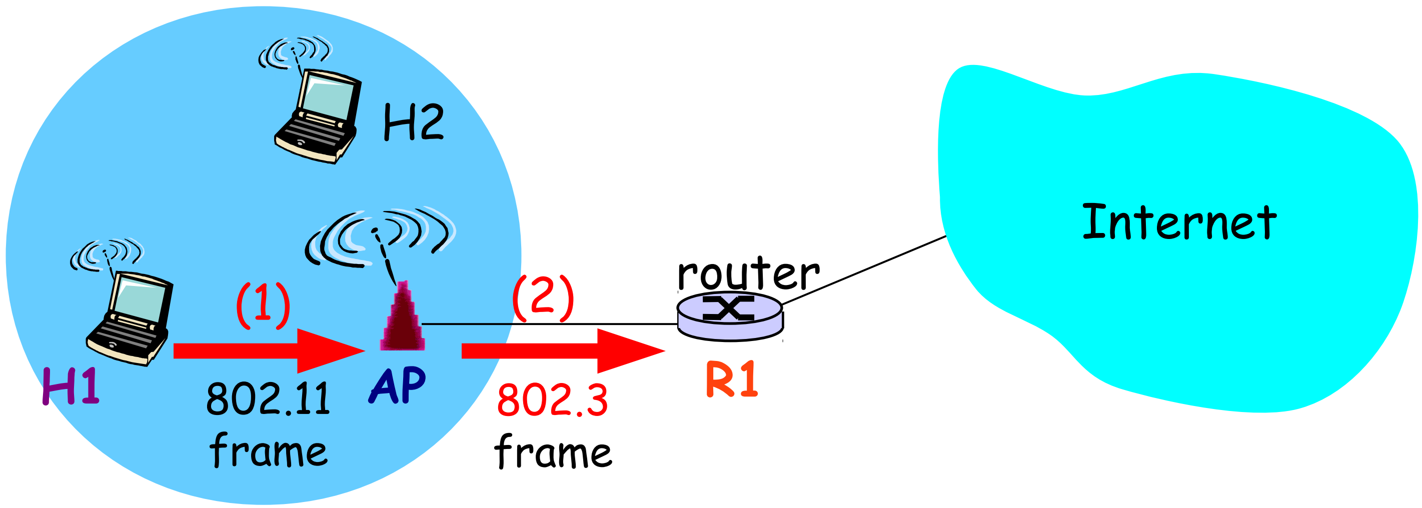
H1 → H2
infrastructure mode

802.11 frame

FC.ToDS=0
FC.FromDS=1
Address 1 (receiver) = **H2**
Address 2 (transmitter) = **AP** (BSSID)
Address 3 = **H1**
Address 4 not used


Host A
(IP=A, MAC=macA)
Access Point
(MAC=macAP)
Host B
(IP=B, MAC=macB)
ICMP echo request [src=A,dst=B]
DATA frame [ToDS=1,FromDS=0,
addr={macAP,macA,macB}]
ACK frame
[ToDS=0,FromDS=0,
addr={macA}]
ICMP echo request [src=A,dst=B]
DATA frame [ToDS=0,FromDS=1,
addr={macB,macAP,macA}]
ACK frame
[ToDS=0,FromDS=0,
addr={macAP}]
ICMP echo reply [src=B,dst=A]
DATA frame [ToDS=1,FromDS=0,
addr={macAP,macB,macA}]
ACK frame
[ToDS=0,FromDS=0,
addr={macB}]
ICMP echo reply [src=B,dst=A]
DATA frame [ToDS=0,FromDS=1,
addr={macA,macAP,macB}]
ACK frame
[ToDS=0,FromDS=0,
addr={macAP}]

802.11 Frame: addressing (4/5)



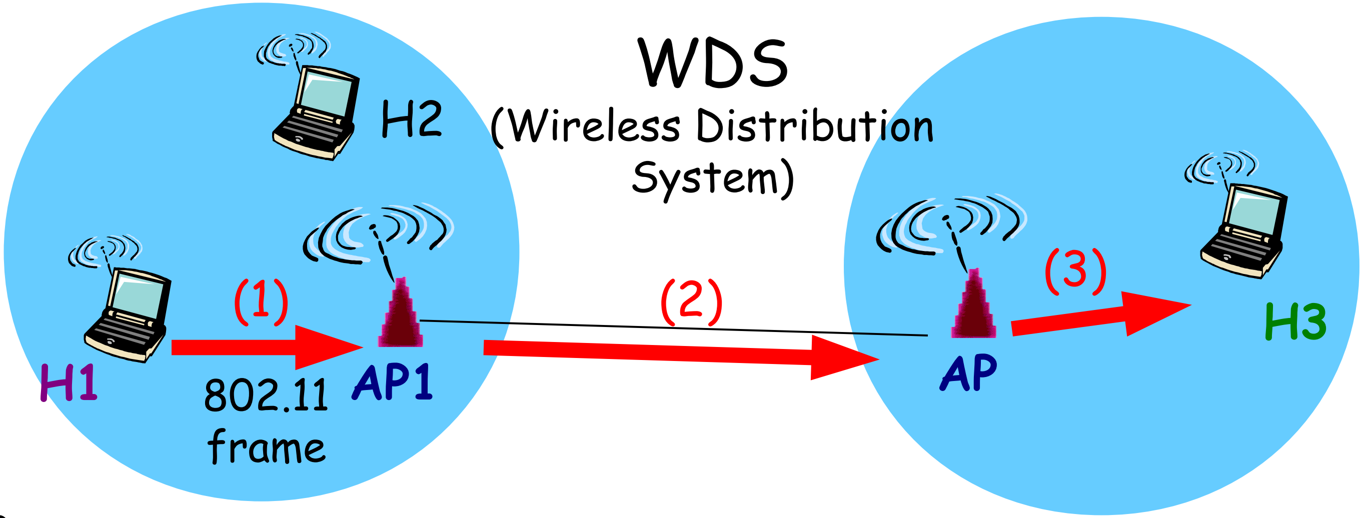
802.11 frame

FC.ToDS=1
FC.FromDS=0
Address 1 (receiver) = **AP** (BSSID)
Address 2 (transmitter) = **H1**
Address 3 = **R1**
Address 4 not used

802.3 frame

Destination address = **R1**
Source address = **H1**

802.11 Frame: addressing (5/5)



(1) 802.11 frame

FC.ToDS=1
FC.FromDS=0
Address 1 (receiver) = **AP1** (BSSID)
Address 2 (transmitter) = **H1**
Address 3 = **H3**
Address 4 not used

(2) 802.11 frame

FC.ToDS=1
FC.FromDS=1
Address 1 (receiver) = **AP2** (BSSID)
Address 2 (transmitter) = **AP1** (BSSID)
Address 3 = **H3**
Address 4 = **H1**

(3) 802.11 frame

FC.ToDS=0
FC.FromDS=1
Address 1 (receiver) = **H3**
Address 2 (transmitter) = **AP2** (BSSID)
Address 3 = **H1**
Address 4 not used

ARP / IP datagram in 802.11 frame

LLC encapsulation

- Network layer packets cannot be directly carried in the payload as can be the case with Ethernet (802.3)
- Instead, they are first encapsulated in a 802.2 LLC SNAP(1) frame.

Frame control	Dur. I/D	Addr.1	Addr.2	Addr.3	Seq. num.	Frame body	FCS

MAC DATA frame

bytes:	1	1	1	3	2	
	DSAP 0xAA	SSAP. 0xAA	Ctrl. field 0x03	0x00-00-00	Type 0x0800	IP datagram

identify a SNAP extension
S/DSAP = source/destination access point

identifies type of payload
0x0800 IPv4
0x0806 ARP
0x86DD IPv6

(1) SNAP = *Sub-Network Access Protocol*

Performance of 802.11

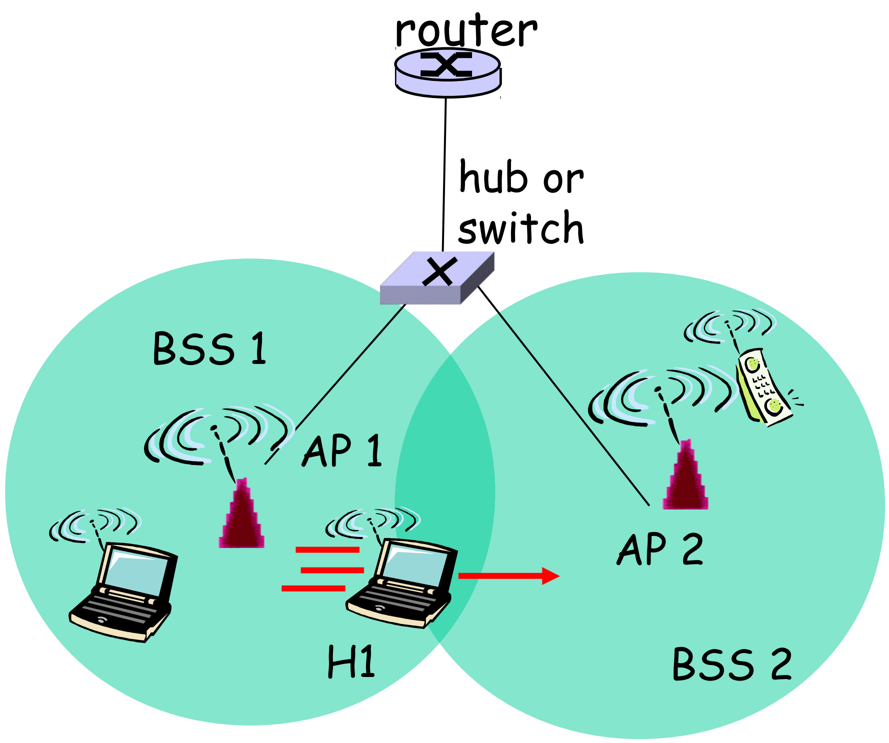
What data rate can be achieved ?

- Consider 802.11a which can provide a theoretical rate of 54 Mbps.
- Station A sends a 1500 bytes frame to station B. There is no collision.
- What parameters are needed ?
  - SIFS = 16 us ; DIFS = 34 us
  - 802.11a preamble (PLCP) size = 20 us
  - ACK frame size = 14 bytes
- Total transmission time ~ 314 us
  → achieved data rate ~ 38 Mbps (~71% of theoretical)

- What is the IP data rate (think of 802.2 encap.) ?
- What if RTS/CTS frames are used ?

802.11 : mobility within same subnet

- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning: switch will see frame from H1 and "remember" which switch port can be used to reach H1

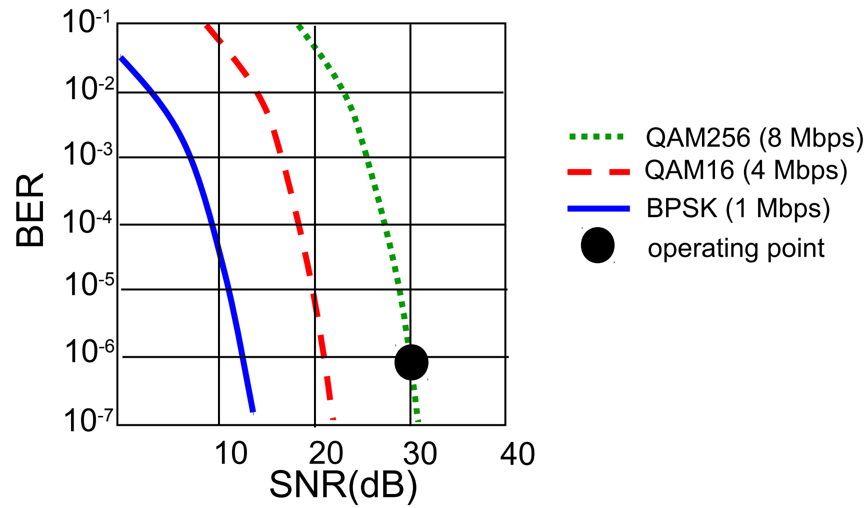


802.11 : advanced capabilities

Rate Adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies

- rate adaptation algorithm not part of standard



1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER

802.11 : advanced capabilities

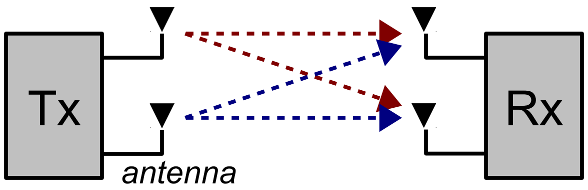
Power Management

- node-to-AP : "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame : contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

802.11 : additional references

- IEEE, ***Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications***, IEEE Std 802.11-2012 (revision of IEEE Std 802.11-1999)
- Matthew S. Gast, ***802.11 Wireless Networks: The Definitive Guide***, 2nd edition, O'Reilly, 2005

802.11n

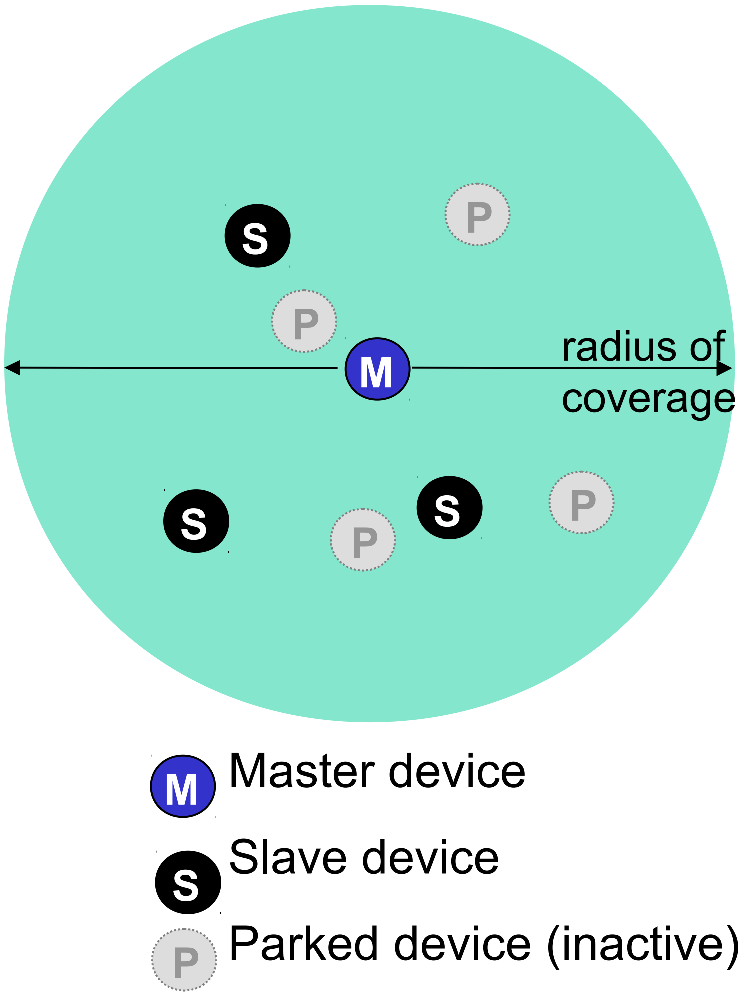


Enhanced throughput

- Multiple-Input / Multiple-Output (MIMO)
  - Multiple antennas and associated RF chains
- Wider channel
  - 802.11a/g use 20MHz channels and 48 data subcarriers (OFDM)
  - 802.11n uses 4 additional data subcarriers
    → ~8% bandwidth improvement
  - 802.11n can optionally use a 40MHz channel (disabled by default) → 2 adjacent channels → less "pilot" subcarriers
    → ~120% bandwidth improvement
- Changes at the MAC layer
  - Frame bursting (and cumulative ACKs)
  - Frame aggregation
  - MAC header compression

802.15 : WPAN

- WPAN – *Wireless Personal Area Network*
  - typ. < 10 m diameter
  - most known = *Bluetooth* (802.15.1)
  - replacement for cables (mouse, keyboard, headphones)
  - ad hoc : no infrastructure
  - master/slaves : slaves request permission to send ; master grants requests
  - 2.4-2.5 GHz radio band
  - up to 721 kbps (v1.1)



802.15.1 - Bluetooth

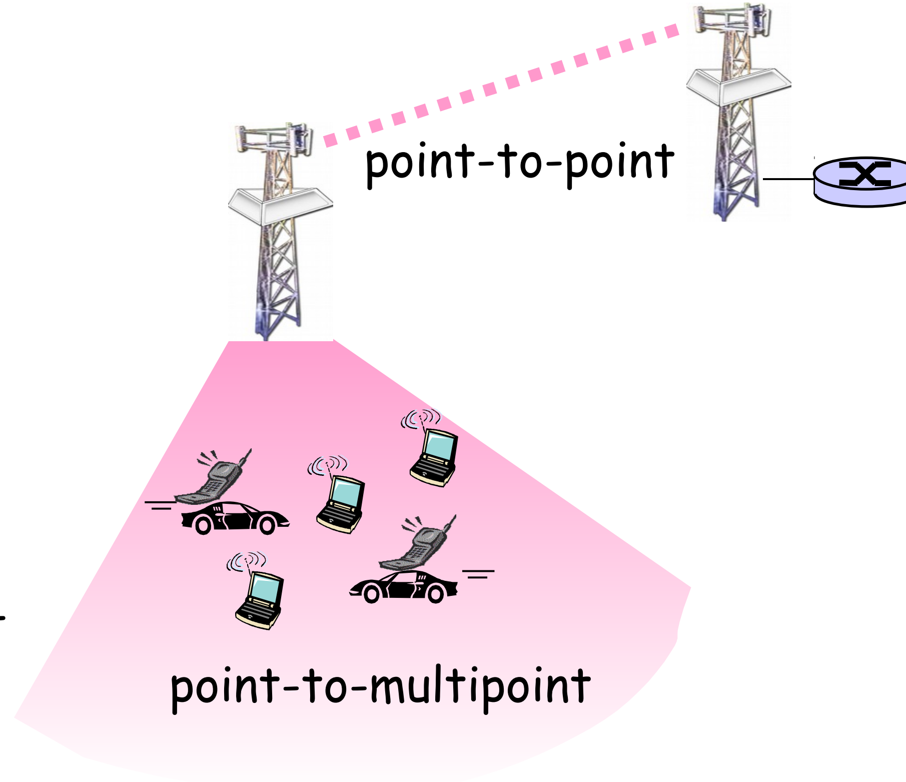
Considéré comme du bruit sur un réseau 802.11

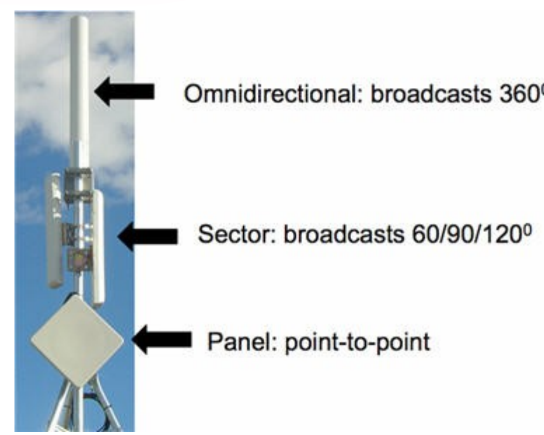
- **Frequency-hopping** (FHSS[1])
  - Single carrier frequency changes along time (according to a pseudo-random pattern)
  - ISM band (2.402–2.480 GHz) partitioned in 79 channels of 1MHz
  - Change channel about 320-1600 times/second
  - Hopping pattern derived from the master's 48-bits channel ID, along a pseudo-random sequence
  - FHSS makes sniffing Bluetooth harder, but doable → see e.g. project "*Ubertooth One*" by Michael Ossmann

(1) FHSS = *Frequency Hopping Spread Spectrum*

802.16 : WiMAX

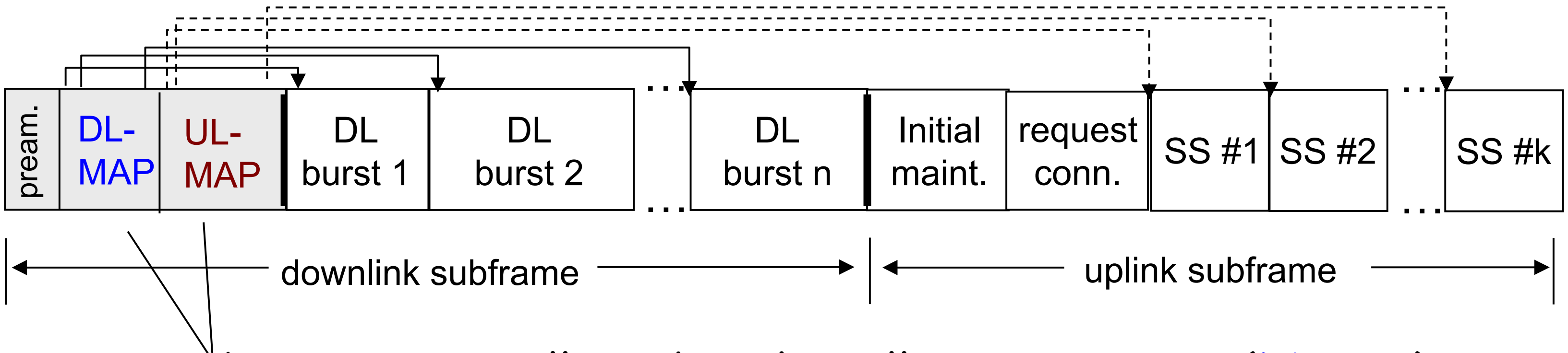
- Like 802.11 & cellular base station model
  - transmissions to/from base station by hosts with omnidirectional antenna
  - base station-to-base station backhaul with point-to-point antenna
- unlike 802.11
  - range ~ 6 miles ("city rather than coffee shop")
  - ~14 Mbps





802.16 : WiMAX: downlink, uplink scheduling

- Transmission super-frame
  - down-link subframe : base station to node
  - uplink subframe : node to base station



base station tells nodes who will get to receive (DL map) and who will get to send (UL map), and when

- WiMAX standard provides mechanism for scheduling, but not scheduling algorithm

Chapter 6 outline

6.1 Introduction

Wireless

- 6.2 Wireless links, characteristics
  - Spread spectrum
- 6.3 IEEE 802.11 wireless LANs ("wi-fi")
- 6.4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Pas vu au cours

Mobility

- 6.5 Principles: addressing and routing to mobile users
- 6.6 Mobile IP
- 6.7 Handling mobility in cellular networks
- 6.8 Mobility and higher-layer protocols

6.9 Summary

Pas vu

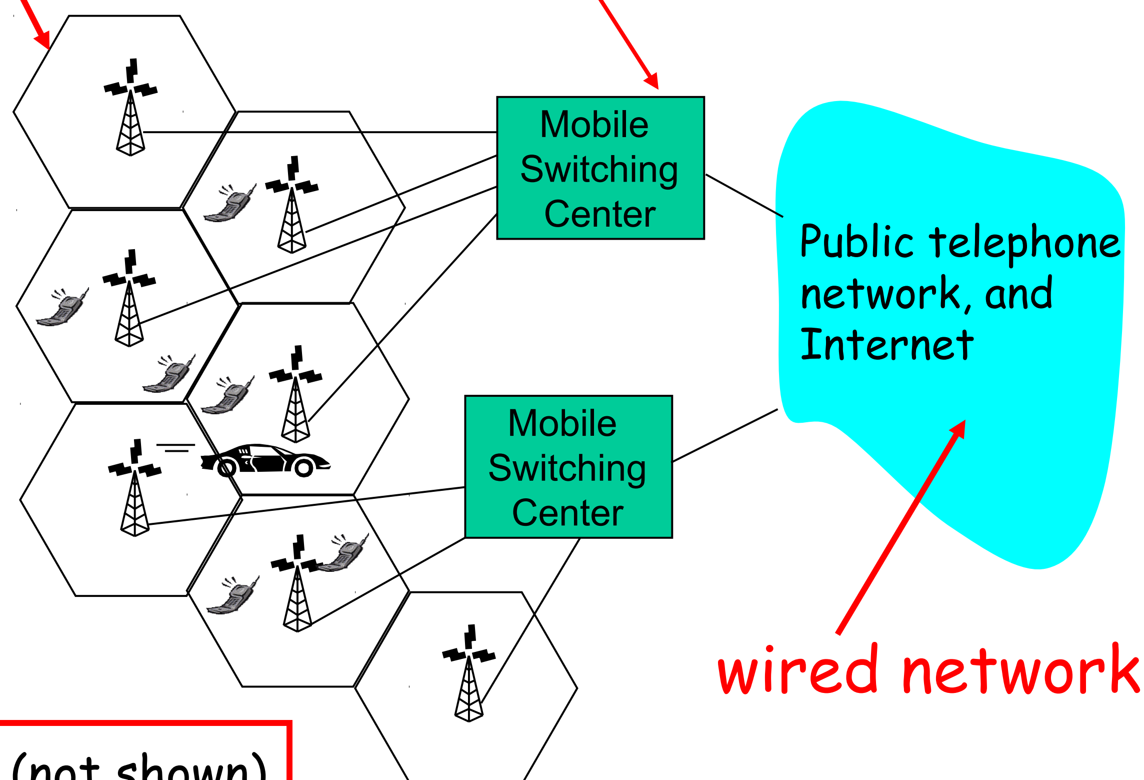
Components of cellular network architecture

cell

- covers geographical region
- *base transceiver station* (BTS) analogous to 802.11 AP
- *mobile users* attach to network through BTS
- *air-interface:* physical and link layer protocol between mobile and BTS

MSC

- connects cells to wide area net
- manages call setup (more later!)
- handles mobility (more later!)



BSC

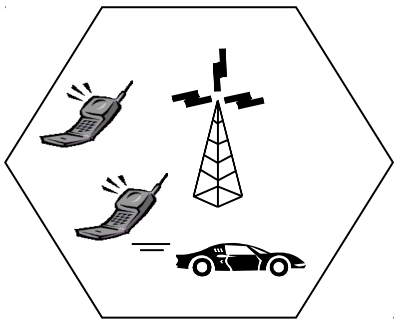
- Base Station Controller (not shown)
- channel allocation, paging, handoff

Pas vu

Cellular networks : the first hop

Sharing mobile-to-BTS radio spectrum : 2 techniques

- combined FDMA/TDMA
  - divide spectrum in frequency channels
  - divide each channel into time slots (GSM)
- CDMA
  - IS-95 CDMA, CDMA 2000



Pas vu

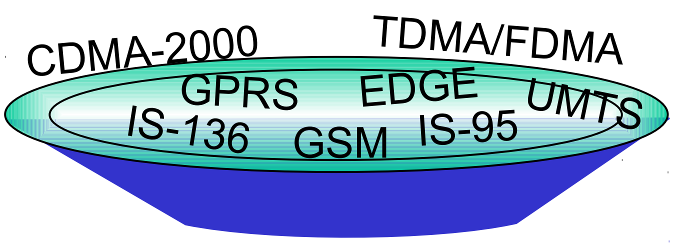
Cellular standards : brief survey

1G systems

- analog voice (FDMA)

2G systems

- voice channels
- IS-136 TDMA : combined FDMA/TDMA (north america)
- GSM (global system for mobile communications): combined FDMA/TDMA
  - most widely deployed (> 80% of mobiles)
- IS-95 CDMA : code division multiple access



Don't drown in a bowl of alphabet soup: use this for reference only

Cellular standards : brief survey

2.5G systems

- voice and data channels
- 2G extensions for those who can't wait for 3G services
- GPRS : *General Packet Radio Service*
  - evolved from GSM
  - data sent on multiple channels (if available)
  - data rates up to 115 kbps
- EDGE : *Enhanced Data rates for Global Evolution*
  - also evolved from GSM, using enhanced modulation
  - data rates up to 384 kbps
- CDMA-2000 (phase 1)
  - data rates up to 144kbps
  - evolved from IS-95

Pas vu

Cellular standards : brief survey

3G systems

- voice/data
- UMTS : *Universal Mobile Telecommunications Service*
  - data service = HSDPA/HSUPA (*High Speed Uplink/Downlink packet Access*), up to 3 Mbps
- CDMA-2000 : CDMA in TDMA slots
  - data service = 1xEVDO (*1xEvolution Data Optimized*), up to 14 Mbps

4G systems

- LTE : *Long-Term Evolution*
  - bitrate depends on modulation technique and use of multiple streams (MIMO), can reach several 100Mbps

..... more (and more interesting) cellular topics due to mobility (stay tuned for details)