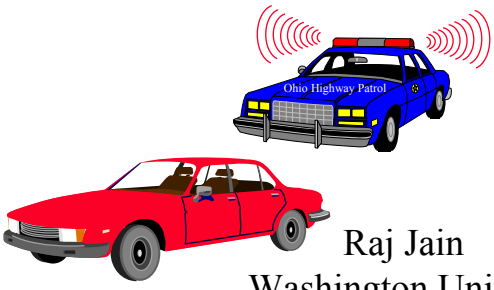
Wireless LANs



Raj Jain
Washington University
Saint Louis, MO 63131
Jain@cse.wustl.edu

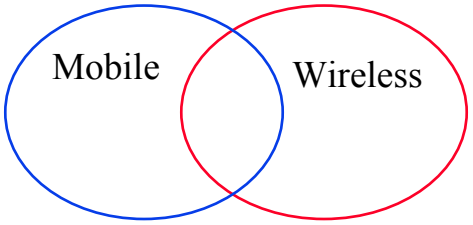
These slides are available on-line at:

http://www.cse.wustl.edu/~jain/cse473-05/

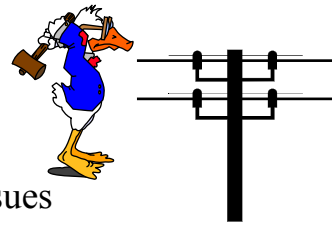
Overview

- Mobile vs Wireless
- Spread Spectrum and Code Division Multiple Access
- Wireless LANs
- IEEE 802.11 Features, MAC, Architecture, Priorities, Power Management, Frame Format
- 802.11 PHYs: 802.11, 802.11a, 802.11b, 802.11g

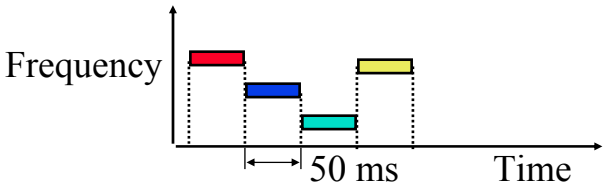
Mobile vs Wireless



- Mobile vs Stationary
- Wireless vs Wired
- Wireless ⇒ media sharing issues
- Mobile ⇒ routing, addressing issues

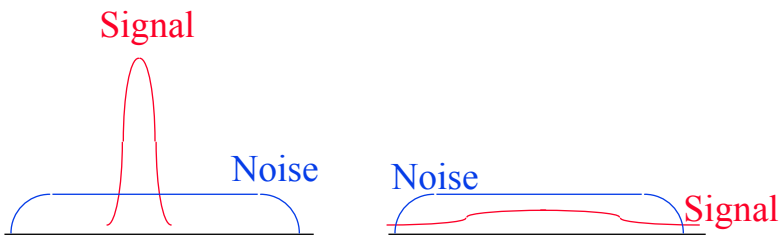


Frequency Hopping Spread Spectrum



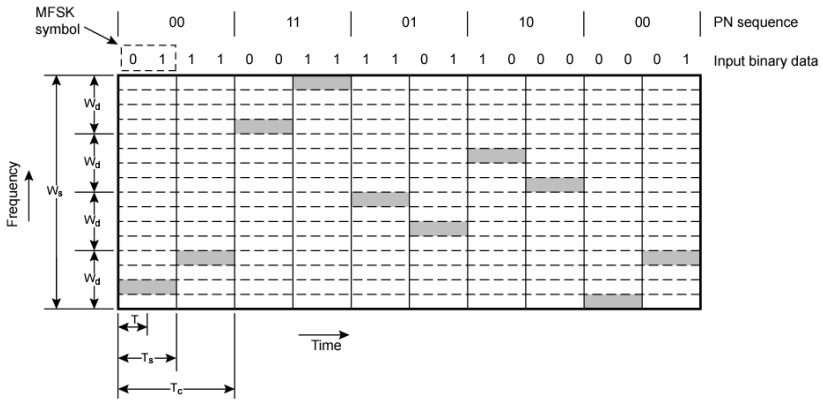
- Pseudo-random frequency hopping
- Spreads the power over a wide spectrum
  ⇒Spread Spectrum
- Developed initially for military
- Patented by actress Hedy Lamarr
- Narrowband interference can't jam

Spectrum



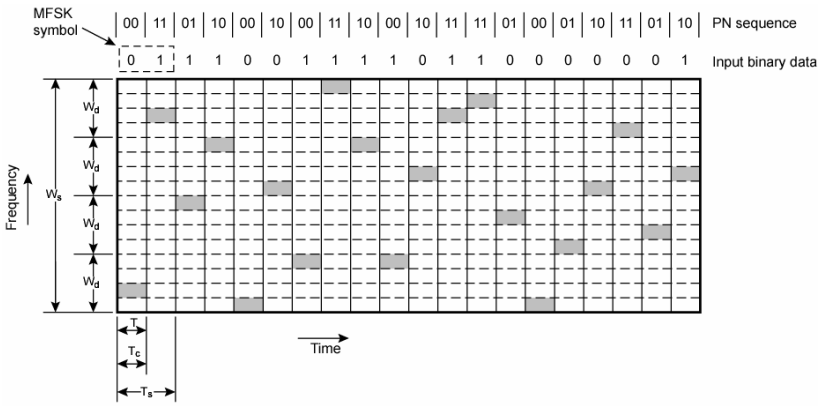
(a) Normal (b) Frequency Hopping

Slow Frequency Hop Spread Spectrum



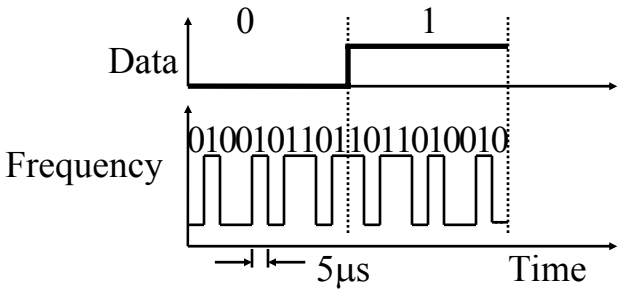
- Two bits/symbol ⇒ 4 frequencies/symbol (Multi FSK)
- Two-bit PN Sequence ⇒ 4 Carrier Channels
- Two symbols/Hop ⇒ Slow Frequency hopping

Fast Frequency Hop Spread Spectrum



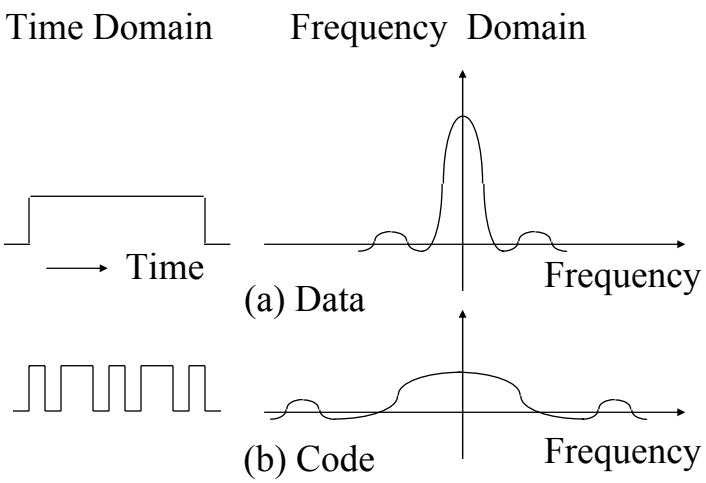
- 2 bits/symbol
- Two-bit pseudo-random number sequence
- Two hops/symbol ⇒ Fast Frequency hopping

Direct-Sequence Spread Spectrum



- Spreading factor = Code bits/data bit, 10-100 commercial (Min 10 by FCC), 10,000 for military
- Signal bandwidth >10 × data bandwidth
- Code sequence synchronization
- Correlation between codes ⇒Interference□Orthogonal

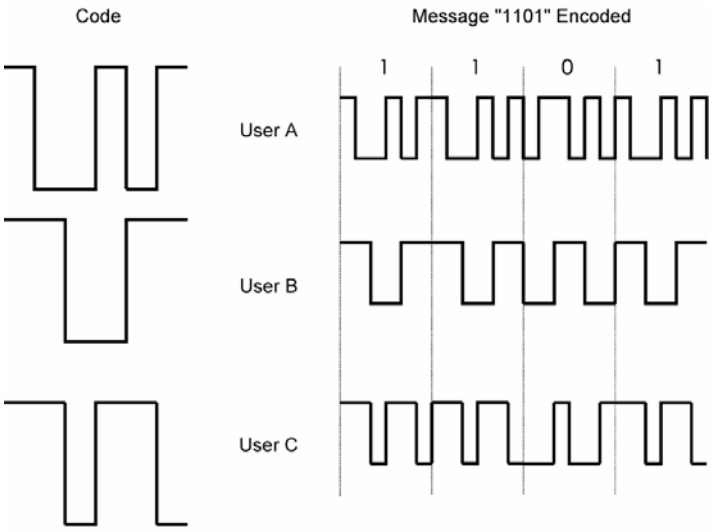
DS Spectrum



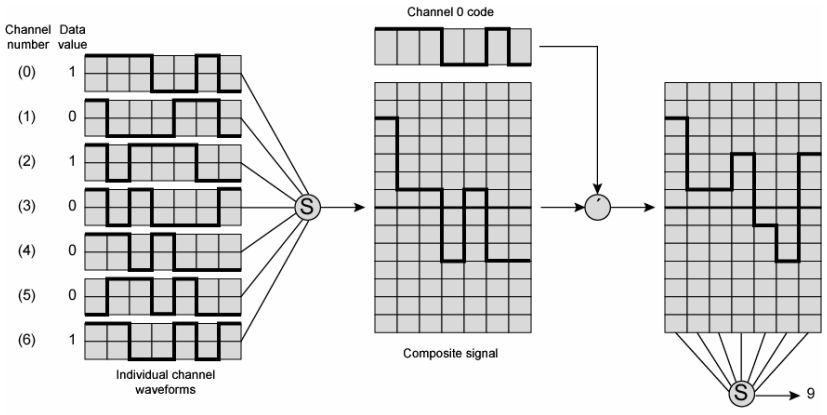
Code Division Multiple Access (CDMA)

- Multiplexing Technique used with spread spectrum
- Start with data signal rate *D*
  - Called bit data rate
- Break each bit into *k* chips according to fixed pattern specific to each user
  - User's code
- New channel has chip data rate *kD* chips per second
- E.g. *k*=6, three users (A,B,C) communicating with base receiver R
- Code for A = <1,-1,-1,1,-1,1>
- Code for B = <1,1,-1,-1,1,1>
- Code for C = <1,1,-1,1,1,-1>

CDMA Example



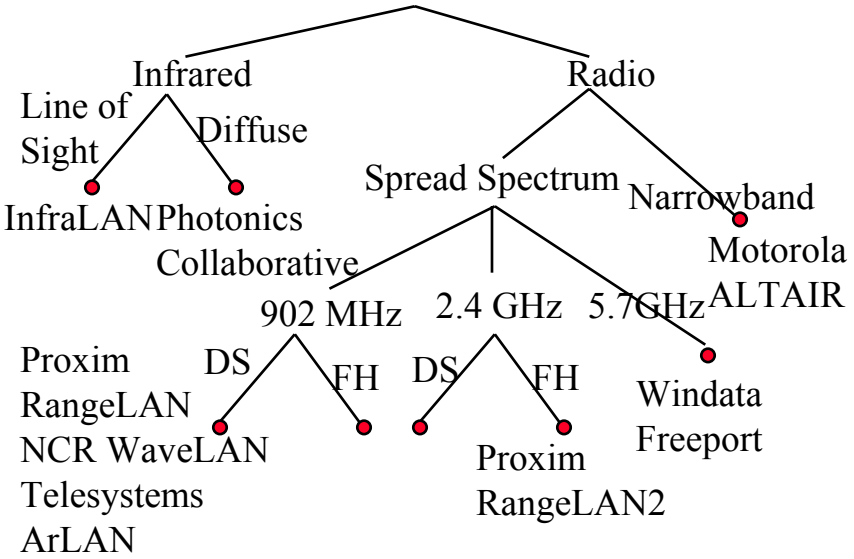
CDMA Encoding and Decoding



Wireless LAN Requirements

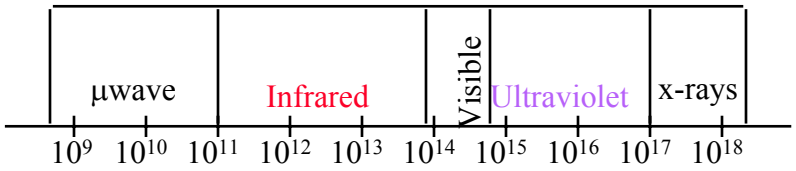
- Low power consumption: Need long battery life
  ⇒ Must not expect nodes to be up all the time
- Transmission robustness and security:
  ⇒ Interference prone and easily eavesdropped
- Collocated network operation:
  ⇒ Two or more wireless LANs in same area
- License-free operation
- Handoff/roaming: Move from one cell to another
- Dynamic configuration: Addition, deletion, and relocation of end systems without disruption to users

Wireless LANs



Infrared LANs

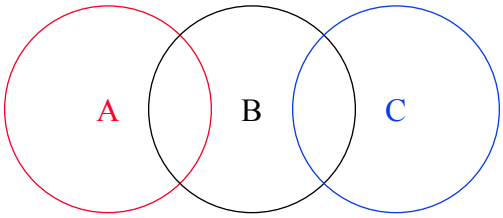
- Directed-beam IR: Point-to-point links
  - Range depends on power - Can be kilometers
  - Used for building interconnect within line of sight
- Omni-directional:
  - Single base station within line of sight of all other stations
    - Typically, mounted on ceiling. Acts as a repeater
  - Other transceivers use directional beam aimed at base
- Diffused configuration: Reflections from walls



IEEE 802.11 Features

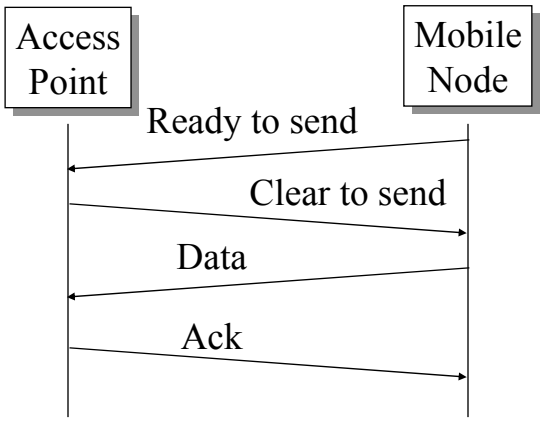
- Original 802.11 at 1 and 2 Mbps
- Supports both Ad-hoc and base-stations
- Spread Spectrum ⇒ No licensing required.
  Three Phys: Direct Sequence, Frequency Hopping, 915-MHz, **2.4 GHz** (Worldwide ISM), 5.2 GHz, and Diffused Infrared (850-900 nm) bands.
- Supports multiple priorities
- Supports time-critical and data traffic
- Power management allows a node to doze off

Hidden Node Problem



- C cannot hear A.
  It may start transmitting while A is also transmitting
  ⇒ A and C can't detect collision.
- Only the receiver can help avoid collisions

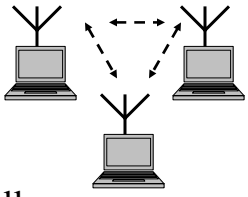
4-Way Handshake



IEEE 802.11 MAC

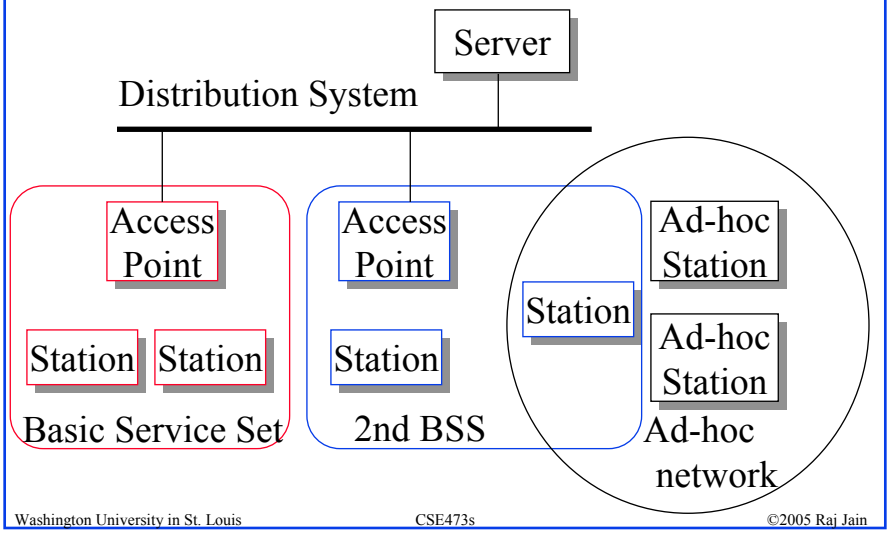
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Listen before you talk. If the medium is busy, the transmitter backs off for a random period.
- Avoids collision by sending a short message:
  Ready to send (RTS)
  RTS contains dest. address and duration of message.
  Tells everyone to backoff for the duration.
- Destination sends: Clear to send (CTS)
- Can not detect collision ⇒ Each packet is acked.
- MAC level retransmission if not acked.

Peer-to-Peer or Base Stations?



- Ad-hoc (Autonomous) Group:
  - Two stations can communicate
  - All stations have the same logic
  - No infrastructure, Suitable for small area
- Infrastructure Based: Access points (base units)
  - Stations can be simpler than bases.
  - Base provide connection for off-network traffic
  - Base provides location tracking, directory, authentication ⇒ Scalable to large networks
- IEEE 802.11 provides both.

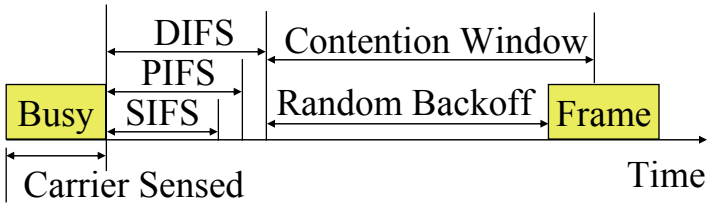
IEEE 802.11 Architecture



Architecture

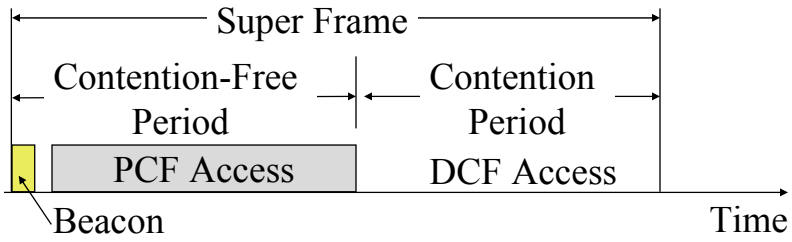
- Basic Service Area (BSA) = Cell
- Each BSA may have several wireless LANs
- Distribution System (DS) - wired backbone
- Extended Service Area (ESA) = Multiple BSAs interconnected via Access Points (AP)
- Basic Service Set (BSS)
  = Set of stations associated with an AP
- Extended Service Set (ESS)
  = Set of stations in an ESA
- Ad-hoc networks coexist and interoperate with infrastructure-based networks.

IEEE 802.11 Priorities



- Initial interframe space (IFS)
- Highest priority frames, e.g., Acks, use short IFS (SIFS)
- Medium priority time-critical frames use "Point Coordination Function IFS" (PIFS)
- Asynchronous data frames use "Distributed coordination function IFS" (DIFS)

Time Critical Services

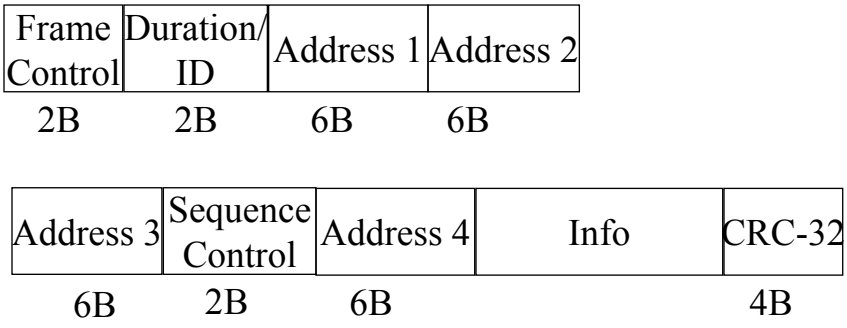


- Timer critical services use Point Coordination Function
- The point coordinator allows only one station to access
- Coordinator sends a beacon frame to all stations. Then uses a polling frame to allow a particular station to have contention-free access
- Contention Free Period (CFP) varies with the load.

Power Management

- A station can be in one of three states:
  - Transmitter on
  - Receiver only on
  - Dozing: Both transmitter and receivers off.
- Access point (AP) buffers traffic for dozing stations.
- AP announces which stations have frames buffered.
  Traffic indication map included in each beacon.
  All multicasts/broadcasts are buffered.
- Dozing stations wake up to listen to the beacon.
  If there is data waiting for it, the station sends a poll frame to get the data.

Frame Format



- **Frame Control**: Type of frame (Control, management, or data)
  - Includes whether frame is to or from DS, fragmentation information, and privacy information

MAC Frame Fields

- **Duration/Connection ID**:
  - If used as duration field, indicates time (in μs) channel will be allocated for successful transmission of MAC frame
  - In some control frames, contains association or connection identifier
- **Sequence Control**:
  - 4-bit fragment number subfield
    - For fragmentation and reassembly
  - 12-bit sequence number
  - Number frames between given transmitter and receiver

802.11 Address Fields

- Address 1: All stations filter on this addr.
- Address 2: Transmitter
- Address 3: Depends upon to/from
- Address 4: Original source

To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
0	0	DA	SA	BSSID	-
0	1	DA	BSSID	SA	-
1	0	BSSID	SA	DA	-
1	1	RA	TA	DA	SA

Station Location

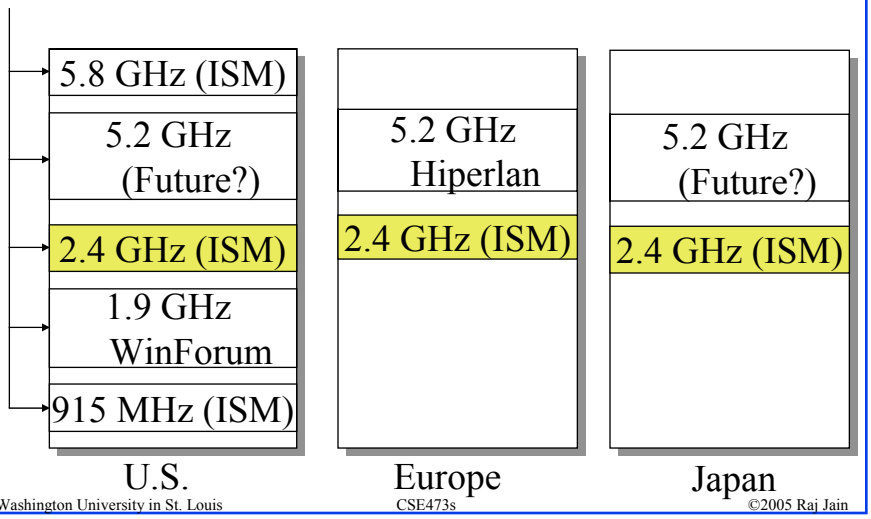
- DS needs to know where destination station is
  - Identity of AP to which message should be delivered
  - Station must maintain association with AP within current BSS
- Three services relate to this requirement:
  - Association: Establishes initial association between station and AP
    - To make identity and address known
    - AP then communicates information to other APs within ESS
  - Re-association: Transfer established association to another AP $\Rightarrow$Allows station to move from one BSS to another
  - Disassociation: when station leaves ESS or shuts down

IEEE 802.11 Phy

- Three Phys specified:
  - Direct Seq. Spread Spectrum (DSSS)
  - Frequency Hopping Spread Spectrum (FHSS)
  - Diffused Infrared (DFIR): Wide angle
- DSSS and FHSS operate in 2.4-2.4835 GHz Industrial, Scientific, and Medical (ISM) band (International)
  Some early systems use 902-928 MHz band.
  Different PHY specifications for 915-MHz, 2.4-, 5.2 GHz, and Infrared (850-900 nm) bands.
- SS at 1 or 2 Mbps. DFIR at 1 Mbps.

Why 2.4 GHz?

IEEE 802.11



FHSS Phy

- 2.4 GHz ISM Band.
- 1 and 2 Mbps
- Three sets of frequency hopping patterns. Each set has 22 hopping sequences (22 Channels).
  Total 66 channels. 12 in Japan.
- Consecutive frequencies in each sequence are at least 6 MHz apart to avoid a narrowband interferer.
- Adjacent or overlapping cells use different patterns.
- Many channels ⇒ FH systems better than DS in dense (overlapping cells) environment.

DSSS Phy

- 2.4 GHz band
- 11 chip spreading factor
- 11 DS center frequencies (11 Channels)
- Only 3 channels without overlap.
- 10 mW to 100 mW transmitted power
- 1 and 2 Mbps
- DBPSK for 1 Mbps. DQPSK for 2 Mbps.

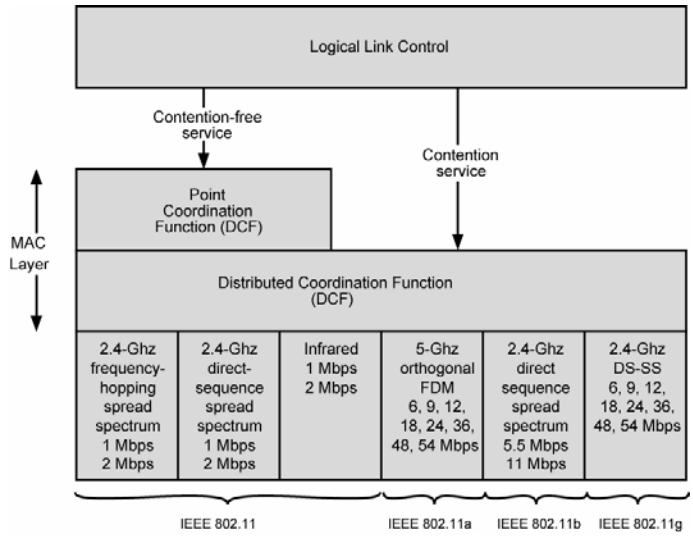
Infrared Phy

- Baseband transmission
- 850 to 950 nm range of IR
- 1 Mbps or 2 Mbps
- Diffuse IR
- Up to 10 m in typical offices
  Could be 20 m with better receivers.
- For 1 Mbps, 4-bits are mapped to 16 pulse position modulation (ppm) symbol
- For 2 Mbps, 2 bits are mapped to 4 ppm symbol

802.11 Physical Layers

- Issued in four stages
- First part in 1997: IEEE 802.11
  - Includes MAC layer and three physical layer specifications
  - Two in 2.4-GHz band and one infrared
  - All operating at 1 and 2 Mbps
- Two additional parts in 1999
  - IEEE 802.11a
    - 5-GHz band up to 54 Mbps
  - IEEE 802.11b
    - 2.4-GHz band at 5.5 and 11 Mbps
- Most recent in 2002
  - IEEE 802.g extends IEEE 802.11b to higher data rates

IEEE 802.11 Protocol Architecture



802.11a

- 5-GHz band
- Uses orthogonal frequency division multiplexing (OFDM)
- Data rates 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
- Up to 52 subcarriers modulated using BPSK, QPSK, 16-QAM, or 64-QAM
  - Depending on rate
  - Sub-carrier frequency spacing 0.3125 MHz
  - Convolutional code at rate of 1/2, 2/3, or 3/4 provides forward error correction

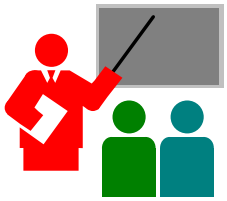
802.11b

- Extension of 802.11 DS-SS scheme
- 5.5 and 11 Mbps
- Chipping rate 11 MHz
  - Same as original DS-SS scheme
  - Same occupied bandwidth
  - Complementary code keying (CCK) modulation to achieve higher data rate in same bandwidth at same chipping rate
  - CCK modulation complex

802.11g

- Higher-speed extension to 802.11b
- Combines physical layer encoding techniques used in 802.11a and 802.11b to provide service at a variety of data rates

Summary



- Frequency hopping and Direct Sequence CDMA
- Ad-Hoc vs Infrastructure-based
- BSS, ESS, AP
- SIFS, PIFS, DIFS
- Frame Format: 4 address fields
- 802.11 PHYs: 802.11, 802.11a, 802.11b, 802.11g

Reading Assignment

- Read Chapters 9 and Chapter 17 of 7th Edition of Stallings
- Try to answer the questions in these two chapters

Homework

Time	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Data	0	1	1	1	1	1	1	0	0	0	1	0	0	1	1	1	1	0	1	0
Freq	F1		F3		F23		F22		F8		F10		F1		F3		F2		F2	
PN	001				110				011				001				001			

- **Problem 1**: The above table illustrates the operation of an FHSS system.

A. The system makes use of a form of FSK what form of FSK is it?
B. What is the number of bits per symbol?
C. How many symbols/hop?
D. Is this a slow or fast FH system?
E. What is the total number of possible carrier channels?

- **Problem 2**: Submit answer to exercise 9.7 in Stallings' book.