Wireless 1: Media Access and Background

Outline

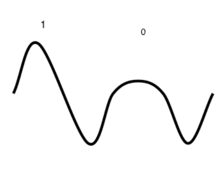
- Wireless background
  - Hopefully some of this is review from ugrad. ☺
  - How do we eke
- Why are wireless networks different from wired?
- Media Access Control (MAC) protocols
  - CSMA/CA (used in 802.1)
  - Reservations with RTS/CTS – MACAW
  - TDMA

Information in the air

- (Not really limited to the air, of course, but we notice it more)
- Encodings: AM, FM, Phase Modulation
- Point of this part: Understanding where limits to wireless transmission and reception come from and what factors influence it

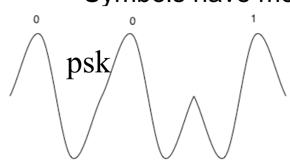
The Nyquist Limit

- A noiseless channel of width H can at most transmit a binary signal at a rate 2 x H.
  - E.g. a 3000 Hz channel can transmit data at a rate of at most 6000 bits/second
  - Assumes binary amplitude encoding

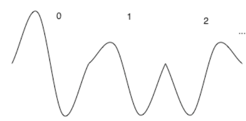


Past the Nyquist Limit

- More aggressive encoding can increase the channel bandwidth.
  - Example: modems
    - Same *frequency* - number of symbols per second
    - Symbols have more possible values



Psk
+
AM

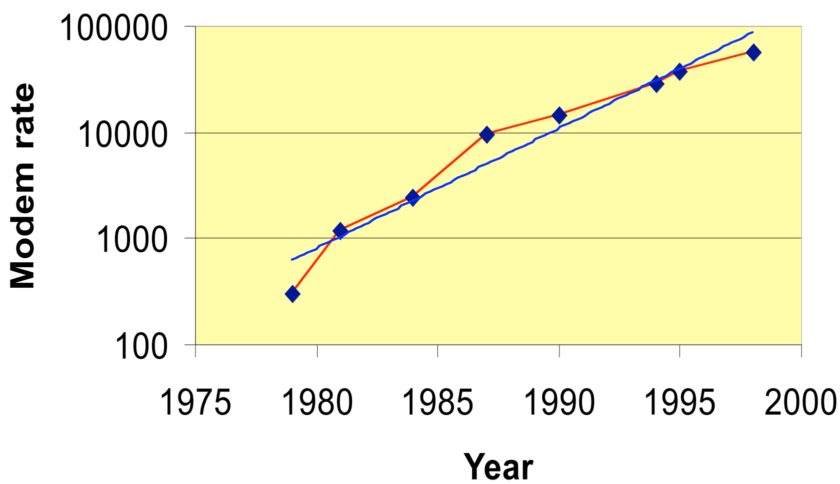


- Every transmission medium supports transmission in a certain frequency range.
  - The channel bandwidth is determined by the transmission medium and the quality of the transmitter and receivers
  - Channel capacity increases over time

Capacity of a Noisy Channel

- Can't add infinite symbols - you have to be able to tell them apart. This is where noise comes in.
- Shannon's theorem:
  - C = B x log(1 + S/N)
  - C: maximum capacity (bps)
  - B: channel bandwidth (Hz)
  - S/N: signal to noise ratio of the channel
    - Often expressed in decibels (db). 10 log(S/N).
- Example:
  - Local loop bandwidth: 3200 Hz
  - Typical S/N: 1000 (30db)
  - What is the upper limit on capacity?
    - Modems: Teleco internally converts to 56kbit/s digital signal, which sets a limit on B and the S/N.

Example: Modem Rates



Limits to Speed and Distance

- Noise: “random” energy is added to the signal.
- Attenuation: some of the energy in the signal leaks away.
- Dispersion: attenuation and propagation speed are frequency dependent.
  - Changes the shape of the signal

- **Attenuation: Loss (dB) = 20 log(4 pi d / lambda)**
  - **Loss ratio is proportional to: square of distance, frequency**
- **BUT: Antennas can be smaller with higher frequencies**
  - **Gain can compensate for the attenuation…**

Modulation vs. BER

- More symbols =
  - Higher data rate: More information per baud
  - Higher bit error rate: Harder to distinguish symbols
- Why useful?
  - 802.11b uses DBPSK (differential binary phase shift keying) for 1Mbps, and DQPSK (quadriture) for 2, 5.5, and 11.
  - 802.11a uses four schemes - BPSK, PSK, 16-QAM, and 64-AM, as its rates go higher.
- Effect: If your BER / packet loss rate is too high, drop down the speed: more noise resistance.
- We'll see in some papers later in the semester that this means noise resistance isn't always linear with speed.

Interference and Noise

- Noise figure: Property of the receiver circuitry. How good amplifiers, etc., are.
  - Noise is random white noise. Major cause: Thermal agitation of electrons.
- Attenuation is also termed "large scale path loss"
- Interference: Other signals
  - Microwaves, equipment, etc. But not only source:
  - Multipath: Signals bounce off of walls, etc., and cancel out the desired signal in different places.
  - Causes "small-scale fading", particularly when mobile, or when the reflective environment is mobile. Effects vary in under a wavelength.

Wireless is Attractive

- No wires to install
  - Easier deployment
  - No copper to steal
- Convenient mobility
- Enable broadcasts naturally

But wireless is *not* wired

- Makes design of networks fun & *hard*.
- Consider resource sharing:
  - Wired network: Put a “network layer” over a “link” layer and a “physical” layer. Assume that they get the bits there for you.
    - Links are physically isolated & shielded
    - Network designer worries about network-level sharing
  - Wireless network:
    - Shared medium (particularly with omni-directional antennas)
    - Nearby transmitters interfere
      - Link layer & physical layer
      - (Link like Ethernet, but fundamentally easier in wired)

More difficulties

- Engineering network-wide capacity is very hard
  - One link: max S/N ratio, etc.
  - Many links: Balance all transmissions and interference, etc. Hard!
- Channel capacity and behavior varies over time and location
  - On many time scales: bit-times to much longer
  - Errors often occur in burst.
  - Coping with these variations is hard
  - Can modulate transmission power / rate / etc.
- Packet delivery is not 100% and not 0%
  - A graph is a poor model for a wireless network
  - Inherently broadcast; reception probabalistic
  - Routing problem much harder – not just finding routes through a topology graph
- Achieving good TCP performance is hard
- Often coupled with mobility
- Often coupled with limited power on devices

Medium Access Control

- Think back to Ethernet MAC:
  - Wireless is a shared medium
  - Transmitters interfere
  - Need a way to ensure that (usually) only one person talks at a time.
    - Goals: Efficiency, possibly fairness
    - Non-goal: Network-wide efficiency. Just local.
    - Aka “Multiple Access” protocols

- But wireless is harder!
  - Can't really do collision detection:
    - Can't listen while you're transmitting. You overwhelm your antenna…
  - Carrier sense is a bit weaker:
    - Takes a while to switch between Tx/Rx.
  - Can't really tell if your packet arrived
    - Need some kind of ACK mechanism
  - Wireless is not perfectly broadcast

Hidden and Exposed Terminal

- A B C
- When B transmits, both A and C hear.
- When A transmits, B hears, but C does not
- … so C doesn't know that if it transmits, it will clobber the packet that B is receiving!
  - Hidden terminal
- When B transmits to A, C hears it…
  - … and so mistakenly believes that it can't send anything to a node other than B.
  - Exposed terminal

A Perfect MAC Protocol…

- Collision avoidance to reduce wasted transmissions
- Reasonable fairness
- Cope with hidden terminals
- Allow exposed terminals to talk

- No MAC protocol does all this!
  - Most favor collision reduction over 100% efficiency

CSMA/CA

- Carrier Sense Multiple Access with Collision Avoidance
  - Each node keeps a contention window CW
  - Picks random "slot" in [0, CW]
    - Transmissions must start at slot start
      - Aloha system showed that slotted > unslotted, since collisions must occur at slot boundaries
    - To xmit: carrier sense; if idle, decrement countdown from slot #. At 0, send data
    - If "busy" (noise level >> "idle" level), *defer*. "hold" countdown timer until idle. (We'll come back to this)

Collision Detection

- Option 1: Link-layer ACK (802.11 does this)
  - If no ACK, assume collision
    - Back off exponentially by doubling CW
- Option 2: Infer likelihood of collision if channel is often busy (before 802.11)
  - Doesn't need ACKs
  - Very unfair. Once you get the channel, you've got it.
  - 802.11 holds countdown timer between busy detects, and only reacts to back off CW. May lose more data, but has better fairness.

CSMA/CD + hidden terminal?

- No explicit mechanisms, but
- Carrier sense heuristics tend to sense busy even if data not decodable
  - Carrier sense range often 2x largest reception range
  - These are *not* fixed quantities, but in practice, it works .. okayish

Reservation-Based Protocols

- MACAW paper (based on MACA)
  - RTS – reserves channel for a bit of time, if sender hasn't heard other CTSes
  - CTS – sender replies if it hasn't heard any other RTSes
  - Both messages include time
  - If no CTS, exponential backoff
  - "RTS-CTS-DATA"

RTS-CTS

- Eliminates need for carrier sense (but must listen for RTS/CTS)
- With link-layer ACKs, must also protect the ACK. Lost ack == retransmission anyway
- Enhancement:
  - Don't send RTS if heard either CTS *or* RTS lately; ditto for receiver
  - Treats all communication as bidirectional
  - Bidirectional traffic assumption eliminates exposed terminal opportunities anyway
  - Handles hidden terminal problem

RTS/CTS in practice

- 802.11 standardized both CSMA/CA and RTS/CTS
- In practice, most operators disable RTS/CTS
  - Very high overhead!
    - RTS/CTS packets sent at “base rate” (often 1Mbit)
      - Avoid collisions regardless of transmission rate
  - Most deployments are celluar (base stations), not *ad hoc*. Neighboring cells are often configured to use non-overlapping channels, so hidden terminals on downlink are rare
    - Hidden terminal on uplink possible, but if clients mostly d/l, then uplink packets are small.
    - THIS MAY CHANGE. And is likely not true in your neighborhood!
  - As previously noted, when CS range >> reception range, hidden terminal less important

TDMA

- Explicitly allocate by time
  - Some cellular networks do this
  - Bluetooth does this
    - Master node divides time into even/odd slots
    - Master gets the odd ones
    - Next even slot goes to the node that received data in the preceding even slot. “Time Division Duplex” (TDD)
- TDMA makes sense at high load. At low load, slots are wasted.
- CSMA-approaches aren’t so hot at high, persistent load from many many sources. But are good at handling one or two talkers at a time.
- Lots of research work in this area. Scheduling, hybrid CSMA/TDMA, RTS/CTS, etc.

Lots Of Detail Slides

- 802.11 details if you're interested
- (Not covered at length in lecture)

802.11 particulars

- 802.11b (WiFi)
  - Frequency: 2.4 - 2.4835 Ghz DSSS
  - Modulation: DBPSK (1Mbps) / DQPSK (faster)
  - Orthogonal channels: 3
    - There are others, but they interfere. (!)
  - Rates: 1, 2, 5.5, 11 Mbps
- 802.11a: Faster, 5Ghz OFDM. Up to 54Mbps
- 802.11g: Faster, 2.4Ghz, up to 54Mbps

802.11 details

- Fragmentation
  - 802.11 can fragment large packets (this is separate from IP fragmentation).
- Preamble
  - 72 bits @ 1Mbps, 48 bits @ 2Mbps
  - Note the relatively high per-packet overhead.
- Control frames
  - RTS/CTS/ACK/etc.
- Management frames
  - Association request, beacons, authentication,

802.11 DCF

- Distributed Coordination Function (CSMA/CA)
- Sense medium. Wait for a DIFS (50 µs)
- If busy, wait 'till not busy. Random backoff.
- If not busy, Tx.
- Backoff is binary exponential

- Acknowledgements use SIFS (short interframe spacing) 10 µs

802.11 RTS/CTS

- RTS sets “duration” field in header to
  - CTS time + SIFS + CTS time + SIFS + data pkt time
- Receiver responds with a CTS
  - Field also known as the “NAV” - network allocation vector
  - Duration set to RTS dur - CTS/SIFS time
  - This reserves the medium for people who hear the CTS

802.11 modes

- Infrastructure mode
  - All packets go through a base station
  - Cards associate with a BSS (basic service set)
  - Multiple BSSs can be linked into an Extended Service Set (ESS)
    - Handoff to new BSS in ESS is pretty quick
      - Wandering around CMU
    - Moving to new ESS is slower, may require re-addressing
      - Wandering from CMU to Pitt
- Ad Hoc mode
  - Cards communicate directly.
  - Perform some, but not all, of the AP functions

802.11 continued

- 802.11b packet header: (MPDU has its own)

Preamble	PLCP header	MPDU

56 bits sync	16 bit Start of Frame

Signal	Service	Length	CRC
8 bits	8 bits	16 bits	16 bits

802.11 packet

FC	D/I	Addr	Addr	SC	Addr	DATA	FCS