Mobile Device and Wireless Network Security

Introduction to Wireless Networks

Wireless communication;

Existing and emerging Wireless networks;

Wireless network security concerns and requirements;

Di Ma

Lecture outline

1 Characteristics of Wireless Communication

2 Existing and Emerging Wireless Networks

3 Wireless Network Security Concerns and Requirements

Background

- Era of wireless networks
  - There are more wireless phones than wired ones
  - Wireless LANs are routinely used
  - Wireless devices have become commonplace
  - Ubiquitous computing
- New computing paradigm
  - Before: limited or no programmability wireless devices managed in a highly centralized fashion
  - Now: full-fledged wireless computing devices that take active role in the networking mechanisms
- New vulnerabilities and security challenges
  - Wired security solutions (mostly *posteriori*) are not suitable
  - Need a systematic a *priori* approach

Wireless Communication

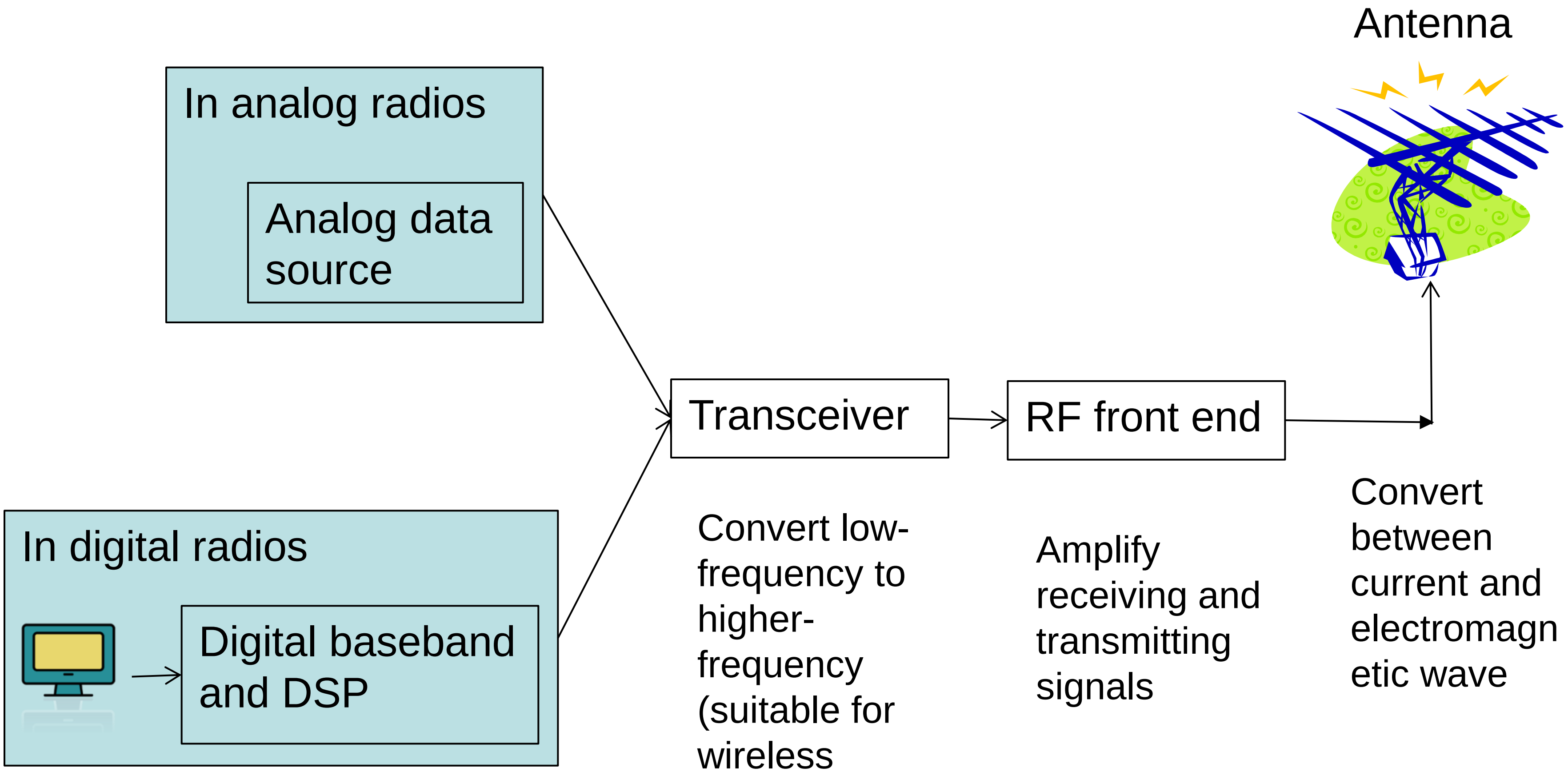
THERE IS NO LINK: electromagnetic waves

- Electromagnetic waves (radio waves) are generated by sinusoidal current running through a transmitting antenna
- Fields induce current in receiving antenna
- Frequency of radio wave: f
  - c (speed of light) = 3×10^8 m/s
  - λ : wavelength

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

- Frequency range: 3Hz ~ 300GHz
  - Microwave oven is not considered a wireless device
    - Its radio waves is not used for communication

A basic communicating system



Antenna

In analog radios

Analog data source

In digital radios

Digital baseband and DSP

Transceiver

RF front end

Data source converted into an analog baseband signal

Convert low-frequency to higher-frequency (suitable for wireless communication)

Amplify receiving and transmitting signals

Convert between current and electromagnetic wave

Wireless Link Characteristics

Differences from wired link …

- Decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- Interference from other sources: standardized wireless network frequencies (e.g., 2.4GHz) shared by other devices (e.g., phone); electromagnetic noise in the environment interfere as well
- Multipath propagation: radio signal reflects off objects ground, arriving at destination at slightly different times

… make communication across (even point to point) wireless link much more "difficult"

… error rate is higher than in wired communication

Summary so far …

- Wireless communication is achieved through electromagnetic waves => anybody with an antenna can receive the signal
- Higher error rates in wireless communication than in wired communication due to interaction with the environment

Multiple Access Techniques

Multiple access techniques: methods that determine how the medium is accessed so that the channel is shared among multiple participants

- Wireless transmission in nature is broadcast

- If everybody sends, then communication is not meaningful, just garbage

- Multiple access such that:
  - Maximize message throughput
  - Minimize mean waiting time

Main Methods

- Three domains in which users can be separated
  - Frequency, time and space
- Frequency division multiple access (FDMA)
- Time division multiple access (TDMA)
- Code division multiple access (CDMA)
- Space division multiple access (SDMA)

FDMA

Users are separated in frequency domain.

- Each station has its own frequency band, separated by guard bands to eliminate inter-channel interference
- Receivers tune to the right frequency
- *Main drawback is under-utilization of the frequency spectrum*
  - *Guard bands are just wasted*
- *Number of frequencies is limited*

TDMA

Users transmit data **on same frequency**, but **at different times**

- *Requires time synchronization*
- Users can be given different amounts of bandwidth
- Synchronization overhead
- Problems with multipath interference on wireless links
  - A signal might have bounced off several times before arriving

CDMA

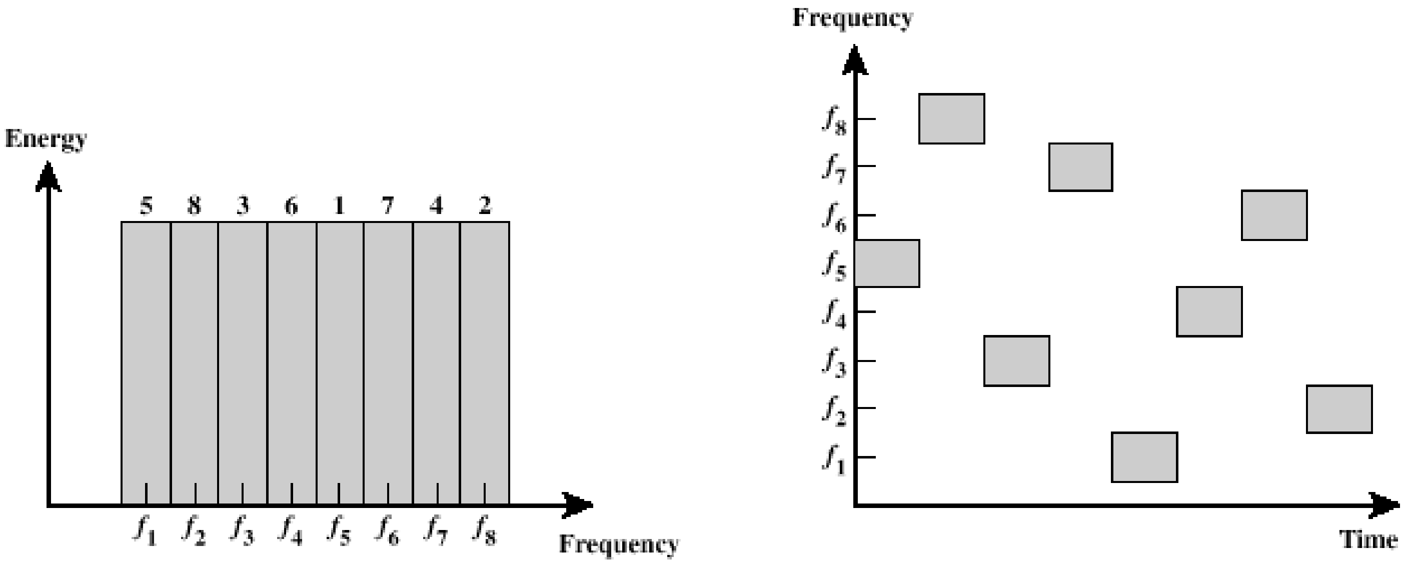
Users separated both by time and frequency

- Send at a different frequency at each time slot (***frequency hopping***)
- Or, convert a single bit to a code (***direct sequence***), receiver can decipher bit by inverse process
- Difficult to spy
- All cells can use all frequencies
- *Increased complexity*

Frequency Hoping Spread Spectrum (FHSS)

- Transmitter hops between available frequencies according to a predefined algorithm, which can be either random or preplanned
- Transmitter operates in synchronization with the receiver
- Large number of frequencies used
- Results in a system that is quite resistant to jamming

FHSS Example



(a) Channel assignment

(b) Channel use

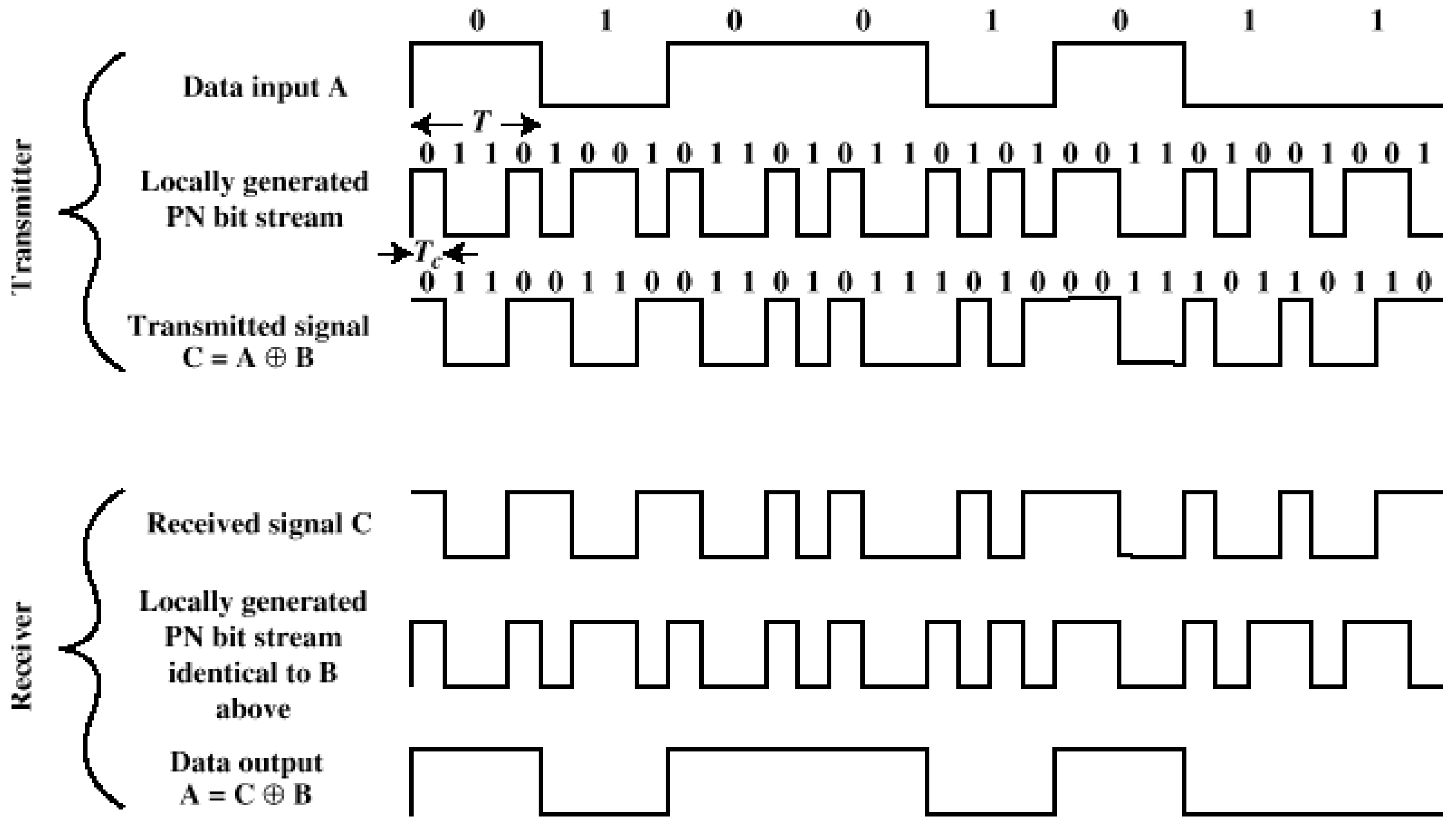
Direct Sequence Spread Spectrum (DSSS)

- Each bit in original signal is represented by multiple bits in the transmitted signal

- Data is chopped in small pieces and spread across the frequency domain

- Performance of DSSS is usually better and more reliable

DSSS Example



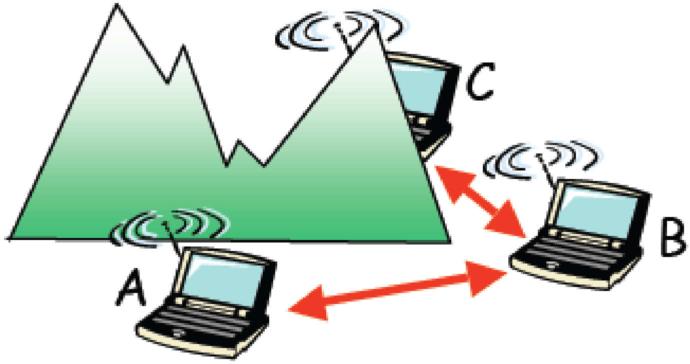
SDMA

Users are separated in space domain

- Several users in the same cell use the same frequency & time slot (in TDMA)
- Each user is separated by the smart antenna by exploiting its unique spatial location
- Different areas can be served using the same frequency
- Expect increase in co-channel interference from adjacent co-channel cells

Wireless Network Characteristics

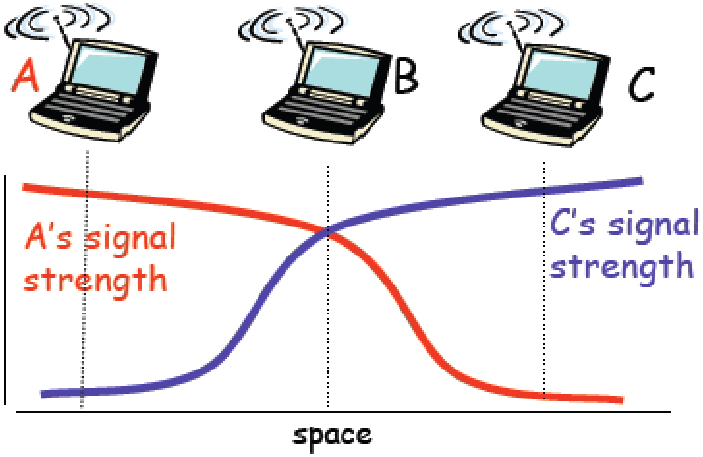
- Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C cannot hear each other

Means A, C unaware of their interference at B



Signal attenuation

- B, A hear each other
- B, C hear each other
- A, C cannot hear each other interfering at B

FDD and TDD for Duplex Channel

- Two ways of converting a wireless medium to a duplex channel

- Frequency Division Duplex (FDD): uplink and downlink use different frequencies
- Time Division Duplex (TDD): uplink and downlink use different time slots

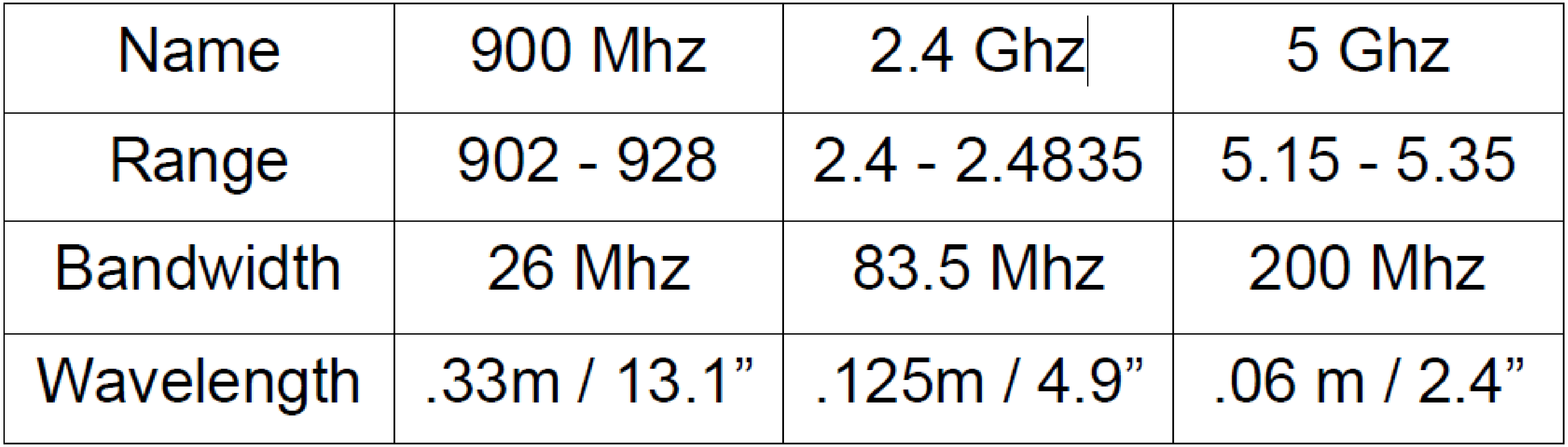
- Can combine with FDMA/TDMA
- Examples
  - TDD/FDMA in second-generation cordless phones
  - FDD/TDMA/FDMA in digital cellular phones

Spectrum Allocation

- Currently done by auctioning to the highest bidder

- Some frequencies are not allocated at all, for example ISM (industrial, scientific and medical) radio bands

Public Use Bands



Name	900 Mhz	2.4 Ghz	5 Ghz
Range	902 - 928	2.4 - 2.4835	5.15 - 5.35
Bandwidth	26 Mhz	83.5 Mhz	200 Mhz
Wavelength	.33m / 13.1”	.125m / 4.9”	.06 m / 2.4”

Summary

- Wireless communication is achieved through electromagnetic waves => anybody with an antenna can receive the signal
- Higher error rates than in wired communication due to interaction with the environment
- Channel is shared, different methods to access the channel, separation in time, frequency and space

Lecture outline

1 Characteristics of Wireless Communication

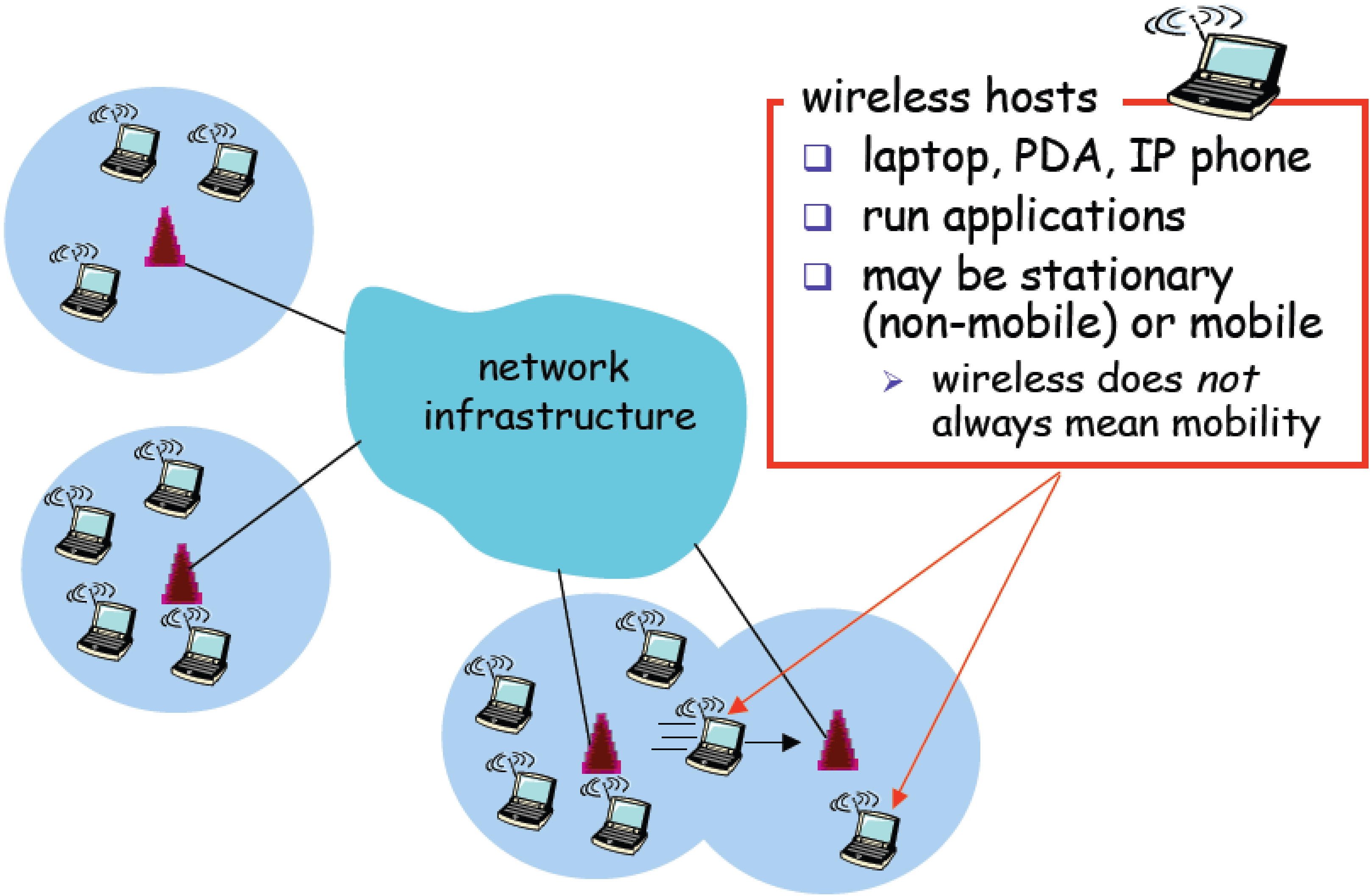
2 Existing and Emerging Wireless Networks

3 Wireless Network Security Concerns and Requirements

Existing and Emerging Wireless Networks

- Existing wireless networks:
  - Cellular networks
  - Wireless LANs (Wi-Fi 802.11)
  - Bluetooth (802.15)
- Upcoming wireless networks:
  - Personal communications:
    - Wireless mesh networks
    - Hybrid ad hoc networks
    - Mobile ad hoc networks
  - Vehicular networks
  - Sensor networks
  - RFID (IoT)
  - ...

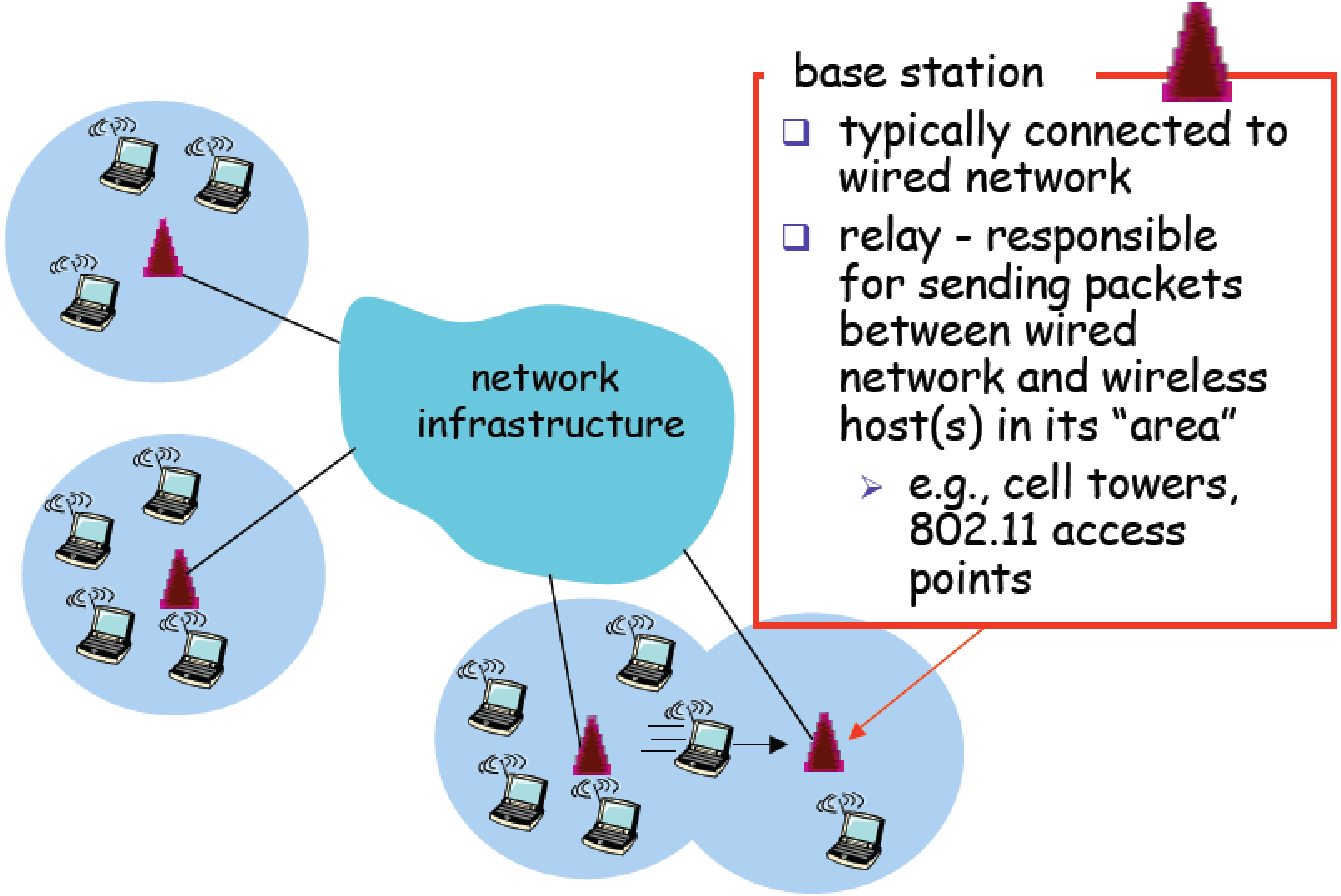
Elements of a wireless network



wireless hosts

- ❑ laptop, PDA, IP phone
- ❑ run applications
- ❑ may be stationary (non-mobile) or mobile
  - ➢ wireless does *not* always mean mobility

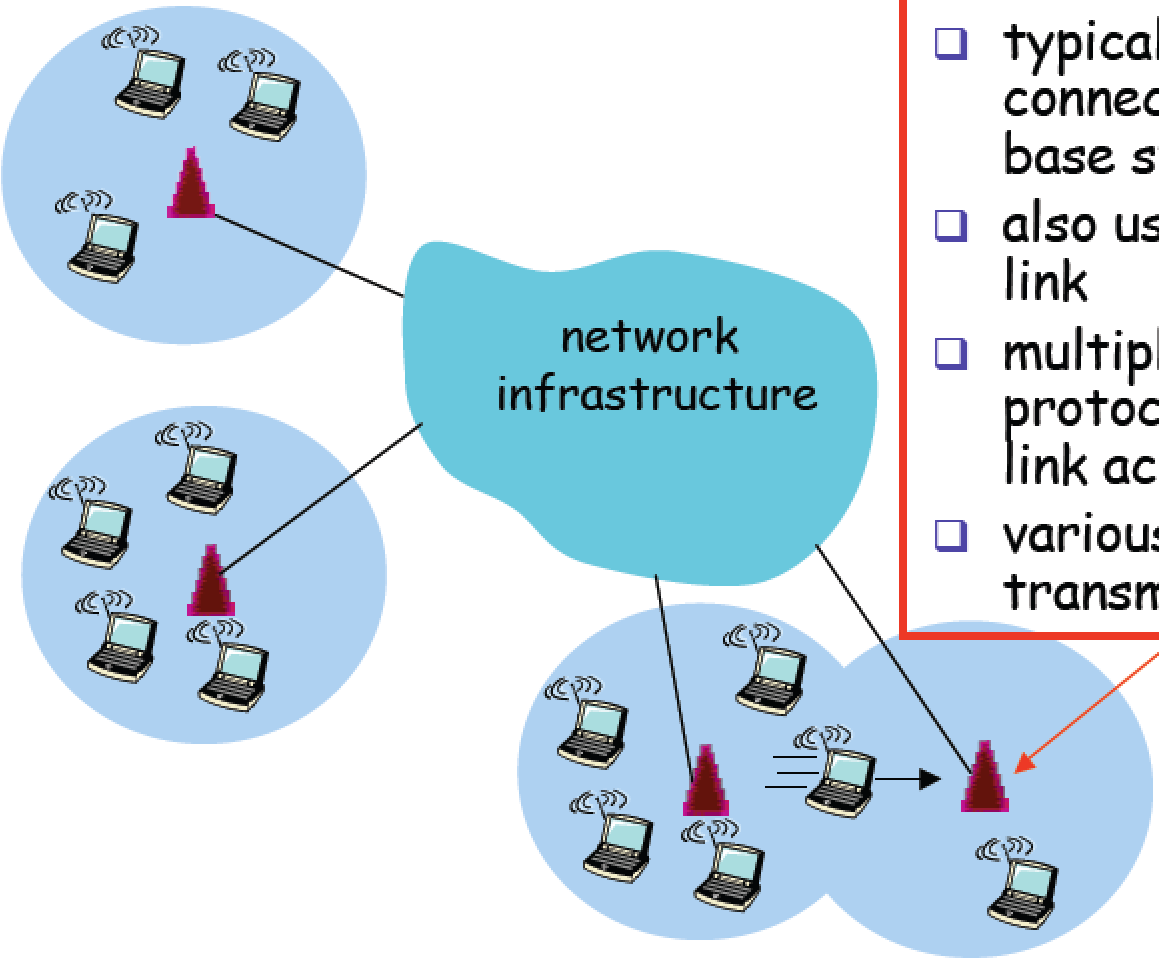
Elements of a wireless network



base station

- ❑ typically connected to wired network
- ❑ relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - ➢ e.g., cell towers, 802.11 access points

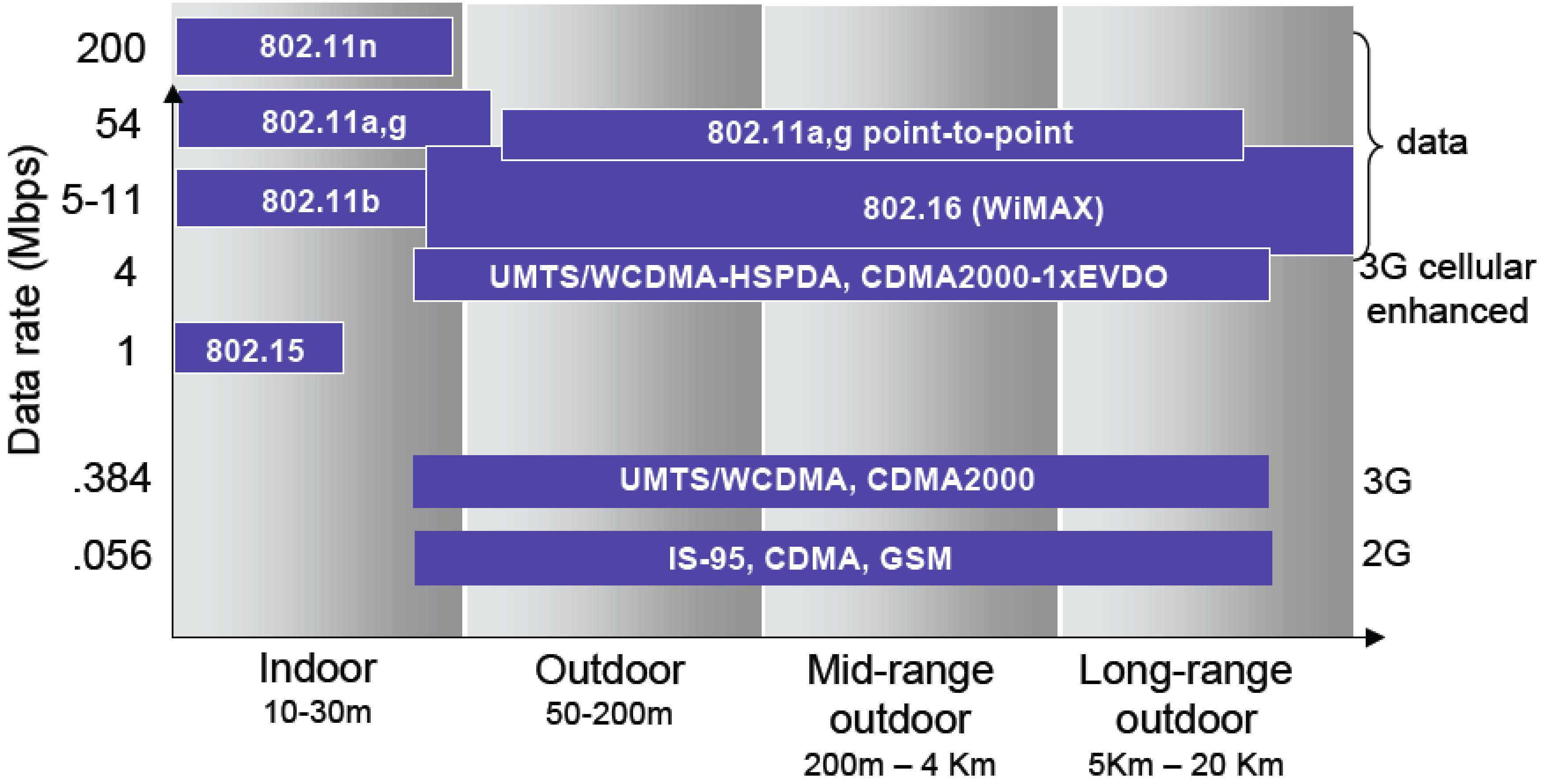
Elements of a wireless network



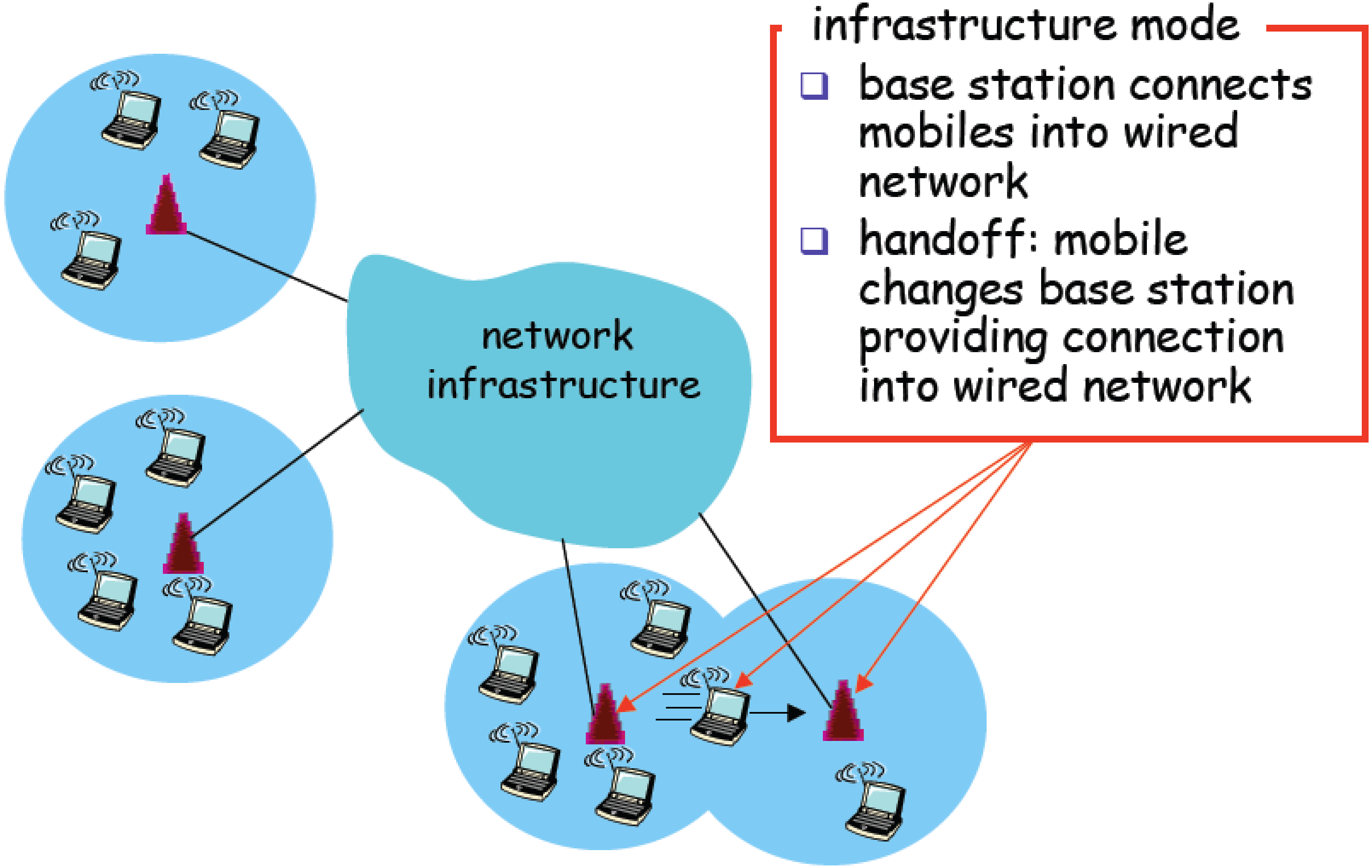
wireless link

- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

Characteristics of selected wireless link standards



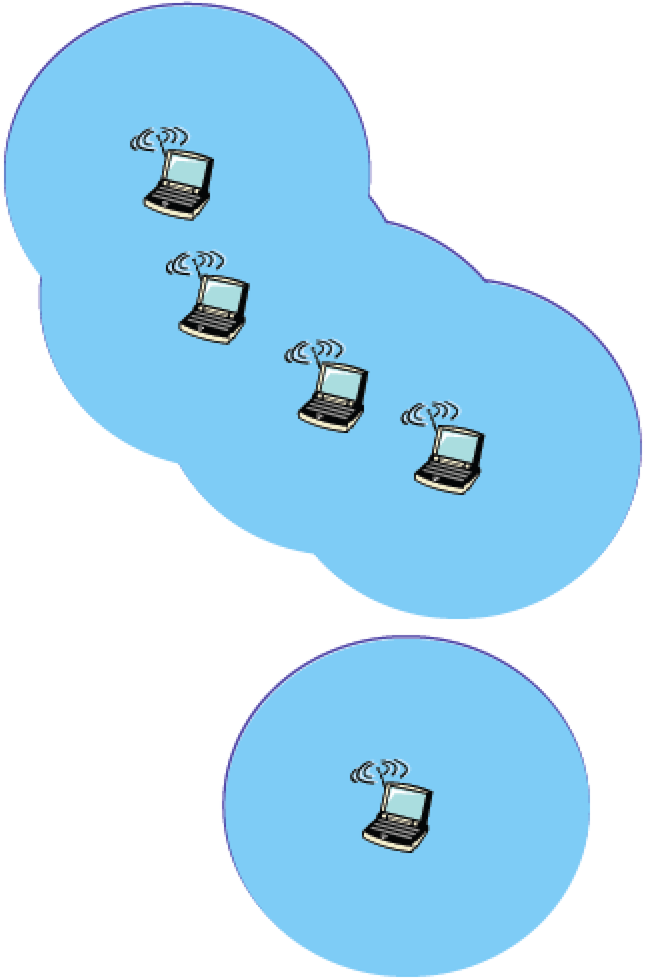
Elements of a wireless network



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

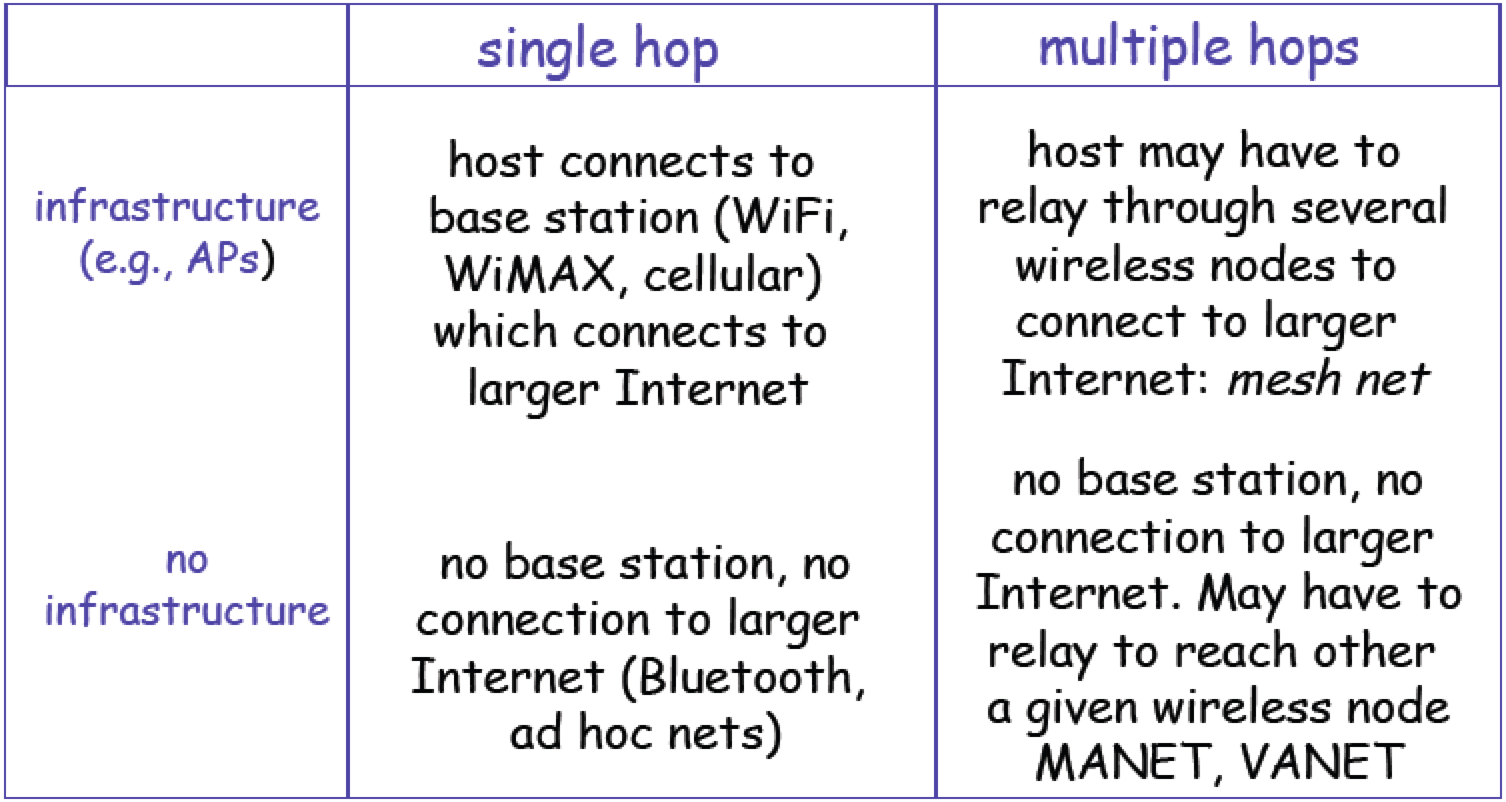
Elements of a wireless network



ad hoc mode

- ❑ no base stations
- ❑ nodes can only transmit to other nodes within link coverage
- ❑ nodes organize themselves into a network: route among themselves

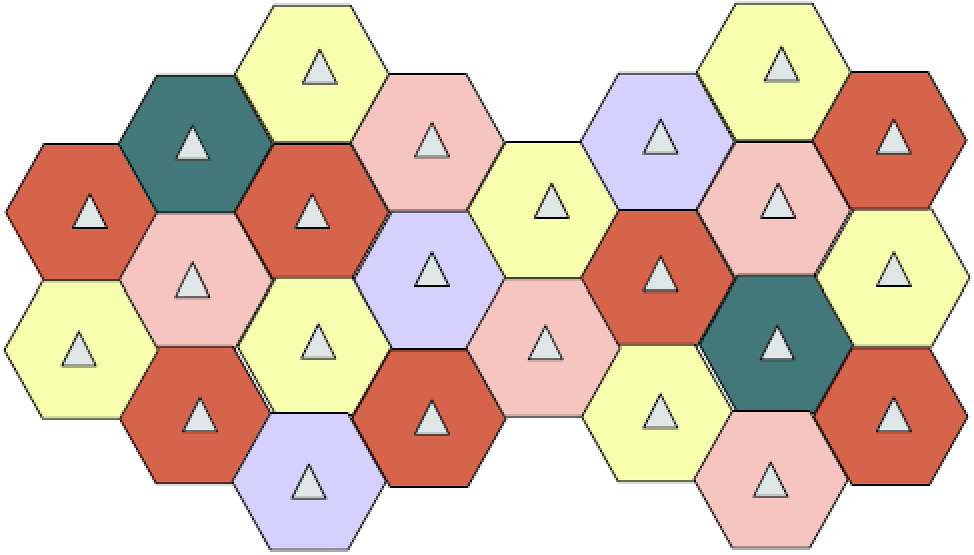
Wireless Network Taxonomy



	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Cellular Networks

Key concept: frequency reused by dividing the area covered by a cellular network in cells, avoid co-channel and adjacent interference



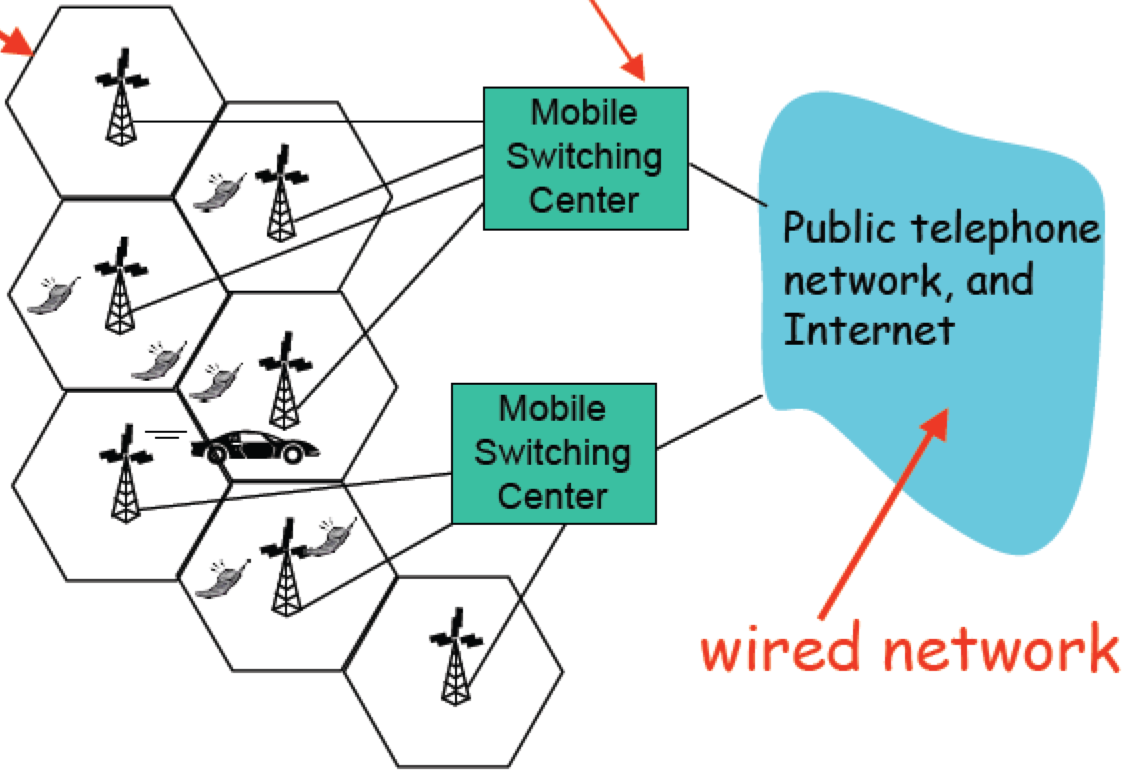
Cellular Network Architecture

cell

- ❑ covers geographical region
- ❑ *base station* (BS) analogous to 802.11 AP
- ❑ *mobile users* attach to network through BS
- ❑ *air-interface:* physical and link layer protocol between mobile and BS

MSC

- ❑ connects cells to wide area net
- ❑ manages call setup
- ❑ handles mobility



Cellular Networks: Features

- Wide coverage
- Large number of users
- Low speeds
- High deployment costs: wired communication between base stations

1G: First-Generation Analog

- **Advanced Mobile Phone Service (AMPS)**
- In North America, two 25-MHz bands allocated to AMPS
- One for transmission from base to mobile unit
- One for transmission from mobile unit to base
- Each band split in two to encourage competition (12.5MHz per operator)
- For voice-only communication
- Almost extinct now, been replaced by 2G

From 1G to 2G

- **From analog to digital:** first-generation systems are almost purely analog (use analog modulation techniques); second generation systems are digital

- **From non-encrypted to encryption** – 2G systems provide encryption to prevent eavesdropping unlike 1G

- **Improved channel access –** 2G provide support for channels to be dynamically shared by a number of users

2G Standards

- GSM in Europe
  - Most widely deployed cellular communications standard
- Digital-AMPS (DAMPS) in US
- Personal Digital Cellular (PDC) in Japan

3G

- Required to provide telephone service as well as data communications at significantly higher speeds, up to 2 Mbps
- Uses CDMA as channel access mechanism
- Major standards
  - Universal Mobile Telecommunications Service (UMTS),
    - Evolution of GSM, in Europe
    - Data service: High Speed Uplink/Downlink Packet access: 3Mbps
  - CDMA-2000: CDMA in TDMA slots
    - Data service: 1xEvlution Data Optimized (1xEVDO) up to 14 Mbps
    - In North American and parts of Asia

IEEE 802.11 Wireless LAN

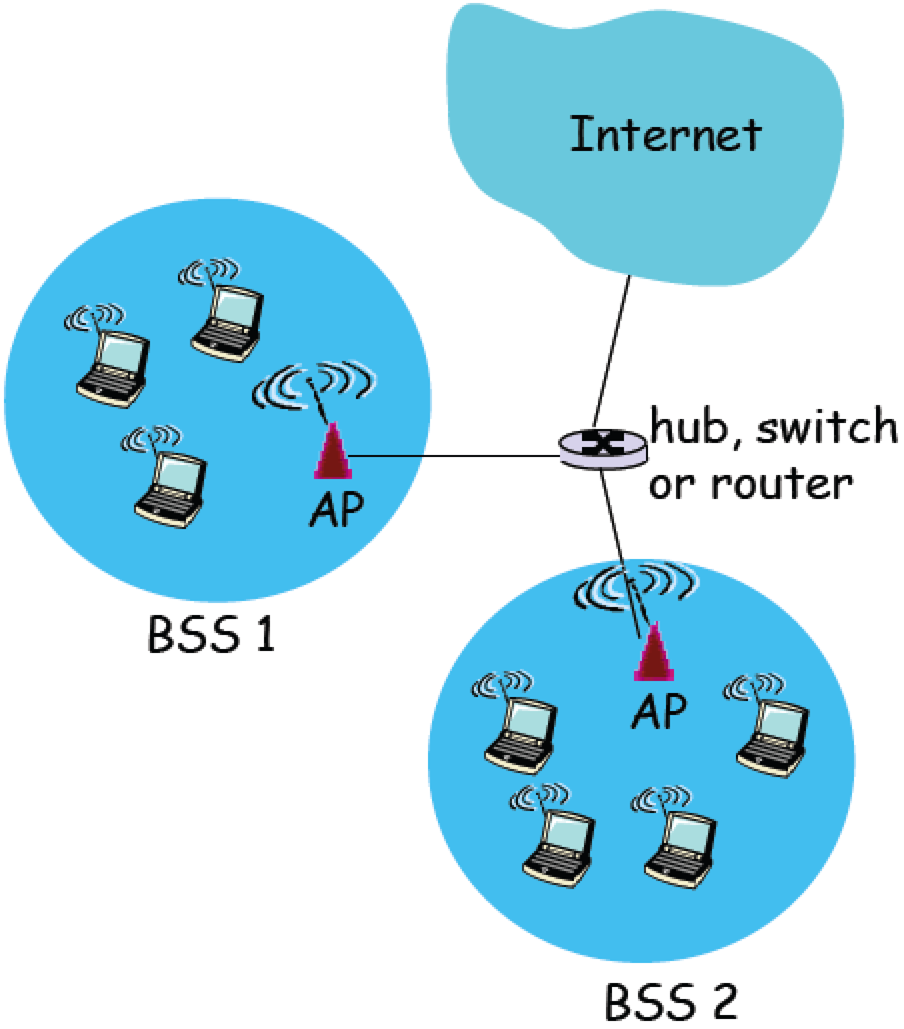
- Provides increased bandwidth (up to 11Mbps for 802.11b and up to 54Mbs for 802.11a)

- ❑ 802.11b
  - 2.4-5 GHz unlicensed spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code

- ❑ 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- ❑ 802.11g
  - 2.4-5 GHz range
  - up to 54 Mbps
- ❑ 802.11n: multiple antennae
  - 2.4-5 GHz range
  - up to 200 Mbps

- ❑ all use CSMA/CA for multiple access
- ❑ all have base-station and ad-hoc network versions

802.11 LAN architecture



- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

802.15: personal area network (Bluetooth)

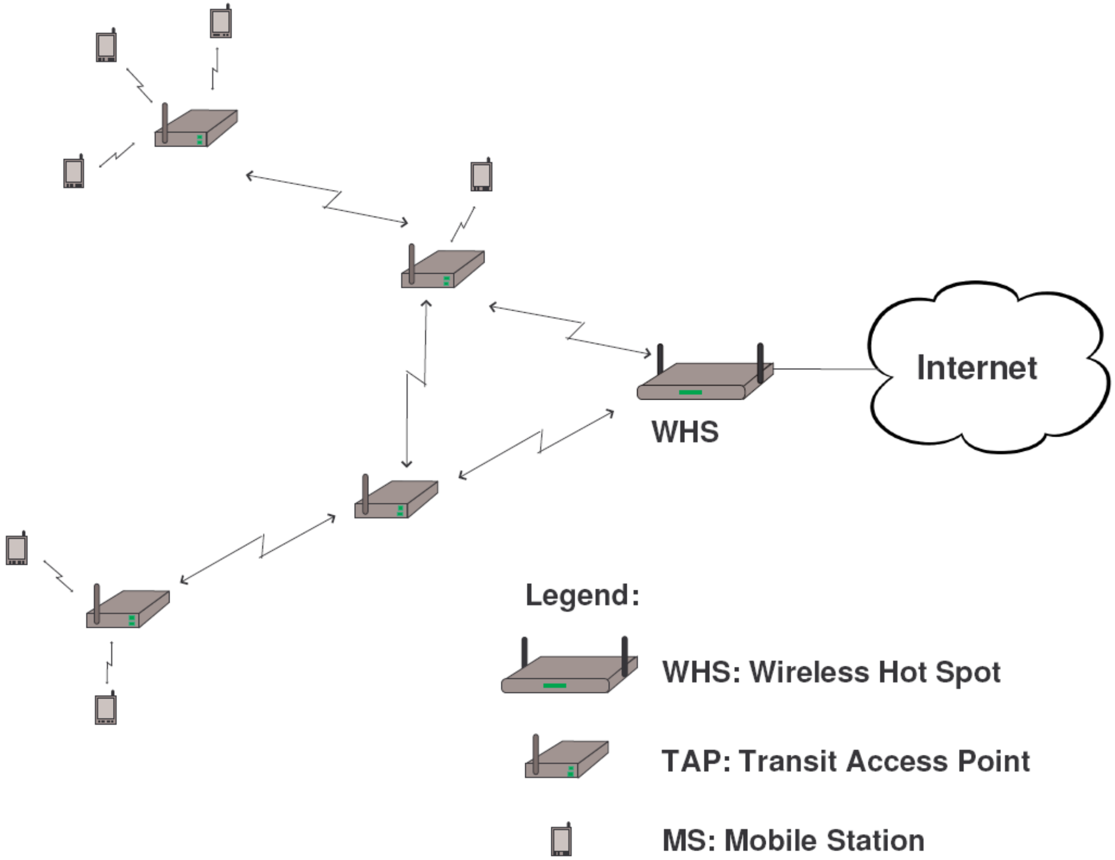
- less than 10 m diameter replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps

Existing and Emerging Wireless Networks

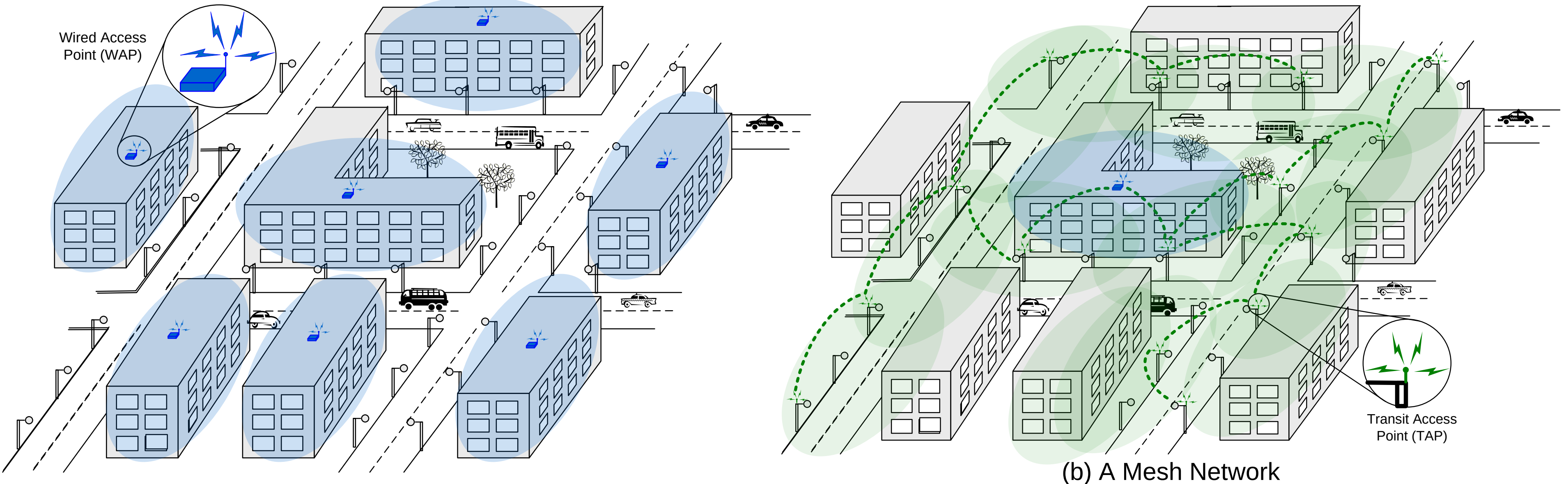
- Existing wireless networks:
  - Cellular networks
  - Wireless LANs (Wi-Fi 802.11)
  - Bluetooth (802.15)
- Upcoming wireless networks:
  - Personal communications:
    - Wireless mesh networks
    - Hybrid ad hoc networks
    - Mobile ad hoc networks
  - Vehicular networks
  - Sensor networks
  - RFID
  - ...

Wireless mesh networks

- Mesh network:
  - One Wireless Hot Spot (WHS)
  - Several Transit Access Points (TAPs)
  - Mobile Stations



Wireless Mesh Networks



(a) A WiFi Network

(b) A Mesh Network

- Wireless Mesh Network (WMN): Same coverage as with WiFi networks but with only one WAP (and several TAPs).
- WMNs allow a fast, easy and inexpensive network deployment.
- However, the lack of security guarantees slows down the deployment of WMNs

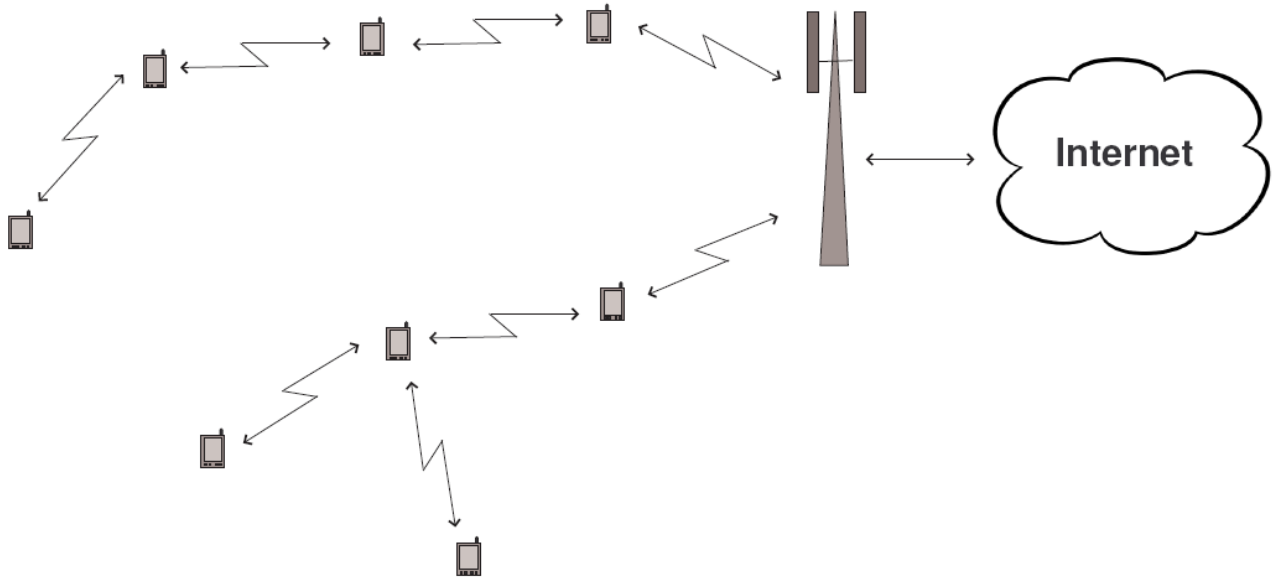
Wireless mesh networks

- Easy to deploy:
  - Single connection point to the Internet
- Providing Internet connectivity in a sizable geographic area:
  - Much lower cost than classic WiFi networks
- Fairness and security are closely related
- Not yet ready for wide-scale deployment:
  - Severe capacity and delay constraints
  - Lack of security guarantees

Hybrid ad hoc networks

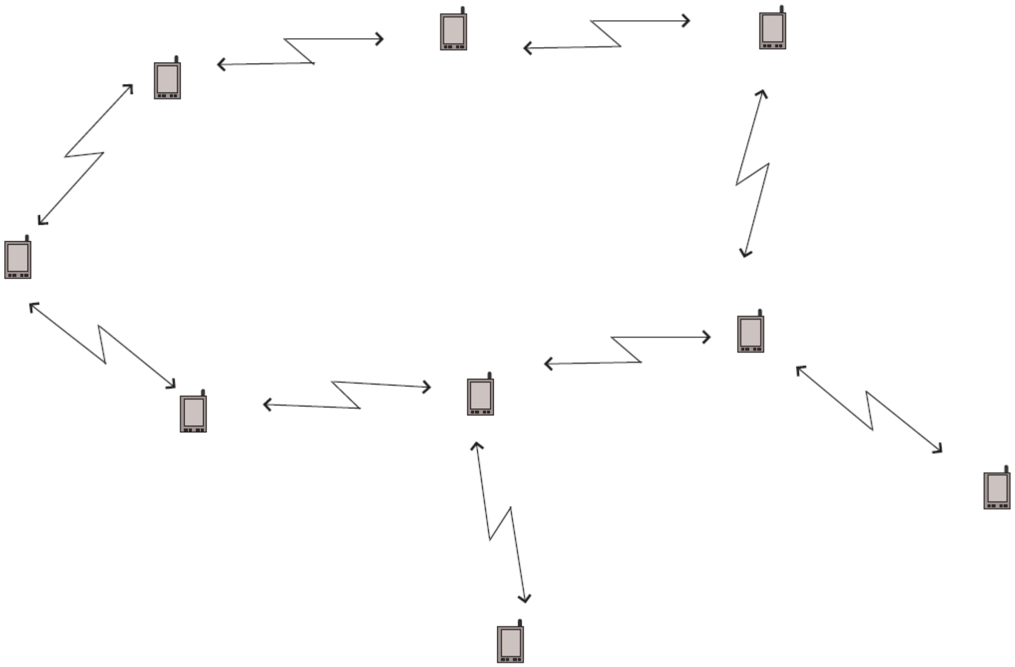
- Hybrid ad hoc networks or multi-hop cellular networks:
  - No relay stations
  - Other mobile stations relay the traffic

- Problem of power management



Mobile ad hoc networks (MANETs)

- Mobile ad hoc networks:
  - Mobile ad hoc networks in hostile environments
  - In self-organized mobile ad hoc networks



Mobile ad hoc networks

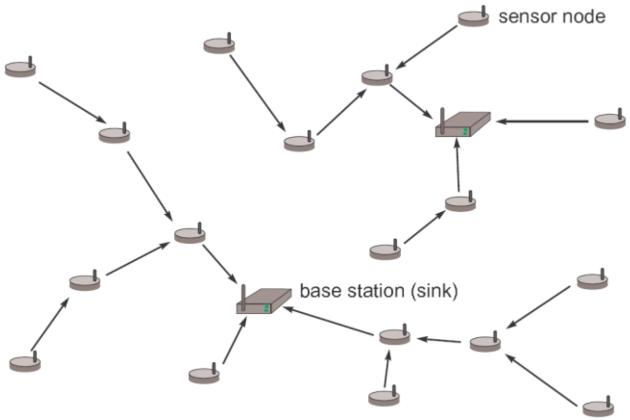
- Mobile ad hoc networks in hostile environments:
  - Presence of a strong attacker: military networks
  - Authority can preload key materials for nodes to secure the communications

- In self-organized mobile ad hoc networks:
  - No authority in the initialization phase
  - Nodes have to figure out how to secure the communications

Wireless Sensor networks

- Large number of sensor nodes, a few base stations
- Sensors are usually battery powered:
  - Main design criteria: reduce the energy consumption

- Multi-hop communication reduces energy consumption:
  - Overall energy consumption can be reduced, if packets are sent in several smaller hops instead of one long hop
  - Fewer re-transmissions are needed due to collisions



Wireless Sensor networks

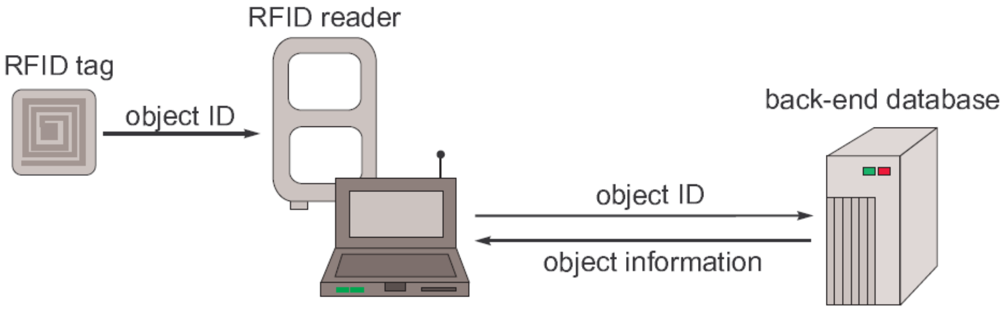
- Security requirements:
  - Integrity
  - Confidentiality
  - Availability

- Special conditions:
  - Energy consumption
  - Computing and storage capacity of sensors is limited
  - Access to the sensors cannot be monitored

RFID

- RFID systems:
  - RFID tags
  - RFID readers
  - Back-end databases

- RFID tag: microchip and antenna
  - Active: have battery
  - Passive: harvest energy from the reader's signal



Wireless Networks: summary

- Architectures:
  - Centralized
  - Peer to peer
  - Hybrid
- Communication:
  - One-hop
  - Multi-hop
- Devices: different computational power and physical Accessibility
- Mobility:
  - Fixed node
  - Mobile nodes

Lecture outline

1 Characteristics of Wireless Communication

2 Existing and Emerging Wireless Networks

3 Wireless Network Security Concerns and Requirements

Why is security more of a concern in wireless?

- no inherent physical protection
  - physical connections between devices are replaced by logical associations
  - sending and receiving messages do not need physical access to the network infrastructure (cables, hubs, routers, etc.)

- broadcast communications
  - wireless usually means radio, which has a broadcast nature
  - transmissions can be overheard by anyone in range
  - anyone can generate transmissions,
    - which will be received by other devices in range
    - which will interfere with other nearby transmissions and may prevent their correct reception (jamming)

That implies …

- eavesdropping is easy
- injecting bogus messages into the network is easy
- replaying previously recorded messages is easy
- illegitimate access to the network and its services is easy
- denial of service is easily achieved by jamming

Also, more security concerns …

- Due to mobility
  - Allows tracing
  - Roaming
    - Agreement between network operators to make transition secure and smooth

- Due to resource constraints
  - Limited storage, computing power and energy
  - Security solutions must be efficient

- Physical security is an issue for small devices , many times we will look at inside attacks (assume the device is controlled by the attacker)

Wireless communication security requirements

- authenticity
  - origin of messages received over wireless links must be verified
- access control
  - access to the network services should be provided only to legitimate entities
  - access control should be permanent
    - it is not enough to check the legitimacy of an entity only when it joins the network and its logical associations are established, because logical associations can be hijacked
- confidentiality
  - messages sent over wireless links must be encrypted

Wireless communication security requirements

- integrity
  - modifying messages on-the-fly (during radio transmission) is not so easy, but possible …
  - integrity of messages received over wireless links must be verified
- privacy
  - User location should never be released
- protection against jamming
  - Availability of network service

Summary

- Wireless channels are vulnerable
- Wireless devices are vulnerable
- Mobility further complicates security issues