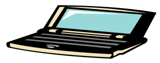


Wireless Networks

COS 461: Computer Networks
Spring 2013

Mike Freedman

http://www.cs.princeton.edu/courses/archive/spring13/cos461/

Widespread Deployment

- Worldwide cellular subscribers
  - 1993: 34 million
  - 2005: more than 2 billion
  - 2011: close to 6 billion

    (1.2B with mobile broadband)

    >> 1.2B landline subscribers

- Wireless local area networks
  - Wireless adapters built into laptops, tablets, & phones
  - As ubiquitous as broadband subscribers? 600M in 2011

http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers

Wireless Links

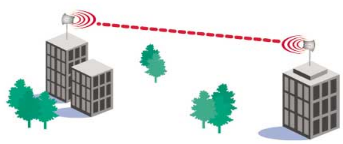
Wireless Properties

- Interference / bit errors
  - More sources of corruption compared to wired
- Multipath propagation
  - Signal does not travel in a straight line
- Broadcast medium
  - All traffic to everyone
- Power trade-offs
  - Important for power constrained devices

5

Wireless Links: High Bit Error Rate

- Decreasing signal strength
  - Disperses as it travels greater distance
  - Attenuates as it passes through matter



6

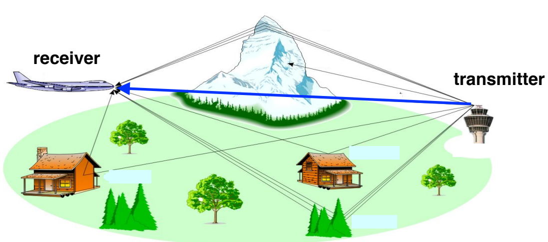
Wireless Links: High Bit Error Rate

- Interference from other sources
  - Radio sources in same frequency band
  - E.g., 2.4 GHz wireless phone interferes with 802.11b wireless LAN
  - Electromagnetic noise (e.g., microwave oven)

7

Wireless Links: High Bit Error Rate

- Multi-path propagation
  - Electromagnetic waves reflect off objects
  - Taking many paths of different lengths
  - Causing blurring of signal at the receiver



8

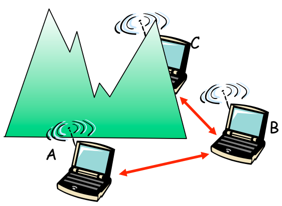
Dealing With Bit Errors

- Wireless vs. wired links
  - Wired: most loss is due to congestion
  - Wireless: higher, time-varying bit-error rate
- Dealing with high bit-error rates
  - Sender could increase transmission power
    - Requires more energy (bad for battery-powered hosts)
    - Creates more interference with other senders
  - Stronger error detection and recovery
    - More powerful error detection/correction codes
    - Link-layer retransmission of corrupted frames

9

Wireless Links: Broadcast Limitations

- Wired broadcast links
  - E.g., Ethernet bridging, in wired LANs
  - All nodes receive transmissions from all other nodes
- Wireless broadcast: hidden terminal problem



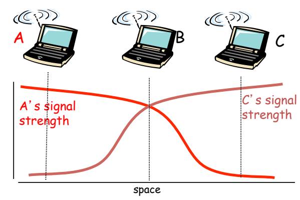
- **A and B hear each other**
- **B and C hear each other**
- **But, A and C do not**

So, A and C are unaware of their interference at B

10

Wireless Links: Broadcast Limitations

- Wired broadcast links
  - E.g., Ethernet bridging, in wired LANs
  - All nodes receive transmissions from all other nodes
- Wireless broadcast: fading over distance



- **A and B hear each other**
- **B and C hear each other**
- **But, A and C do not**

So, A and C are unaware of their interference at B

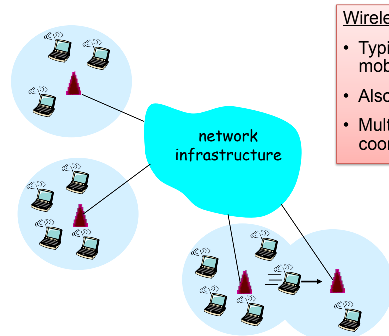
11

Example Wireless Link Technologies

- Data networks
  - 802.15.1 (Bluetooth): 2.1 Mbps – 10 m
  - 802.11b (WiFi): 5-11 Mbps – 100 m
  - 802.11a and g (WiFi): 54 Mbps – 100 m
  - 802.11n (WiFi): 200 Mbps – 100 m
  - 802.16 (WiMax): 70 Mbps – 10 km
- Cellular networks, outdoors
  - 2G: 56 Kbps
  - 3G: 384 Kbps
  - 3G enhanced ("4G"): 4 Mbps
  - LTE

12

Wireless Network: Wireless Link

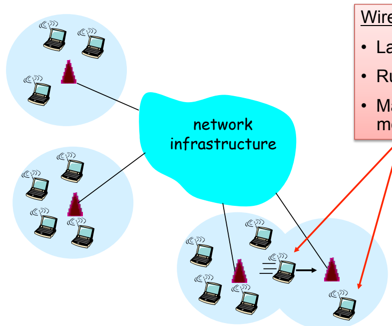


Wireless link

- Typically used to connect mobile(s) to base station
- Also used as backbone link
- Multiple access protocol coordinates link access

Wireless Network: Wireless Hosts

13

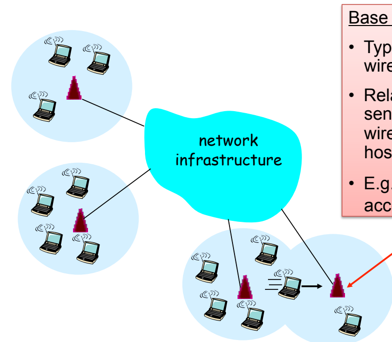


Wireless host

- Laptop, smartphone
- Run applications
- May be stationary (non-mobile) or mobile

Wireless Network: Base Station

14

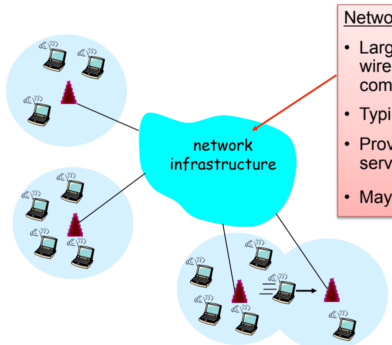


Base station

- 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

Wireless Network: Infrastructure

15

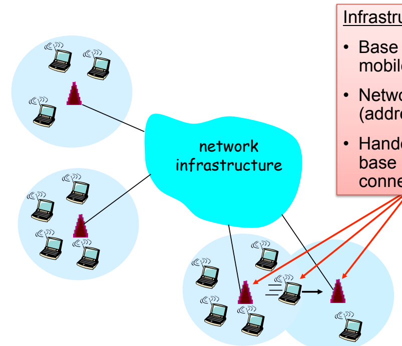


Network infrastructure

- Larger network with which a wireless host wants to communicate
- Typically a wired network
- Provides traditional network services
- May not always exist

Infrastructure Mode (APs)

16



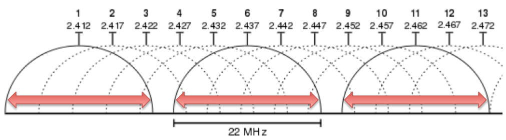
Infrastructure mode

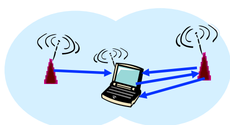
- Base station connects mobiles into wired network
- Network provides services (addressing, routing, DNS)
- Handoff: mobile changes base station providing connection to wired network

17

Channels and Association

- Multiple channels at different frequencies
  - Network administrator chooses frequency for AP
  - Interference if channel is same as neighboring AP

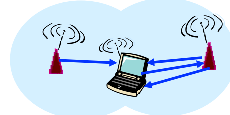




18

Channels and Association

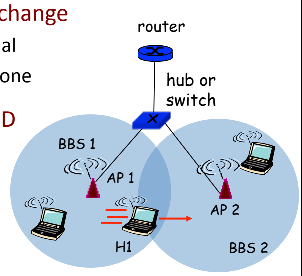
- Multiple channels at different frequencies
  - Network administrator chooses frequency for AP
  - Interference if channel is same as neighboring AP
- Access points send periodic beacon frames
  - Containing AP's name (SSID) and MAC address
  - Host scans channels, listening for beacon frames
  - Host selects an access point: association request/response protocol between host and AP



19

Mobility Within the Same Subnet

- H1 remains in same IP subnet
  - IP address of the host can remain same
  - Ongoing data transfers can continue uninterrupted
- H1 recognizes the need to change
  - H1 detects a weakening signal
  - Starts scanning for stronger one
- Changes APs with same SSID
  - H1 disassociates from one
  - And associates with other
- Switch learns new location
  - Self-learning mechanism



20

Questions

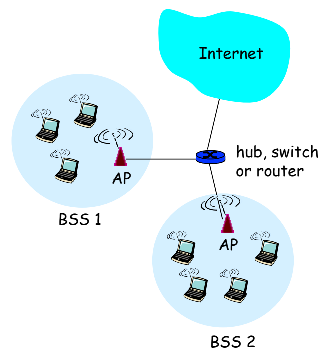
- Loss is primary caused by bit errors
  - (A) Ethernet (Wired)
  - (B) 802.11 (Wireless)
  - (C) Both
  - (D) Neither
- All hosts on subnet see all communication
  - (A) Ethernet (Wired)
  - (B) 802.11 (Wireless)
  - (C) Both
  - (D) Neither

21

WiFi: 802.11 Wireless LANs

22

802.11 LAN Architecture



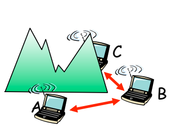
- Access Point (AP)
  - Base station that communicates with the wireless hosts
- Basic Service Set (BSS)
  - Coverage of one AP
  - AP acts as the master
  - Identified by an "network name" known as an SSID

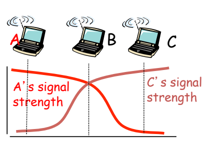
SSID: Service Set Identifier

23

CSMA: Carrier Sense, Multiple Access

- Multiple access: channel is shared medium
  - Station: wireless host or access point
  - Multiple stations may want to transmit at same time
- Carrier sense: sense channel before sending
  - Station doesn't send when channel is busy
  - To prevent collisions with ongoing transfers
  - But, detecting ongoing transfers isn't always possible





24

CA: Collision Avoidance, Not Detection

- Collision detection in wired Ethernet
  - Station listens while transmitting
  - Detects collision with other transmission
  - Aborts transmission and tries sending again
- Problem #1: cannot detect all collisions
  - Hidden terminal problem
  - Fading

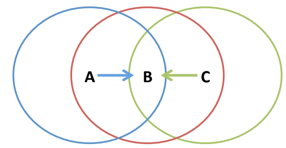
CA: Collision Avoidance, Not Detection

25

- Collision detection in wired Ethernet
  - Station listens while transmitting
  - Detects collision with other transmission
  - Aborts transmission and tries sending again
- Problem #1: cannot detect all collisions
  - Hidden terminal problem
  - Fading
- Problem #2: listening while sending
  - Strength of received signal is much smaller
  - Expensive to build hardware that detects collisions
- So, 802.11 does collision avoidance, not detection

Hidden Terminal Problem

26



- A and C can't see each other, both send to B
- Occurs b/c 802.11 relies on physical carrier sensing, which is susceptible to hidden terminal problem

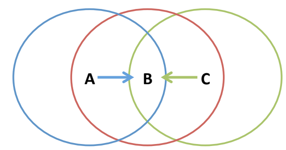
Virtual carrier sensing

27

- First exchange control frames before transmitting data
  - Sender issues "Request to Send" (RTS), incl. length of data
  - Receiver responds with "Clear to Send" (CTS)
- If sender sees CTS, transmits data (of specified length)
- If other node sees CTS, will idle for specified period
- If other node sees RTS but not CTS, free to send

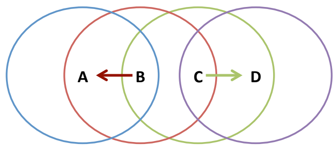
Hidden Terminal Problem

28



- A and C cant see each other, both send to B
- RTS/CTS can help
  - Both A and C would send RTS that B would see first
  - B only responds with one CTS (say, echoing A's RTS)
  - C detects that CTS doesn't match and wont send

Exposed Terminal Problem



- B sending to A, C wants to send to D
- As C receives packets, carrier sense would prevent it from sending to D, even though wouldn't interfere
- RTS/CTS can help
  - C hears RTS from B, but not CTS from A
  - C knows it's transmission will not interfere with A
  - C is safe to transmit to D

29

Impact on Higher-Layer Protocols

- Wireless and mobility change path properties
  - Wireless: higher packet loss, not from congestion
  - Mobility: transient disruptions, and changes in RTT
- Logically, impact should be minimal …
  - Best-effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- But, performance definitely *is* affected
  - TCP treats packet loss as a sign of congestion
  - TCP tries to estimate the RTT to drive retransmissions
  - TCP does not perform well under out-of-order packets
- Internet not designed with these issues in mind

30

Questions

- RTS/CTS more like:
  A. Statistical multiplexing
  B. Time-division multiplexing
  C. Frequency-division multiplexing
- Which of following is NOT true?
  A. Collisions are minimized when RTS/CTS used.
  B. Sender can always detect a collision without feedback from receiver.
  C. TCP congestion control works poorly in wireless without link-layer retransmission.
  D. Wireless generally has higher loss rates than wired.

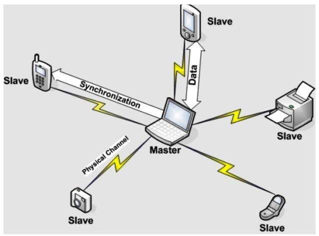
31

Bluetooth: 802.15.1 "personal-area-networks"

32

33

Bluetooth piconets



- Up to 7 “slave devices and 225 “parked” devices
- Operates on unlicensed wireless spectrum
  - How to prevent interference?

34

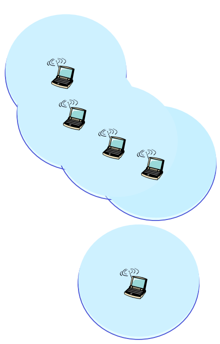
PHY: Spread Spectrum – Frequency Hopping

- Nodes rapidly jump between frequencies
- Sender and receiver coordinated in jumps
  - How coordinate? Pseudorandom number generator, with shared input known to sender/receiver
- If randomly collide with other transmitted, only for short period before jump again

- Bluetooth
  - 79 frequencies, on each frequency for 625 microseconds
  - Each channel also uses TDMA, with each frame taking 1/3/5 consecutive slots.
  - Only master can start in odd slot, slave only in response

35

Ad-Hoc Networks



Ad hoc mode

- No base stations
- Nodes can only transmit to other nodes within link coverage
- Nodes self-organize and route among themselves
- Can create multi-hop wireless networks, vs. wired backend

36

Infrastructure vs. Ad Hoc

- Infrastructure mode
  - Wireless hosts are associated with a base station
  - Traditional services provided by the connected network
  - E.g., address assignment, routing, and DNS resolution

- Ad hoc networks
  - Wireless hosts have no infrastructure to connect to
  - Hosts themselves must provide network services

- Similar in spirit to the difference between
  - Client-server communication
  - Peer-to-peer communication

37

Delay Tolerant Networking

- Nodes can both route and store
  - Next hop is available, forward
  - Otherwise, store packets
- Useful for data collection with no time limit
  - e.g., sensors in the field
- Analogous to email
  - Hold onto packets until another hop can take it from you
  - Eventually reach its destination

38

The Upside to Interference

- Some systems leverage interference
- If packets collide once, likely will again
  - Can use both collisions to construct original packets
  - Reduce effective error rate significantly
- If two hosts send to each other through an AP, and collide, AP can broadcast collision to both
  - Both know what they sent, can "subtract" that from collision to get the other
  - Improves throughput of system!

39

Conclusions

- Wireless
  - Already a major way people connect to the Internet
  - Gradually becoming more than just an access network
- Mobility (not discussed)
  - Today's users tolerate disruptions as they move
  - … and applications try to hide the effects
  - Tomorrow's users expect seamless mobility
- Challenges the design of network protocols
  - Wireless breaks the abstraction of a link, and the assumption that packet loss implies congestion
  - Mobility breaks association of address and location
  - Higher-layer protocols don't perform as well