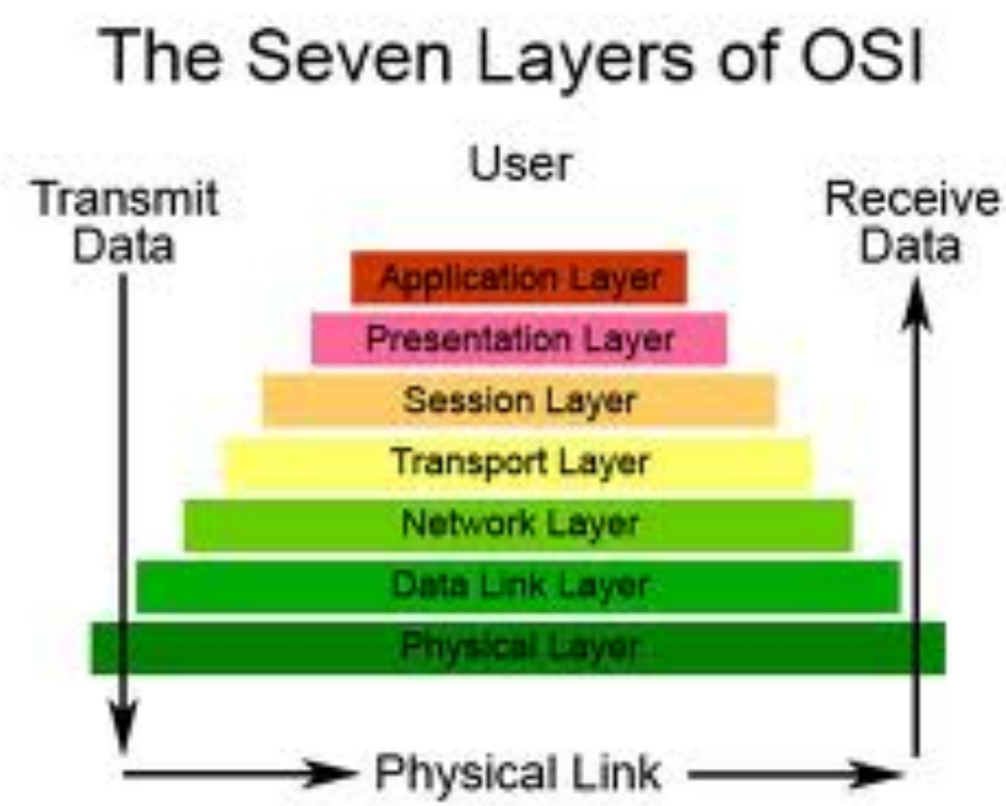
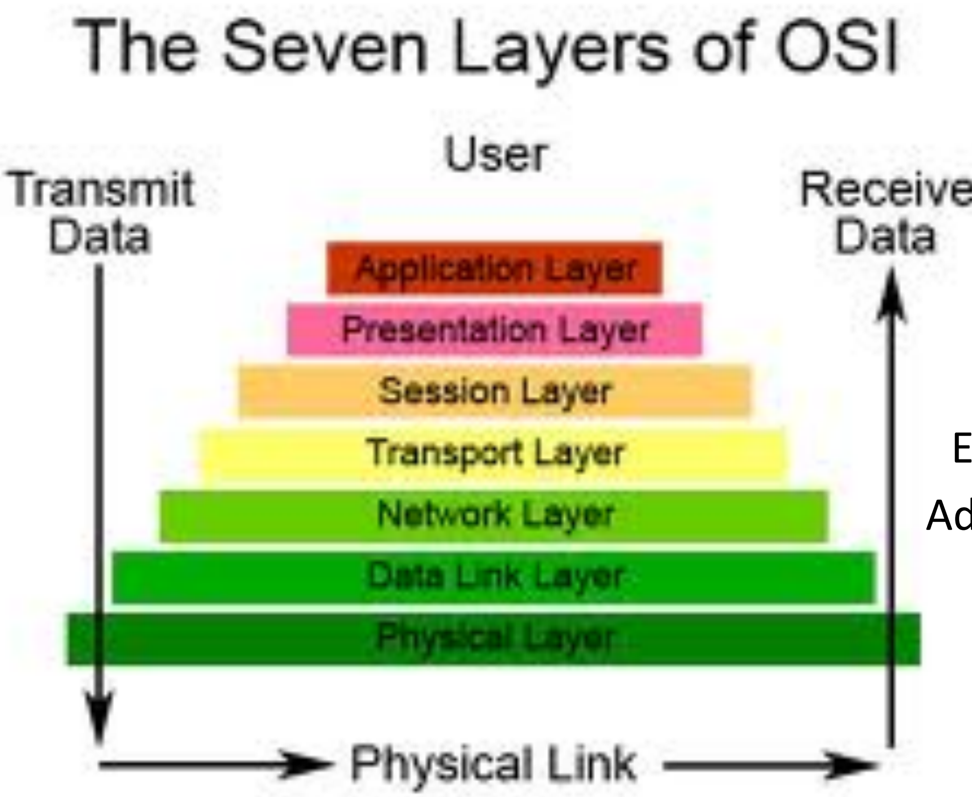
Wireless Networking

CS 407

The Networking Stack



What do they do?



Interact with apps

Rendering content

Group of flows

End-to-end

Addressing, routing

Channel contention

Signal to bits

Why use layers?

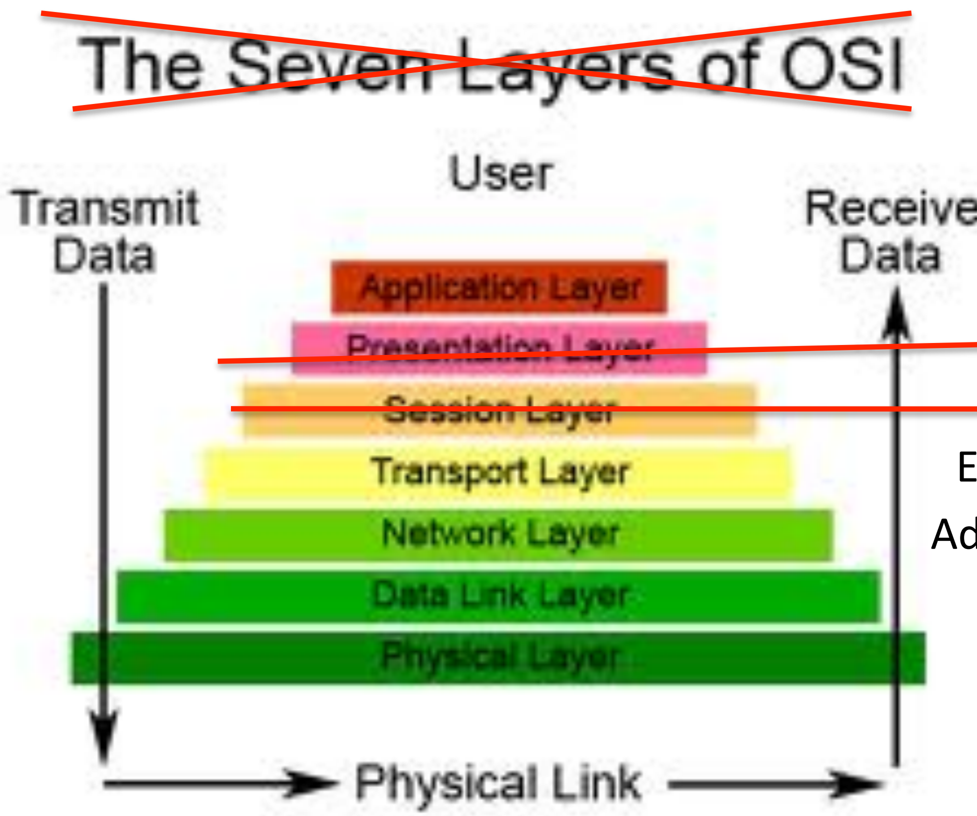
- Separation of functions
- Modularity and providing an abstraction of a function to higher layers
  - A good software engineering practice

- Can change the implementation of one layer without affecting any other layer as long as we keep to the API exposed by the layer

What does each layer do?

- Physical – Convert bits to signals and vice versa
- Data link – How to contend for a channel, especially important in wireless environments
- Network – Addressing, routing, especially getting packets from point A to B
- Transport – mostly with reliable, in-order delivery
- Session – handle a group of flows
- Presentation – How to render content on the screen (browser)
- Application – how applications specifically communicate between endpoints

What matters?



TCP/IP Stack

Interact with apps

~~Rendering content~~

~~Group of flows~~

End-to-end

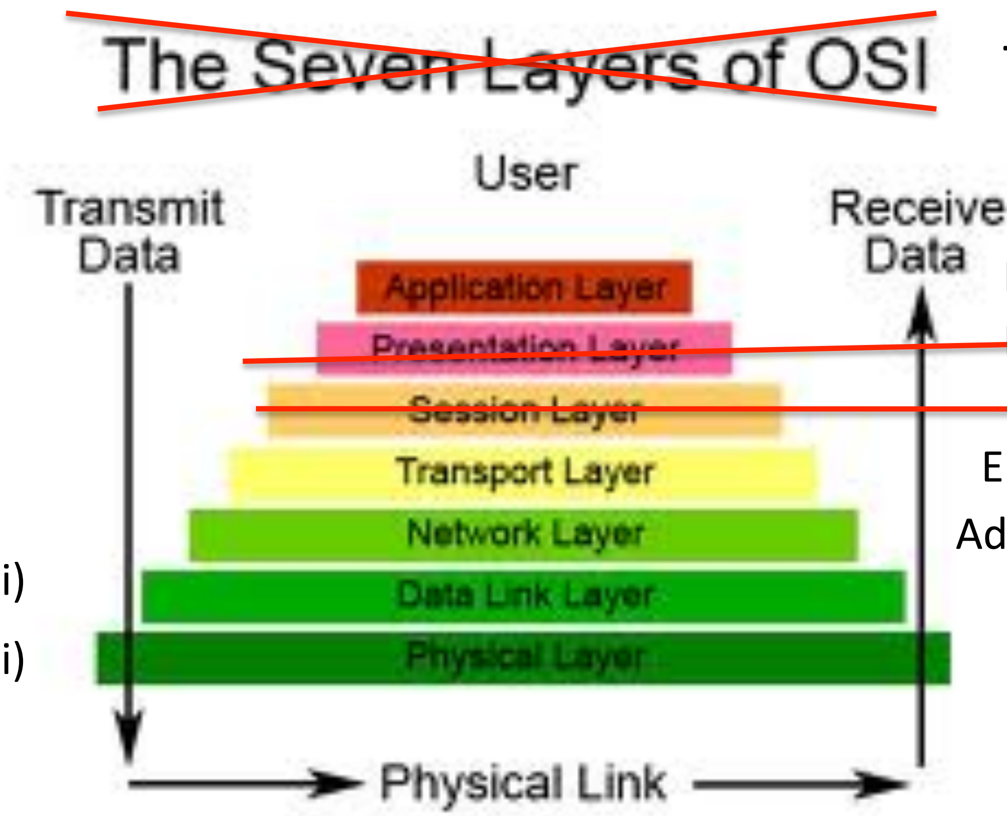
Addressing, routing

Channel contention

Signal to bits

Examples

TCP/IP Stack



Browser HTTP	Application Layer	Interact with apps
	Presentation Layer	~~Rendering content~~
	Session Layer	~~Group of flows~~
TCP, UDP	Transport Layer	End-to-end
IP	Network Layer	Addressing, routing
802.11 (WiFi)	Data Link Layer	Channel contention
802.11 (WiFi)	Physical Layer	Signal to bits

TCP

- Transmission Control Protocol
- Connection-oriented
- Reliable
- Congestion Control
- Flow Control
- “End-to-end” semantics

- Source and Destination IP and port numbers

UDP

- User Datagram Protocol
- Connectionless
- Unreliable

- Source and Destination IP and port numbers

Intro to networking

- What is an IP address
  - Identifies your location in the Internet
  - Can change
  - Assigned to a specific NIC
- What is a flow
  - <Src IP, Src port, Dst IP, Dst Port, protocol>

Wireless networking

- No wires!
- Shared media
- Interference and noise
- Bandwidth and range limits
- Variable performance
- Mobility
- Implications for higher network layers

Understand your assumptions

- Disconnected operations
  - Does your app require you to be connected always?
- Delay tolerant
  - Can you handle unpredictable delays?
  - Is caching strategies useful to your app?
- Always on
  - What happens when the app is not running?

Cellular vs WiFi

Cost: Expensive licensed spectrum

Range: 1 to 20 km

Tx power: 1-10 W

Protocols: Highly coordinated

Throughputs: ~ 10 Kbps – 2 Mbps

Cost: Cheap and unlicensed use

Range: ~100 m

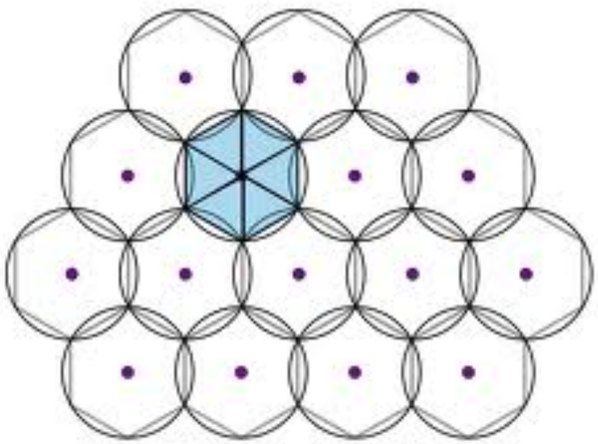
Tx power: ~0.1 W

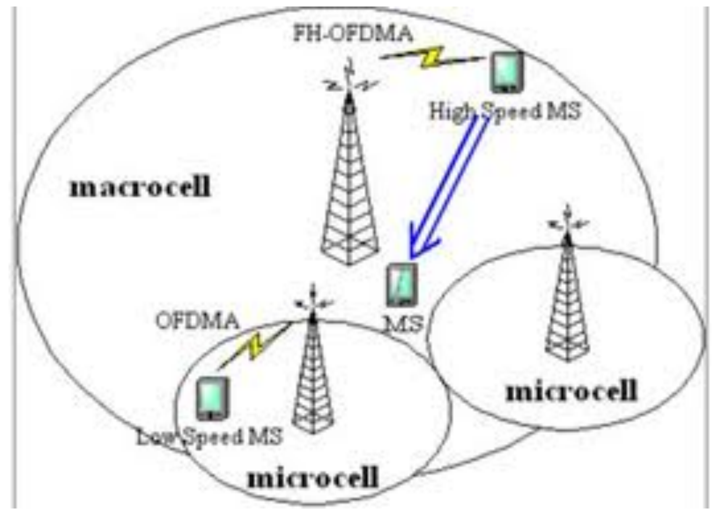
Protocols: Uncoordinated

Throughputs: ~ 1 Mbps – 100 Mbps

Cellular network planning

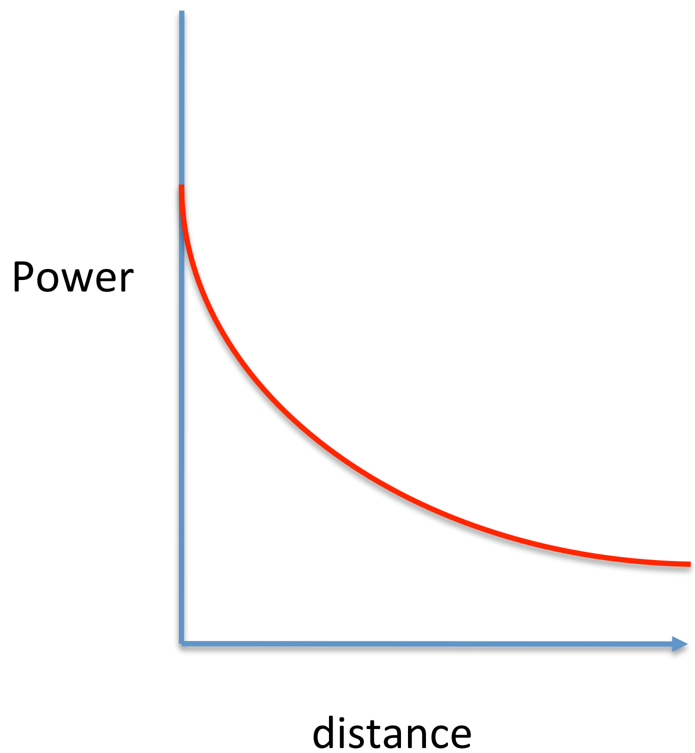
- Ideal - Hexagonal patterns

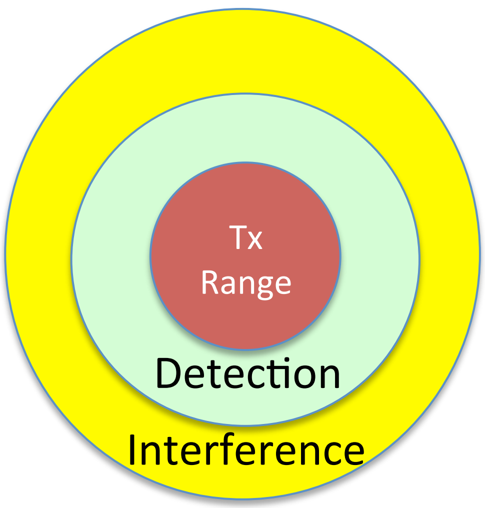




- In real life – Macro and Microcells

Signal attenuation





Signal attenuation

- Energy radiates in all directions
  - Consider a sphere (4 *pi *r ^2)

- SINR = Signal to Interference + Noise Ratio

Example 1

Consider an extremely noisy channel in which the value of the signal-to-noise ratio is almost zero. In other words, the noise is so strong that the signal is faint. For this channel the capacity C is calculated as

$$\boxed{C = B \log_2 (1 + \text{SNR}) = B \log_2 (1 + 0) = B \log_2 1 = B \times 0 = 0}$$

This means that the capacity of this channel is zero regardless of the bandwidth. In other words, we cannot receive any data through this channel.

Example 2

We can calculate the theoretical highest bit rate of a regular telephone line. A telephone line normally has a bandwidth of 3000. The signal-to-noise ratio is usually 3162. For this channel the capacity is calculated as

$$\begin{aligned} C &= B \log_2 (1 + \text{SNR}) = 3000 \log_2 (1 + 3162) = 3000 \log_2 3163 \\ &= 3000 \times 11.62 = 34{,}860 \text{ bps} \end{aligned}$$

This means that the highest bit rate for a telephone line is 34.860 kbps. If we want to send data faster than this, we can either increase the bandwidth of the line or improve the signal-to-noise ratio.

Example 3

The signal-to-noise ratio is often given in decibels. Assume that SNR_{dB} = 36 and the channel bandwidth is 2 MHz. The theoretical channel capacity can be calculated as

$$SNR_{dB} = 10 \log_{10} SNR \rightarrow SNR = 10^{SNR_{dB}/10} \rightarrow SNR = 10^{3.6} = 3981$$

$$C = B \log_2 (1 + SNR) = 2 \times 10^6 \times \log_2 3982 = 24 \text{ Mbps}$$

Example 4

For practical purposes, when the SNR is very high, we can assume that SNR + 1 is almost the same as SNR. In these cases, the theoretical channel capacity can be simplified to

$$\boxed{C = B \times \frac{\mathrm{SNR_{dB}}}{3}}$$

For example, we can calculate the theoretical capacity of the previous example as

$$\boxed{C = 2\ \mathrm{MHz} \times \frac{36}{3} = 24\ \mathrm{Mbps}}$$

Example 5

We have a channel with a 1-MHz bandwidth. The SNR for this channel is 63. What is the appropriate bit rate?

Solution

We use the Shannon formula to find the upper limit.

$$\boxed{C = B \log_2 (1 + \text{SNR}) = 10^6 \log_2 (1 + 63) = 10^6 \log_2 64 = 6 \text{ Mbps}}$$

dB

- dB = deciBels

- dBm = 10 log10 (power in mW)

- dBW = 10 log10 (power in W)

- Express 1 W in dBW and dBm
- Express 1 mW in dBW and dBm
- Expres 10 mW in dBW and dBm

Channel capacity

- Shannon' law
  - C = B log (1 + SINR)

- Spectral efficiency: units of b/s/Hz

- Check http://en.wikipedia.org/wiki/Spectral_efficiency for some example spectral efficiencies

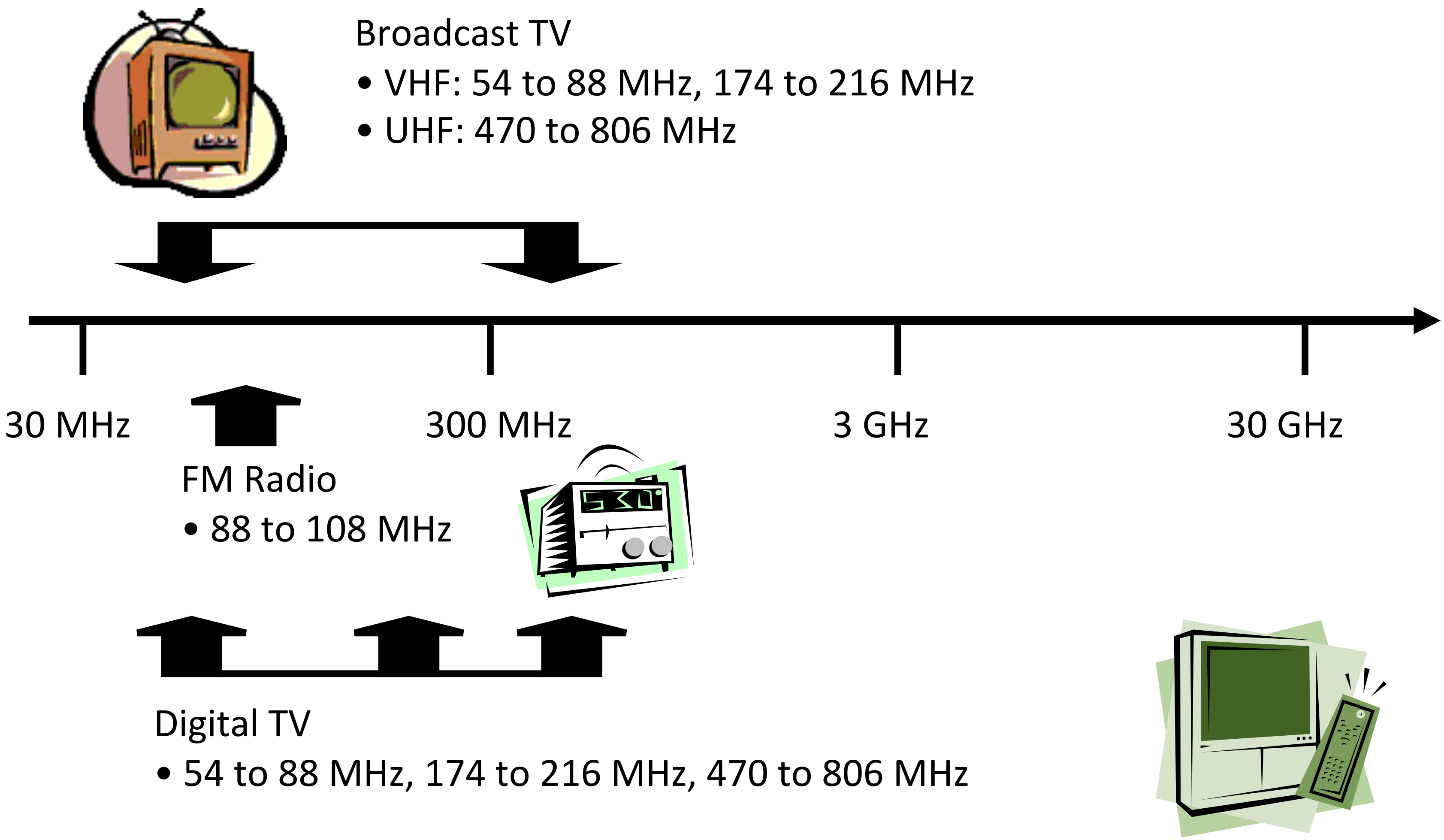
Spatial re-use

- Macrocell vs Microcell vs Pico/Femtocells

Impact of Wireless Environment on Networks

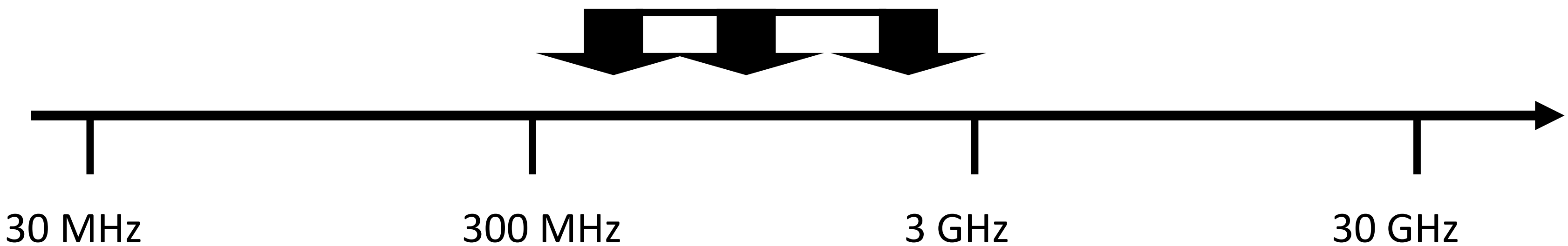
- The wireless spectrum
- Physical impairments
- Contention for the shared medium
- Effects of mobility
- Restrictions on terminal equipment
- Security

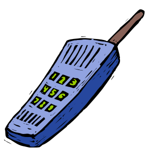
Wireless Spectrum (1)



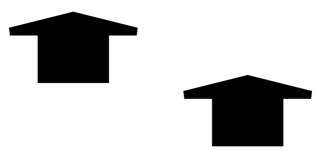
Wireless Spectrum (2)

3G Broadband Wireless
- 746-794 MHz, 1.7-1.85 GHz, 2.5-2.7 GHz



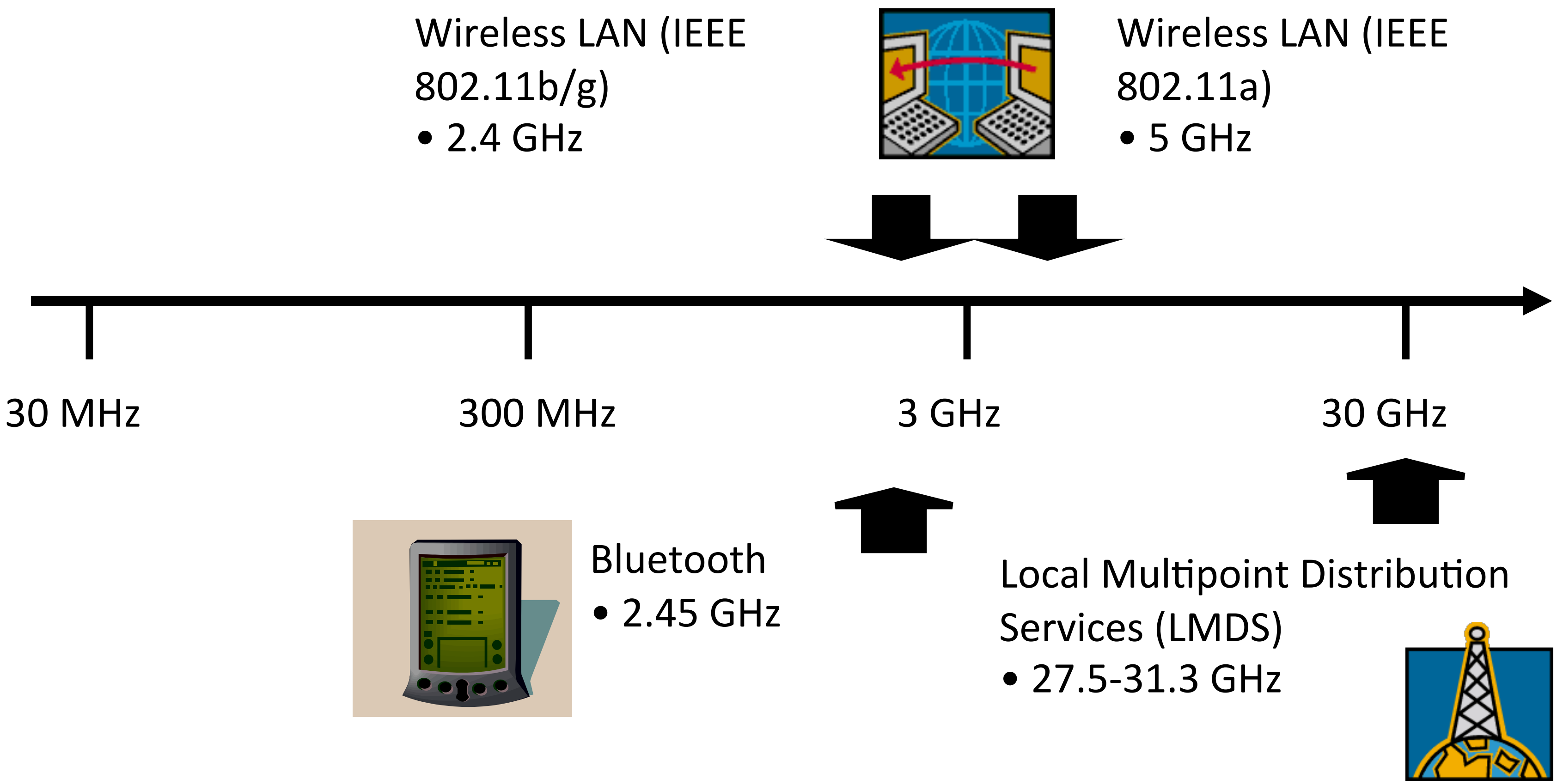


Cellular Phone
- 800-900 MHz



Personal Communication Service (PCS)
- 1.85-1.99 GHz

Wireless Spectrum (3)



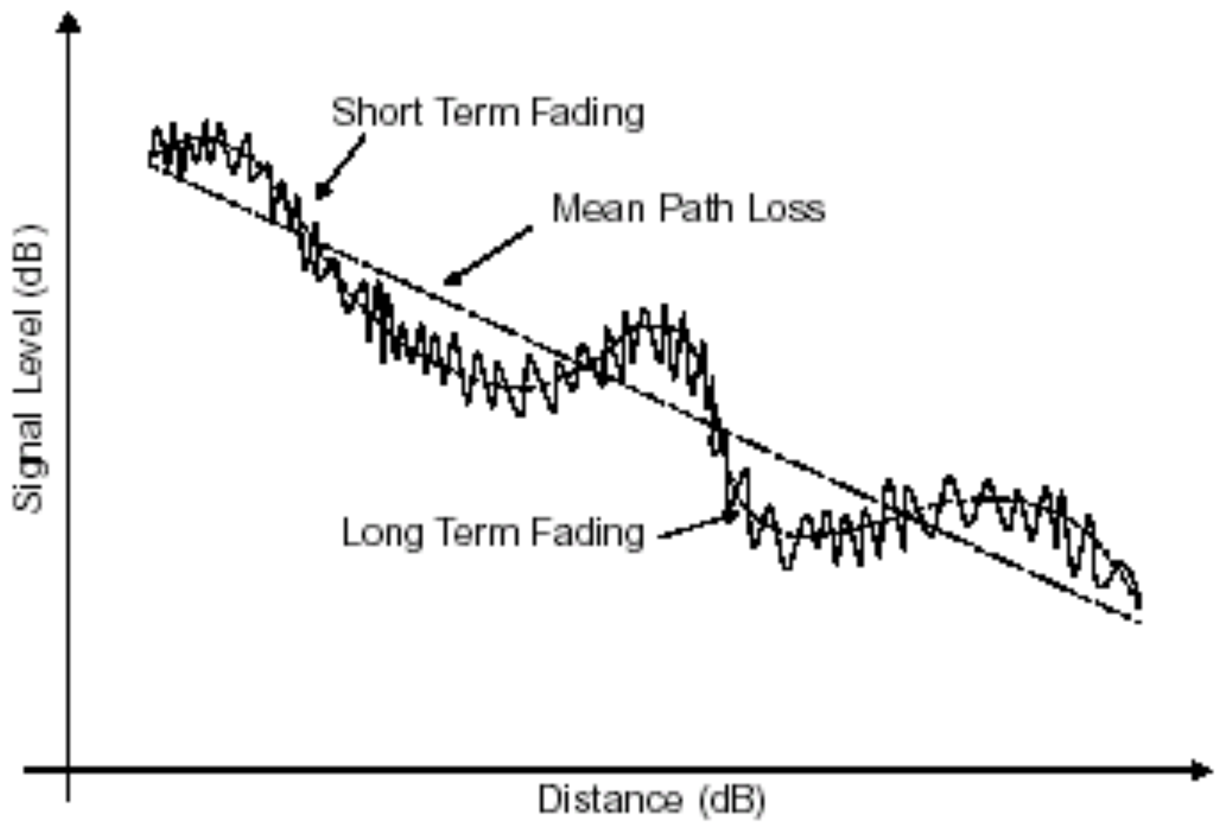
Physical Impairments: Noise

- Unwanted signals added to the message signal
- May be due to signals generated by natural phenomena such as lightning or man-made sources, including transmitting and receiving equipment as well as spark plugs in passing cars, wiring in thermostats, etc.
- Sometimes modeled in the aggregate as a random signal in which power is distributed uniformly across all frequencies (white noise)
- Signal-to-noise ratio (SNR) often used as a metric in the assessment of channel quality

Physical Impairments: Interference

- Signals generated by communications devices operating at roughly the same frequencies may interfere with one another
  – Example: IEEE 802.11b and Bluetooth devices, microwave ovens, some cordless phones
  – CDMA systems (many of today's mobile wireless systems) are typically interference-constrained
- Signal to interference and noise ratio (SINR) is another metric used in assessment of channel quality

Physical impairments: Fading (1)



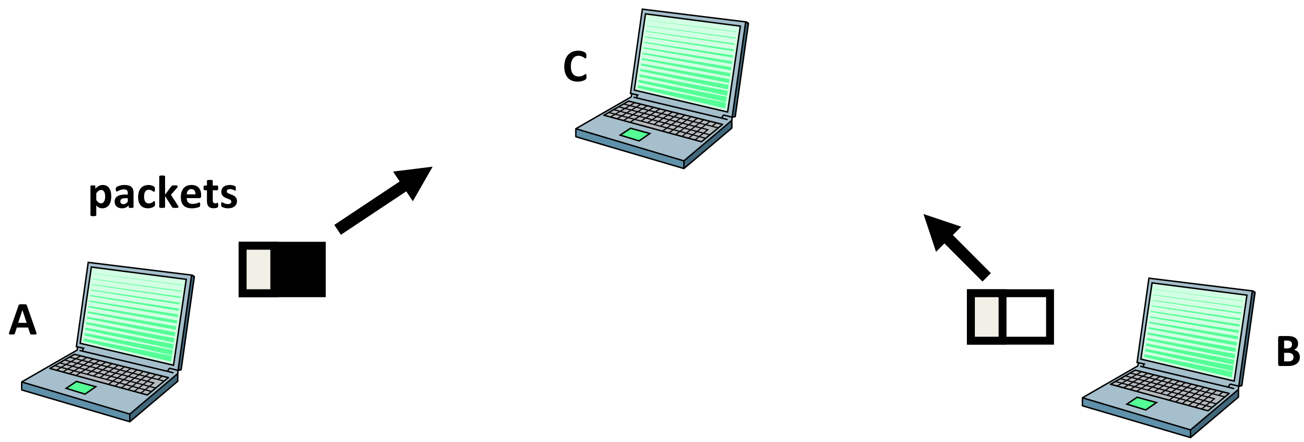
Physical impairments: Fading (2)

- Strength of the signal decreases with distance between transmitter and receiver: path loss
  - Usually assumed inversely proportional to distance to the power of 2.5 to 5
- Slow fading (shadowing) is caused by large obstructions between transmitter and receiver
- Fast fading is caused by scatterers in the vicinity of the transmitter

Diversity

- A diversity scheme extracts information from multiple signals transmitted over different fading paths
- Appropriate combining of these signals will reduce severity of fading and improve reliability of transmission
- In space diversity, antennas are separated by at least half a wavelength
  - Other forms of diversity also possible
  - Polarization, frequency, time diversity

Contention for the Medium



- If A and B simultaneously transmit to C over the same channel, C will not be able to correctly decode received information: a collision will occur
- Need for medium access control mechanisms to establish what to do in this case (also, to maximize aggregate utilization of available capacity)

Effects of Mobility

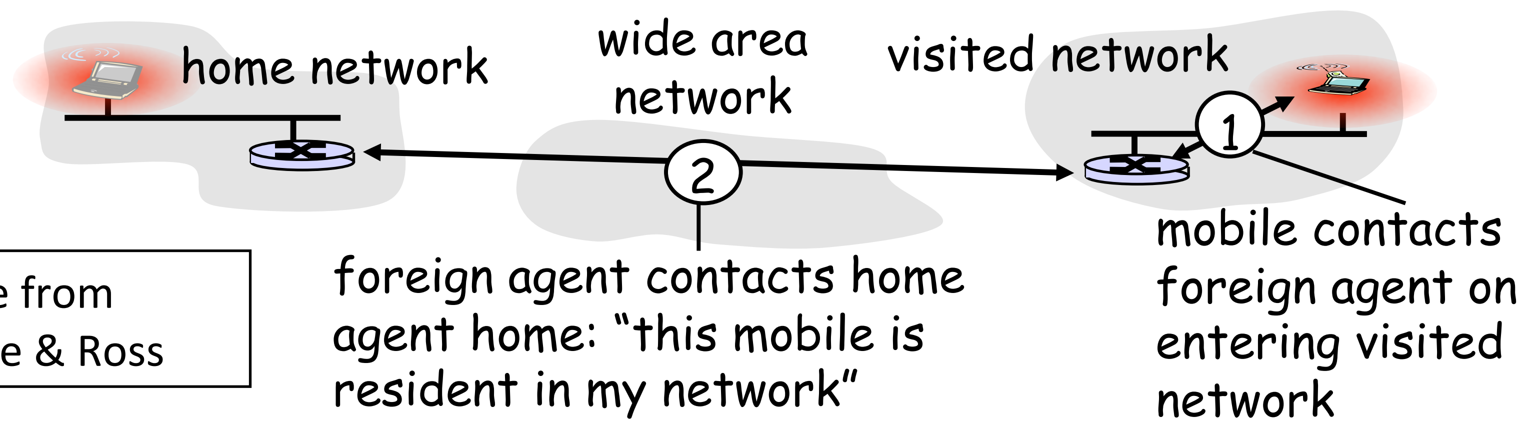


Figure from Kurose & Ross

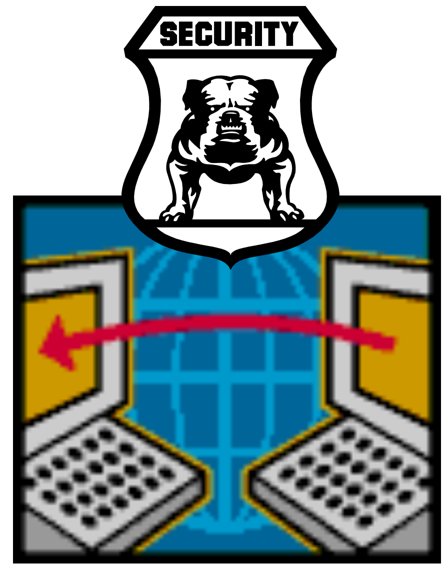
- Destination address not equal to destination location
- Addressing and routing must be taken care of to enable mobility
- Can be done automatically through handoff or may require explicit registration by the mobile in the visited network
- Resource management and QoS are directly affected by route changes

Form Factors

- Form factors (size, power dissipation, ergonomics, etc.) play an important part in mobility and nomadicity
  - Mobile computing: implies the possibility of seamless mobility
  - Nomadic computing: connections are torn down and re-established at new location
- Battery life imposes additional restrictions on the complexity of processing required of the mobiles units

Security

- Safeguards for physical security must be even greater in wireless communications
- Encryption: intercepted communications must not be easily interpreted
- Authentication: is the node who it claims to be?



Medium sharing approaches

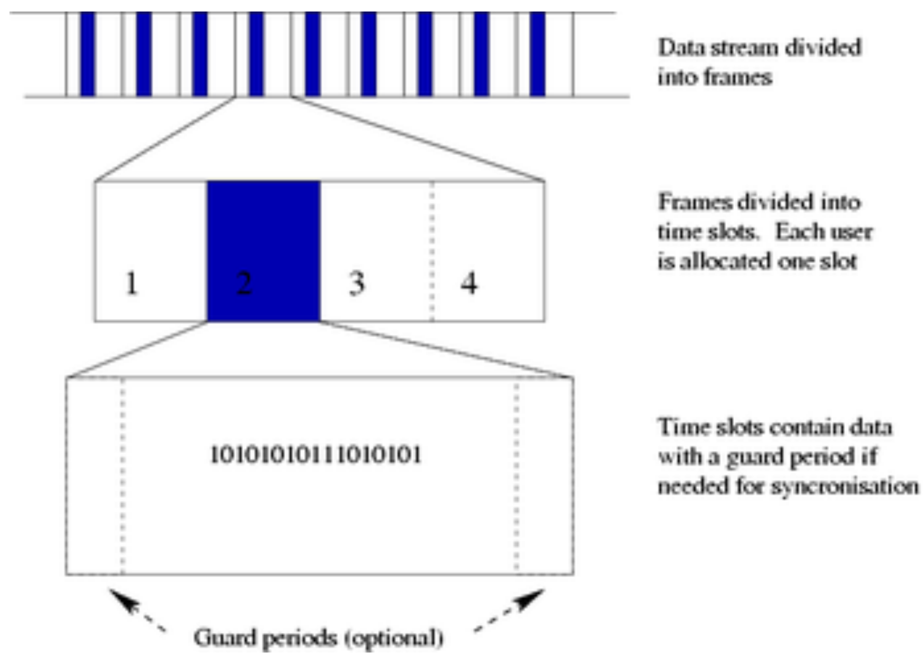
- Time division multiple access (TDMA)

- Frequency division multiple access (FDMA)

- Code division multiple access (CDMA)

TDMA

- Examples
  - GSM
  - IS136
  - iDen
  - DECT
  - Satellite communications



TDMA

- Advantages
  - Active only during own time slot, can do anything else in other time slots
    - Measure the channel, search for other transmitters in different frequencies, etc.
    - Facilities inter-frequency handoffs efficiently (imagine a macrocell and a microcell operating in the same region with different frequencies)
- Disadvantages
  - Need guard slots to protect between two transmitters (to avoid very tight synchronization)
  - This wastes capacity of the channel

Spread Spectrum

- Introduction
- Frequency Hopping Spread Spectrum
- Direct Sequence Spread Spectrum

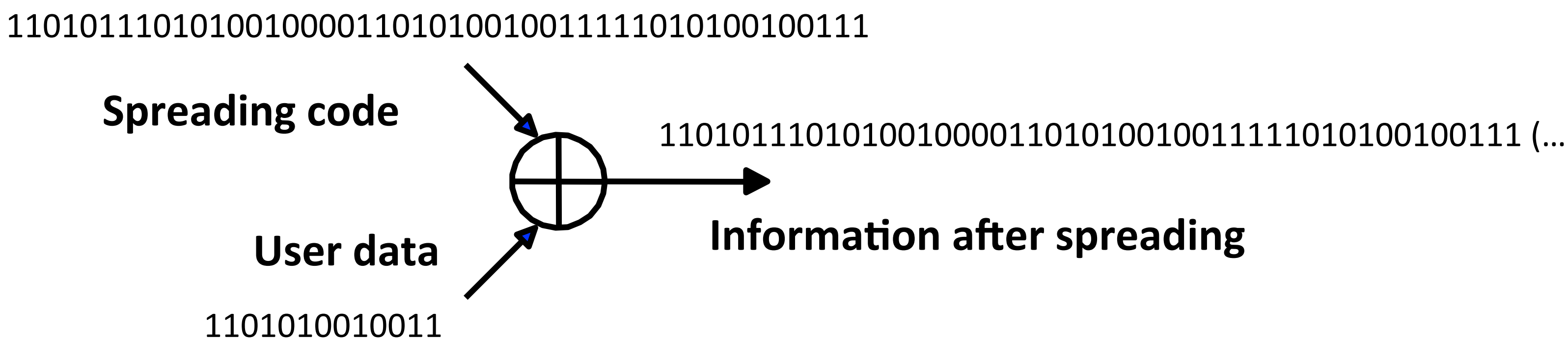
Why Spread Spectrum?

- Spread spectrum signals are distributed over a wide range of frequencies and then collected back at the receiver
  - These wideband signals are noise-like and hence difficult to detect or interfere with
- Initially adopted in military applications, for its resistance to jamming and difficulty of interception
- More recently, adopted in commercial wireless communications

Frequency Hopping Spread Spectrum (FHSS)

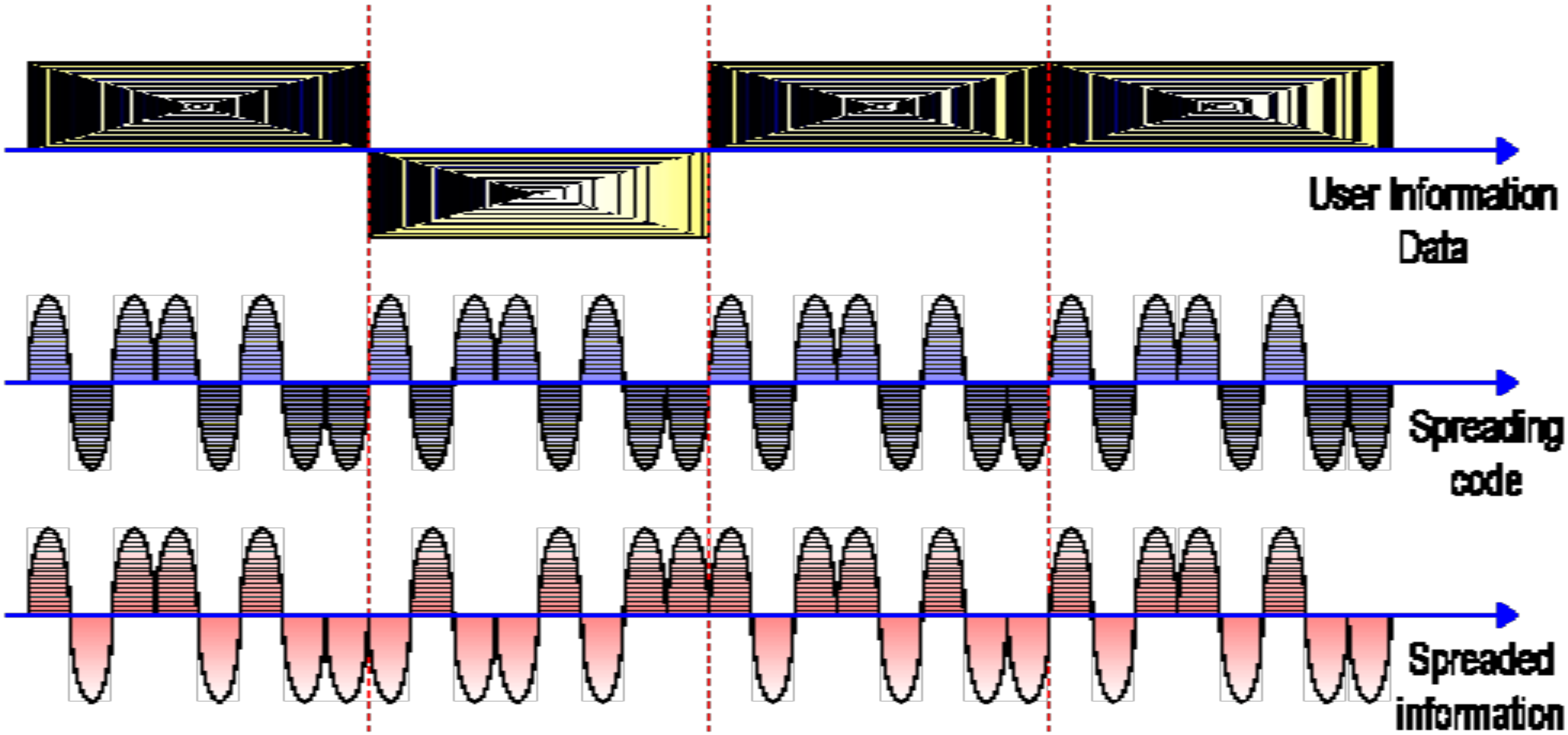
- Data signal is modulated with a narrowband signal that *hops* from frequency band to frequency band, over time
- The transmission frequencies are determined by a spreading, or hopping code (a pseudo-random sequence)

Direct Sequence Spread Spectrum (DSSS)

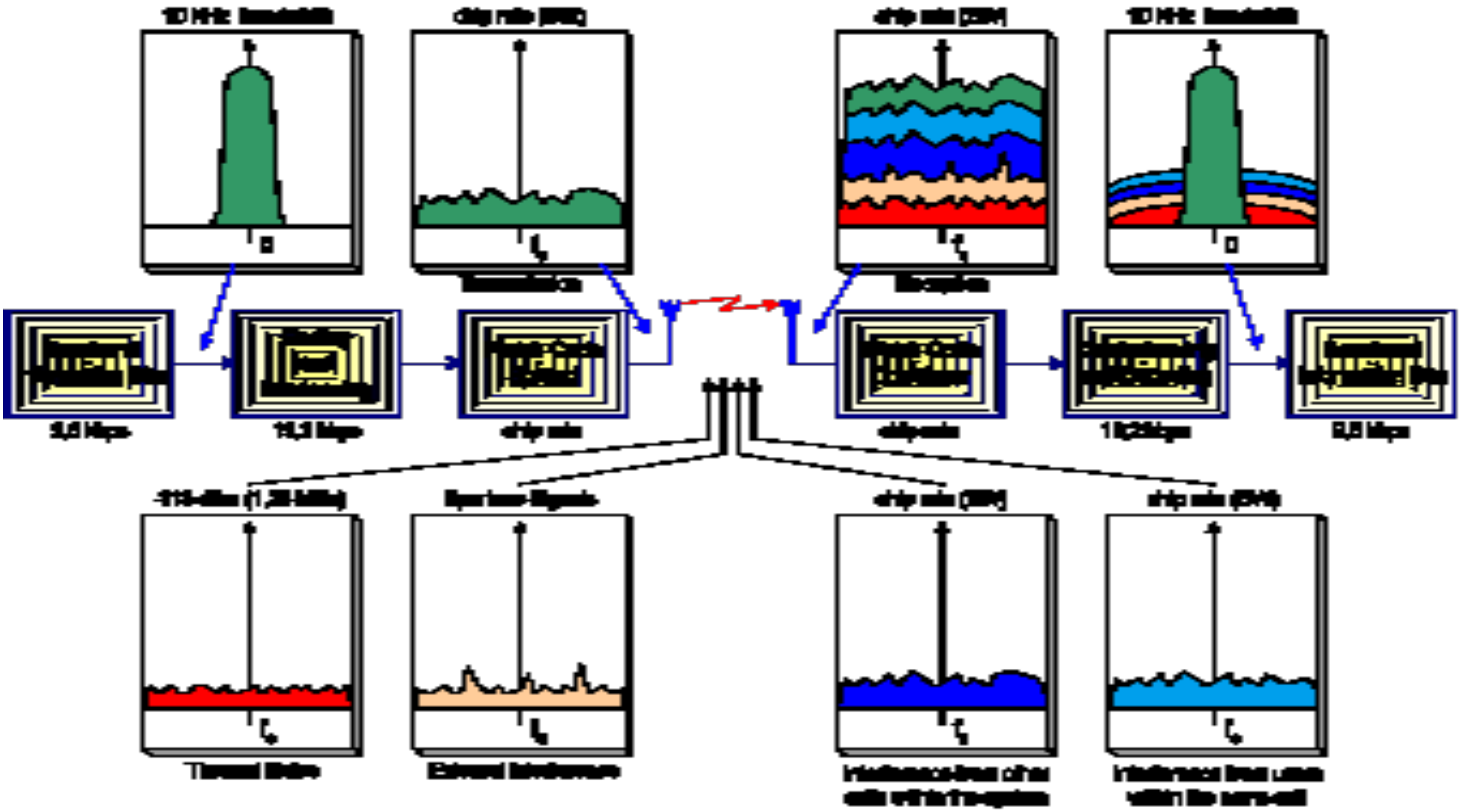


- Data signal is multiplied by a spreading code, and resulting signal occupies a much higher frequency band
- Spreading code is a pseudo-random sequence

DSSS Example



Spreading and De-spreading DSSS



Wireless Networks

- Mobile wireless WANs
- Fixed wireless WANs
- WLANs: the 802.11 family
- WLANs/WPANs: Bluetooth

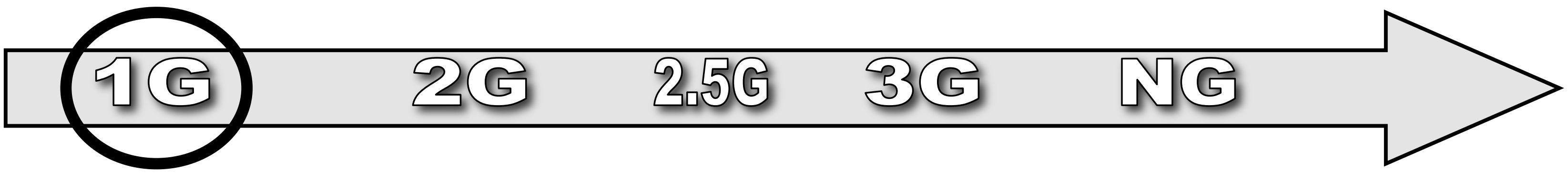
Generations in Mobile Wireless Service

- First Generation (1G)
  - Mobile voice services
- Second Generation (2G)
  - Primarily voice, some low-speed data (circuit switched)
- Generation 2½ (2.5G)
  - Higher data rates than 2G
  - A bridge (for GSM) to 3G
- Third Generation (3G)
  - Seamless integration of voice and data
  - High data rates, full support for packet switched data

Evolution of Mobile Wireless (1)

Advance Mobile Phone Service (AMPS)

- FDMA
- 824-849 MHz (UL), 869-894 MHz (DL)
- U.S. (1983), So. America, Australia, China



European Total Access Communication System (E-TACS)

- FDMA
- 872-905 MHz (UL), 917-950 MHz (DL)
- Deployed throughout Europe

Cellular generations

- 1G – AMPS
  - Advanced mobile phone systems
  - Used a FDMA style communication system
  - Separate channel for each user
  - Allowed for spatial frequency re-use

  - Limitations:
    - Analog and hence suspectible to noise, eavesdropping
      - Can overhear ESN and replay

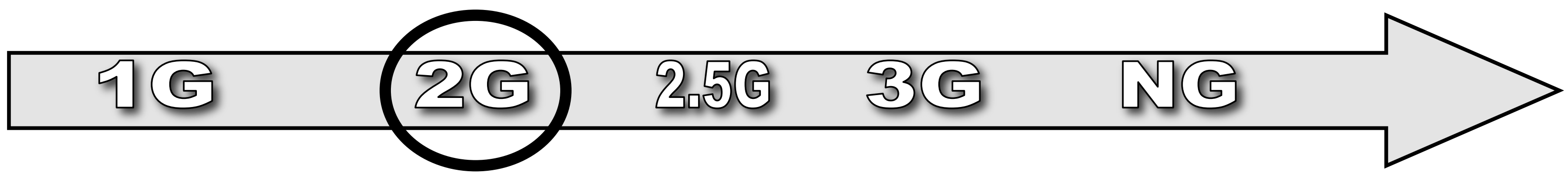
Cellular generations

- 1G
  - Had separate uplink and downlink frequencies
  - 824 to 849 MHz (uplink)
  - 869 to 894 MHz (downlink)
  - Each channel was 30 KHz wide

Evolution of Mobile Wireless (2)

Global System for Mobile communications (GSM)

- TDMA
- Different frequency bands for cellular and PCS
- Developed in 1990, expected >1B subscriber by end of 2003

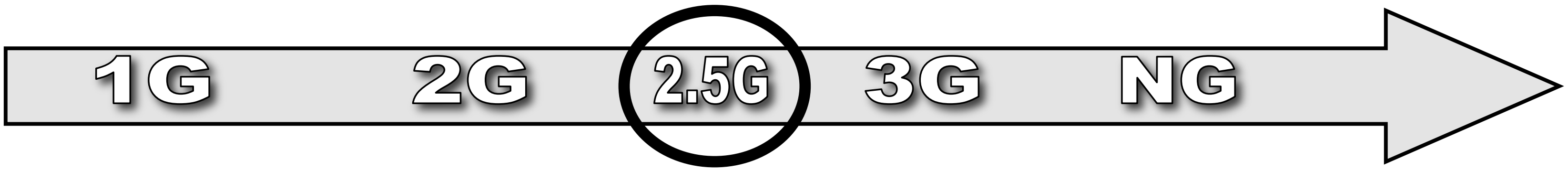


IS-95

- CDMA
- 800/1900 MHz – Cellular/PCS
- U.S., Europe, Asia

Evolution of Mobile Wireless (3)

General Packet Radio Services (GPRS)
- Introduces packet switched data services for GSM
- Transmission rate up to 170 kbps
- Some support for QoS



Enhanced Data rates for GSM Evolution (EDGE)
- Circuit-switched voice (at up to 43.5 kbps/slot)
- Packet-switched data (at up to 59.2 kbps/slot)
- Can achieve on the order of 475 kbps on the downlink, by combining multiple slots

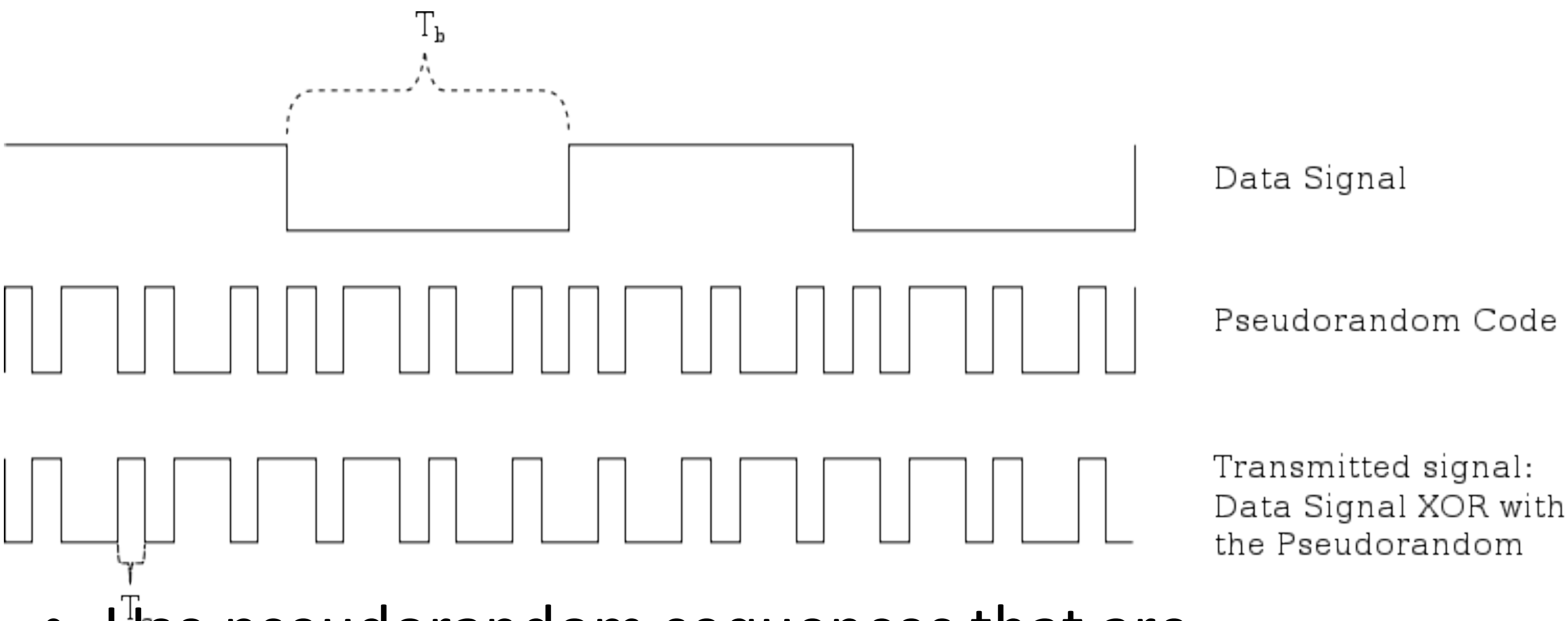
Cellular generations

- 2G
  - GSM or Global System for Mobile Communications (voice)
  - 2.5G
    - Data extensions were called GPRS (Generalized Packet Radio Services)
    - Speeds further increased in EDGE (Enhanced Data rates for GSM Evolution)
  - Communication channels: 850/1900 MHz (Canada/US) or 900/1800 MHz
  - Uses TDMA communication

Cellular generations

- 2G
  - IS95
    - CDMA (Code Division Multiple Access)
  - CDMA allows parallel communication at the same time and frequency but using separate codes

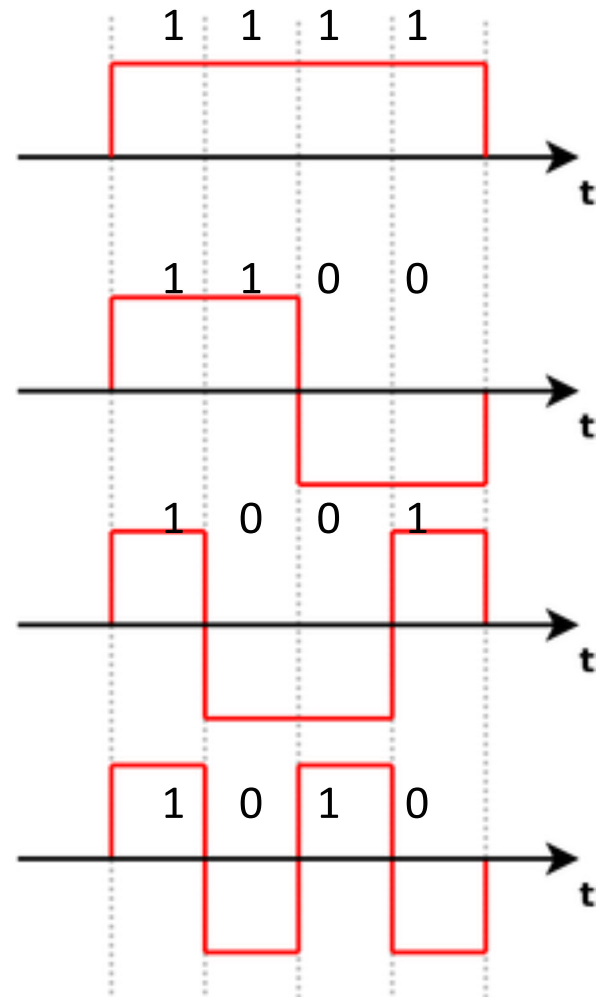
CDMA example



- Use pseudorandom sequences that are orthogonal (cancel out)

CDMA example

- Assume dot product
- 4 orthogonal codes
  - a.b = 0



CDMA example

- Consider a simpler model of 2 bit codes
  - Sender 0: (1, -1) and Sender 1: (1, 1)
  - Data: 1, 0, 1, 1 Data: 0, 0, 1, 1

  Encoded sender 0: (1, -1, -1, 1, 1, -1, 1, -1)

  Encoded sender 1: (-1, -1, -1, -1, 1, 1, 1, 1)
- Simultaneous transmit in medium:
  - (0, -2, -2, 0, 2, 0, 2, 0)

CDMA example

- Simultaneous transmit in medium:
  - (0, -2, -2, 0, 2, 0, 2, 0)
- Sender 0 code: (1, -1)
- Multiply received pattern with sender code
  - ((0, -2), (-2, 0), (2, 0), (2, 0)) . (1, -1)

  = (2, -2, 2, 2), i.e., 1, 0, 1, 1

CDMA example

- Sender 0 code = a, data = x
- Sender 1 code = b, data = y
- Sent a.x + b.y

- Decode a.(a.x + b.y) = (a.a) x + a.b.y = (a.a) x

CDMA

- Advantages
  - Avoids narrow-band interference
  - Does not require strong coordination across different transmitters
  - Uses much more bandwidth than minimum requirements
  - Can allow a single handset to simultaneously talk to two different base stations (use two codes) and achieves better handoffs
- Disadvantages
  - Need to balance transmit power of different transmitters

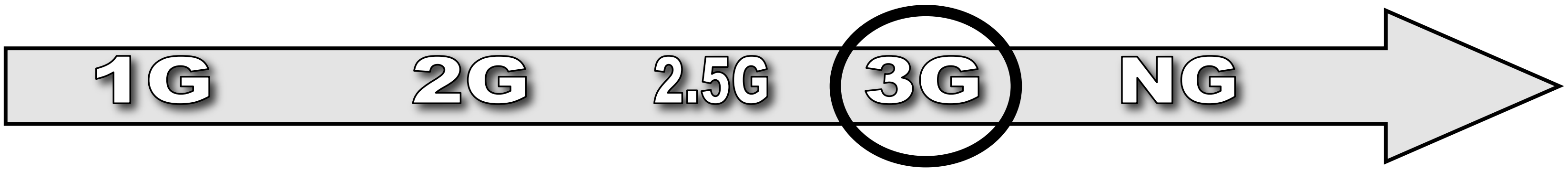
Asynchronous CDMA

- Synchronous CDMA assumes all users synchronized and use orthogonal codes
- In asynchronous, each user picks a pseudo-random code, and there is some unwanted interference from other sources
  - Equalizing received power from different sources is an important necessity
  - Adding more users, adds to the noise level and so gracefully degrades performance

Evolution of Mobile Wireless (4)

Universal Mobile Telecommunication Systems (UMTS)

- Wideband DS-CDMA
- Bandwidth-on-demand, up to 2 Mbps
- Supports handoff from GSM/GPRS



IS2000

- CDMA2000: Multicarrier DS-CDMA
- Bandwidth on demand (different flavors, up to a few Mbps)
- Supports handoff from/to IS-95

Fixed Wireless

- Microwave
  - Traditionally used in point-to-point communications
  - Initially, 1 GHz range, more recently in the 40 GHz region
- Local Multipoint Distribution Service (LMDS)
  - Operates around 30 GHz
  - Point-to-multipoint, with applications including Internet access and telephony
  - Virginia Tech owns spectrum in SW VA and surroundings
- Multichannel Multipoint Distribution Service (MMDS)
  - Operates around 2.5 GHz
  - Initially, for TV distribution
  - More recently, wireless residential Internet service

WLANs: IEEE 802.11 Family

- 802.11 working group
  - Specify an open-air interface between a wireless client and a base station or access point, as well as among wireless clients
- IEEE 802.11a
  - Up to 54 Mbps in the 5 GHz band
  - Uses orthogonal frequency division multiplexing (OFDM)
- IEEE 802.11b (Wi-Fi)
  - 11 Mbps (with fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band
  - Uses DSSS
- IEEE 802.11g
  - 20+ Mbps in the 2.4 GHz band

WLANs/WPANs: Bluetooth

- Cable replacement technology
- Short-range radio links
- Small, inexpensive radio chip to be plugged into computers, phones, palmtops, printers, etc.
- Bluetooth was invented in 1994
- Bluetooth Special Interest Group (SIG) founded in 1998 by Ericsson, IBM, Intel, Nokia and Toshiba to develop an open specification
  – Now joined by > 2500 companies

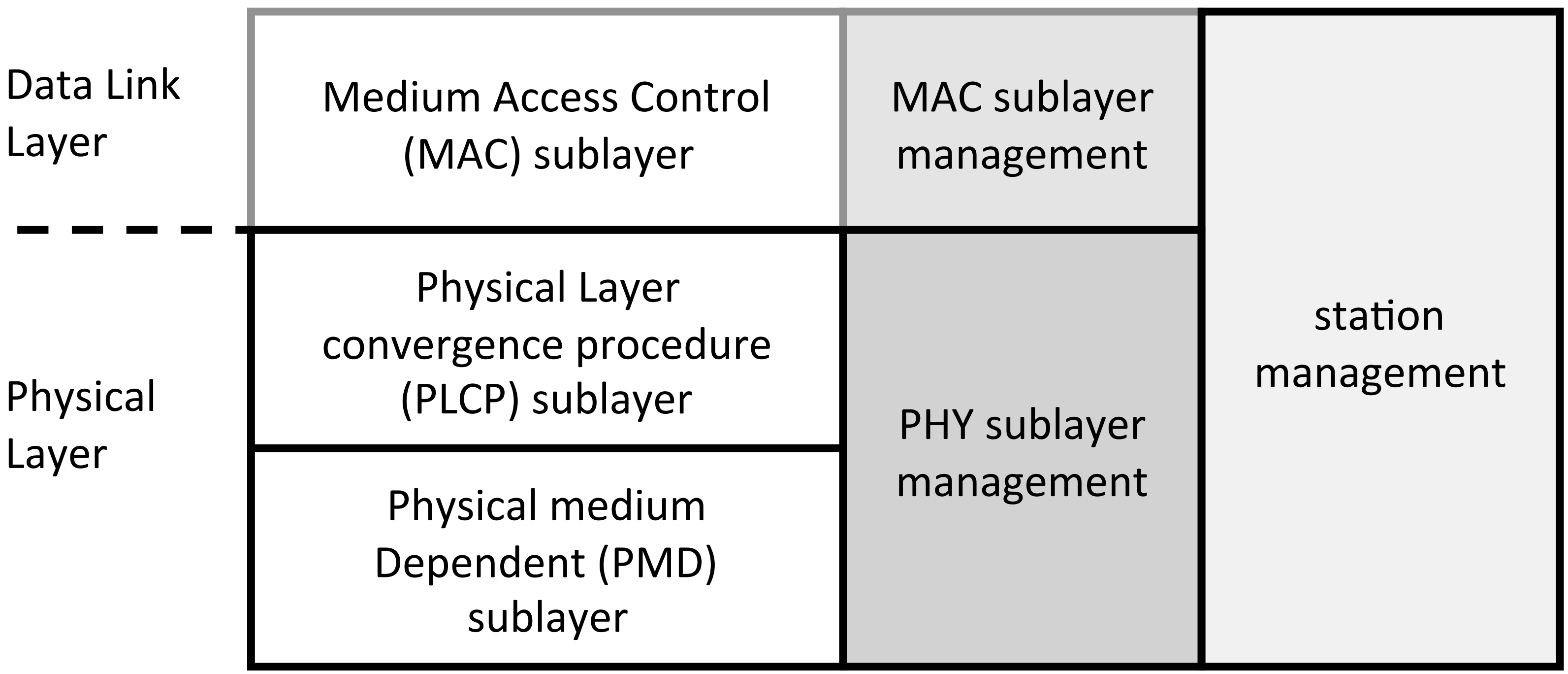
IEEE 802.11

- Characteristics
- Modes of operation
- Association, authentication and privacy

IEEE 802.11 Standard

- Final draft approved in 1997
- Operates in the 2.4 GHz industrial, scientific and medical (ISM) band
- Standard defines the physical (PHY) and medium access control (MAC) layers
  - Note that the 802.11 MAC layer also performs functions that we usually associated with higher layers (e.g., fragmentation, error recovery, mobility management)
- Initially defined for operation at 1 and 2 Mbps
  - DSSS, FHSS or infrared
  - Extensions (IEEE 802.11b, IEEE 802.11a, etc.) allow for operation at higher data rates and (in the case of 802.11a) different frequency bands

Reference Model (1)



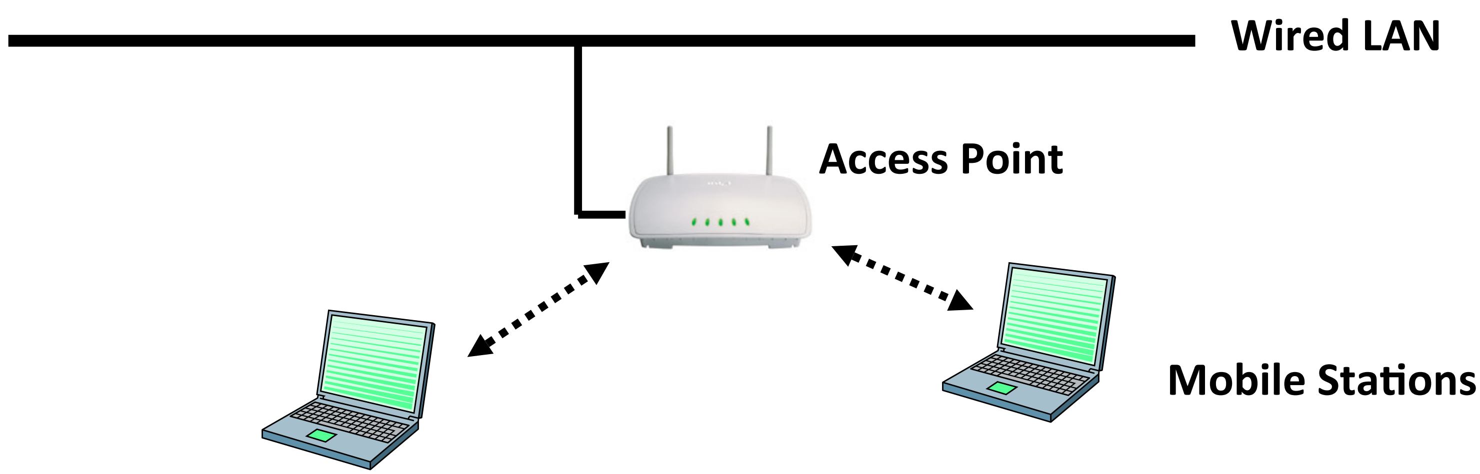
Reference Model (2)

- Physical Medium Dependent (PMD) sublayer
  - Defines a method for transmitting and receiving data through the medium, including modulation and coding
  - Dependent on whether DSSS, FHSS or IR is used
- Physical Layer Convergence Procedure (PLCP) sublayer
  - Maps MAC layer PDUs into a packet suitable for transmission by the PMD sublayer
  - Performs carrier sensing
- MAC sublayer
  - Defines access mechanism, based on CSMA
  - Performs fragmentation and encryption of data packets

IEEE 802.11b

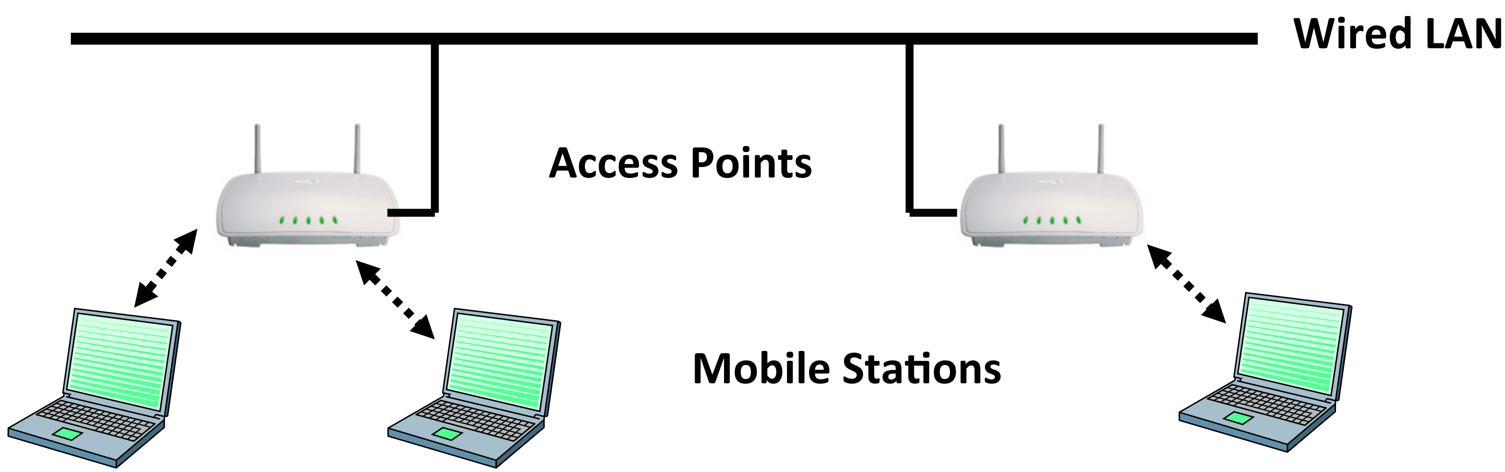
- Standard released in 1999
- 2.4 – 2.483 GHz band
- Uses DSSS
- Data rates of up to 11 Mbps
  - Data rates are automatically adjusted for noisy conditions, so can operate at 1, 2, 5.5 or 11 Mbps
- Modes of operation
  - Infrastructure-based
  - Ad-hoc
- Most widely implemented to date

Infrastructure Mode (1)



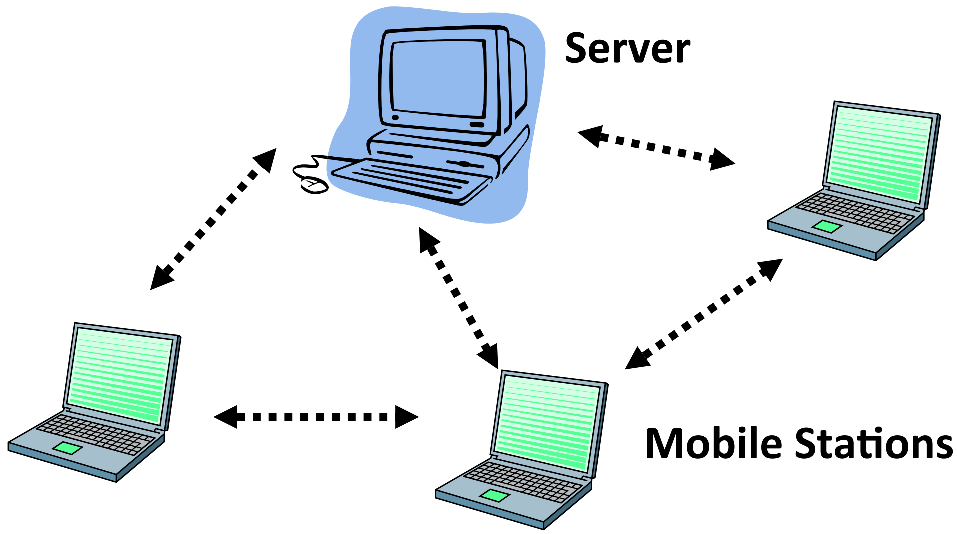
- Basic Service Set (BSS)
- Access point serves as a local bridge
- Stations communicate through the access point, which relays frames to/from mobile stations

Infrastructure Mode (2)



- Extended Service Set (ESS)
- A set of infrastructure BSSs
- Access points communicate among themselves to forward frames between BSSs and to facilitate movement of stations between BSSs

Ad Hoc Mode

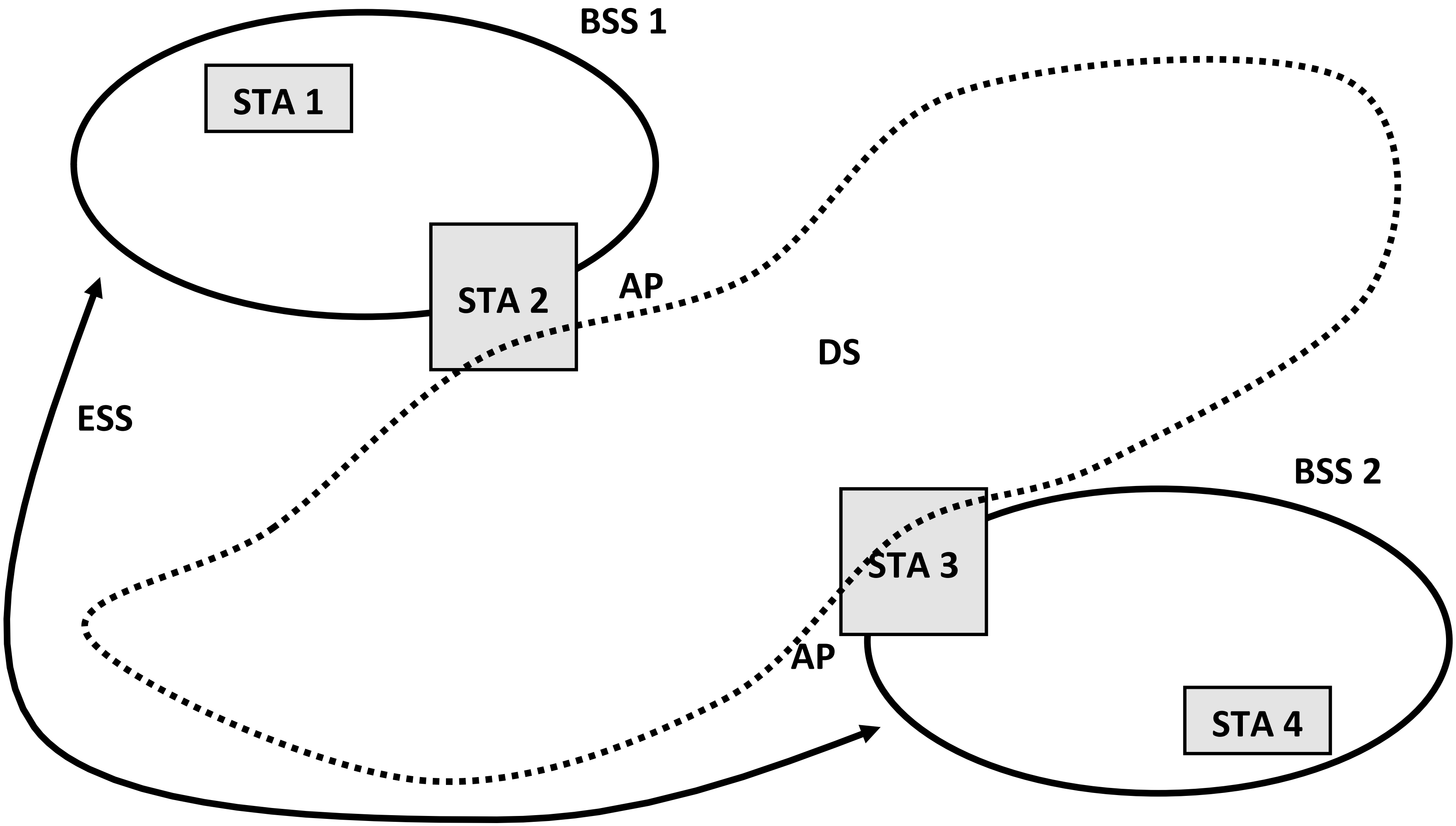


- Independent Basic Service Set (IBSS) or Peer to Peer
- Stations communicate directly with each other
- When no direct link is feasible between two station, a third station may act as a relay (multi-hop communications)

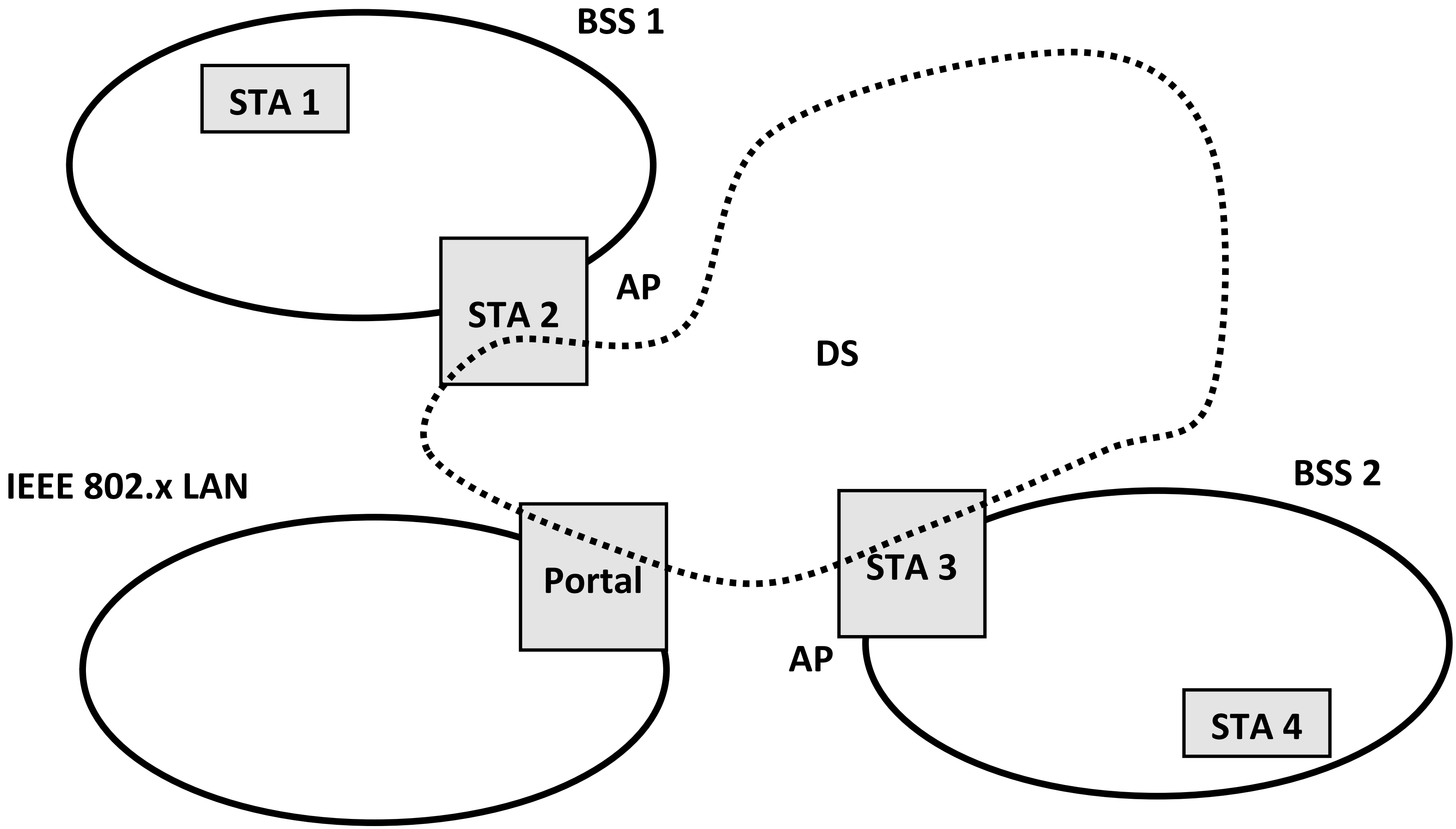
Distribution Systems

- The architectural component used to interconnect BSSs is the <u>distribution system</u> (DS)
- DS enable mobile device support
  - Address-to-destination mapping
  - Seamless integration of several BSSs
- In practice, an access point implements DS services

Distribution Systems and Access Points



Integration with Wired LANs



Association

- To deliver a message within the DS, must know which AP to access for a given mobile station
- Before a station is allowed to send a message through an AP, it must <u>associate</u> itself with that AP
  - At any given time, a station must be associated with no more than one AP
  - An AP may be associated with multiple stations
- As it moves between BSSs, a mobile station may <u>reassociate</u> itself with a different AP

Authentication

- 802.11 provides link-level authentication between stations
- 802.11 also supports shared key authentication
  - Requires that wired equivalent privacy (WEP) be enabled
  - Identity is demonstrated by knowledge of a shared, secret, WEP encryption key
- Typically, authentication is performed at association with an AP

Privacy

- Default state is "in the clear" – messages are *not* encrypted
- Optional privacy mechanism, WEP, is provided
  - Goal is to achieve a level of security at least as good as in a wired LAN
- Note that encryption provided by WEP is relatively easy to break

Bluetooth

- Characteristics
- Comparison with IEEE 802.11

Introduction

- Motivation: cable replacement in peripherals and embedded devices
- Named after Harald Blaatand "Bluetooth" II, king of Denmark 940-981 A.D.
- Estimated > 670 M Bluetooth-enabled devices by 2005

Requirements

Bluetooth phone and headset

Bluetooth printer module

- Universal framework to integrate a diverse set of devices in a seamless, user-friendly, efficient manner
- Devices must be able to establish ad hoc connections
- Support for data and voice
- Similar security as cables
- Simple, small, power-efficient implementation
- Inexpensive!

Characteristics

- Operates in the ISM band (like 802.11b)
- Frequency hopping spread spectrum
- Up to 720 kbps data transfer with a range of 10 m
  - Transmission rate decreases if interference from other devices is present
- Master/slave architecture
  - A collection of master + slaves is called a piconet
  - Up to 7 slave devices may communicate with a master
  - Piconets can be linked together to form a scatternet

Comparison with 802.11

Characteristic	Bluetooth	IEEE 802.11b	IEEE 802.11a
Spectrum	2.4 GHz	2.4 GHz	5 GHz
Max Data Rate	725 kbps	11 Mbps	54 Mbps
Connections	Point-to-Multipoint	Point-to-Point	Point-to-Point
Frequency Selection	FHSS	DSSS	OFDM
Circuit cost (est. 2001)	$ 11.00	$ 46.00	N/A