Wireless Networks

- wireless ad-hoc networks (continued)

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

wireless mesh networks

- a wireless mesh network consists of static wireless nodes
- possibly with some wired nodes coordinating to provide Internet access
  - e.g. a mesh of wireless access points
  - only some of them are connected to the Internet
- mobile nodes may obtain Internet access from nodes in a mesh network
- mesh networks tend to be static, routes are more stable, and energy is not as much of an issue as in ad-hoc networks