

Wireless Networks

Wenyuan Xu

Department of Computer Science and Engineering
University of South Carolina

2008

CSCE790: Security and Privacy for Emerging Ubiquitous Communication system

Outline

- Wireless Fundamentals
 - Physical layer
- Various standards and the corresponding wireless networks:
 - 802.11
 - WiFi Hotspots
 - MANET / VANET
 - Wireless Mesh Networks
 - 802.15
 - Bluetooth
 - RFID

Wireless networks

■ Wireless networks

- “*any* type of network whose interconnections between nodes is implemented without the use of wires.”
- “generally implemented with some type of remote information transmission system that uses **electromagnetic waves**
 - radio
 - infrared

Radio Frequency Communication

- Wikipedia: RF = “portion of the electromagnetic spectrum in which electromagnetic waves can be generated by alternating current fed to an antenna”



Some History

- 1873 – “*A Dynamical Theory of the Electromagnetic Field.*” by James Clerk Maxwell
- 1887 - Heinrich Hertz demonstrates spark-gap transmitter – *didn't think it is very useful!*
- 1890 - Edouard Branly demonstrates practical coherer
- 1893-97 - Nikola Tesla, Oliver Lodge, Jagdish Chandra Bose, Alexander Popov, Guglielmo Marconi demonstrated “lab” models of their “wireless devices”
- 1897 - Wireless Telegraph and Signal Company, Ltd. In London
- 1901 – successful transmission across the Atlantic Ocean (“a bit more” power and bigger antennas)

Some History (contd)



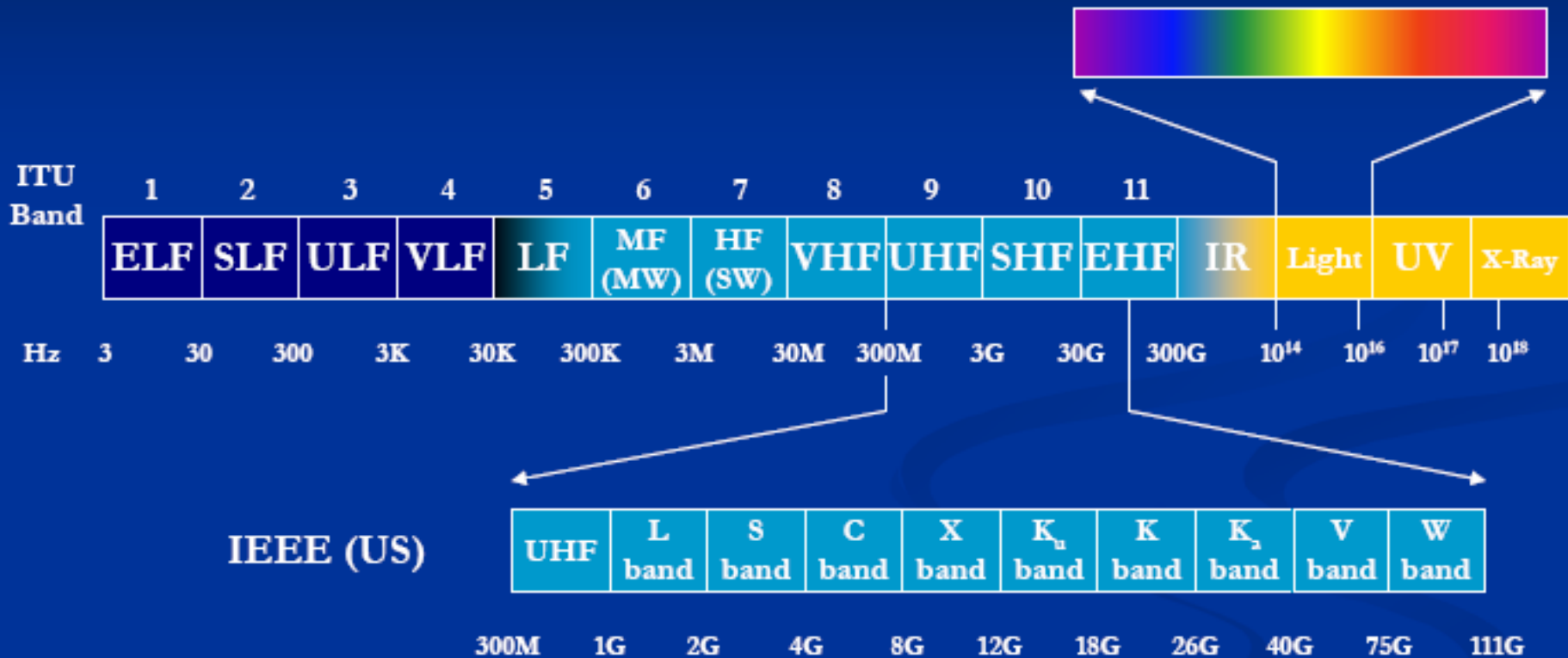
- Q: What do they have to do with radio?
- A: Nothing but after Titanic, spark-gap transmitters quickly became universal on large ships
- Radio Act of 1912 – all ships must maintain 24-hour radio watch and keep in contact with nearby ships and coastal radio stations
 - → interference → tuning → modulation
- Radio Act of 1927 – created Federal Radio Commission to regulate radio use "as the public convenience, interest, or necessity requires."
- Communications Act of 1934 – established Federal Communications Commission (FCC)
- Telecommunications Act of 1996, 2006

Spectrum

- EM waves have medium dependant properties such as: speed (refraction), resonance (absorption), reflection, scattering
- Propagation in atmosphere:
 - $f < 2$ MHz: ground-waves (waves follow the contour of the earth)
 - $2 \text{ MHz} < f < 30 \text{ MHz}$: sky-wave propagation (reflections from ionosphere)
 - $f > 30 \text{ MHz}$: line-of-sight (atmospheric scattering)
- In vacuum:

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

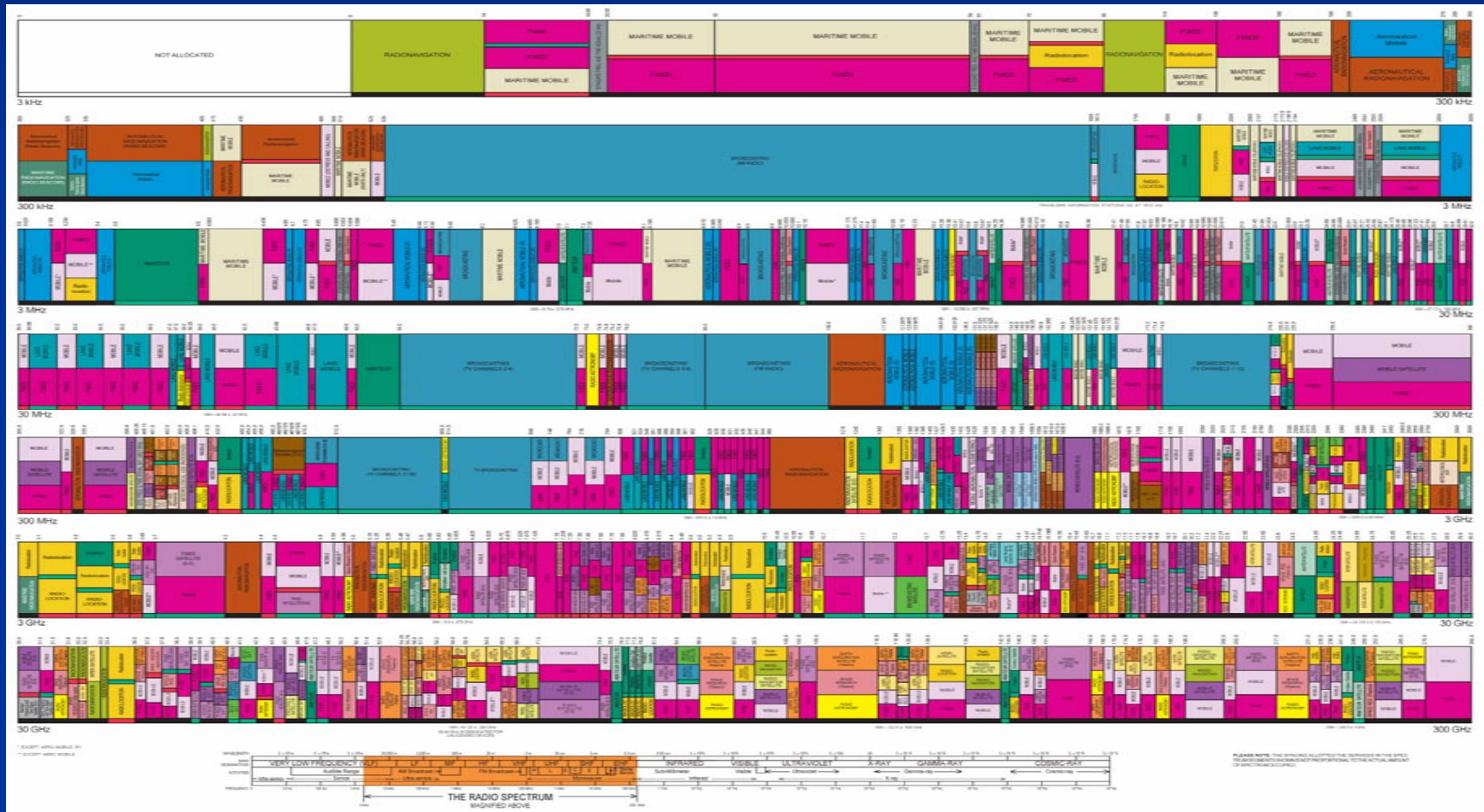
Spectrum Classification



Spectrum Allocation

- Spectrum – national resource under government control (usually split between commercial and military)
 - US: Federal Communications Commission (**FCC**) and Office of Spectral Management (**OSM**) in US
 - EU: European Conference of Post and Telecommunications Administrations (**CEPT**)
European Communications Office (ECO) -> Electronic Communications Committee (ECC)
 - Japan: Ministry of Public Management, Home Affairs, Posts and Telecommunications (**MPHPT**)
- International Telecommunications Union (**ITU**: ITU-T,ITU-R)
- Commercial allocation
 - Fixed
 - Auctions
 - Unlicensed
 - Underlay
 - Secondary market and spectrum leasing
- Policy shift: Cognitive radio

Spectrum Allocation (cont'd)



Spectrum Allocation

■ Unlicensed spectrum (US)

| | |
|---|-----------------|
| ISM band I* | 902 - 928 MHz |
| ISM band II | 2.4-2.4835 GHz |
| ISM band III (Wireless PBX) | 5.725-5.850 GHz |
| ISM | 59-64 GHz |
| U-NII band I (indoor systems, WLAN) | 5.15-5.25 GHz |
| U-NII band I (short-range outdoor, WLAN) | 5.25-5.35 GHz |
| U-NII band I (indoor/outdoor) | 5.47-5.725 GHz |
| U-NII band III (long-range outdoor, WLAN) | 5.725-5.825 GHz |

ISM = Industrial, Scientific and Medical

U-NII = Unlicensed National Information Infrastructure

Standards

- **Availability of interoperable equipment from multiple vendors**
- **Prevents a “Tower of Babel” situation**
 - Equipment from different vendors will interoperate if it complies with the standard
 - Alliances and certification bodies assure interoperability
 - Wi-Fi for 802.11 WiMax for 802.16
- **Lowers costs to consumers**
 - Both through competition and economies of scale

IEEE 802 Standards

Maintained by IEEE 802 LAN/MAN Standards Committee (LMSC):

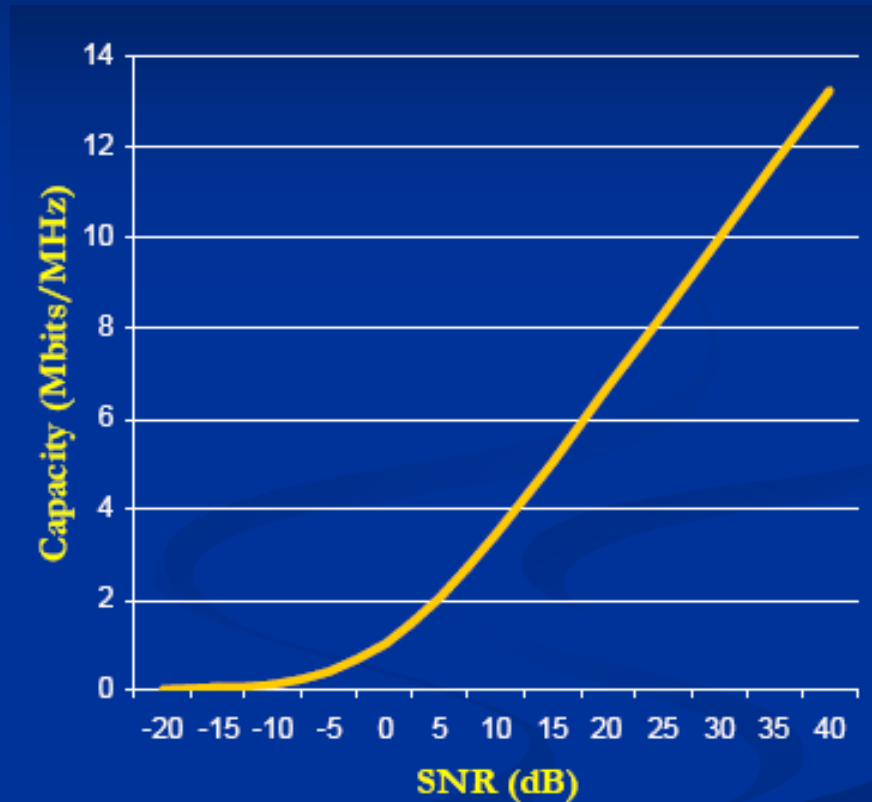
- 802.1 Overview, Architecture, Internetworking and Management
- 802.2 Logical Link Control
- **802.3 Ethernet (CSMA/CD PHY and MAC)**
- 802.5 Token Ring PHY and MAC
- **802.11 Wireless LAN**
- 802.12 Demand Priority Access
- **802.15 Wireless PAN**
- **802.16 Broadband Wireless Access**
- 802.17 Resilient Packet Ring
- 802.18 Radio Regulatory
- 802.19 Coexistence
- **802.20 Mobile Broadband Wireless Access**
- 802.21 Media Independent Handoff
- 802.22 Wireless Regional Area Network

■ Claude Shannon (1916-2001)

Upper bound on achievable communication rate in AWGN environments (1948):

$$C = B \log_2 \left(1 + \frac{S}{N} \right)$$

- C is the channel capacity in bits per second;
- B is the bandwidth of the channel in hertz;
- S is the signal power, measured in watt or volt²;
- N is the noise power
- S/N is the signal-to-noise ratio (SNR)



Noise

- “Any unwanted input” that limits systems ability to process weak signals
- Measure of the signal “noisiness” = signal-to-noise
- ratio (frequency dependant)
- Noise sources:
 - External
 - Atmospheric
 - Interstellar
- Receiver internal
 - Thermal
 - Flicker noise (low frequency)
 - Shot noise

Antennas

- “Interface” between the transmitter (receiver) and channel

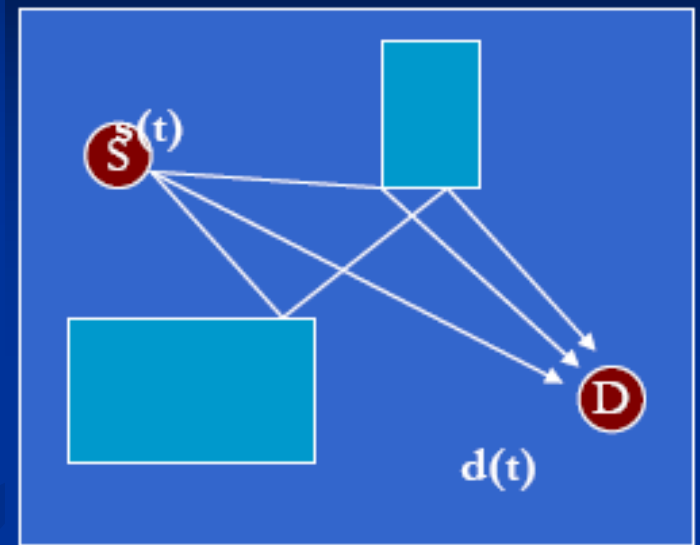
EMPIRICAL OBSERVATION:

For efficient transmission antenna needs to be longer than $1/10$ of the wavelength

| | f | λ | $\lambda/10$ |
|---------------|--------------|--------------|--------------|
| AM Radio | 600-1500 KHz | 500-200 m | 20 m |
| UHF (TV) | 0.3-3 GHz | 1-0.1m | 0.01m |
| Mobile phone | 824-2000 MHz | 0.36-0.158 m | 0.015m |
| LEO Satellite | 1.6 GHz | 0.188m | 0.0188m |

Multipath

- Objects in the environment
 - Reflection
 - Diffraction
 - Scattering
- Multiple signal copies added together
 - Attenuated
 - Delayed
 - Phase shifted
- Frequency selective fading
- Flat fading
- Ultimately causes ISI which limits performance



Technical Challenges for Wireless Systems

- Either
 - Channel impairments
 - Bandwidth
 - Access
 - Privacy and security
- Mobility
- Energy

Cellular System

Multiple Access

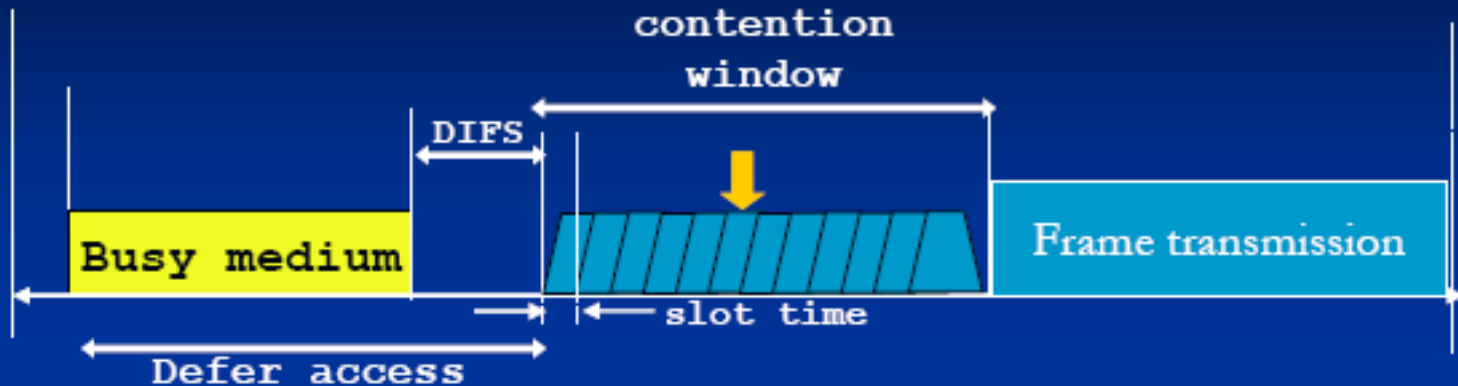
- Spectral sharing = dividing the signaling dimensions along the time, frequency, or code
 - Frequency division multiple access (FDMA)
 - Time division multiple access (TDMA)
 - Frequency hopping multiple access (FHMA)
 - Code division multiple access (CDMA)
 - Space division multiple access (SDMA)
- The goal is to improve spectral efficiency
 - Number of user/unit bandwidth/unit area

Packet Radio

Packet Radio Access

- Data is divided into chunks – packets:
 - Each packet fights for resources
 - Each packet can be routed independently
- Resource allocation (switching)
 - ALOHA:
 - unslotted (pure), slotted
 - Carrier-sense :
 - non-persistent, p-persistent, CD, CA, DSMA
 - Polling
 - PRMA

CSMA/CA

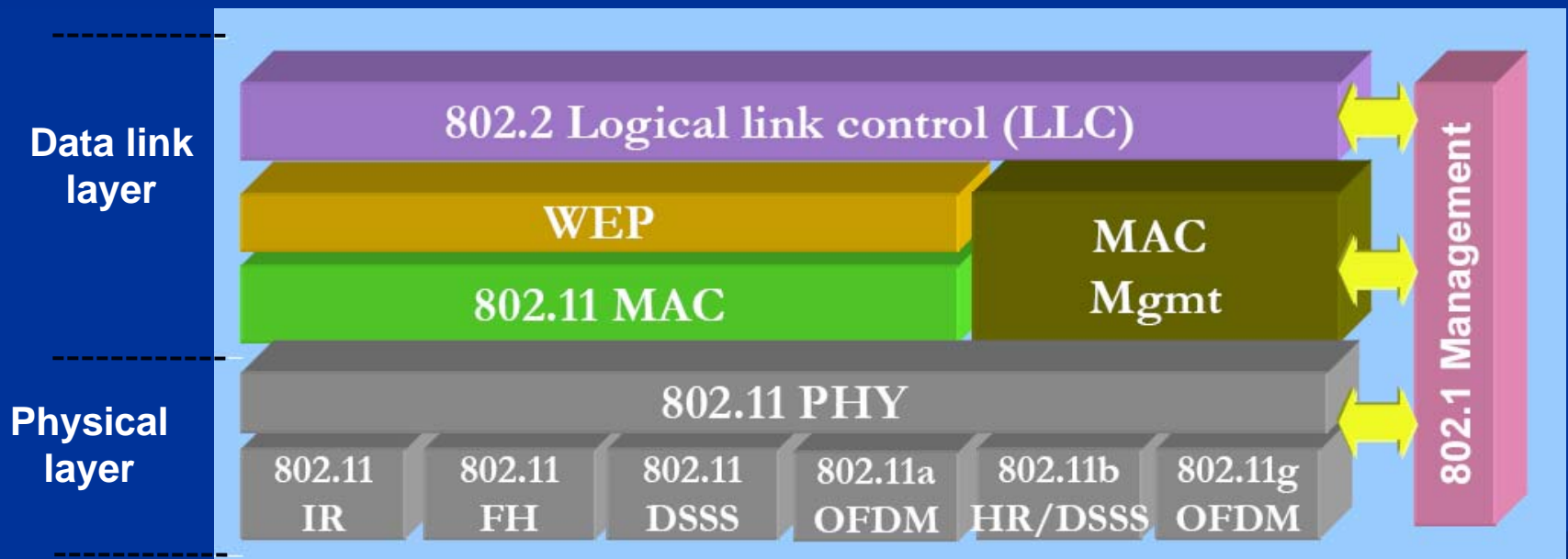


- Use CSMA with collision Avoidance
 - Based on carrier sense function called Clear Channel Assessment (CCA)
- Reduce collision probability where mostly needed
- Efficient backoff algorithm stable at high loads
- Possible to implement different fixed priority levels

802.11

802.11

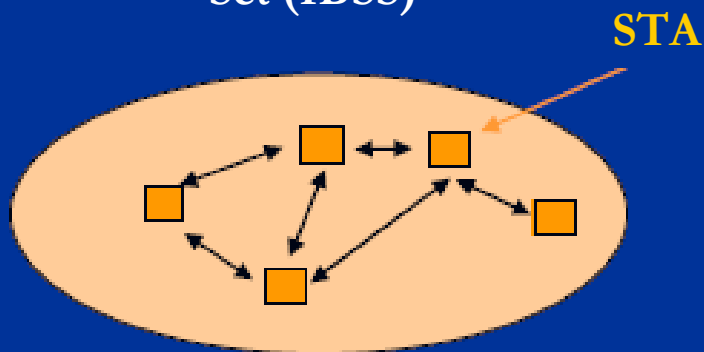
- Member of IEEE 802 family (Specifications for Local Area Networks)



System Architecture

Basic Service Set (BSS): a set of stations which communicate with one another

Independent Basic Service Set (IBSS)

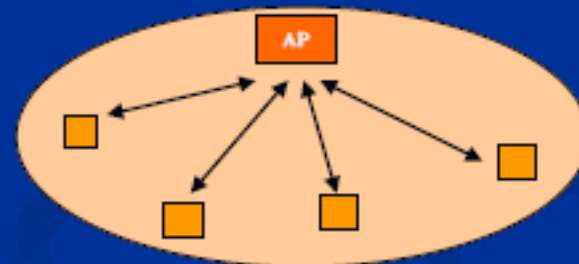


- only direct communication possible
- no relay function

Ad Hoc Network

MANET: mobile ad hoc network

Infrastructure Basic Service Set (BSS)



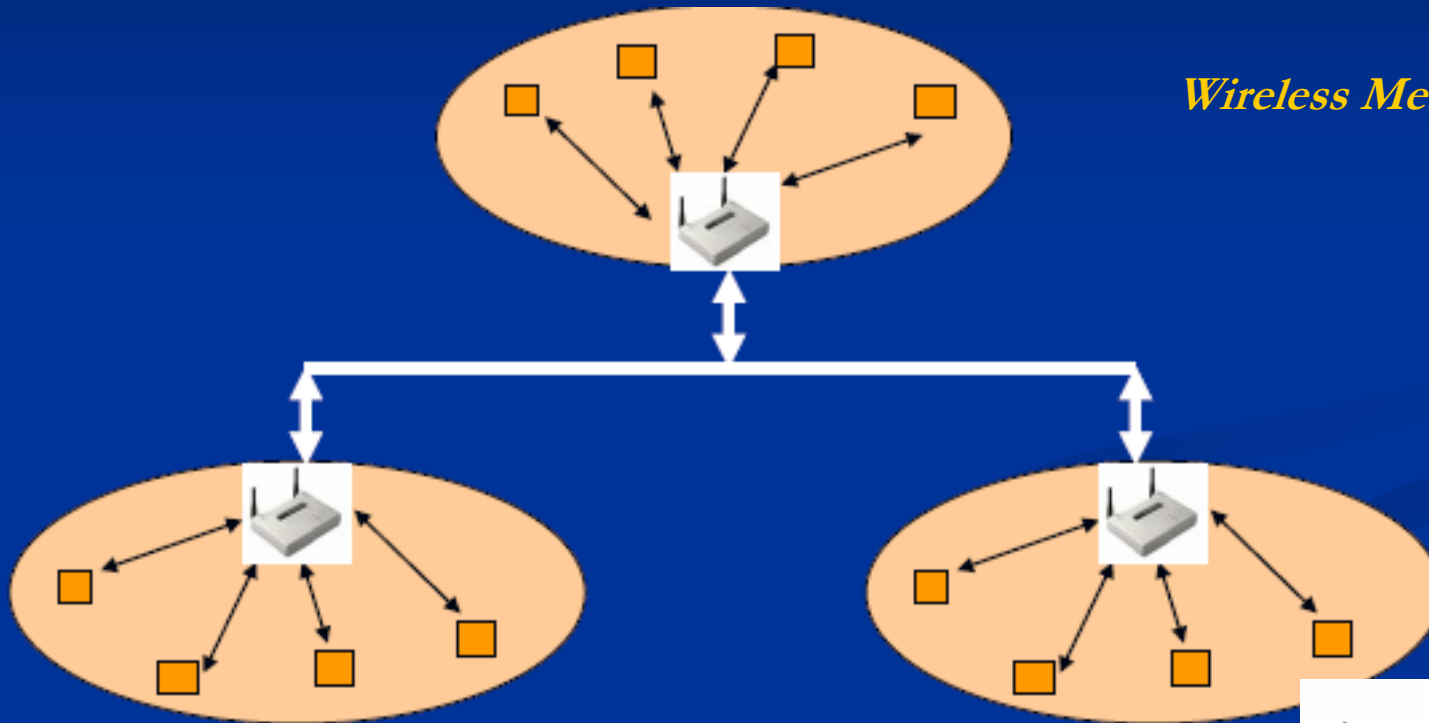
- AP provides
 - connection to wired network
 - relay function
- stations not allowed to communicate directly

WiFi Hotspots

Home wireless networks

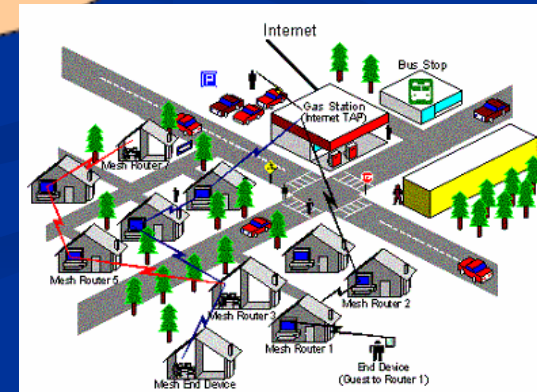
System Architecture (cont'd)

Extended Service Set (ESS): a set of BSSs interconnected by a distribution system



Wireless Mesh Networks

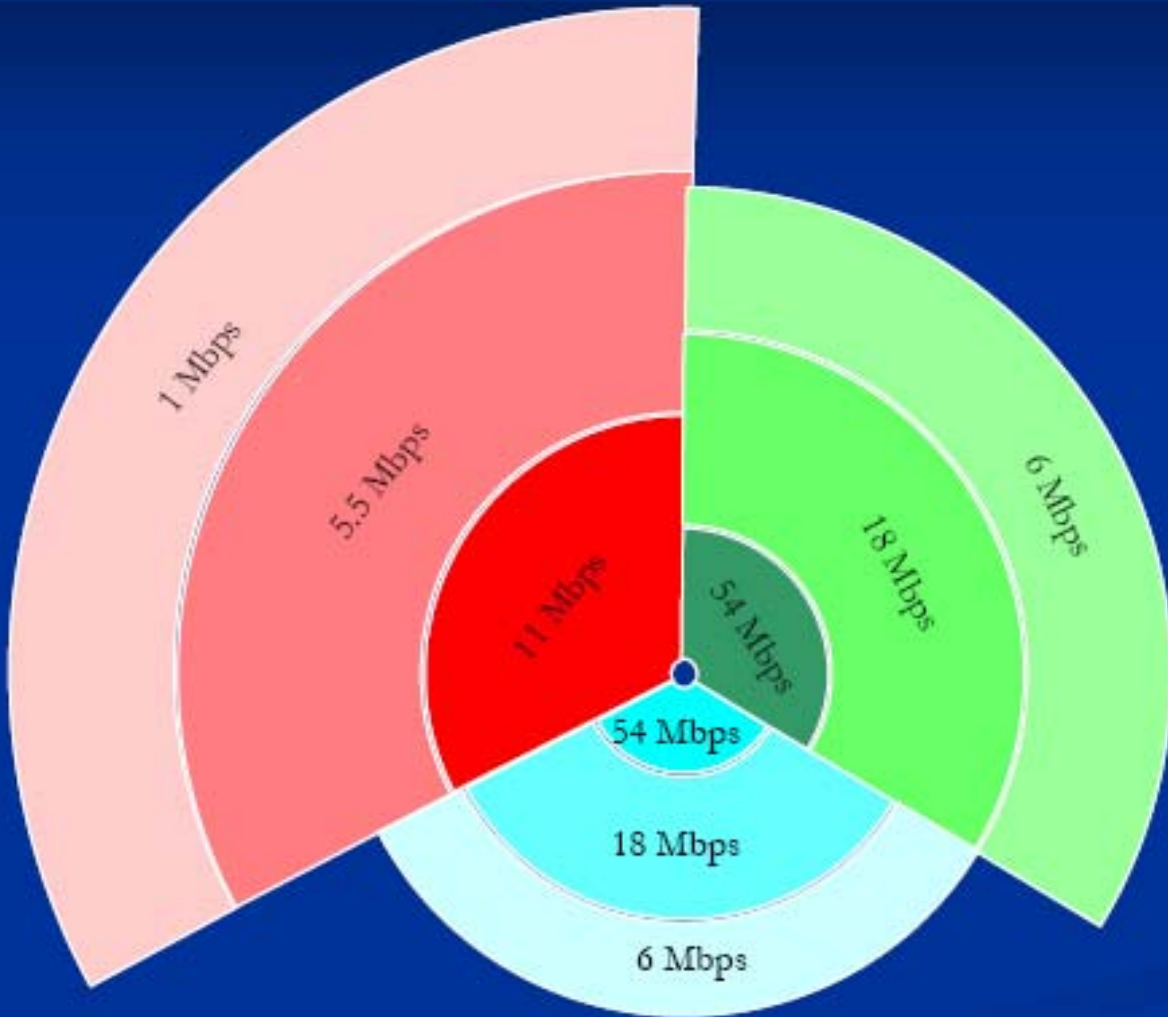
- APs interconnected with wireless links
- automatic topology learning and dynamic path configuration
- AP communicate among themselves to forward traffic



Wireless “Alphabet Soup”

- 802.11b:
 - Most common wireless protocol. Uses 2.4GHz frequency, with 1, 2, 5.5, 11 Mbps bandwidth. (5 Mbps is more typical).
- 802.11a:
 - Uses 5.5GHz range, 54 Mbps bandwidth (~20 Mbps is typical performance). Produces too much radio power to be certified in medical areas.
- 802.11g:
 - Uses 2.4GHz band and is compatible with 802.11b. Also 54 Mbps bandwidth (~20 Mbps typical)

802.11 Range



| 802.11 b | |
|----------|--------|
| 1 | 410 ft |
| 5.5 | 310 ft |
| 11 | 160 ft |
| 802.11 g | |
| 6 | 300 ft |
| 18 | 210 ft |
| 54 | 90 ft |
| 802.11 a | |
| 6 | 210 ft |
| 18 | 150 ft |
| 54 | 60 ft |

802.11 MAC

1-Persistent CSMA

- Sense the channel.
 - If busy, keep listening to the channel and transmit *immediately* when the channel becomes idle.
 - If idle, transmit a packet immediately.
- If collision occurs,
 - Wait a random amount of time and start over again.
- Greedy algorithm

802.11 Media Access Control

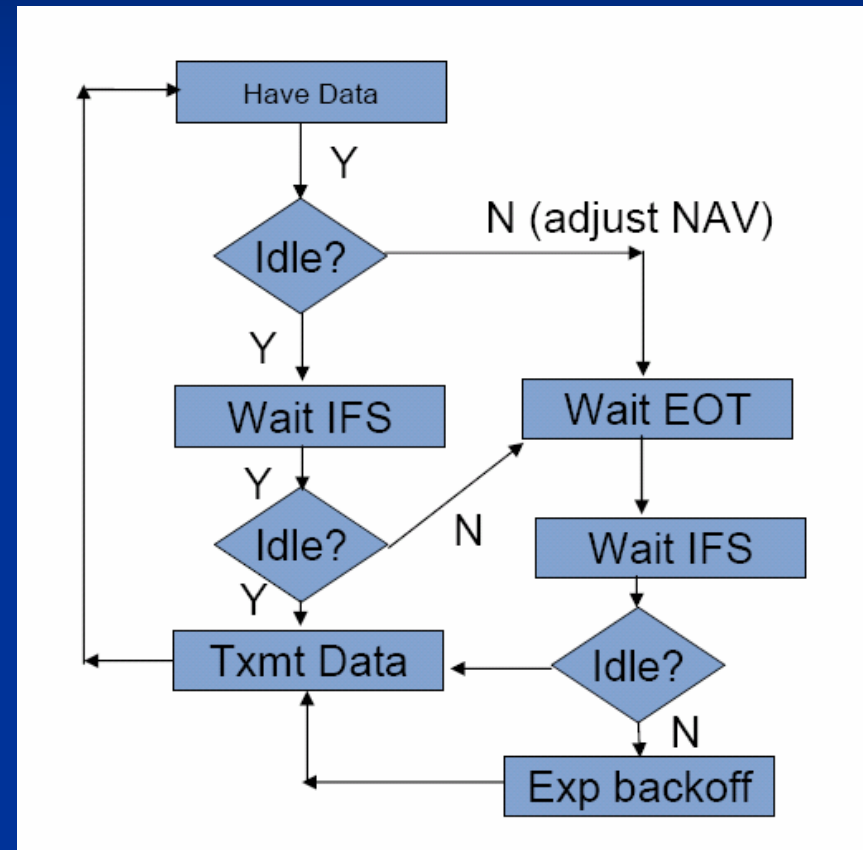
- Handshaking to infer collisions
 - DATA-ACK packets
- Collision Avoidance
 - RTS-CTS-DATA-ACK to request the medium
 - Duration information in each packet
 - Random Backoff after collision is determined
- Two carrier sensing functions:
 - Physical carrier-sensing
 - Virtual carrier-sensing

802.11 DCF

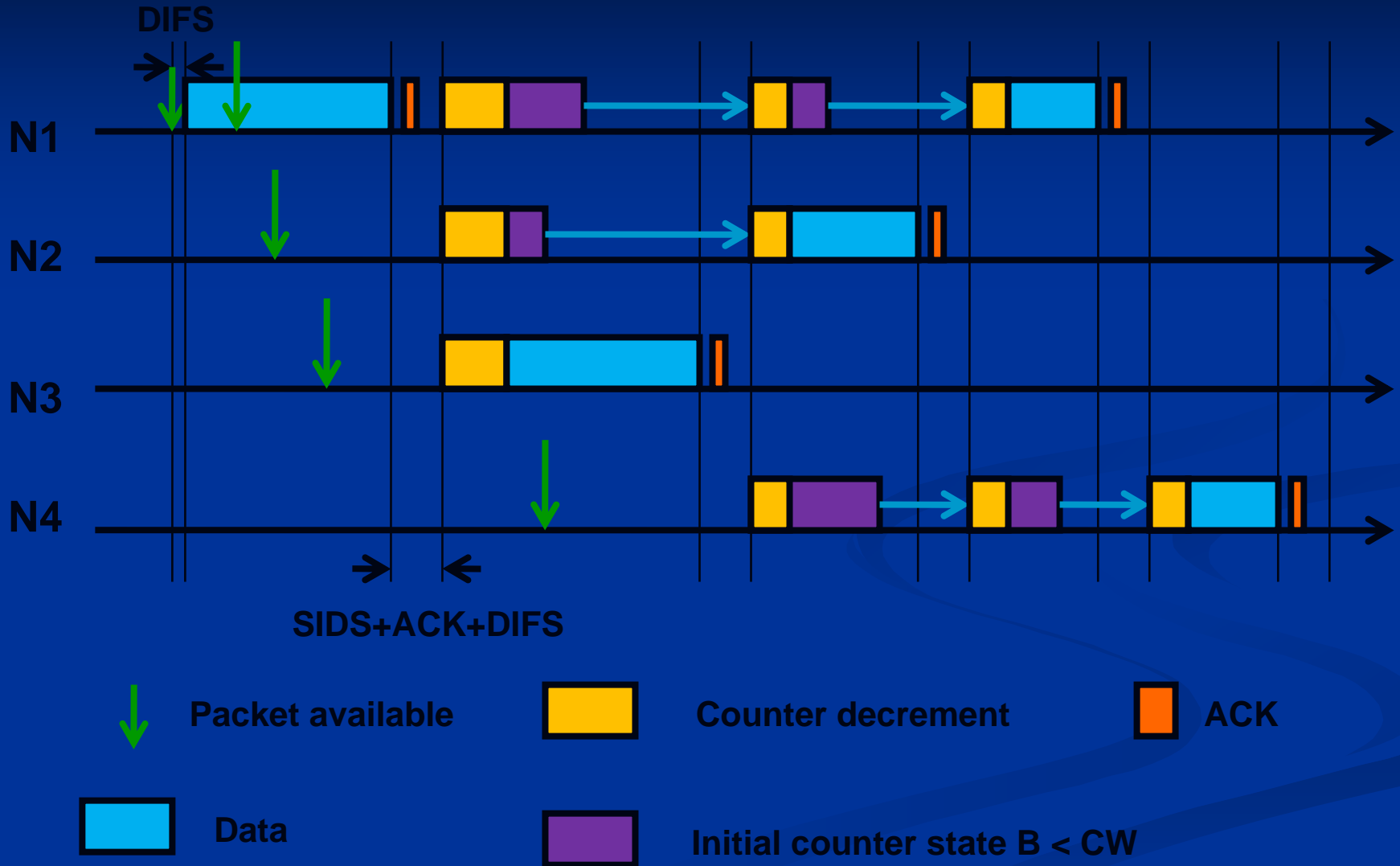
- Uses CSMA/CA
- Uses random backoff to avoid collisions
- Can use RTS/CTS to lower collision probability
- Uses positive acknowledgements and sender initiated retries
- DCF state machine can get quite complex
- Incremental NAV-based reservations (virtual carrier sense)

802.11 Access Control

- Carrier sensing
- Is the medium idle? → Wait for an amount of time (IFS), if still idle transmit
 - IFS = inter frame spacing
- Is the medium busy?
- Wait until current txm ends, wait (IFS), if idle wait for random amount of time, else wait until current txm ends and repeat
 - (exponential backoff for collisions)
- ACKs and immediate response actions can be sent after SIFS (Short IFS) < PIFS < DIFS value used in multiple access control
 - Virtual carrier-sensing
 - NAV = network allocation vector



Basic access in absence of collisions



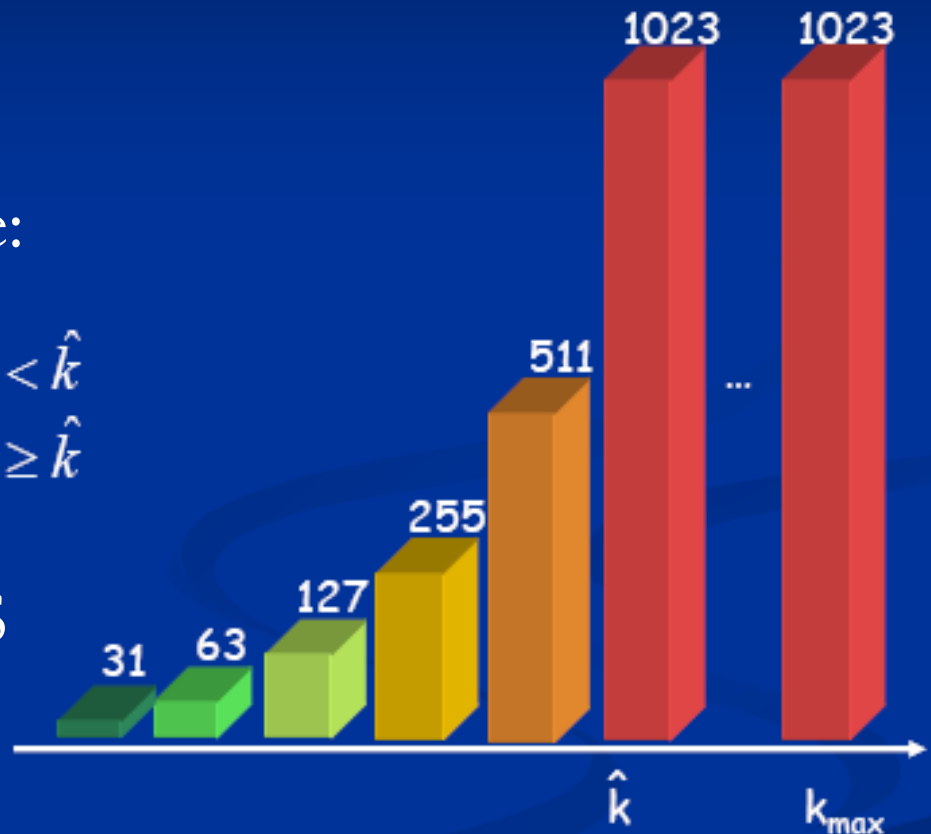
Binary random backoff

- initial counter state:
 - $B = U[0, CW - 1]$
- contention window size:

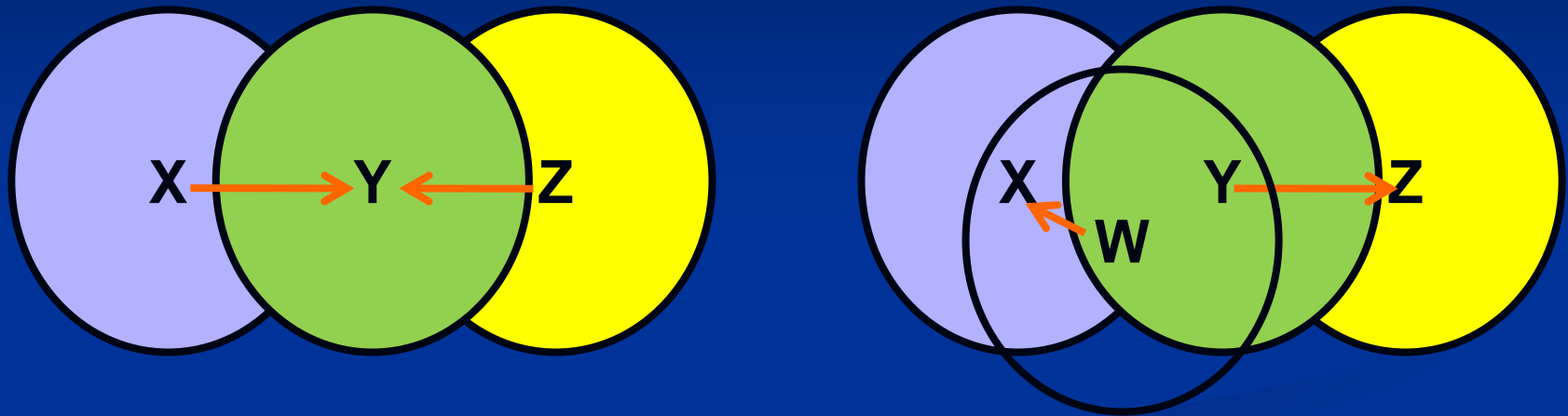
$$CW = \begin{cases} 2^k \cdot CW_{\min} & k < \hat{k} \\ CW_{\max} & k \geq \hat{k} \end{cases}$$

- example: 802.11b DSSS

| | |
|-------------|------|
| CW_{\min} | 32 |
| \hat{k} | 5 |
| CW_{\max} | 1024 |



Problems with Carrier Sensing



■ Hidden terminal problem

- Z does not hear X; hence transmits to Y and collides with transmission from X
- No carrier does not imply send

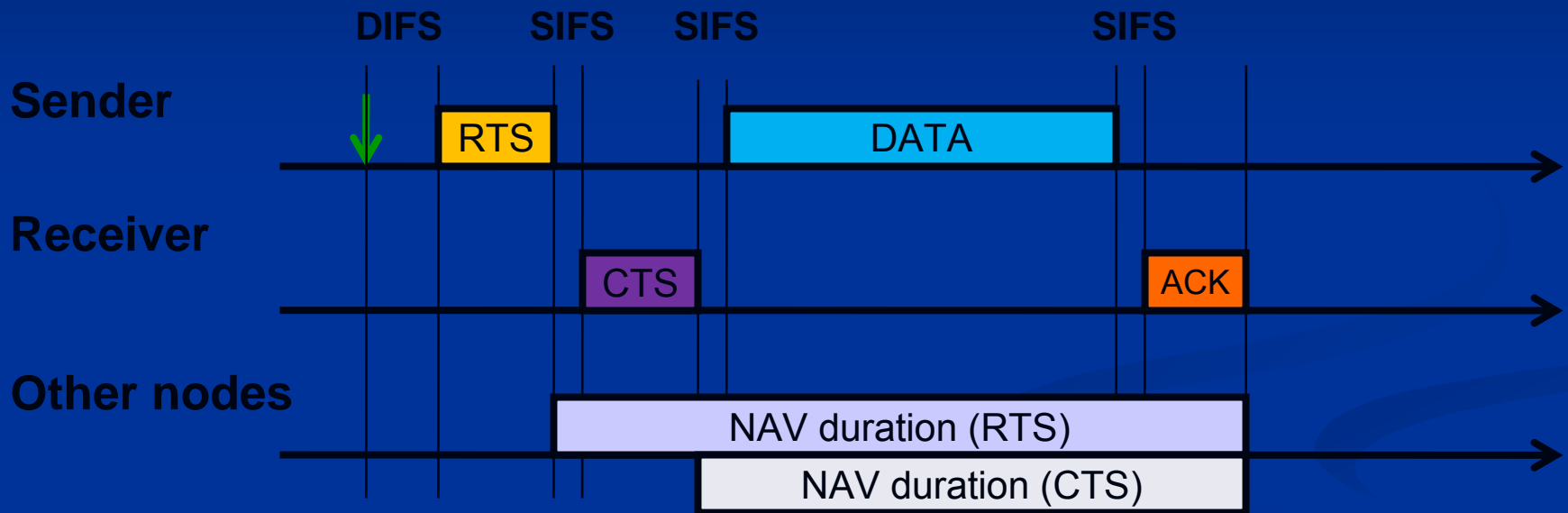
■ Exposed terminal problem

- W hears Y but can safely transmit to X
- Carrier may not imply don't send

Use of RTS, CTS

- Sender sends a small packet **RTS (request to send)** before sending data
- Receiver sends **CTS (clear to send)**
- All potential senders hearing RTS waits until a CTS is heard from some receiver
- If no CTS, transmit
- If CTS, wait for a time for sender to send data
- **Hear RTS, but no CTS, then send**
 - **Exposed terminal case**
- **Don't hear RTS, but CTS receiver is close, don't send**
 - **Hidden terminal case**

RTS/CTS access method



MACA protocol

- Multiple access coordinated by sending RTS/CTS messages
- This pair of messages reserve spatially and temporally the channel
- RTS/CTS are two small control packets that need to be sent before actual data transmission
- Sender sends RTS before transmitting
- Receiver responds with CTS
- If source does not hear CTS with a timeout it retries

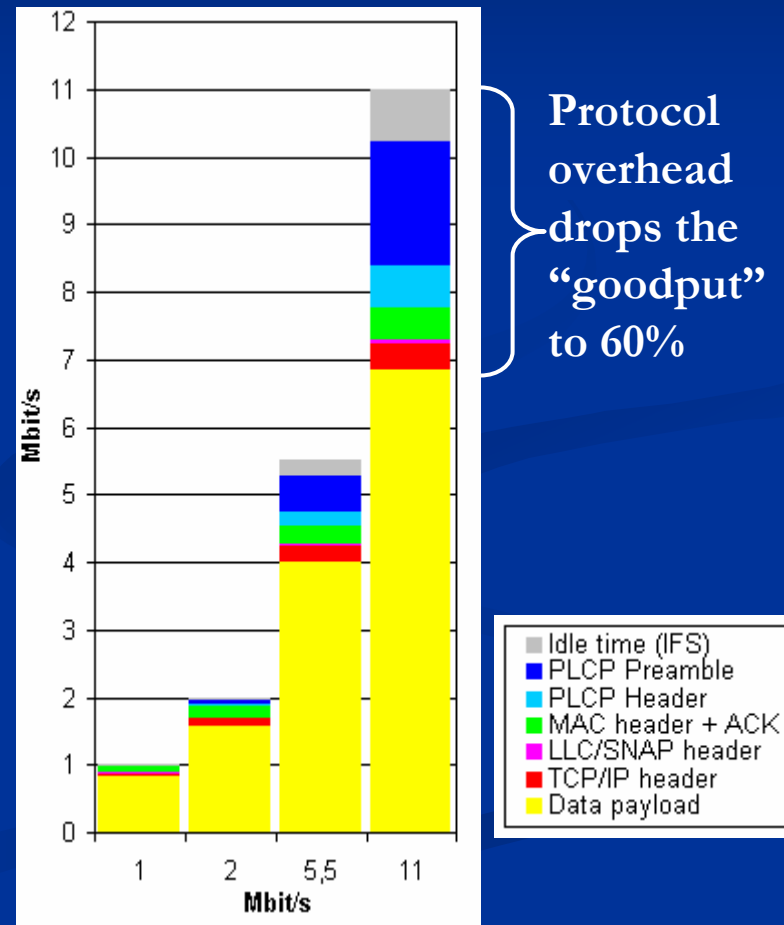
MACA protocol

- When a CTS is received, the source sends its data packets
- Any node, other than the destination, that hears a RTS, defers transmission long enough to hear CTS
- Any node, other than the source, that hears a CTS, defers transmission long enough for the data to be transmitted

802.11 MAC parameters

| Parameter | 802.11a | 802.11b DSSS |
|-------------|---|-----------------------|
| CW_{min} | 16 slots | 32 slots |
| CW_{max} | 1024 slots | 1024 slots |
| Slot time | 9 μ s | 20 μ s |
| SIFS | 16 μ s | 10 μ s |
| DIFS | 34 μ s | 50 μ s |
| ACK | 14 bytes | 14 bytes |
| RTS | 20 bytes | 20 bytes |
| CTS | 14 bytes | 14 bytes |
| PLCP header | 24 μ s | 192 μ s |
| MAC header | 34 bytes | 34 bytes |
| PHY rates | 6, 9, 12, 18, 24, 36, 48, 54 Mbps | 1, 2, 5.5, 11 Mbps |

Protocol Overhead without any collisions, RTS/CTS or backoffs



Bluetooth

IEEE 802.15

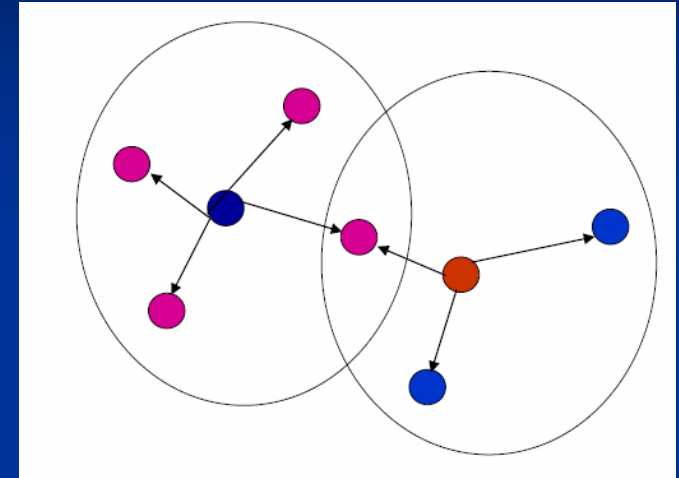
Bluetooth

- A cable replacement technology
- Operates in the ISM band (2.4Ghz to 2.8 Ghz)
- Range is 10 cm to 10 meters can be extended to 100 meters by use of power control
- Data rates up to 1 Mbps (721Kbps)
- Supposed to be low cost, single chip radio
- Ideal for connecting devices in close proximity (piconet)
 - Phone and earpiece
 - Computer and printer
 - Camera and printer/fax etc
- Can form personal area networks (piconet and scatternet)

Personal area networks

■ Piconet

- Master/slave nodes
- Master and up to 7 slaves
- Master allocates channels



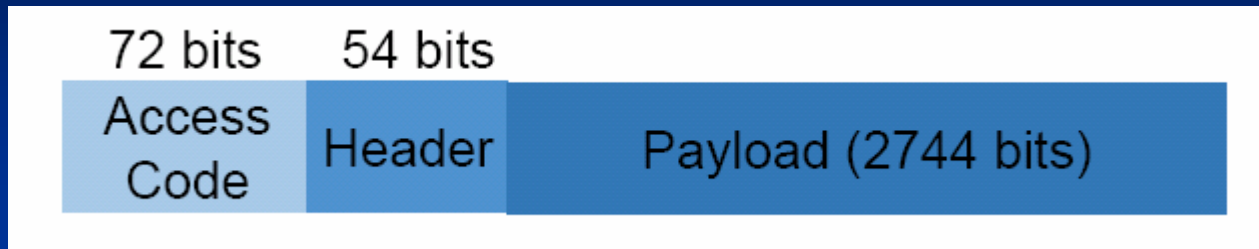
■ Scatternet

- Node may be master in one network and slave in another network
- Allows devices to be shared in different networks

Bluetooth Radio Link

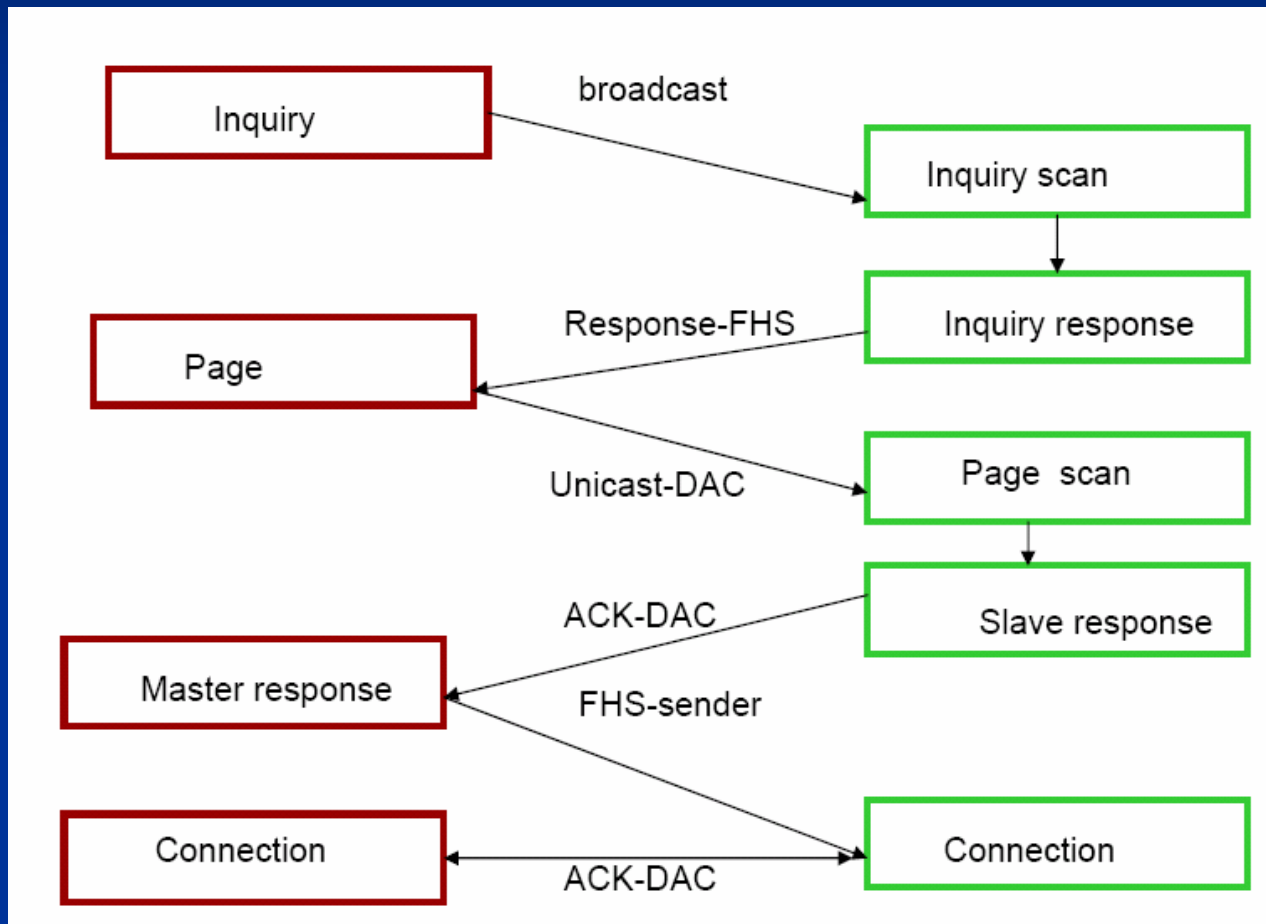
- IEEE 802.11 operates in the same band using DSSS
- Bluetooth uses Frequency Hopping
- 83.5 MHz channel is divided into 79 1-MHz channels
 - 1600 hops per second (stays at one frequency for 625 microseconds)
 - Hopping sequence is 16 or 32
 - Selected by the master based on its MAC address
 - Master can connect up to seven slaves to form a piconet
- All members of the piconet use the same hopping sequence
- Masters starts to transmit in the **even slots** and the slaves start to transmit in the **odd slots**

Bluetooth Packet Format



- Access code identifies the master
 - Channel access code, device access code, inquiry access code
- Header contains address (3 bits) and packet types (4 bits)
 - Which of the 8 devices the frame is intended for
- Voice packets with different FEC rates
- Data packets with low bit rate and high bit rate (with varying FEC as well)

Connection establishment

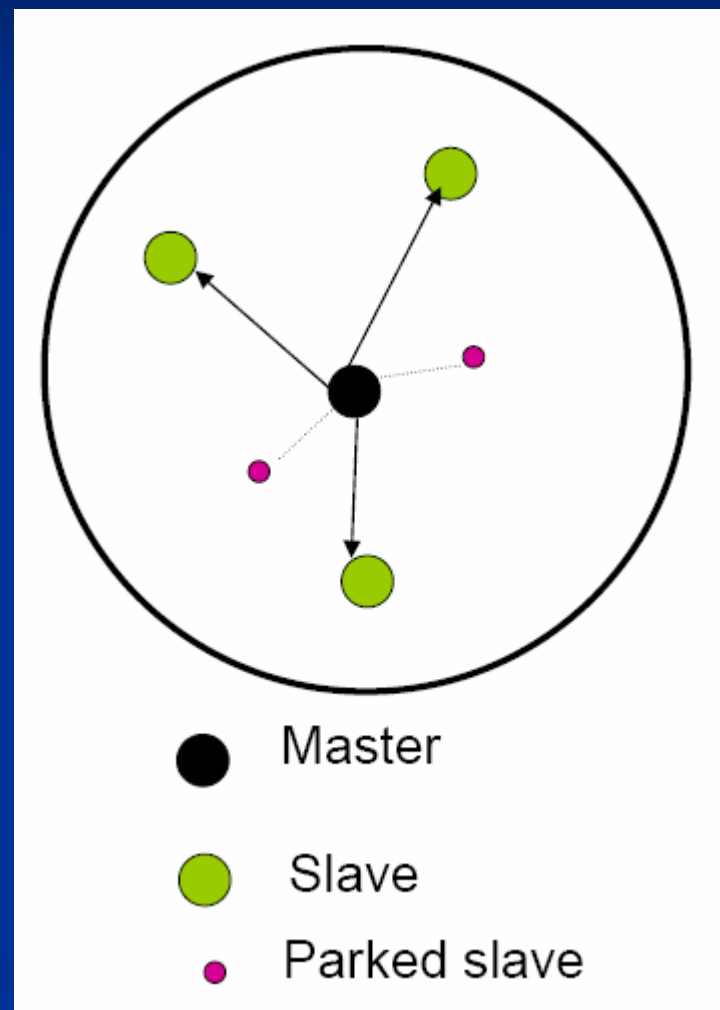


piconet

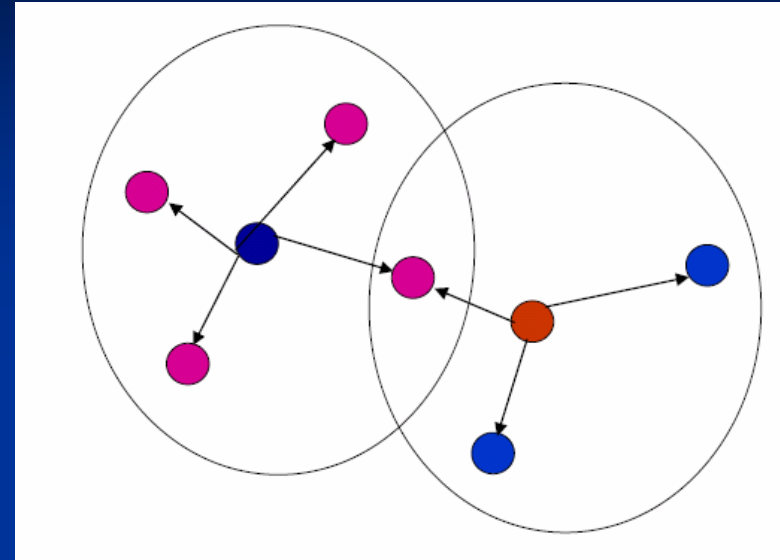
- A set of bluetooth devices connected to a master
- Scatternet: a set of piconets

Bluetooth Link Formation

- Master inquires who is around
 - Active slaves respond and the master learns who is around
- Master pages slaves and informs them of hopping sequence, active member address
 - Active slaves get packets when header matches active member address
 - A link is formed between master and each slave
- Inactive slaves can go into “park” state and give up address



Scatternet



- A device can co-exist as a master in one piconet and slave in another piconet
- Allow devices to share an area
- Efficient communication