

ICS 351: Today's plan

- Peer-to-Peer Networking
- Wireless ad-hoc Networks
- Wireless Sensor 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 are often anonymous or at least unidentified
- peer-to-peer often brings to the infrastructure the same anonymity of a web client

Different uses of Peer-to-Peer

- routing is a peer-to-peer process, but the routers are identified by IP address if nothing else
- there could be authenticated peer-to-peer networks, set up for the reliability rather than the anonymity aspect
- 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 accepted

Peer-to-Peer Examples

- Bittorrent, eDonkey – 50% of Internet traffic worldwide in 2008/09
(<http://www.ipoque.com/sites/default/files/mediafiles/documents/internet-study-2008-2009.pdf>)
 - share content
 - unregulated
- FreeNet
 - share content
 - some cryptographic protection

Wireless Ad-hoc Networks

- Mobile computers: laptops (and everything else), vehicle-mounted computers, etc.
- Fields of sensors, including building monitoring, bridge monitoring, environmental monitoring
- Radios with low power and short range: 802.11/Wifi (< 150m), 802.15.4/Zigbee (< 50m), Bluetooth (< 10m)
- Ad-hoc networking: every computer can relay data for others

Some Applications of Wireless Ad-Hoc Networks

- Sensor Networks:
 - agriculture
 - science and ecology
- Emergency Communications (P2P)
- Vehicle Ad-hoc Networks (VANETs):
 - Vehicle-to-vehicle
 - Vehicle-to-infrastructure
 - Infra-Vehicle

Wireless Ad-hoc Networks: More Applications

- Monitoring of wide areas, buildings, dangerous locations, long-term unintrusive monitoring, etc
- Robots for rescuing people in damaged buildings
- Communication among individuals at a conference, classroom etc.
- Environmental controls for buildings

Ad-hoc Network Research Issues

- Routing: minimal overhead, any-to-any or any-to-sink routing
- Broadcasting/Flooding
- Security
- Initialization and Configuration
- Reliable transmission

Wireless Ad-hoc Networks: Routing and Broadcasting

- The sink collects data from other nodes
- The sink can broadcast an initial message
- Everyone in range of the sink retransmits it, increasing the *distance* field in the header
- Everyone at distance 2 retransmits the packet
- At the end, everyone knows:
 - ○ Their distance to the sink
 - ○ The next hop node to use to reach the sink
 - But flooding can lead to mutual interference

Wireless Ad-hoc Networks: Security

- Monitoring networks can be used to detect forest fires or enemy attack
- An adversary (or a prankster) might wish to send a *false positive* signal
- Or a false negative, suppressing a real alarm
- It is likely that the adversary will obtain access to one or more nodes
- What should be protected?
- Which node(s) should be trusted?

Wireless Ad-hoc Networks: Reliable Transmission

- Assume a number of nodes in a straight line
- Each node is only in range of two other nodes
- When the second node receives a packet, it must retransmit it, but this may interfere with the second packet transmitted by the first node
- So, transmit in blocks, use acks to confirm
- Hardware acks acknowledge reception by the hardware, but packet may still be discarded due to lack of buffer space