The IEEE 802.11 standard

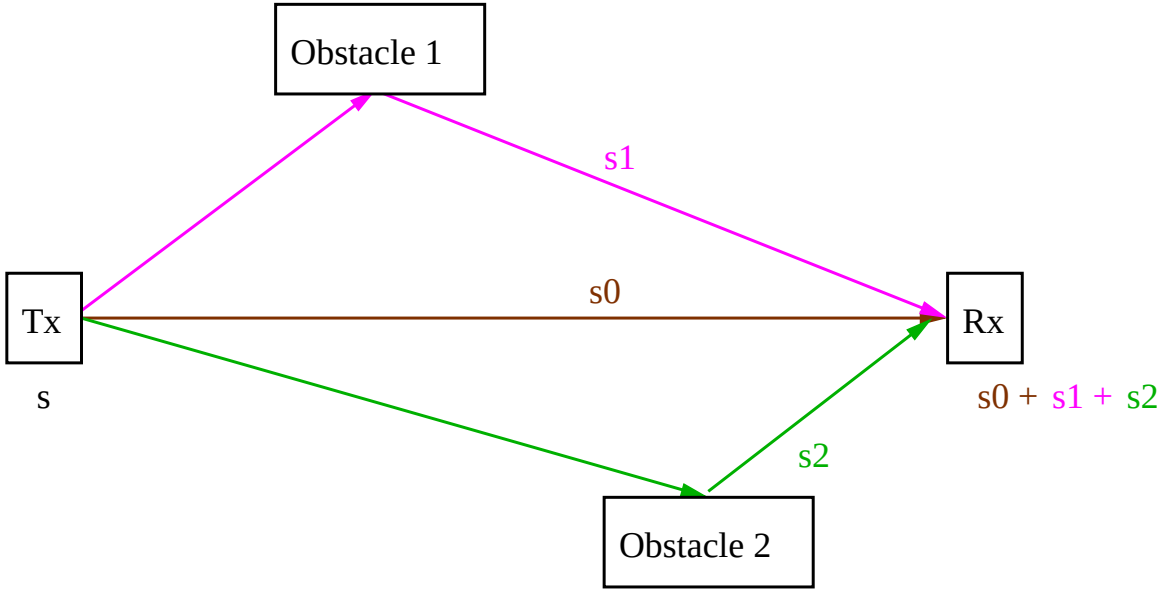
INRIA, Planete team

Outline

- **WLANs vs. Wired LANs**
- History
- Working modes
- MAC sub-layer
- The PHY layer (1997)
- The PHY Extensions (1999)
- Security

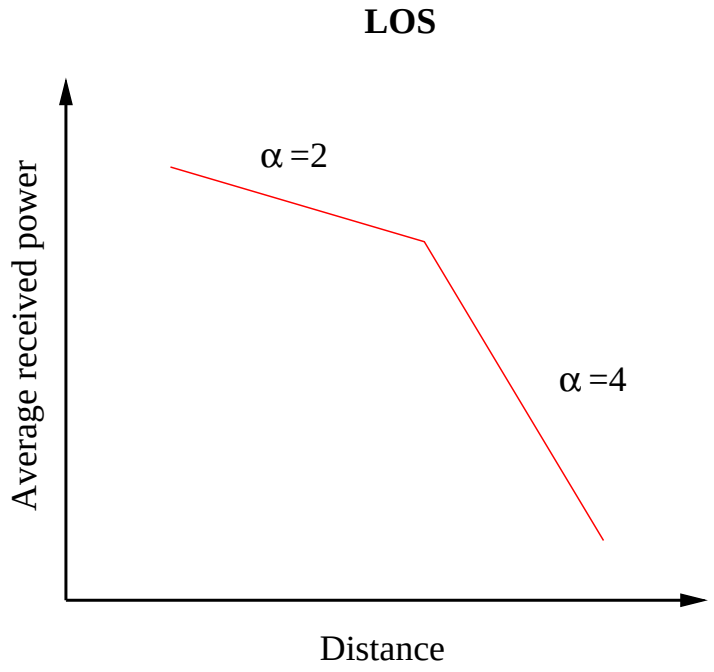
WLANs vs. Wired LANs

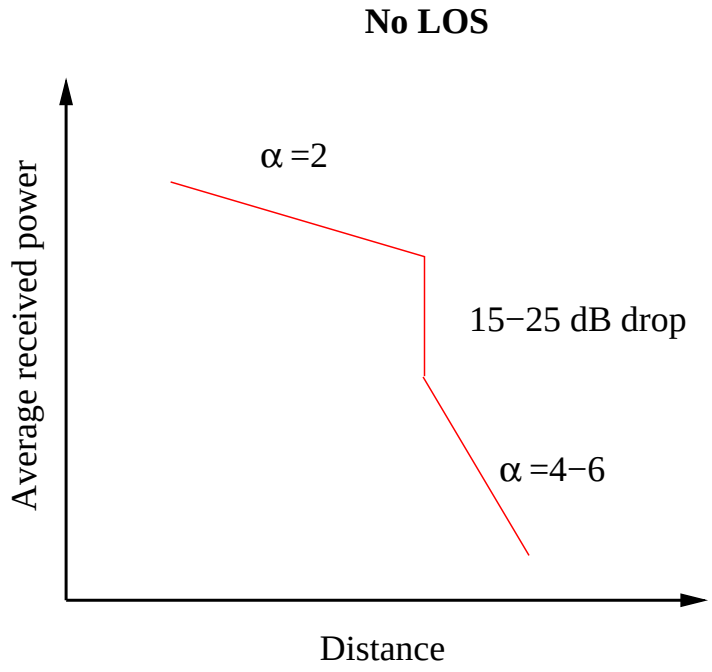
- No wires → Mobility
- Scarse bandwidth (?)
- Multipath, pathloss, interference / noise → BER



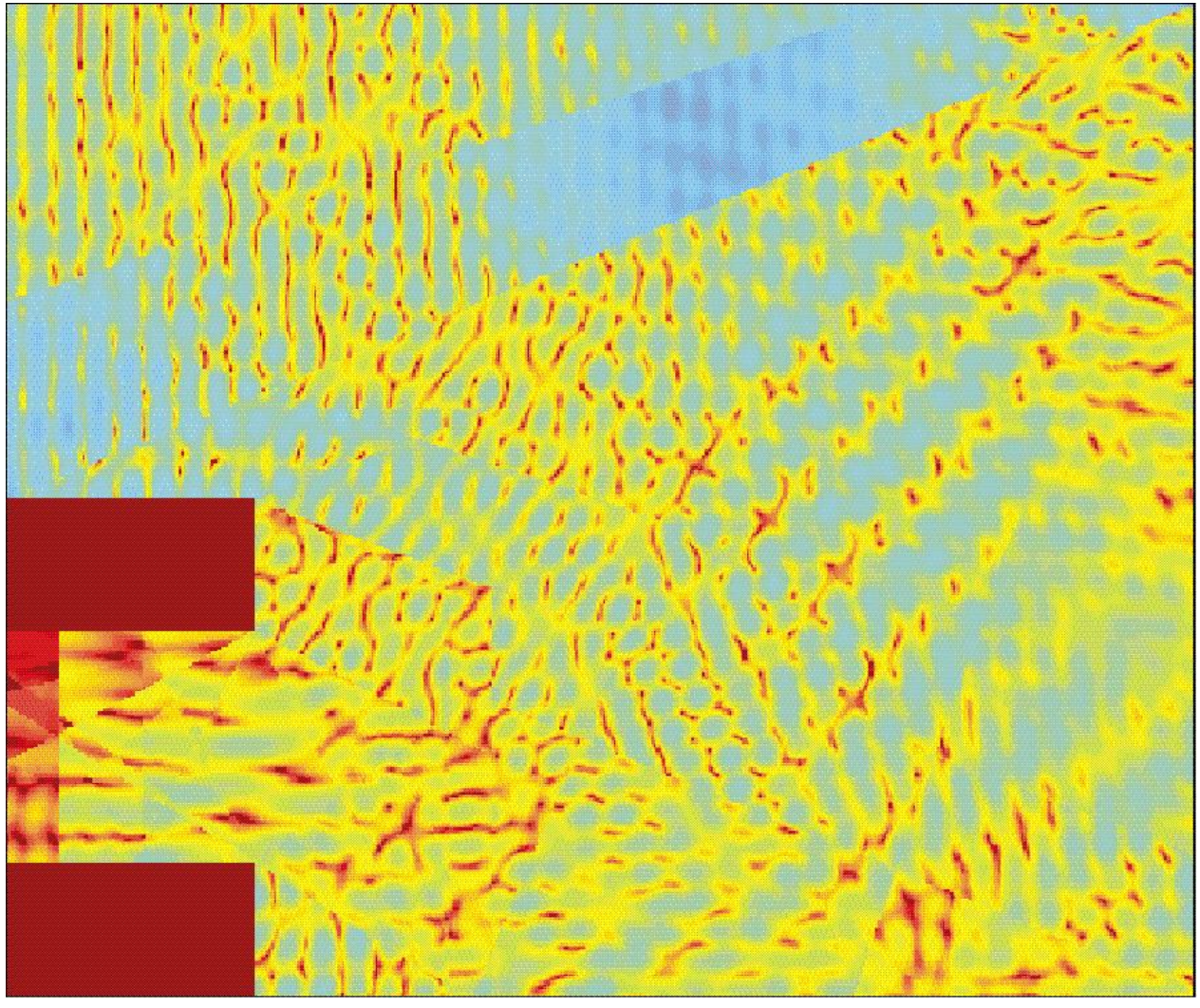
WLANs vs. Wired LANs

- No wires $\rightarrow$ Mobility
- Scarse bandwidth (?)
- Multipath, pathloss, interference / noise $\rightarrow$ BER





WLANs vs. Wired LANs

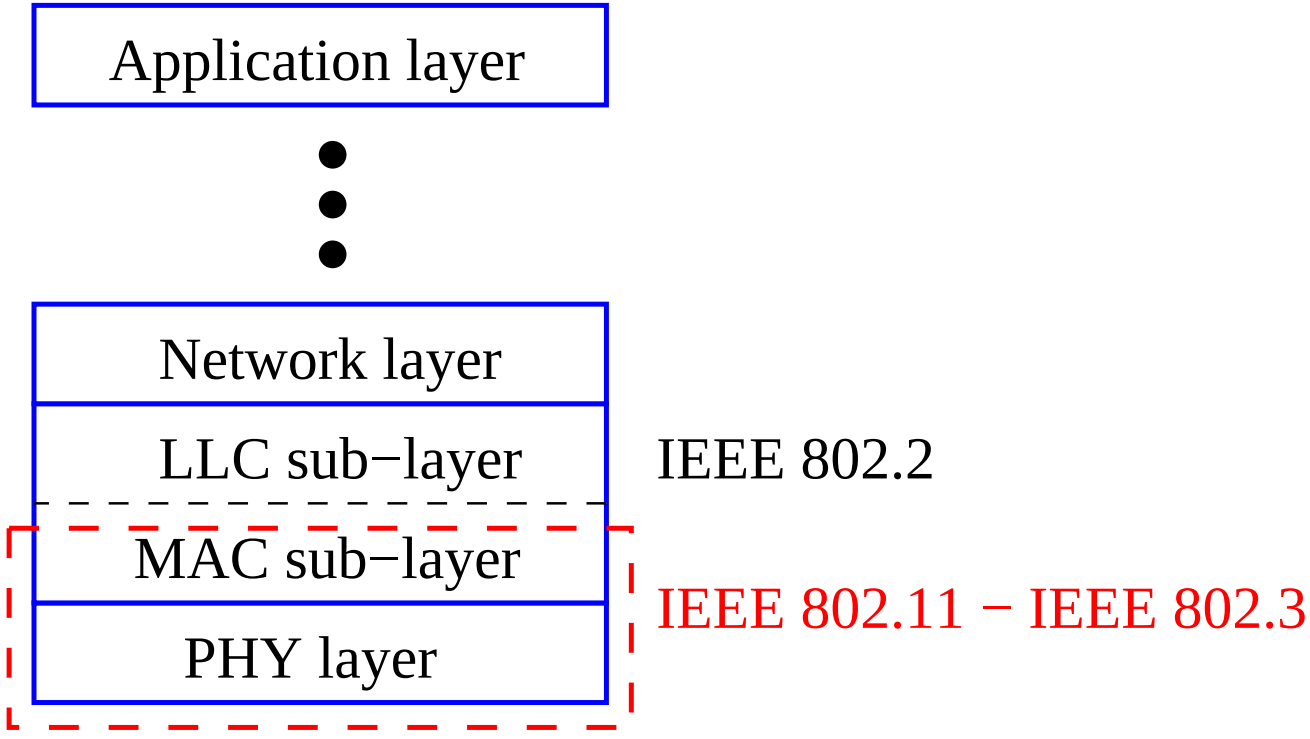


WLANs vs. Wired LANs

- No wires $\rightarrow$ Mobility
- The hidden node problem
- Scarse bandwidth (?)
- Multipath, pathloss, interference / noise $\rightarrow$ BER
- Protection / Privacy

WLANs vs. Wired LANs

WLANs vs. Wired LANs

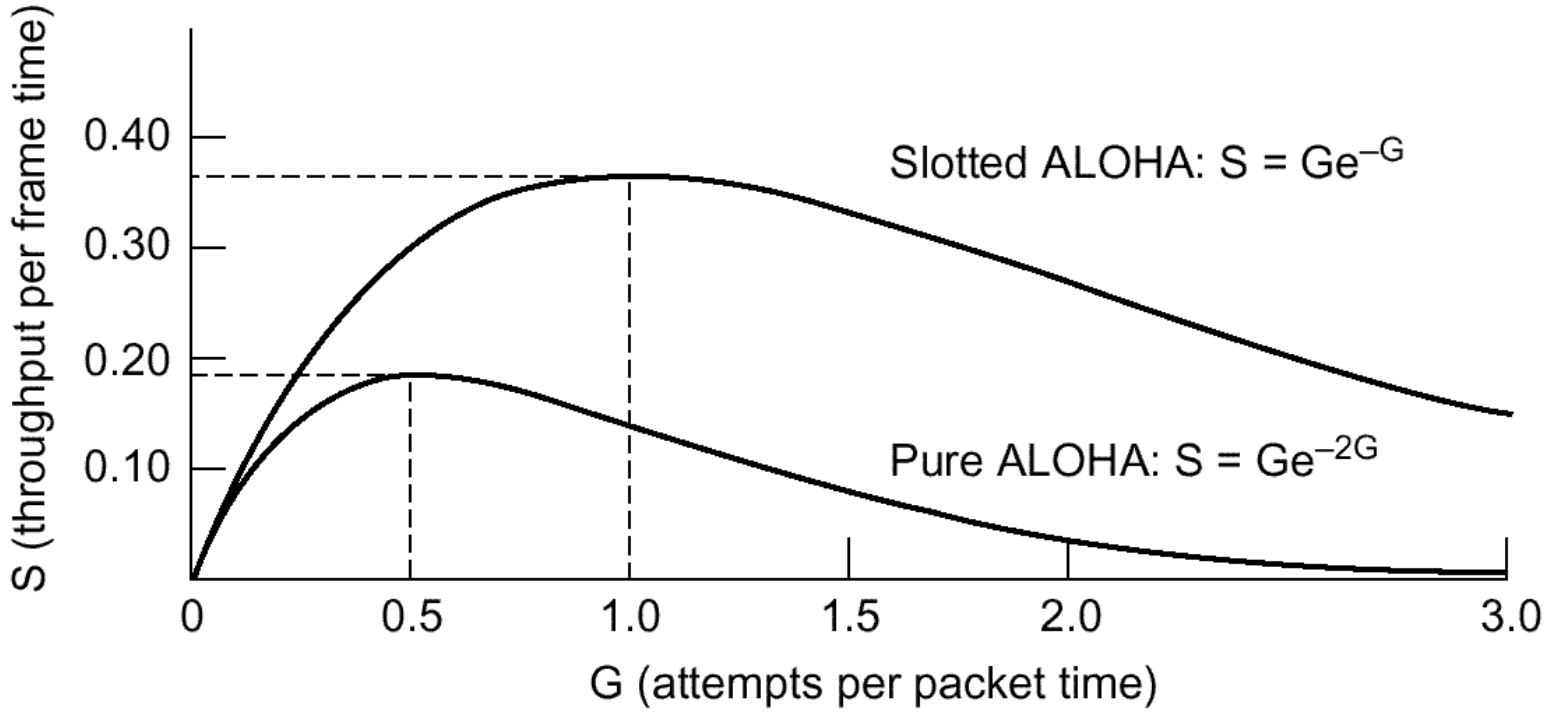


Outline

- WLANs vs. Wired LANs
- **History**
- Working modes
- MAC sub-layer
- The PHY layer (1997)
- The PHY Extensions (1999)
- Security

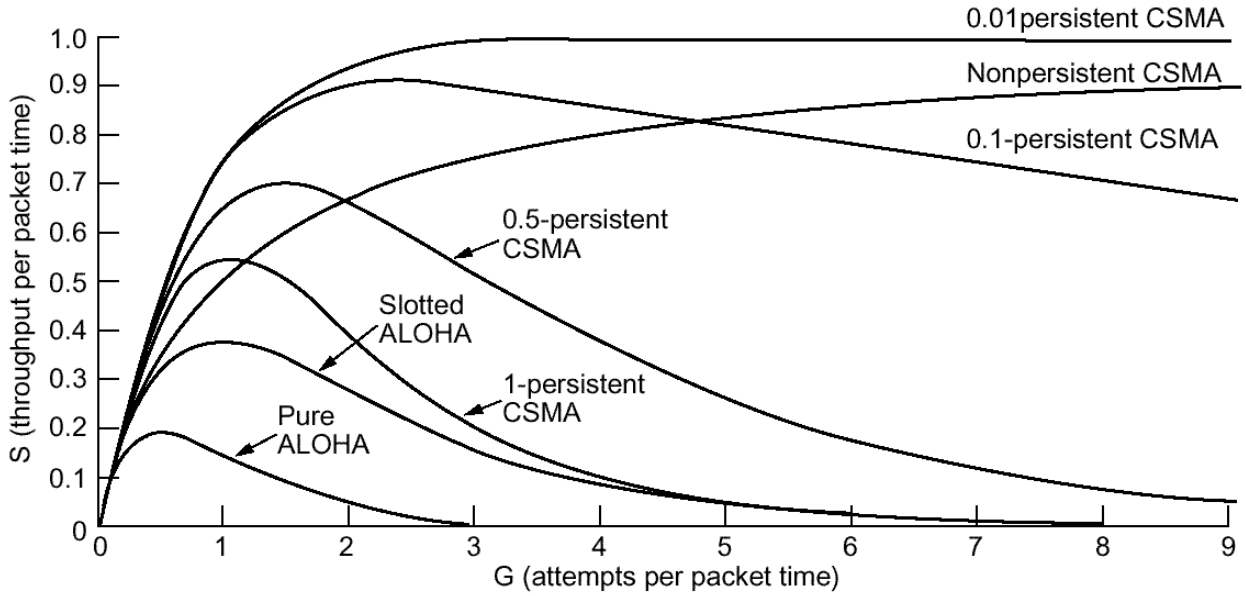
History

- 1970s: ALOHA
- 1972: Slotted ALOHA



History

- 1970s: ALOHA
- 1972: Slotted ALOHA
- 1975: Carrier Sense Multiple Access (CSMA)
  - non persistent
  - p-persistent



History

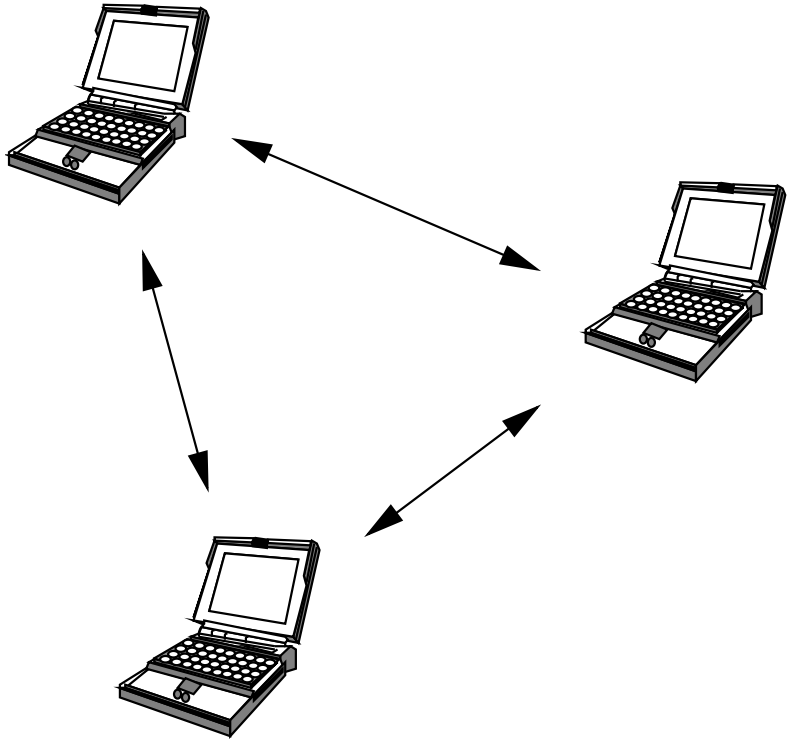
- 1970s: ALOHA
- 1972: Slotted ALOHA
- 1975: Carrier Sense Multiple Access (CSMA)
  - non persistent
  - p-persistent
- CSMA with collision detections (CD): Ethernet (1976)
- CSMA w/ coll. avoidance (CA): **IEEE 802.11 (1997)**

Outline

- WLANs vs. Wired LANs
- History
- **Working modes**
- MAC sub-layer
- The PHY layer (1997)
- The PHY Extensions (1999)
- Security

Working modes

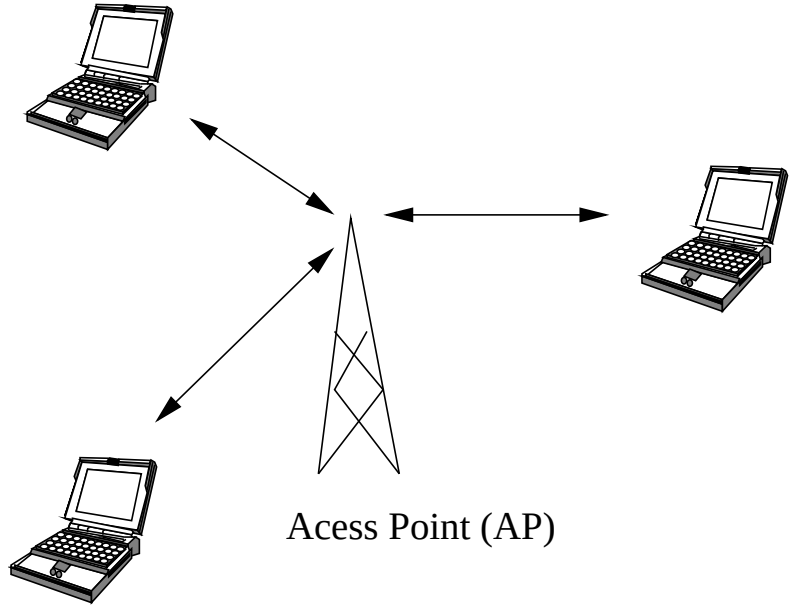
- Ad-hoc mode vs. Infrastructure mode (IS)
- Independent BSS (IBSS), Basic Service Set (BSS), Extended Service Set (ESS)



IBSS

Working modes

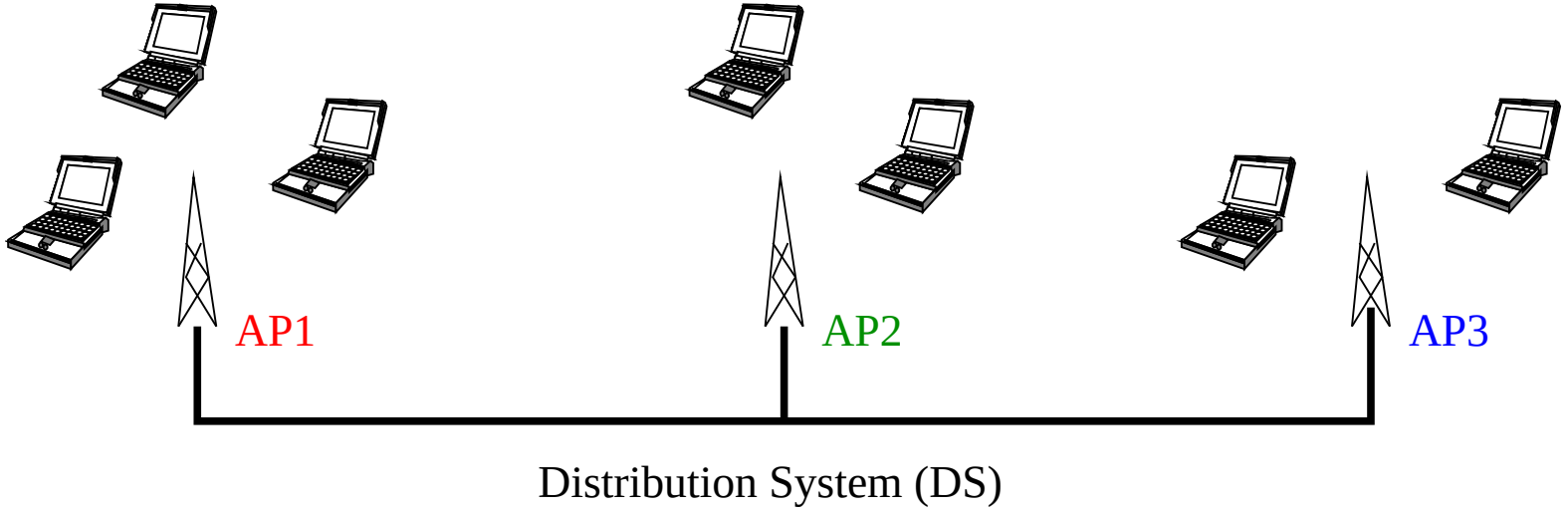
- Ad-hoc mode vs. Infrastructure mode (IS)
- Independent BSS (IBSS), Basic Service Set (BSS), Extended Service Set (ESS)



BSS

Working modes

- Ad-hoc mode vs. Infrastructure mode (IS)
- Independent BSS (IBSS), Basic Service Set (BSS), Extended Service Set (ESS)



ESS

- Handoff on the MAC sub-layer

Outline

- WLANs vs. Wired LANs
- History
- Working modes
- **MAC sub-layer**
- The PHY layer (1997)
- The PHY Extensions (1999)
- Security

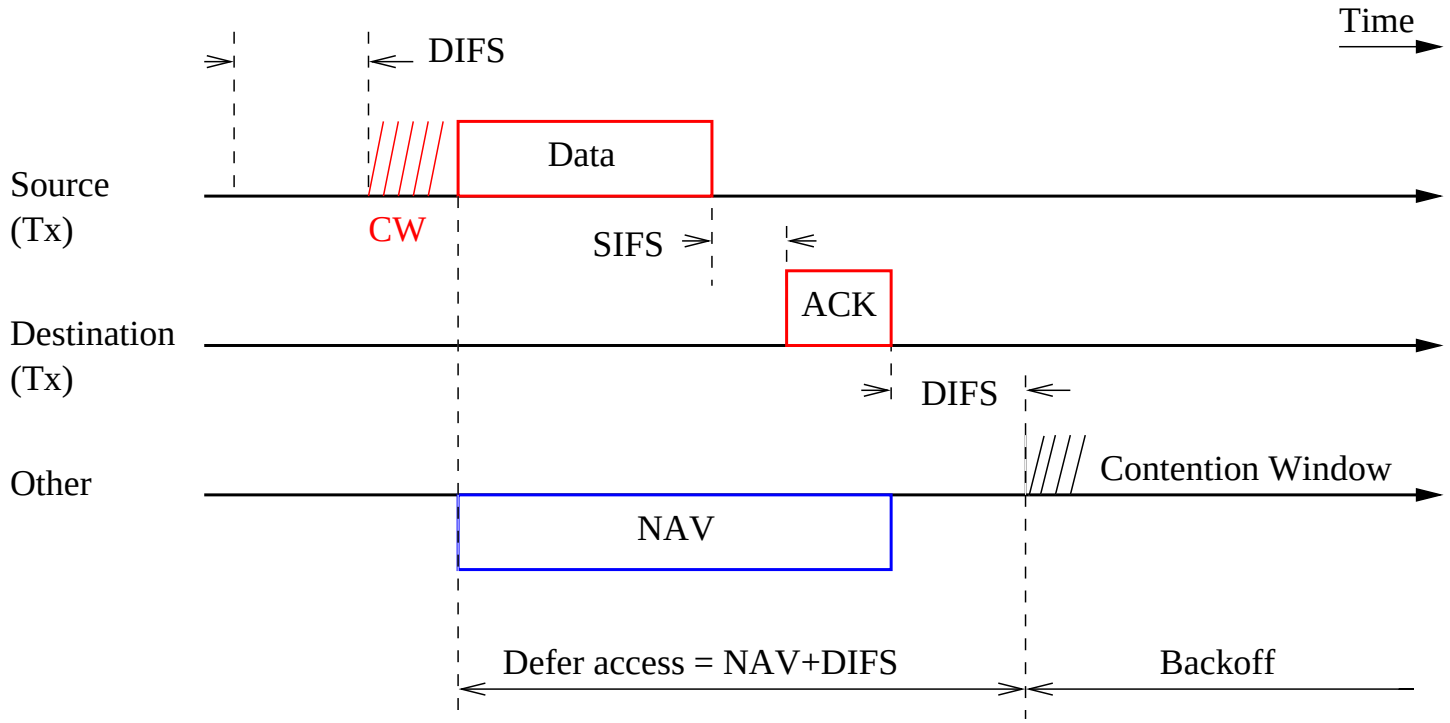
MAC sub-layer

DCF: Distributed Coordination Function (ad-hoc, IS modes)

PCF: Polling Coordination Function (in IS mode, optional)

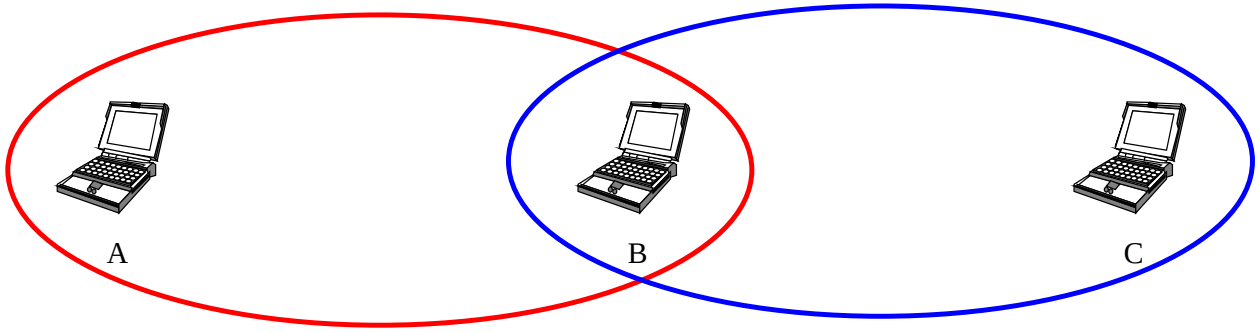
MAC sub-layer

DCF: Distributed Coordination Function (ad-hoc, IS modes)
- Basic machanism ($pktsize < RTSthreshold$)



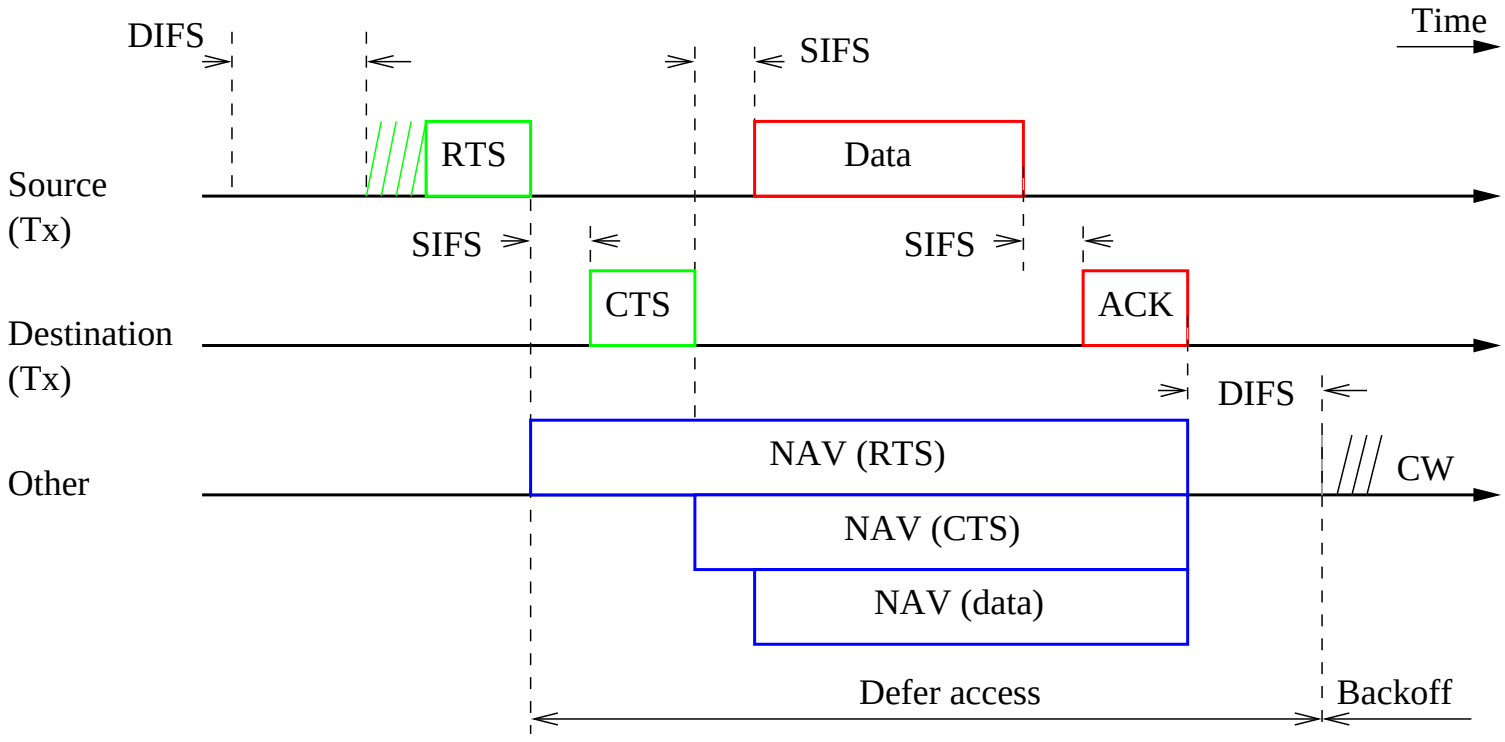
MAC sub-layer

DCF: Distributed Coordination Function (ad-hoc, IS modes)
- The hidden node problem



MAC sub-layer

DCF: Distributed Coordination Function (ad-hoc, IS modes)
- RTS/CTS mechanism ($pktsize \geq RTSthreshold$)



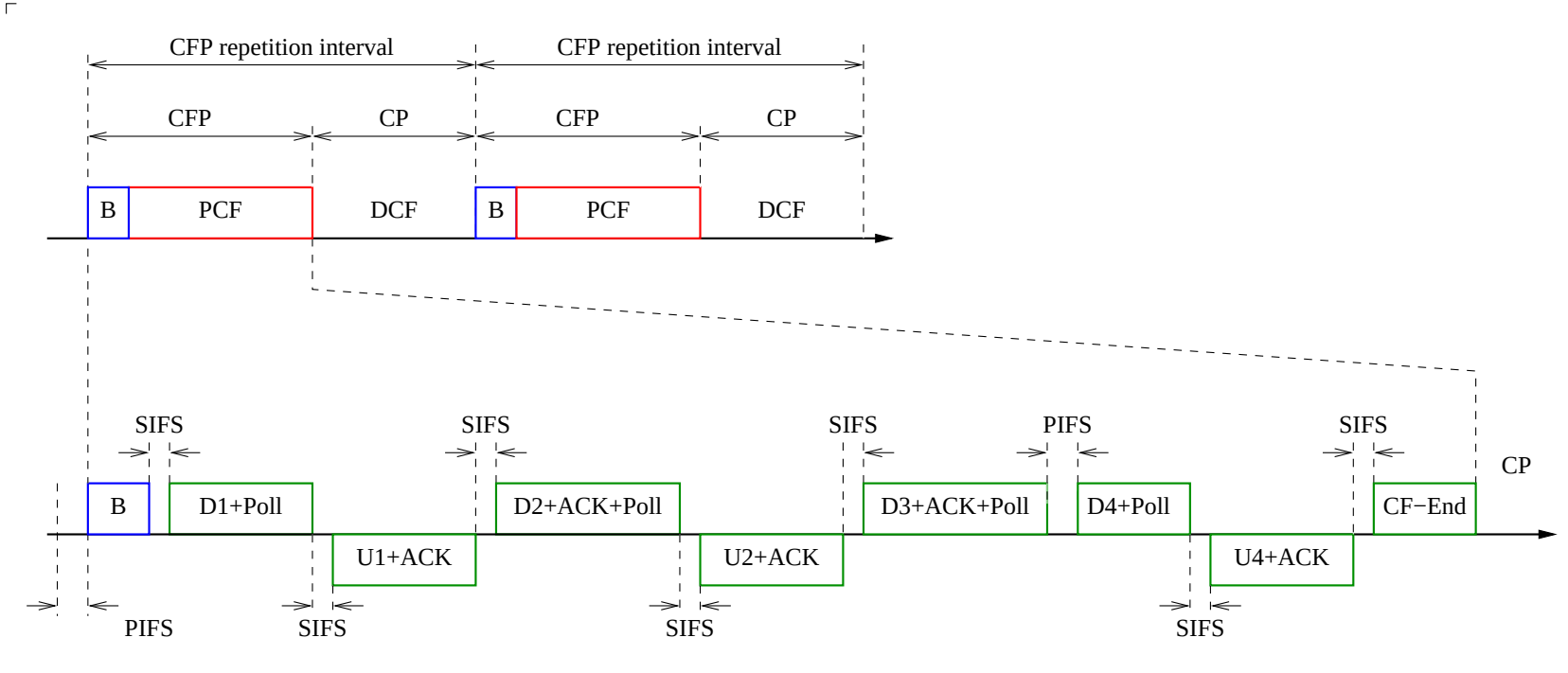
MAC sub-layer

DCF: Distributed Coordination Function (ad-hoc, IS modes)
- Fairness ? ... depends on scenario
- QoS ? ... not yet ... wait for 802.11e

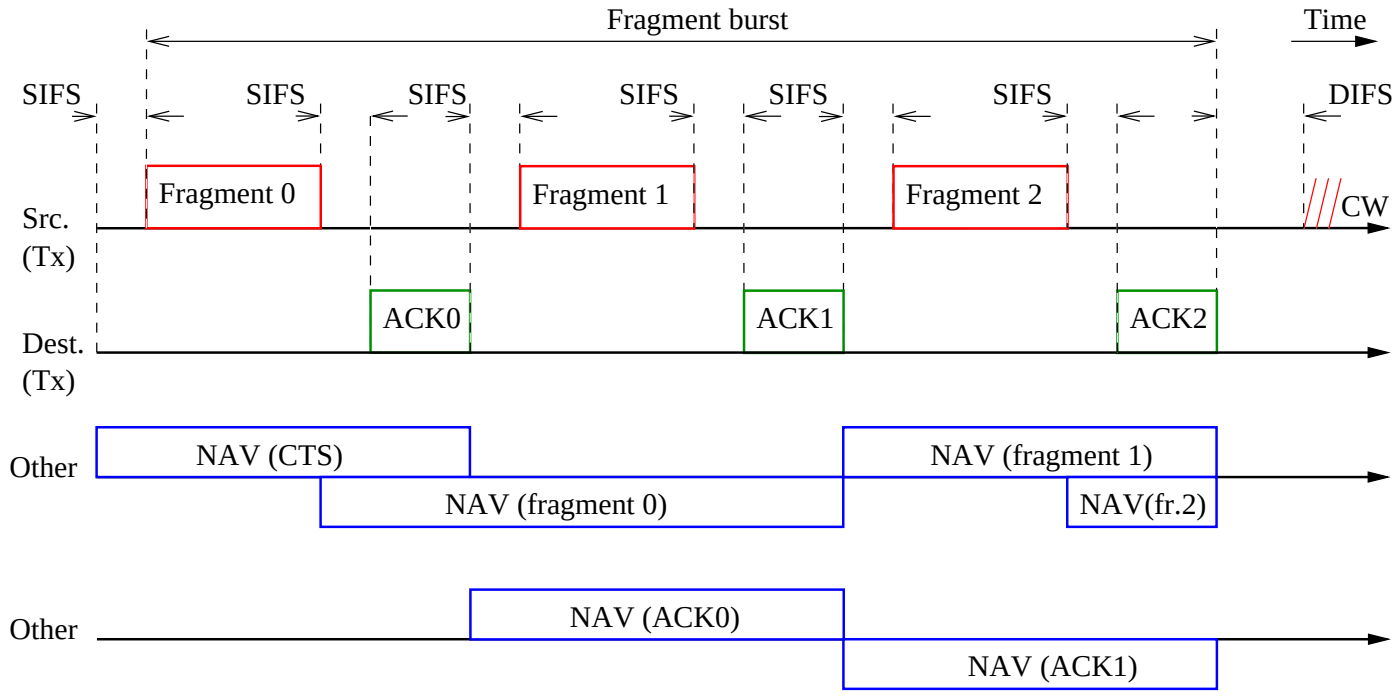
MAC sub-layer

DCF: Distributed Coordination Function (ad-hoc, IS modes)

PCF: Polling Coordination Function (in IS mode, optional)



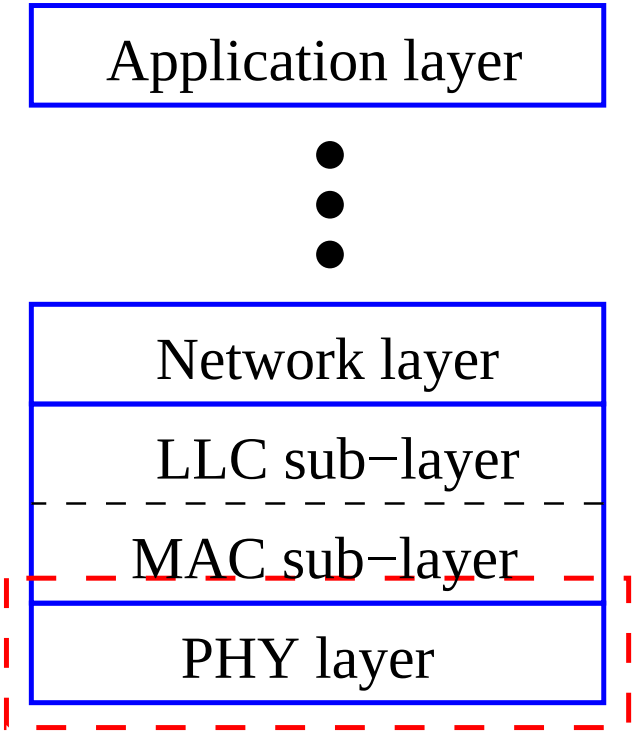
Packet fragmentation



Outline

- WLANs vs. Wired LANs
- History
- Working modes
- MAC sub-layer
- **The PHY layer (1997)**
- The PHY Extensions (1999)
- Security

The PHY layer (1997)

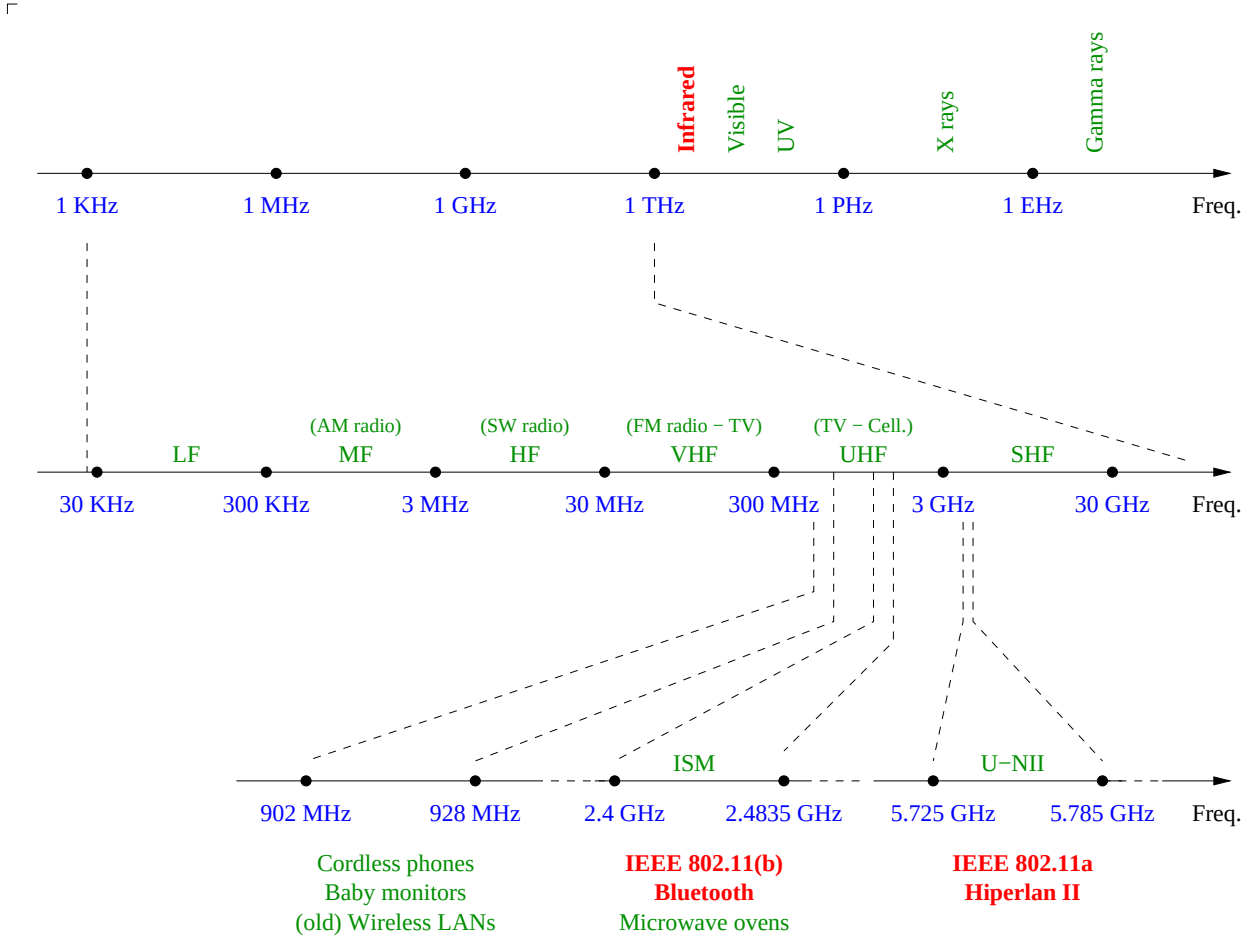


3 PHY types:

- DSSS (most products)
- FHSS (less products)
- IR (unknown products)

The PHY layer (1997)

the EM spectrum allocation

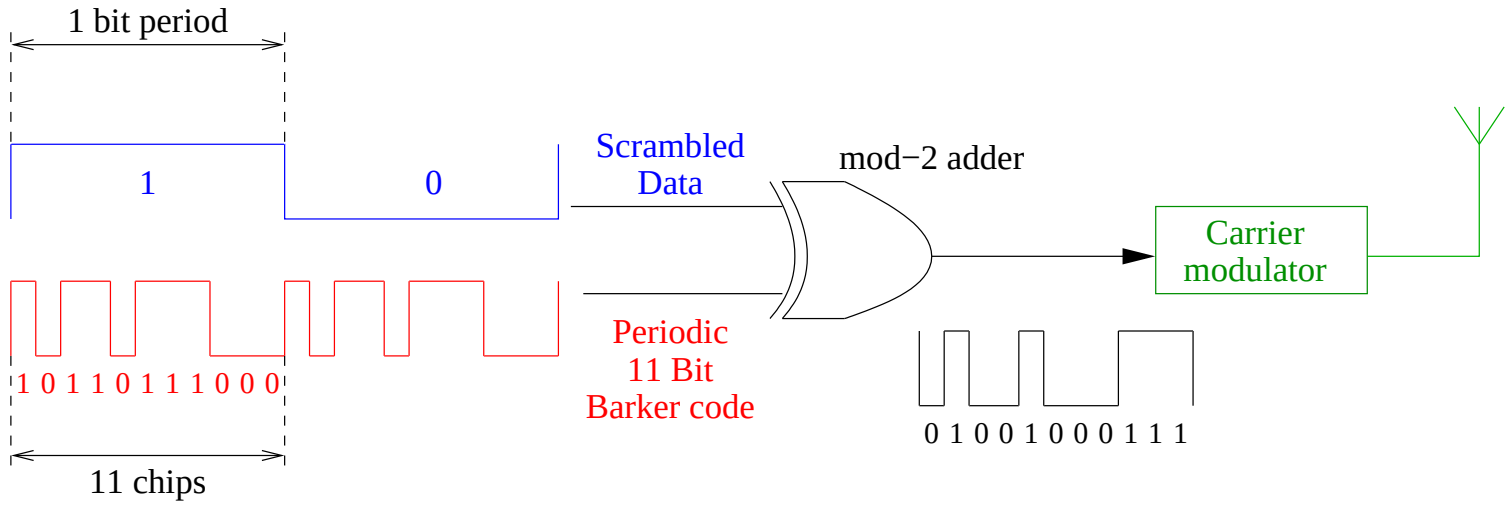


The PHY layer (1997)

- **DSSS (Direct Sequence Spread Spectrum)**
- FHSS (Freq. Hopping Spread Spectrum)
- IR (Infra Red)

The PHY layer (1997)

DSSS: principle

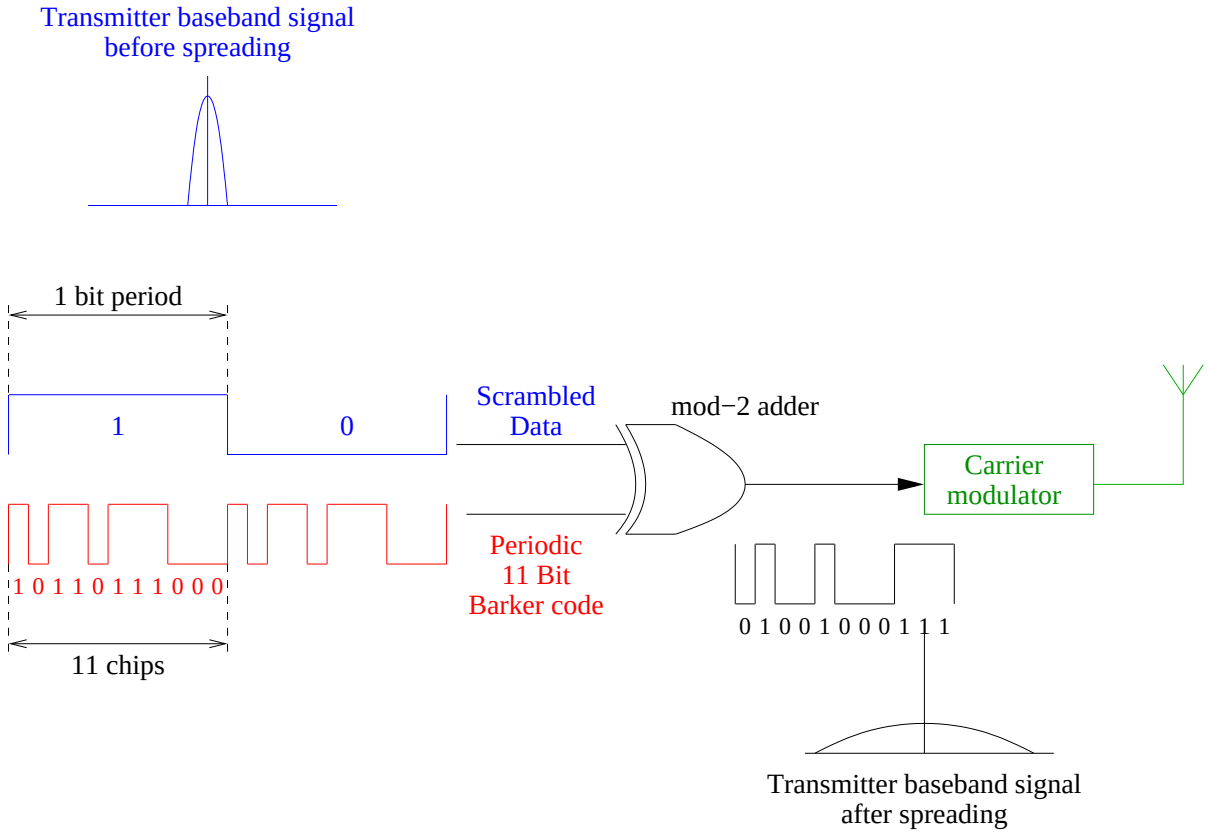


Note:

- single code (11-chips)
- multiple access ? ... no
- security ? ... no

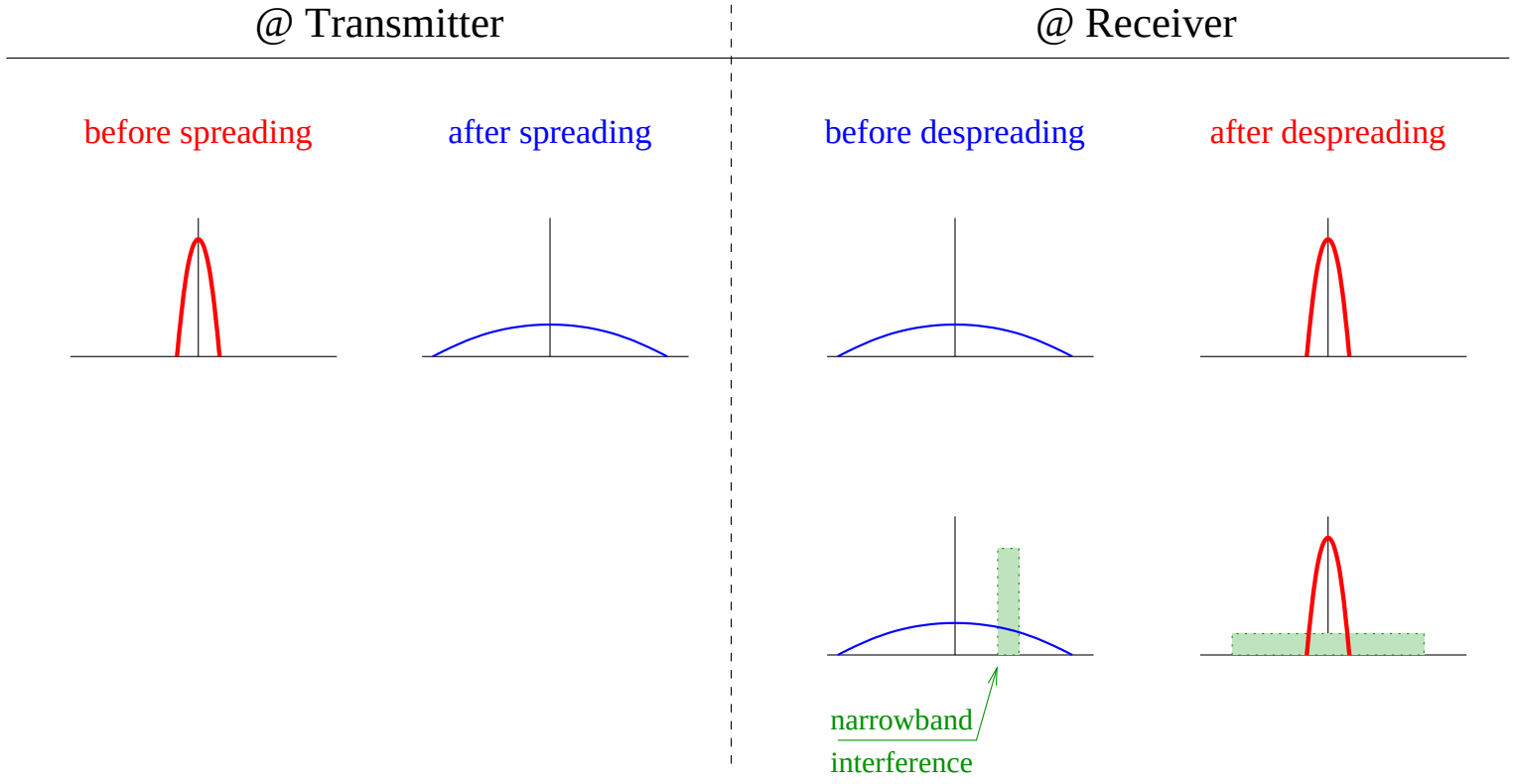
The PHY layer (1997)

DSSS: principle



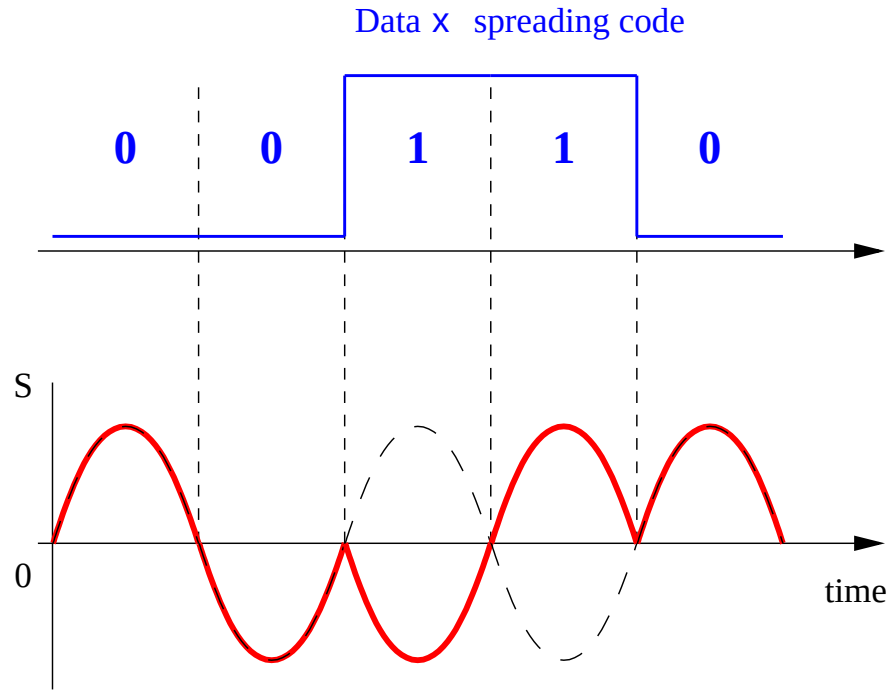
The PHY layer (1997)

DSSS: principle



The PHY layer (1997)

PSK (Phase Shift Keying)

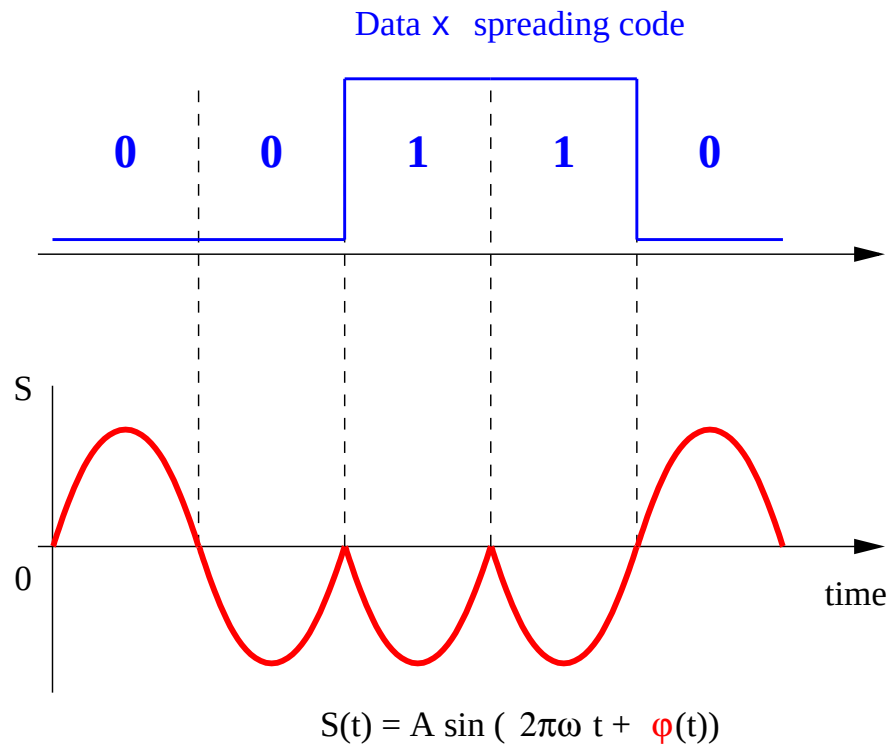


$S(t) = A \sin(2\pi\omega t + \varphi(t))$

$\varphi = 0$

The PHY layer (1997)

DPSK (Differential PSK):
no reference signal needed

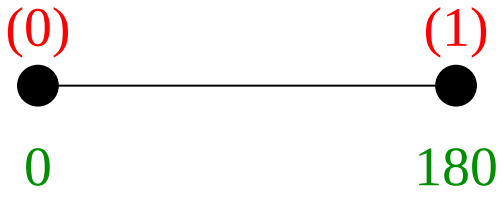


$S(t) = A \sin(2\pi\omega t + \varphi(t))$

The PHY layer (1997)

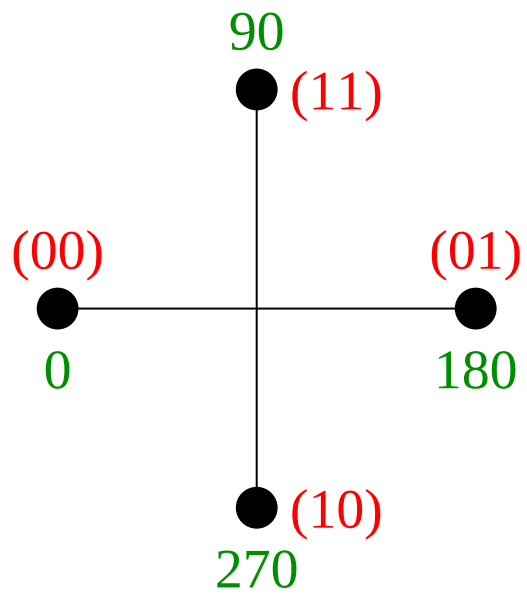
DSSS: modulation

DBPSK



1 Mbps

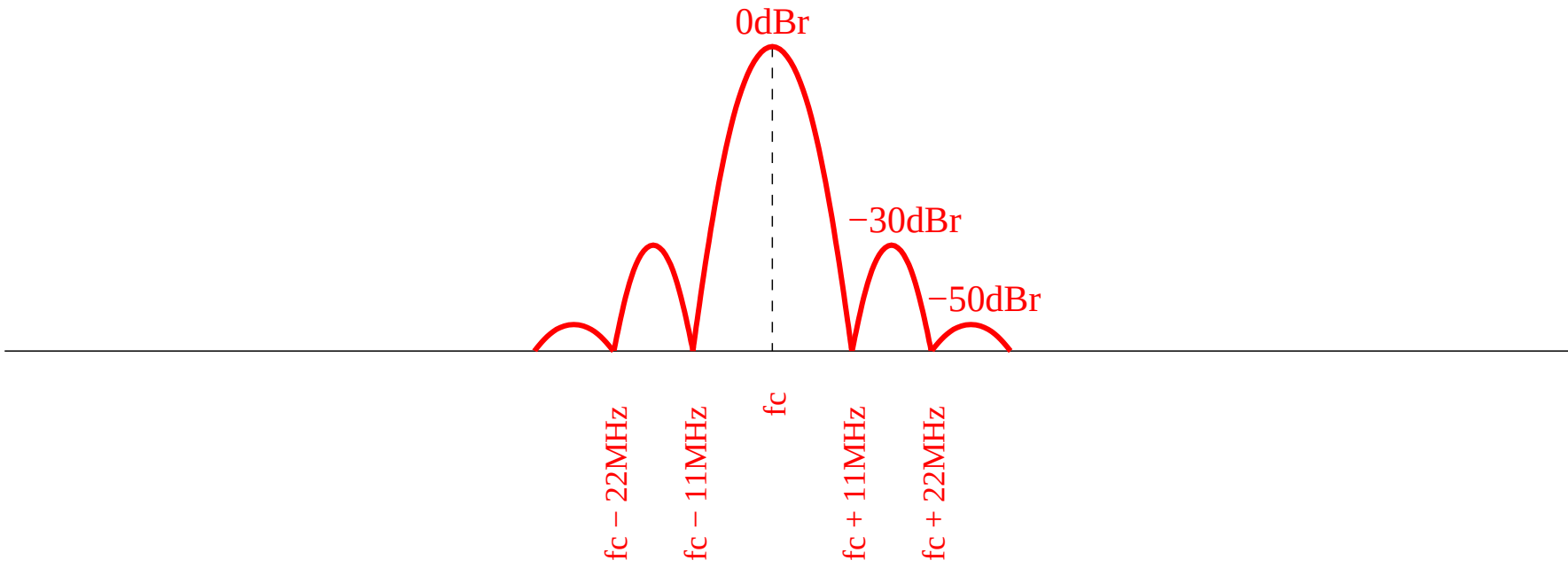
DQPSK



2Mbps

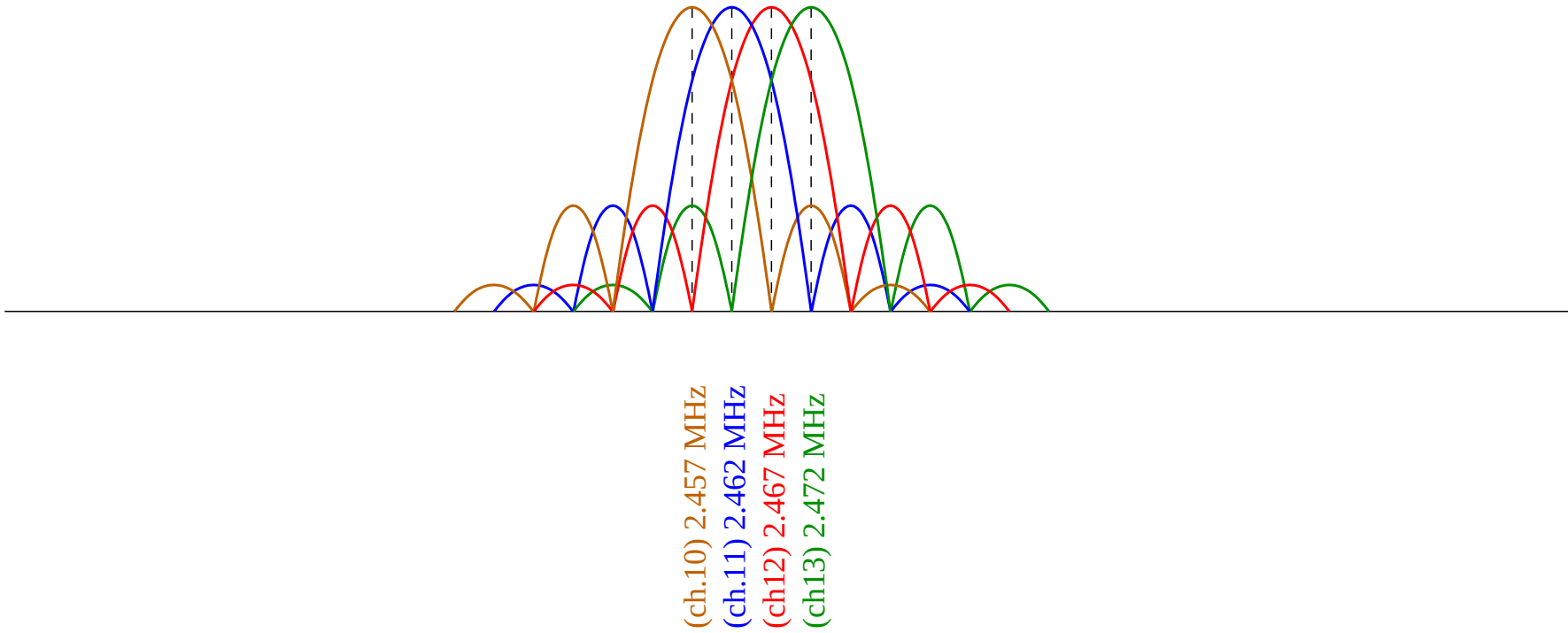
The PHY layer (1997)

DSSS: Spectrum @ modulator output



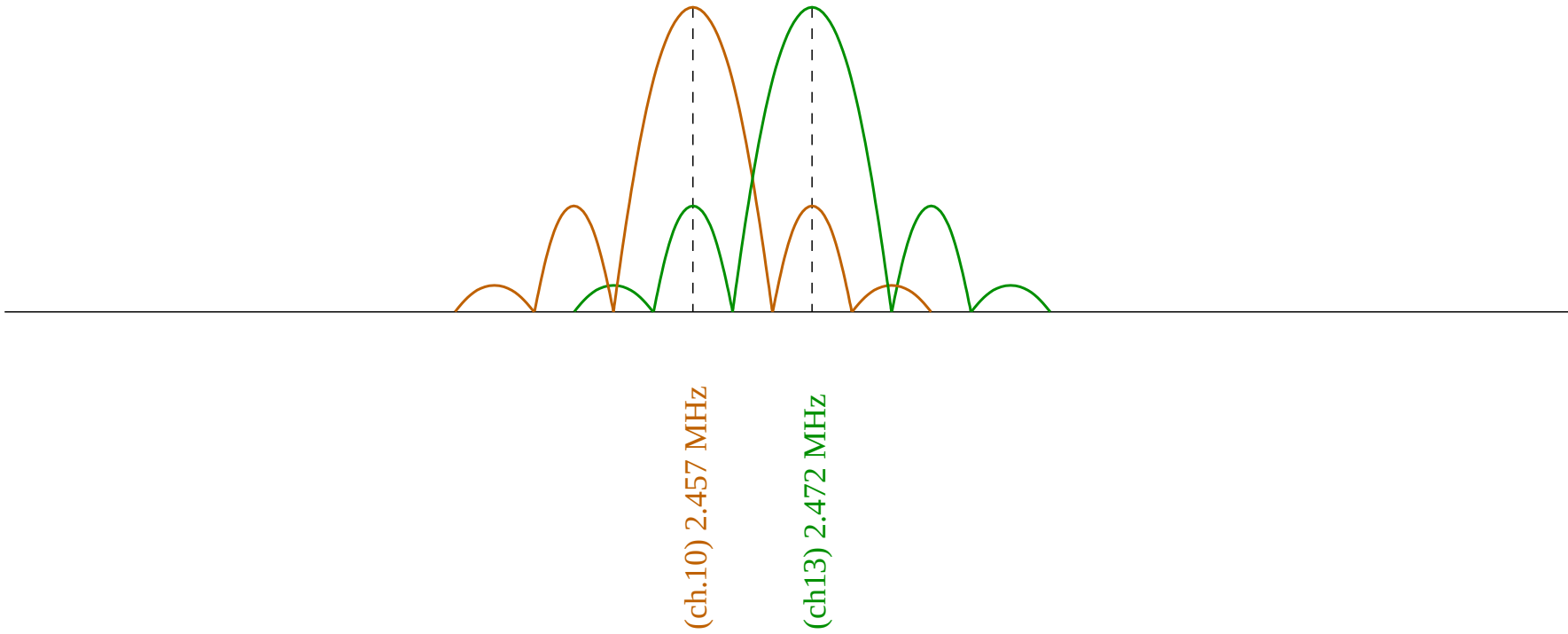
The PHY layer (1997)

in France (few months ago): allowed channels



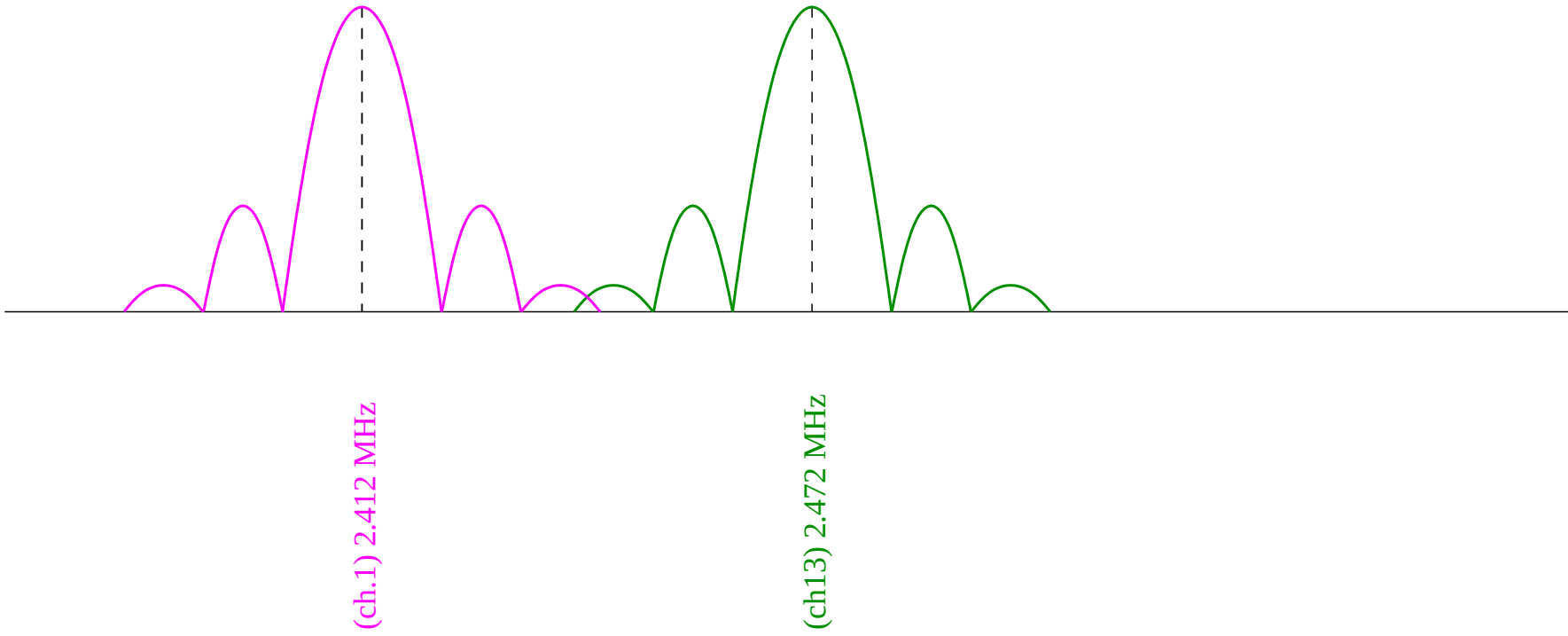
The PHY layer (1997)

in France (few months ago): maximum channel separation



The PHY layer (1997)

in Europe



The PHY layer (1997)

Transmission power

	GSM	μ wave oven	IEEE 802.11
Typical	100 mW - 600 mW	0.2mW/cm^2	6.3 mW
Regulations		1-5 mW/cm^2 @ 5cm	100 mW (Eur.)

The PHY layer (1997)

- DSSS (Direct Sequence Spread Spectrum)
- **FHSS (Frequency Hopping Spread Spectrum)**
- IR (Infra Red)

The PHY layer (1997)

FHSS

- Modulation: GFSK
  binary 0/1: $F_c \pm f_d$ (for 1 Mbps)
  00, 01, 10, 11: $F_c \pm 2f_d$ (for 2 Mbps)
- F_c sequence = $F_x(i) = [b(i) + x] mod(35) + 48$ (France)
  $b(i)$: tables
  x: 3 sets
- Fast-FH vs. Slow-FH: min 2.5 hops/s
- Bluetooth interference ?... YES

The PHY layer (1997)

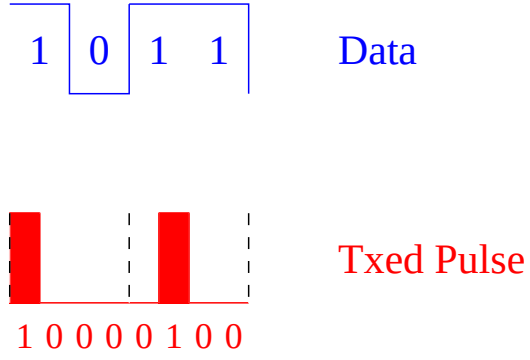
- DSSS (Direct Sequence Spread Spectrum)
- FHSS (Freq. Hopping Spread Spectrum)
- **IR (Infra Red)**

The PHY layer (1997)

Infra Red (IR)
Pulse Position Modulation (PPM)

- 1 Mbps: 4 data bits $\rightarrow$ 16-PPM symbol
- 2 Mbps: 2 data bits $\rightarrow$ 4-PPM symbol

Data bits	4−PPM symbol
00	0001
01	0010
10	0100
11	1000



Outline

- WLANs vs. Wired LANs
- History
- Working modes
- MAC sub-layer
- The PHY layer (1997)
- **The PHY Extensions (1999)**
- Security

PHY Extensions (1999)

IEEE 802.11b: 2.4 GHz. 1Mbps, 2Mbps, 5.5Mbps 11 Mbps.

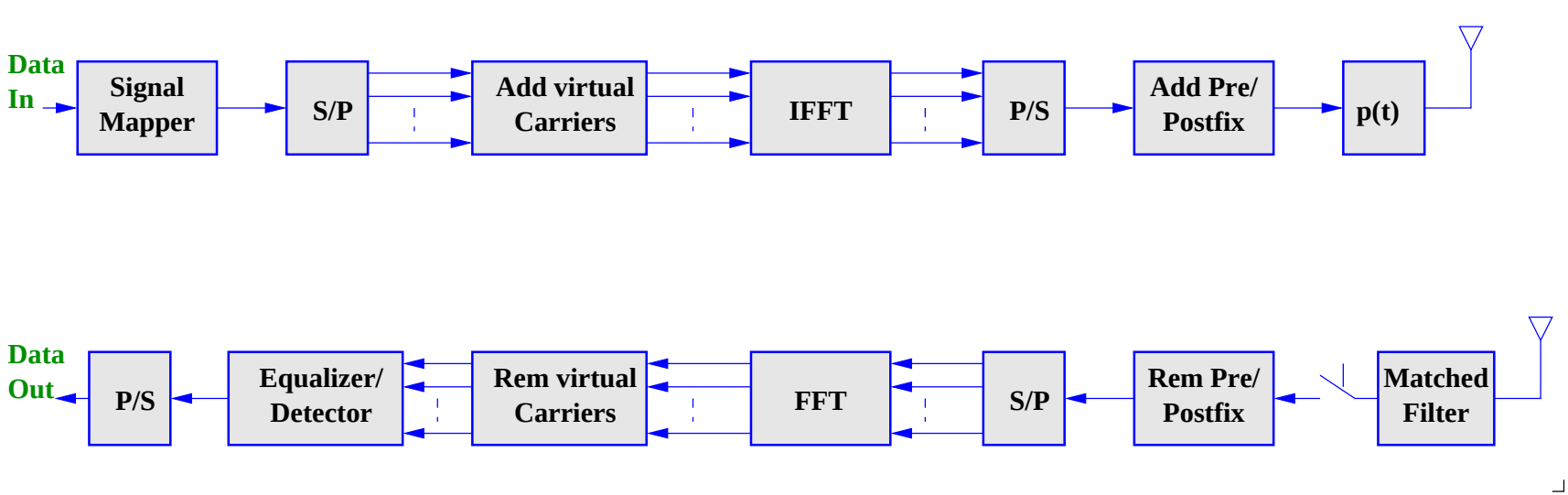
- High Rate DSSS
- Modulation: (backward compatible)DBPSK, DQPSK Complementary Code Keying (CCK) + DQPSK, (opt.) Packet Binary Convolutional Coding (PBCC) + (BPSK,QPSK)
- Currently the most widely used one

PHY Extensions (1999)

IEEE 802.11a: 5.7 GHz, 6 Mbps $\rightarrow$ 54 Mbps!!

- OFDM (Orthogonal Frequency Division Multiplexing)
  - Principle:
    High-rate data is devided into several lower rate binary signals.
    Each low-rate signal modulates a different sub-carrier (48)
    Sub-carrier sets are orthogonal.
  - Modulation: BPSK, QPSK, 16QAM and 64QAM
- FEC: Convolutional encoding needed (Viterbi)
- Close to Hiperlan 2 specs.
- “coming soon”

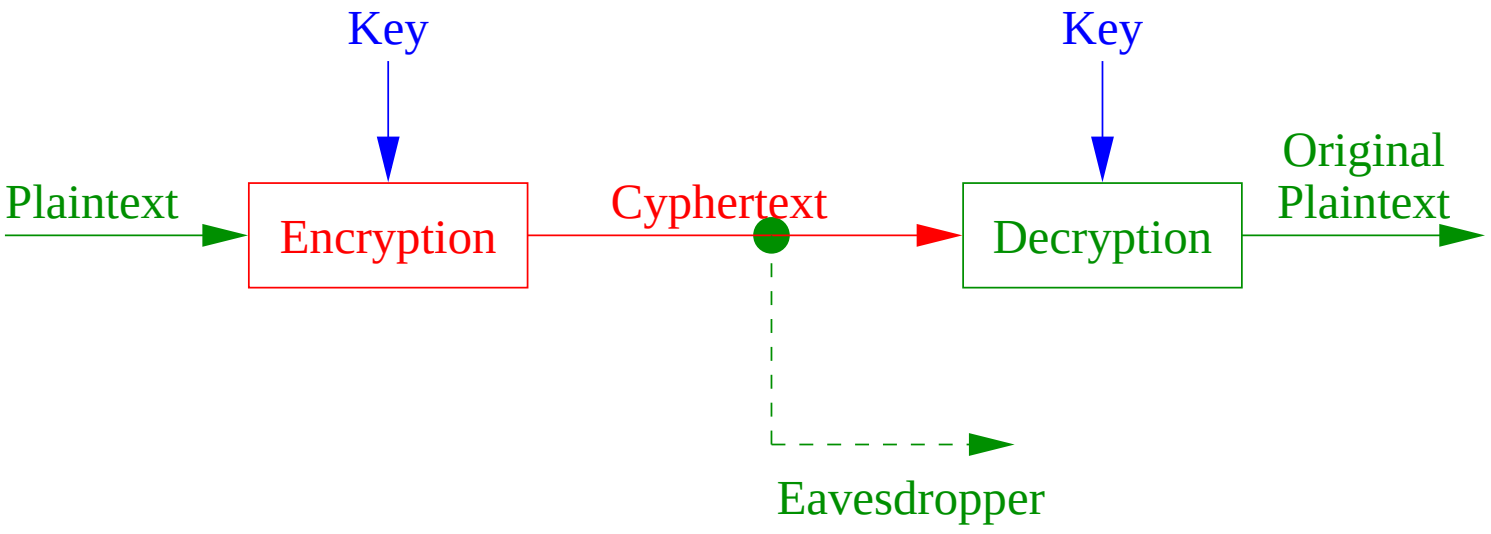
PHY Extensions (1999)



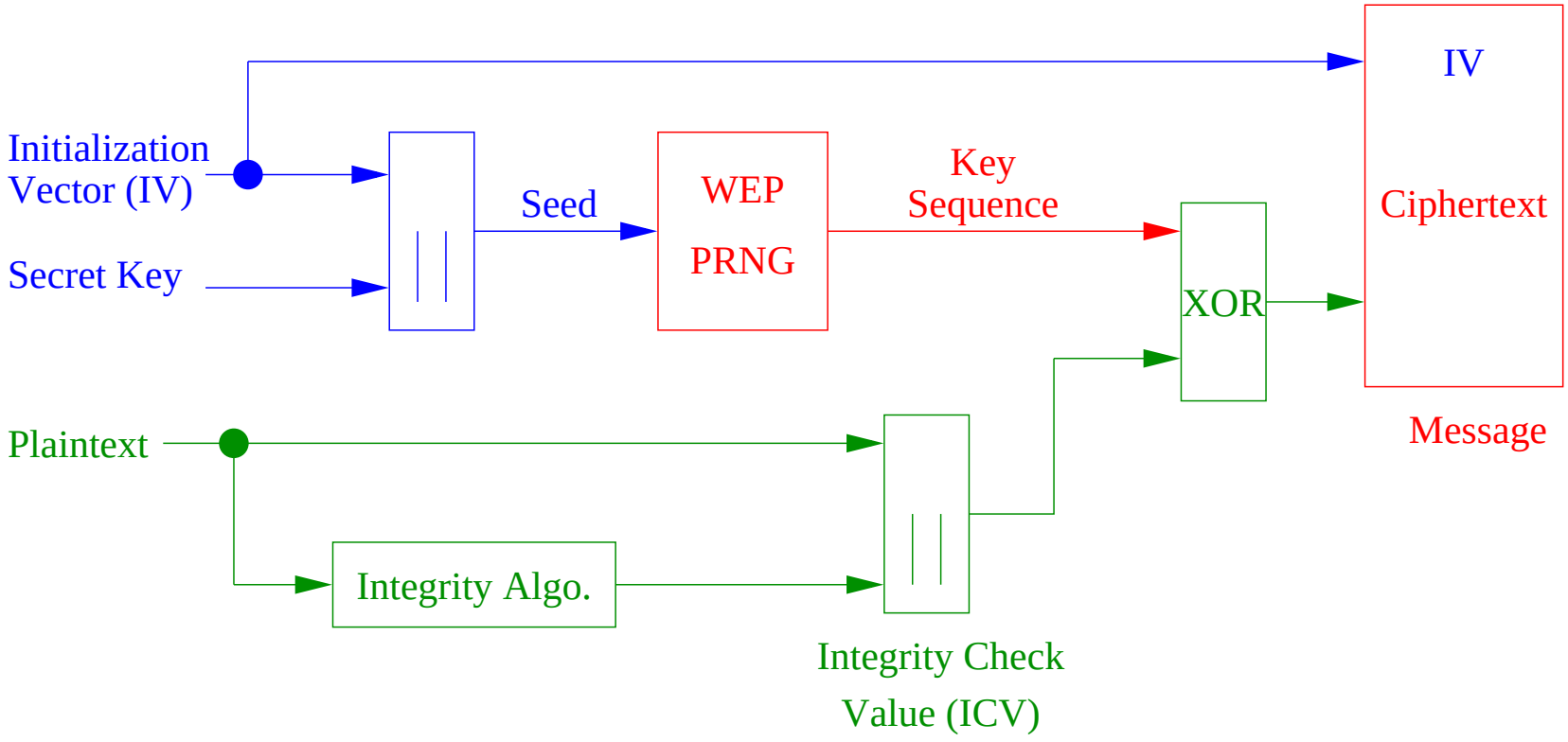
Outline

- WLANs vs. Wired LANs
- History
- Working modes
- MAC sub-layer
- The PHY layer (1997)
- The PHY Extensions (1999)
- **Security**

WEP (Wired Equivalent Privacy)



WEP (Wired Equivalent Privacy)



Security

WEP (Wired Equivalent Privacy)

- default keys / established keys
- 40-128 bit key
- Algorithm: RC4 (symmetric stream cypher)
- Cracking tools: WEPcrack, AirSnort:
  if “100MB-1GB of data can be gathered” then one “can guess the encryption password in less than a second”!!

Access control table ? ... inefficient
Network ID ? ... inefficient

Conclusion

- it works!
- looks just like ethernet to higher layers
- no QoS support... yet.
- limited security management.