Networking technologies and applications

Rolland Vida

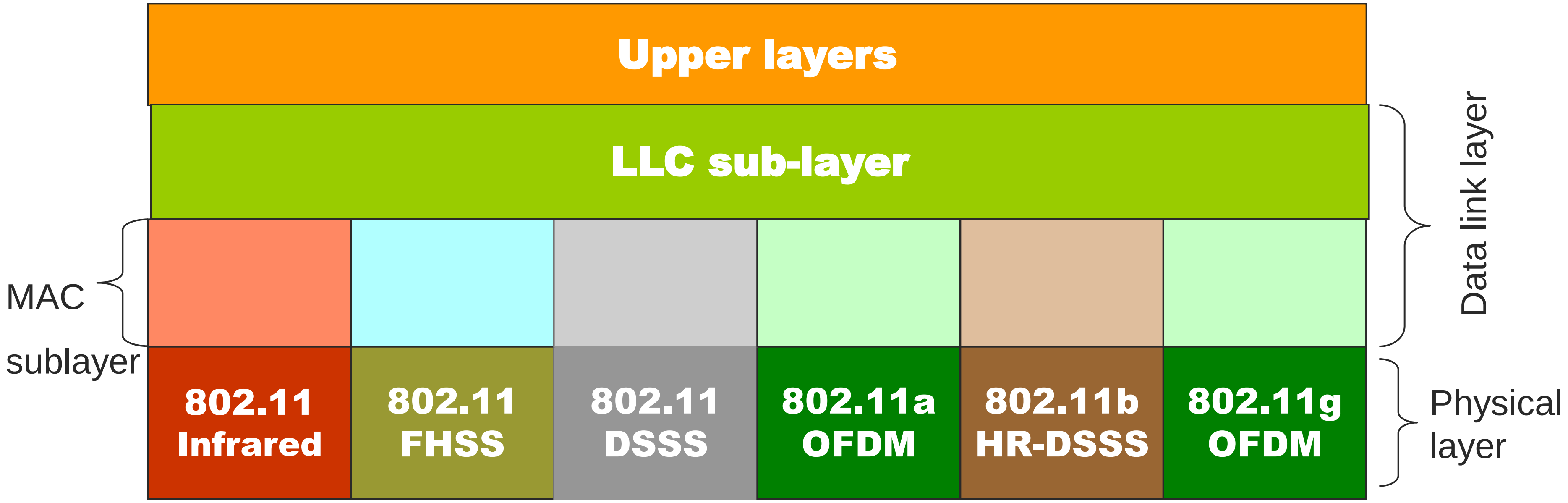
April 20, 2015

IEEE 802.11

- WLAN – Wireless Local Area Network
  - The most popular WLAN solution defined by the IEEE 802.11 standard
  - Other solutions: HiperLAN, HomeRF
- What to use it for?
  - In-building WLANs
  - Connecting buildings with each other
  - Home use
    - Extending the home broadband connection (DSL, Cable, etc.) with a wireless link
  - Public internet services (hotspots)
    - Airports, hotels, internet cafés

The 802.11 protocol stack

- Physical layer
  - Different solutions defined in different standards
- MAC sub-layer – Medium Access Control
  - Controls the access to the communication channel
    - Who is the next station to send
- LLC sub-layer – Logical Link Control
  - Hides the different IEEE 802.11 versions from the upper layers
  - Ensures reliable communication in the data link layer, if needed



Physical layer

- The 802.11 standard (1997)defines three transmission modes in the physical layer:
  - Infrared
  - FHSS – Frequency Hopping Spread Spectrum
  - DSSS – Direct Sequence Spread Spectrum
- 802.11a, 802.11b (1999) – new transmission modes, higher speeds
  - OFDM – Orthogonal Frequency Division Multiplexing
  - HR-DSSS – High Rate DSSS
- 802.11g (2001) - new OFDM modulation scheme, in a different frequency domain

Infrared

- Similar solution to a remote control
  - No line of sight required

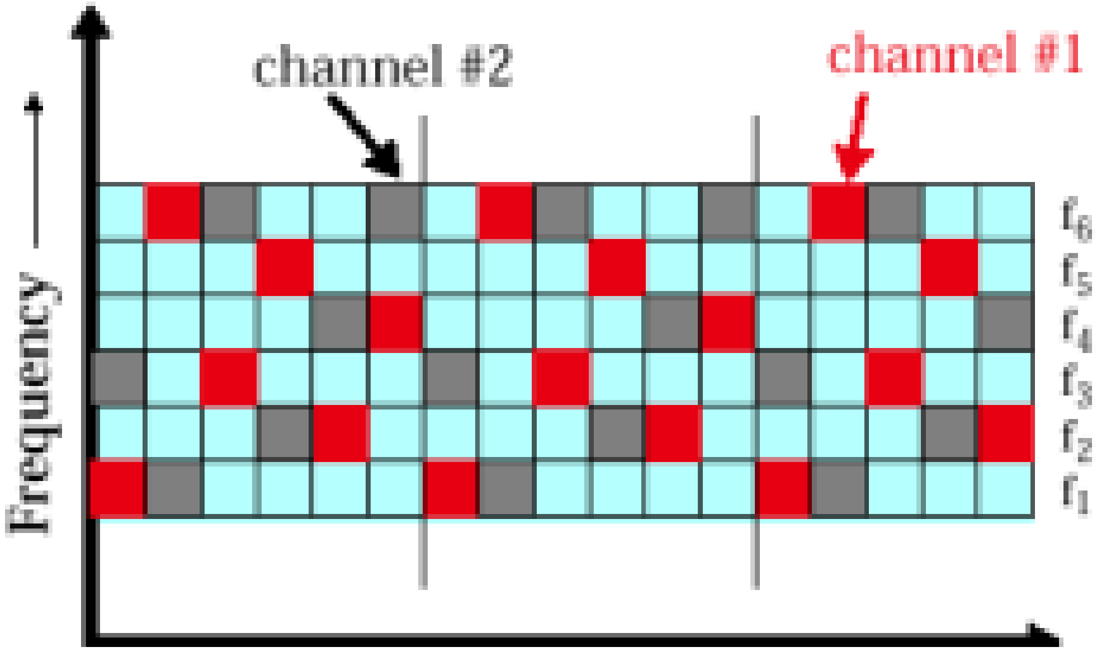
- Advantages:
  - Simple, cheap solution
  - Infrared signals do not cross the walls
    - Cells in different rooms are naturally separated
- Drawbacks
  - Low bandwidth
    - 1 or 2 Mb/s transmission speed
  - Infrared signals do not cross the walls
    - To talk to an access point, you should be in the same room
  - Sunshine attenuates the infrared signals

- Not a popular solution

FHSS

- Frequency Hopping Spread Spectrum
  - In the 2.4 GHz ISM band
    - 79 channels, 1 MHz wide each, between 2.402 GHz and 2.480 GHz (Europe, USA)
    - 23 channels, between 2.473 GHz and 2.495 GHz (Japan)
  - Hopping sequence generated with a pseudo-random number generator
    - If two stations use the same starting frequency (seed), they will hop in parallel to the same frequencies
      - Have to remain synchronized in time
    - 78 hoping sequences, each with 79 channels (USA, Europe)
      - The 1st sequence in the US: 3,26,65,11,46,19,74,50,22,64,79,32,62...
    - In Japan, 12 hoping sequences, each with 23 channels
  - The dwell time on each frequency can be modified if needed
    - Cannot be larger than 400
    - Usually used values. 32 ms or 128 ms

FHSS

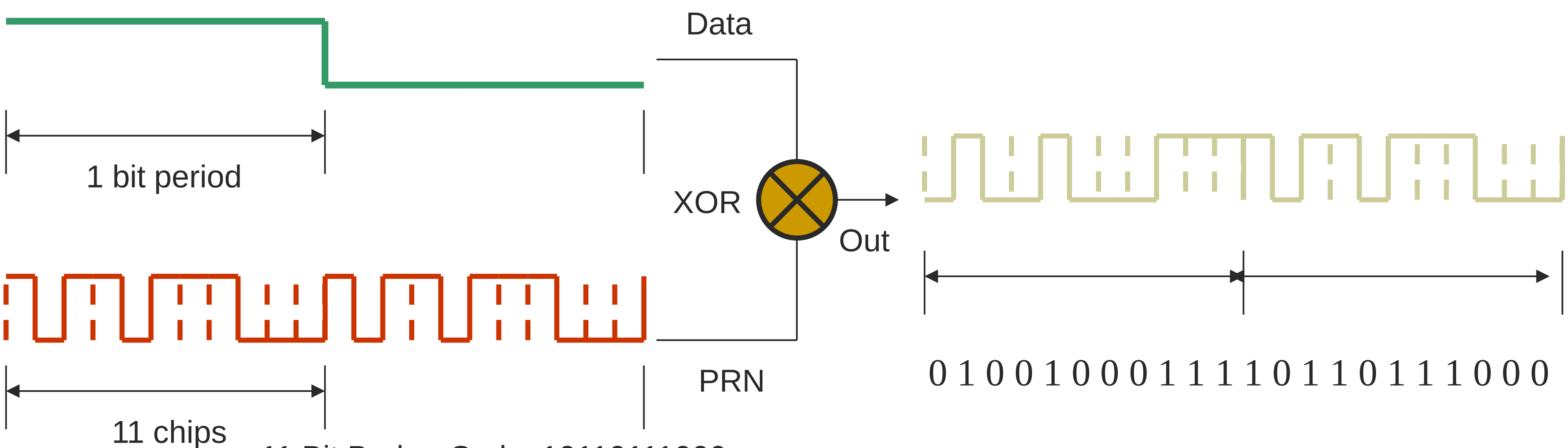


FHSS

- Advantages
  - Efficient use of the spectrum in the open ISM band
  - Secure (to a given extent)
    - For eavesdropping, one has to know the hoping sequence and the dwell times
  - Good protection against multipath fading
    - The signal is reflected by different objects
      - Reaches several times the receiver
    - The receiver listens to a given frequency only for a limited time interval
      - No interference with the signal reaching the receiver with some delay, on the „old" channel
  - Not so sensible to radio interferences
    - Interfering signals restricted to a given frequency domain
      - The receiver jumps off rapidly from that frequency
- Drawbacks
  - Slow speeds (1 Mb/s)

DSSS

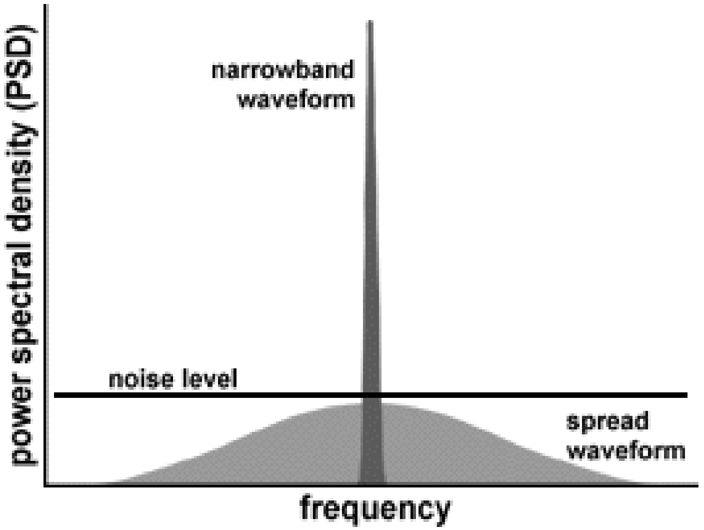
- Direct Sequence Spread Spectrum
  - Transfer speeds also 1 or 2 Mbps
  - The „useful” data spread over a larger frequency domain
    - XOR operation with an 11 bit chip-code (noise)
      - Pseudo-random bit string, on a much higher frequency than the original signal
    - The noise is filtered out by the receiver
      - With a second XOR operation the data can be regenerated



11 Bit Barker Code: 10110111000

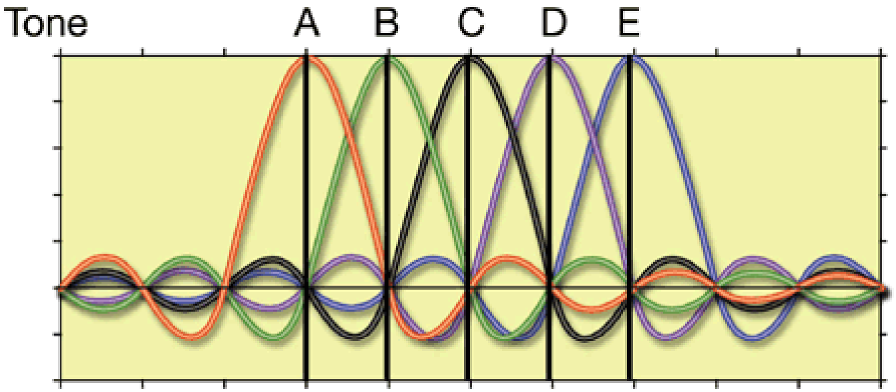
DSSS

- The useful data is spread over a large frequency domain
  - The broadband signal harder to detect
    - An eavesdropper sees only a „noise”
      - Cannot filter out the useful information
    - Originally used for military purposes
  - For an 11 bit chip-code, signal spread over a 22 MHz wide domain
    - 30 MHz between two DSSS systems, to avoid interferences
    - The ISM band is 83.5 MHz wide
      - Only 3 DSSS systems can operate in parallel without interferences



802.11a (Wi-Fi5)

- New solutions to increase bandwidth ('99)
- OFDM - Orthogonal Frequency Division Multiplexing
  - 5 GHz ISM band
  - Up to 54 Mbps transfer speed
    - The frequency domain split in many small slices (sub-carriers)
    - The signal to transmit also split in several parts
    - Transmission on several sub-carriers in parallel, higher speed
  - In traditional FDM guard bands to avoid interferences
    - Fewer possible carriers
  - In OFDM orthogonal frequencies
    - The peak of each sub-carrier corresponds to a zero level of every other sub-carrier



802.11b (Wi-Fi)

- Wireless Fidelity
- The first 802.11x standard
  - Not a follow-up of 802.11a, they were developed in parallel
- HR-DSSS
  - High Rate Direct Sequence Spread Spectrum
    - More efficient modulation than in DSSS
  - 4 transfer speeds in the 2,4 GHz ISM band
    - 1, 2, 5.5 or 11 Mbps
  - In practice usually 11 Mbps, over a 100 meter service range
- Lower speed than for 802.11a
  - Larger service range

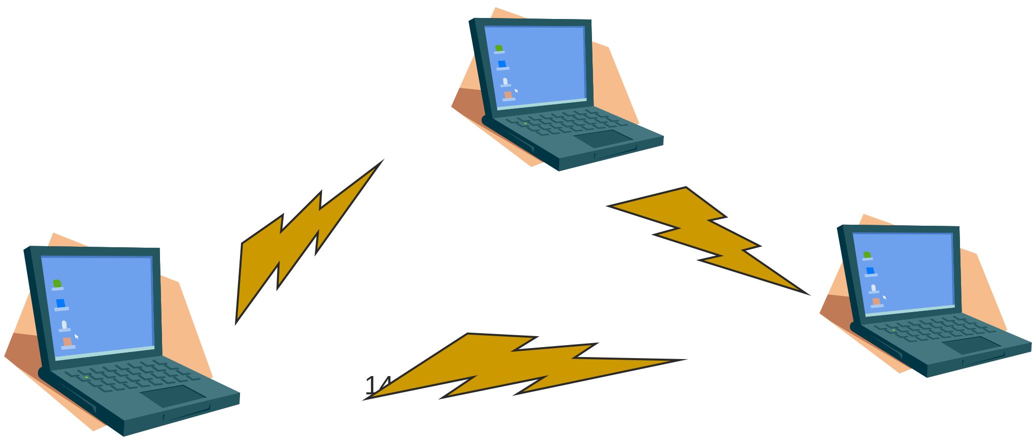
802.11g

- Adopted in 2001
  - Uses OFDM, similarly to 802.11a
  - In the 2,4 GHz ISM band, as the 802.11b
    - Sensible to the interferences
- 54 Mbps transfer speeds

- Promises to be the technology „of the future”
  - Or it is already...
  - Huge number of deployed 802.11b networks, devices
    - Until the return on the investment is not obtained, they will not be upgraded

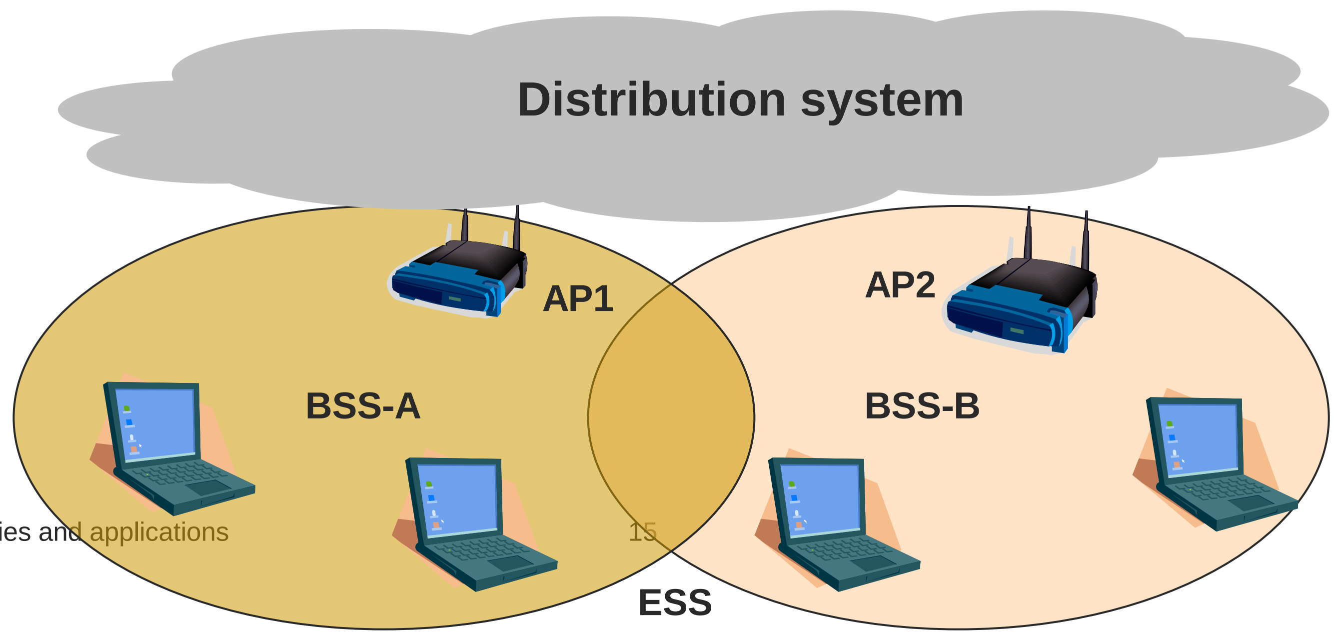
Ad-hoc mode

- Each node communicates directly with the other nodes in its radio range
- Communication between distant nodes through ad-hoc routing protocols
  - AODV, DSR, DSDV, etc.
- Each station is a router as well
  - Multi-hop ad-hoc network
  - No need for an AP
- A temporary network can be built very fast
  - Between the participants of a conference for example



Infrastructure mode

- Cellular system
  - Basic Service Set (BSS) – cell
  - Access Point (AP)
    - Each cell is controlled by an AP
    - Periodically polls the nodes, controls the communication
  - Distribution System (DS)
    - A wireless or wired connection linking the APs
- Many cells form an Extended Service Set – ESS



802.11b channels

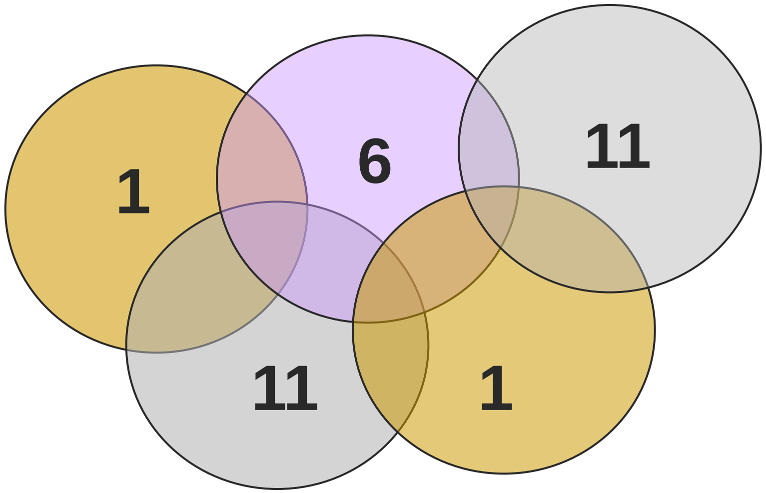
- What frequency to use inside a cell?
- 802.11b in the 2.4 GHz ISM band
  - Maximum 14 channels
  - Partially overlapping
- Different regulations in different countries
  - In Europe the channels 1-13 used
  - In the US, channels 1-11
  - In Japan all the 14 channels

Channel	Frequencies (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

The IEEE 802.11b channel frequencies used in the US

802.11b channels

- We form small channels
  - Each neighboring cell uses a different channel
  - The corresponding frequencies do not overlap



802.11b channels

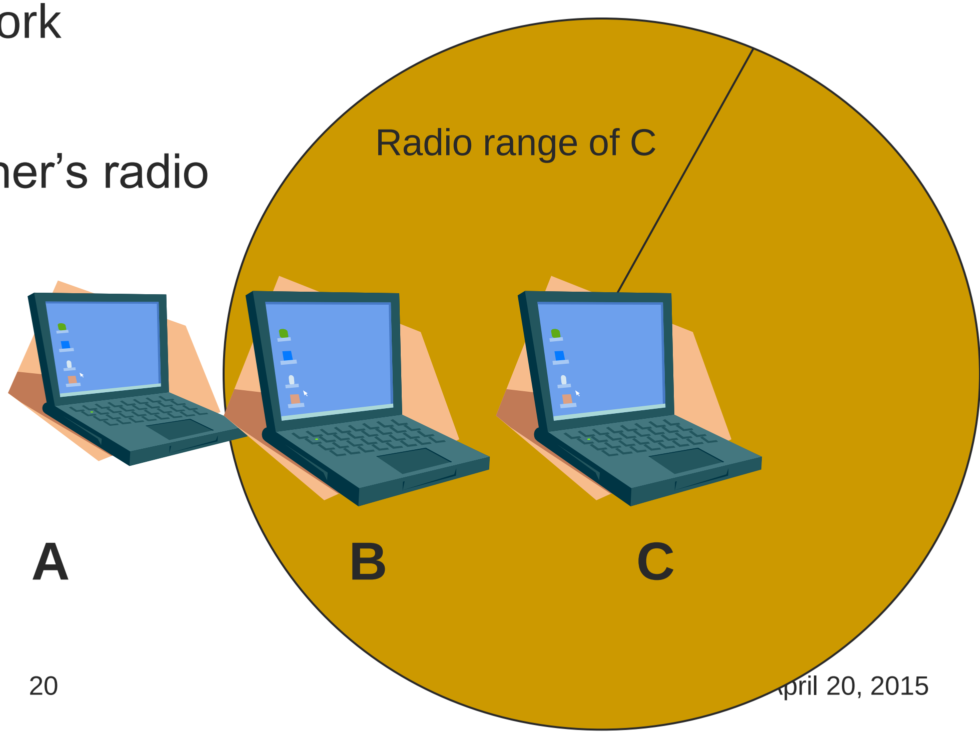
- The channel is defined by the middle frequency
  - E.g., around 2,412 GHz channel 1, around 2,417 GHz channel 2
    - Only 5 MHz distance between the middle frequencies
  - The 802.11b signal covers a 30 MHz wide spectrum
    - The signal occupies about 15 MHz of spectrum on both sides of the middle frequency
    - Overlap and interferences between neighboring channels
  - In cellular systems two neighboring cells have to be at least 5 channels away from each other
    - Usual combination - (1, 6, 11)

Joining a new cell

- A station joins a BSS when...
  - It is powered up
  - It exits sleep mode
  - It moves inside a BSS
- Passive Scanning
  - The station waits for a Beacon Frame from the AP
  - The AP periodically sends it, it contains synchronization information
- Active Scanning
  - The station tries to find an AP
  - Probe Request message is sent
  - Probe Response answer is expected from the API
- If many APs respond, chooses the „best one”
  - The best SNR – Signal to Noise Ratio

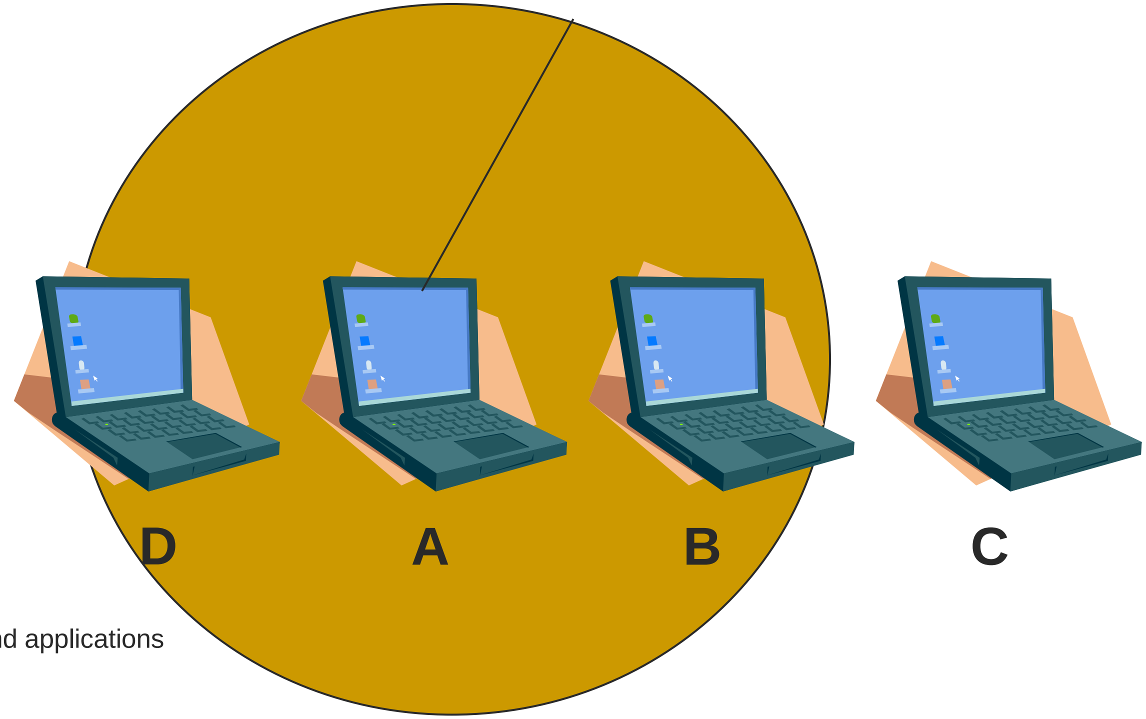
802.11 MAC sublayer

- Different from Ethernet (CSMA/CD)
  - An Ethernet station waits for the channel being unused, then starts to send
    - Collision detected, if it occurs
  - Does not work in a wireless network
- Hidden terminal problem
  - Not al the stations are in each other's radio range
    - C sends to B
    - A thinks the channel is empty
    - A starts to send to B
      - Interference occurs



Exposed terminal problem

- B wants to send to C
  - Listens to the channel, and sees that it is occupied by A
  - B thinks that it cannot send to C, to avoid collisions
  - It might happen that A sends something to D, thus B would not cause interference at node C



DCF vs. PCF

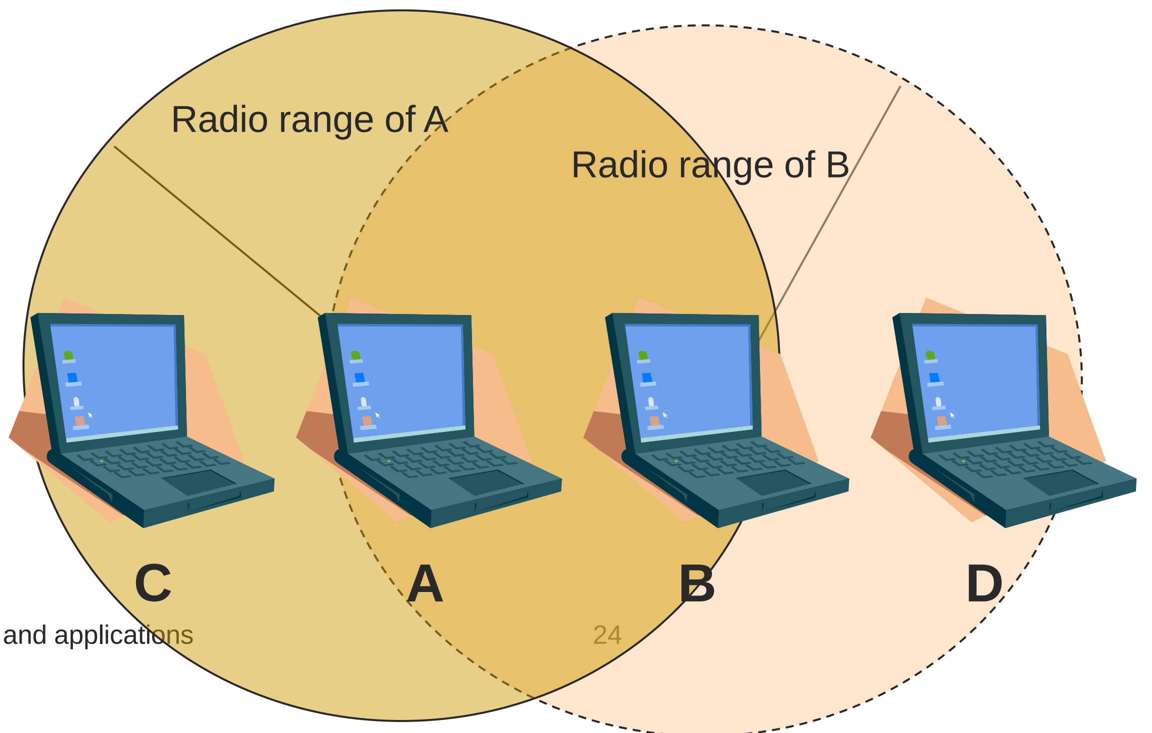
- In 802.11, no CSMA/CD
- Two other solutions:
  - DCF – Distributed Coordination Function
    - No central control
    - Each device should support it
  - PCF – Point Coordination Function
    - The access point controls all the activities inside the cell
    - Optional support

802.11 DCF

- CSMA/CA (instead of CD)
  - Carrier Sense Multiple Access with Collision Avoidance
  - Two operation modes:
    - Physical and virtual carrier sensing
- Physical carrier sensing:
  - If a station wants to send, it senses the channel
    - If empty, it starts the sending
  - It does not listen to the channel while sending
    - There might be interferences at the receiver
  - If the channel is not empty, waits until it becomes free

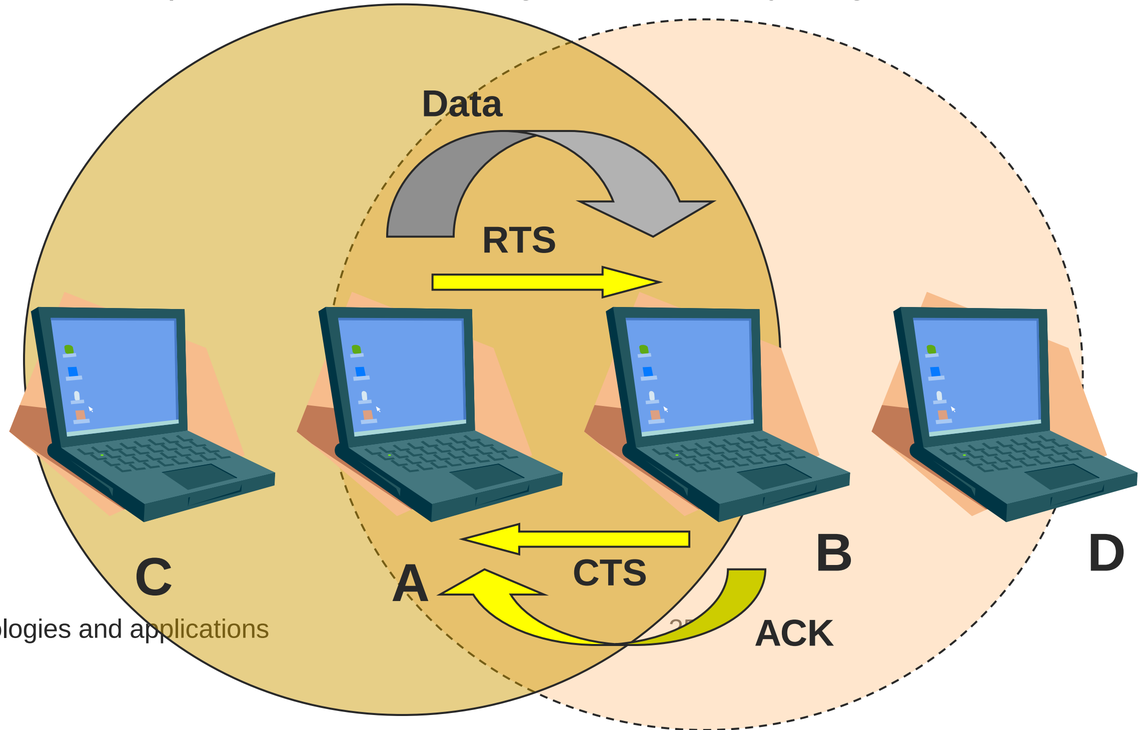
MACAW

- Multiple Access with Collision Avoidance for Wireless
  - Virtual carrier sensing
- A wants to send data to B
  - C in the radio range of A
  - D in the range of B, but outside the range of A



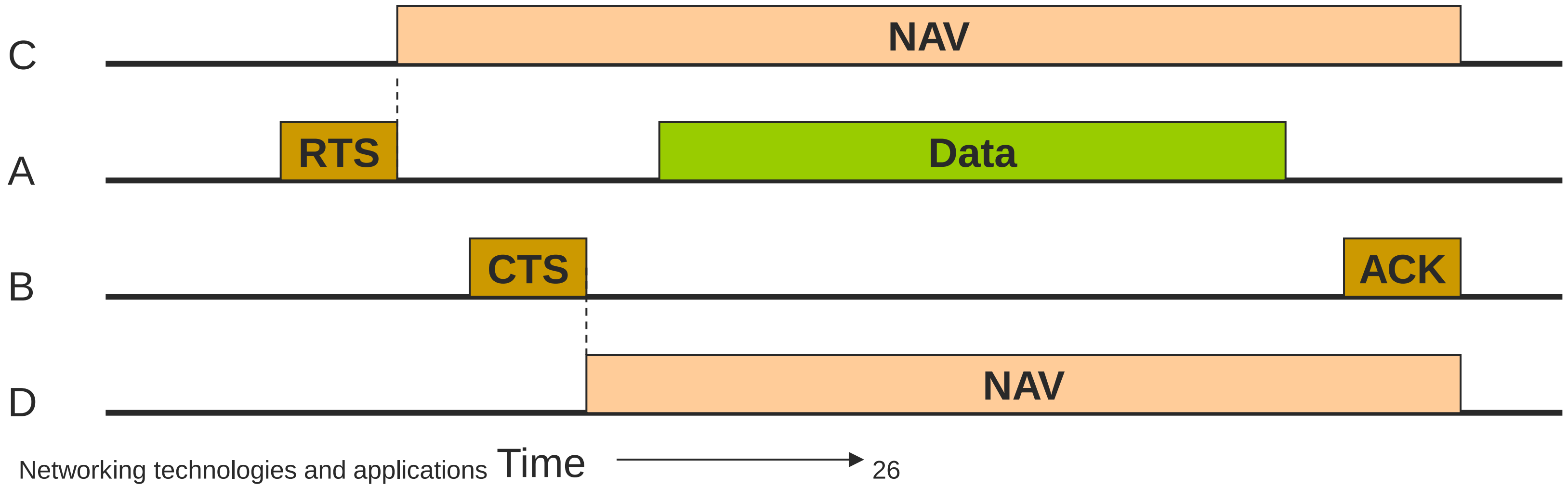
MACAW

- A sends an RTS frame to B, asking the permission to send a data frame
  - Request To Send
- If B gives the permission, it sends back a CTS frame
  - Clear To Send
- A sends the data frame, and starts an ACK timer
  - If B receives the packets in order, it replies with an ACK frame
  - If the timer expires without receiving an ACK, everything starts from scratch



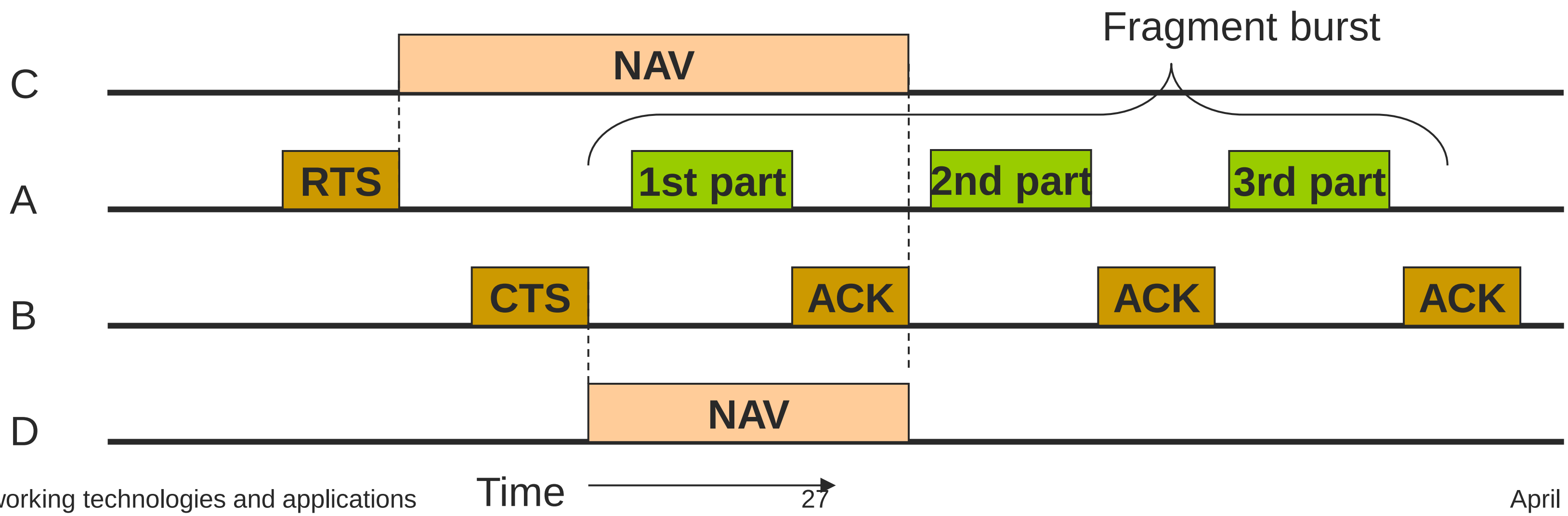
MACAW

- C hears A, receives the RTS frame
  - Deduces that in the next moments someone will start to send data
  - It stops its own transmission, while the other conversation is not finished
    - Knows when it ends from the ACK timer, included in the RTS frame
  - It sets an internal reminder to himself, saying that the channel is virtually occupied
    - NAV – Network Allocation Vector
- D does not hear about the RTS, but hears the CTS
  - Also sets a NAV for himself



Fragment burst

- In wireless networks, too much noise and high packet loss
  - The bigger a frame is, the higher the probability of an error is
- Frames can be split
  - If access to the channel is obtained through RTS/CTS, send several consecutive parts
    - **Fragment burst**
  - Increases transfer capacity
    - In case of an error, only the given part should be retransmitted
  - The NAV process avoids the collisions only for the first part
    - Newer solutions can take care of the entire burst



802.11 PCF

- The AP controls the communication
  - No collisions
- The AP polls the other stations, to find out who has data to send
  - The standard defines only some basic features of the poll
    - Does not define the frequency, or the order in which different stations are polled
    - Does not ask for equal treatment for all the stations
- The AP periodically sends a beacon frame
  - 10-100 beacons / s
  - It contains system parameters
    - Hopping sequence and dwell times (for FHSS), clock synchronization, etc.
  - New stations are invited to participate in the polling
- The AP can send some stations to sleep mode
  - Until the AP or the user does not wake them up
    - Spares the battery
  - The AP buffers (for a while) the packets intended to the sleeping node