Lecture 2
Wireless & 802.11

David Andersen
Department of Computer Science
Carnegie Mellon University

15-849, Fall 2005
http://www.cs.cmu.edu/~dga/15-849/
From Signals to Packets

Analog Signal

“Digital” Signal

Bit Stream

Packets

Packet Transmission

Sender ▸ Receiver

0 0 1 0 1 1 1 0 0 0 1 1
Today’s Lecture

- Modulation.
- Bandwidth limitations.
- Frequency spectrum and its use.
- Multiplexing.
- Coding.
- Framing.
Modulation

- **Sender** changes the nature of the signal in a way that the receiver can recognize.
  - Similar to radio: AM or FM
- **Digital transmission**: encodes the values 0 or 1 in the signal.
  - It is also possible to encode multi-valued symbols
- **Amplitude modulation**: change the strength of the signal, typically between on and off.
  - Sender and receiver agree on a “rate”
  - On means 1, Off means 0
- **Similar**: frequency or phase modulation.
- **Can also combine method modulation types.**
Amplitude and Frequency Modulation

0 0 1 1 0 0 1 1 0 0 0 1 1 1 0 0 0 1 1 0 0 0 1 1 1 0

0 1 1 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0

0 1 1 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0
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
More aggressive encoding can increase the channel bandwidth.

- Example: modems
  - Same frequency - number of symbols per second
  - Symbols have more possible values

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:
  - $C = B \times \log(1 + S/N)$
  - $C$: 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

The graph illustrates the trend of modem rates from 1975 to 2000. The vertical axis represents the modem rate, while the horizontal axis shows the year. The data indicates a steady increase in modem rates over the years.
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) = \(20 \log\left(\frac{4 \pi d}{\lambda}\right)\)
  - 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.
Frequency Division Multiplexing: Multiple Channels

Determines Bandwidth of Link

Determines Bandwidth of Channel

Different Carrier Frequencies
Wireless Technologies

- Great technology: no wires to install, convenient mobility, ..
- High attenuation limits distances.
  - Wave propagates out as a sphere
  - Signal strength reduces quickly ($1/distance^3$)
- High noise due to interference from other transmitters.
  - Use MAC and other rules to limit interference
  - Aggressive encoding techniques to make signal less sensitive to noise
- Other effects: multipath fading, security, ..
- Ether has limited bandwidth.
  - Try to maximize its use
  - Government oversight to control use
Antennas and Attenuation

- **Isotropic Radiator:** A theoretical antenna
  - Perfectly spherical radiation.
  - Used for reference and FCC regulations.

- **Dipole antenna (vertical wire)**
  - Radiation pattern like a doughnut

- **Parabolic antenna**
  - Radiation pattern like a long balloon

- **Yagi antenna (common in 802.11)**
  - Looks like |--|--|--|--|--|--|
  - Directional, pretty much like a parabolic reflector
Antennas

- Spatial reuse:
  » Directional antennas allow more communication in same 3D space

- Gain:
  » Focus RF energy in a certain direction
  » Works for both transmission and reception

- Frequency specific
  » Frequency range dependant on length / design of antenna, relative to wavelength.

  » Favors directionality. E.g., you can use an 8dB gain antenna b/c of spatial characteristics, but not always an 8dB amplifier.
Spread Spectrum and CDMA

● Basic idea: Use a wider bandwidth than needed to transmit the signal.

● Why??
  » Resistance to jamming and interference
    – If one sub-channel is blocked, you still have the others
  » Pseudo-encryption
    – Have to know what frequencies it will use

● Two techniques for spread spectrum…
Frequency Hopping SS

- Pick a set of frequencies within a band
- At each time slot, pick a new frequency
  » Ex: original 1Mbit 802.11 used 300ms time slots
- Frequency determined by a pseudorandom generator function with a shared seed.
Direct Sequence SS

- Use more bandwidth than you need to
  - Generate extra bits via a spreading sequence

<table>
<thead>
<tr>
<th>Data</th>
<th>Code</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 0 0 1</td>
<td>1 0 0 1 0 1 1 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0 1 0 1 0 1 0 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CDMA

- DSS with orthogonal codes
  - If receiver is using code ‘A’:
    - Data xor A = signal
    - Output = sum(signal xor A)
  - Let’s say someone else transmits with code ‘B’ at the same time:
    - Signal = Data xor A + other xor B
    - Output: sum((signal xor A + other xor B) xor A)
      - = Data if A and B or orthogonal (dot product is zero)
      - Ex: A: 1 -1 -1 1 -1 1
      - B: 1 1 -1 -1 1 1
      - Decode function: sum (bitwise received)
      - Rx A1: 1*1 + -1*1 + -1*1 + 1*1 + -1*1 + 1*1 = 6
      - A1 + B1 signal: 2 0 -2 0 0 2
      - Decode at A: 2*1 + 0 + -2*-1 + 0 + 0 + 2*1 = 6 (!)
  - In practice: use pseudorandom numbers, depend on balance and uniform distribution to make other transmissions look like noise.
CDMA, continued

» Lots of codes
  – Useful if many transmitters are quiescent
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

- 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.
  - 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
MAC discussion
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, etc.
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)

<table>
<thead>
<tr>
<th>Preamble</th>
<th>PLCP header</th>
<th>MPDU</th>
</tr>
</thead>
<tbody>
<tr>
<td>56 bits sync</td>
<td>16 bit Start of Frame</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signal</th>
<th>Service</th>
<th>Length</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 bits</td>
<td>8 bits</td>
<td>16 bits</td>
<td>16 bits</td>
</tr>
</tbody>
</table>
802.11 packet

FC D/I Addr Addr SC Addr DATA FCS