

# Wireless Networks

- P2P (continued)
- wireless ad-hoc networks

# Peer-to-peer vs. Client-Server

- a server is a program that provides a service
- typically, a server is found at a given address and port number, and is maintained by an individual or an organization
- clients may be anonymous or unidentified
- peer-to-peer (P2P) often brings to the infrastructure the anonymity of clients
- could imagine authenticated P2P networks, set up for reliability rather than anonymity

# Peer-to-peer vs. Client-Server II

- for a very different example, routing is a peer-to-peer process
  - routers identified by IP address or ID
- the ultimate appeal of peer-to-peer for some networking people is a self-organizing, self-managing scalable network
- peer-to-peer networks seem to be widely used

# wireless ad-hoc networks

- using the ad-hoc mode of 802.11, any device ("node") may directly talk to any other device
  - could also use Zigbee (802.15.4), Bluetooth
- if nodes agree to forward data for each other, they can form a wireless ad-hoc network
- machines may move or go to sleep, so routing can be challenging
- also, the notion of a "link" is different for wired and wireless networks
  - some successful wireless protocols benefit from broadcasting
- generally machines should discover each other and automatically send data to the destination

# interference in wireless networks

- devices  $D_1, D_2, D_3, \dots D_n$
- each in range of the next, but not the one after
  - $D_1$  can reach  $D_2$ , but not  $D_3$
  - $D_3$ 's transmissions interfere with  $D_2$ 's receiving
- if all traffic goes left-to-right,
  - how many nodes can be transmitting at once?
  - if traffic goes in both directions?

# routing in ad-hoc networks

- simplest method: broadcast everything
  - everyone retransmits each message at most once
  - retransmissions must be delayed by random amounts to avoid excess collisions
- initial broadcast, then source route (DSR)
  - each device adds its ID, then rebroadcasts packet
  - the intended destination gets a route
  - broadcast is repeated when route fails
- also more conventional routing: AODV, OLSR

# energy conservation in wireless ad-hoc networks

- transmission requires energy
- receiving also requires energy, sometimes as much as transmitting
  - radio on and receiving a packet requires the most
  - but even leaving on the radio still uses energy
- keep the radio off as much as possible, limit the number of packets sent
  - hard to know when to turn on the radio to receive

# security in wireless ad-hoc networks

- devices may be compromised in deployed networks
- attackers may deploy additional devices
- if really ad-hoc, other devices belong to others
- devices we don't control should not be trusted
  - majority rule (byzantine consensus), or
  - wait to sound the alarm until multiple sensors report a problem
  - encrypt and authenticate traffic
    - but remember device may be compromised!
  - monitor other nodes, see if they are behaving

# energy conservation in wireless networks

- transmission requires energy
- receiving also requires energy, sometimes just as much as transmitting
  - radio on and receiving a packet requires the most
  - just leaving on the radio still uses energy
  - put the processor into low-power mode when possible
    - can wake up after a certain time, or a measurable event
    - the opposite of overclocking
- keep the radio off as much as possible, limit the number of packets sent
  - hard to know when to turn on the radio to receive

# types of wireless ad-hoc networks

- MANET, Mobile Ad-hoc Network
- VANET, Vehicular Ad-hoc Network
  - includes vehicle-to-roadside and vehicle-to-vehicle communication
- underwater networks
  - using sound instead of radio waves
- Wireless Sensor Networks
  - the Internet of Things, IoT