Wireless LANs: outline

- wireless 802.11 and WiFi.
- 802.11 security: WEP, 802.11i, WPA, WPA2.
- networking security
- wireless ad-hoc and mesh networks
ISM bands

- To operate most radios, a license is needed from a government body (in the U.S., the FCC).
- To operate a microwave oven, no license is needed.
- Microwave ovens work on a resonant frequency of water, 2.4GHz.
- The 2.4GHz-2.5GHz band has been designated an **Industrial, Scientific, and Medical** (ISM) band, free to use worldwide without a license.
  - As long as transmission power is limited.
  - And some countries restrict part of this band.
Using ISM bands

- ISM equipment needs to tolerate interference (e.g., from microwave ovens!)
- there are many ISM bands, but most are limited to only some countries
  - e.g. 900MHz band only available in the Americas
- due to the unprecedented availability of the 2.4GHz ISM band, many applications have been developed for it
Wireless 802.11/WiFi

- an early marketing term for 802.11 was WiFi
  - a pun on HiFi, High Fidelity audio equipment
- 802.11 works mostly in the 2.4GHz ISM band, though 802.11a works in the 5GHz band
- many successive standards:
  - 802.11 (1-2Mb/s)
  - 802.11a (54Mb/s)
  - 802.11b (11Mb/s)
  - 802.11g (54Mb/s)
- foreseeably, future versions
802.11/WiFi Operation

- 802.11 has two modes: ad-hoc (point-to-point) and managed
- In managed mode, all communication is to or from a central access point
- End-nodes contend for the medium: this contention may result in collisions that require retransmissions
tapping a wired network requires physical access to the wires

tapping a wireless network requires being in range of the signal

originally, cryptographic Wired Equivalent Privacy (WEP) was introduced to hide the contents of the messages

the original design for WEP was not widely published – unfortunately, this resulted in a lack of serious examination of the protocol:

security by obscurity often does not work
802.11 Security: WPA and WPA2

- unfortunately, WEP is sufficiently weak that it can be cracked by listening to a few minutes of busy traffic

802.11i introduced:
- WiFi Protected Access (WPA), a simple but much stronger encryption protocol, and
- WPA2, stronger than WPA and requiring more resources for implementation (including, in some cases, newer equipment)
networking security

- "in the clear" protocol can be easily broken when information is snooped: telnet, ftp, http, many email protocols
- encrypted protocols are secure against many attacks, including someone examining the data: ssh/scp, https, secure POP/IMAP, PGP
  - most protocols are not secure against traffic analysis
- *host security* is more concerned with installing applications, running foreign code, firewalls/NATs, etc
security principles

- it is usually better to have more security than less security
- security that inconveniences users is more likely to be resisted or circumvented
- security can lock out people who should have access
- data requiring security should not be sent unencrypted over the Internet
  - because some of the links may be accessible to adversaries
- data requiring security is still often sent unencrypted over the Internet
  - though data with monetary value is usually protected these days
wireless ad-hoc networks

- using the ad-hoc mode of 802.11, any machine ("node") may directly talk to any other node
- 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: successful wireless protocols take advantage of broadcasting
- generally machines should discover each other and automatically send data to the destination
wireless mesh networks

- a wireless mesh network consists of static wireless nodes
- possibly with some wired nodes coordinating to provide Internet access
- mobile nodes may obtain Internet access from nodes in a mesh network