Lecture 13: Wireless Networking
Outline

• Wireless physical layer challenges
  - Signal, noise, modulation
  - A little bit of EE goes a long way

• Wireless link layers
  - Hidden terminals, exposed terminals
  - CSMA/CA
  - RTS/CTS

• Wireless routing and throughput

• Wireless trends today
Ethernet: 802.3

- Dominant wired LAN technology
  - 10BASE5 (vampire taps)
  - 10BASE-T, 100BASE-TX, 1000BASE-T

- Frame format:

<table>
<thead>
<tr>
<th>Physical</th>
<th>Link</th>
<th>Layer 3</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preamble</td>
<td>SFD</td>
<td>Src</td>
<td>Dest</td>
</tr>
<tr>
<td>7 x 10101010</td>
<td>10101011</td>
<td>6 bytes</td>
<td>6 bytes</td>
</tr>
</tbody>
</table>

Gap: 96 ns, 960 ns, 9600 ns
Physical Layer (Layer 1)

• **Responsible for specifying the physical medium**
  - Category 5 cable (Cat5): 8 wires, twisted pair, RJ45 jack
  - WiFi wireless: 2.4GHz

• **Responsible for specifying the signal**
  - 100BASE-T: 5-level pulse amplitude modulation (PAM-5)
  - 802.11b: Binary and quadrature phase shift keying (BPSK/QPSK)

• **Responsible for specifying the bits**
  - 100BASE-T: 4-to-6 bit-to-chip encoding, 3 chip symbols
  - 802.11b: Barker code (1-2Mbps), complementary code keying (5.5-11Mbps)
Wireless is Different

• Variable: signal attenuates over space
• Interference: other RF sources can interfere with signal
• Multipath: signal can self-interfere
• Distributed: nodes cannot detect collisions
• To address these differences, wireless link layers use slightly different mechanisms
• Also, can’t just abstract away the physical and link layers: need a brief introduction to underlying EE
Attenuation Over Space

- Signal weakens as distance from transmitter increases
- Reflections, obstructions, etc. complicate the attenuation
- Depending on the antenna, not uniform in all directions
- Much more complex than the wired model
Signal Strength Over Space
Directional Antennas
Interference

- In unlicensed bands (e.g., 802.11), there are lots of transmitters
  - 802.11 cards
  - 802.15.1 (Bluetooth)
  - 802.15.4 (ZigBee)
  - 2.4GHz phones
  - Microwave ovens

- This interference can be stronger or weaker than the signal, and can prevent successful reception
Analog Signals

- Amplitude
- Wavelength
Specifying the Signal: Modulation

On-Off Keying (OOK)

Amplitude Shift Keying (ASK)
Modulation, Continued

Frequency Shift Keying (FSK)

Phase Shift Keying (PSK)
I/Q Modulation

- I: in-phase, Q: quadrature
- Sum of two sines is a sine
- Show what the carrier looks like compared to a simple, unmodulated signal
- Use I/Q because this is how it’s actually done in hardware
The diagram illustrates the concepts of I and Q, which are often used in signal processing and communications. The I+Q signals are depicted as superimposed waveforms, showing the phase relationship and amplitude characteristics of the signals.
Modulation in I/Q Plots

OOK
ASK
FSK
BPSK
QPSK
Example measurements from 16-QAM
Signal, Noise, and Interference

- Signal: energy of desired transmission
- Noise/Noise floor: energy of hardware thermal effects
- Interference: energy of other transmitters
- Usually measured in dBm/dBW: 0dBm = 1mW, 0dBW = 30dBm = 1W
  - Note dB is a logarithmic scale: 10dBm = 10mW, 20dBm = 100mW
Signal Plus Noise
SINR

• Signal to Interference-and-Noise Ratio

• Measured in dB: \[ \frac{|S|}{|N+I|} \]
  - S = -50dBm, N+I = -95dBm, SINR = 45dB
  - S = -89dBm, N+I = -93dBm, SINR = 4dB

• SINR is particularly critical in wireless because of attenuation over space
Bit Error Rates

- There is a theoretical limit on how much information a channel can carry (Shannon limit)
- Bit error rate depends on the SINR and the modulation
- This is why wireless link layers use more complex chip/bit encoding
  - If signal is strong (high SINR), have few chip errors, can use low encoding
  - If signal is weak (low SINR), have many chip errors, use higher encoding to recover from errors
After the signal is received and digitized, it is fed through a series of adaptive delay stages which are summed together via feedback loops. This technique is particularly effective in slowly changing environments such as transmission over telephone lines, but is more difficult to implement in rapidly changing environments like factory floors, offices and homes where transmitters and receivers are moving in relation to each other. The main drawback is the impact on system cost and complexity. Adaptive equalizers can be expensive to implement for broadband data links.

Spread spectrum systems are fairly robust in the presence of multipath. Direct Sequence Spread Spectrum (DSSS) systems will reject reflected signals which are significantly delayed relative to the direct path or strongest signal. This is the same property which allows multiple users to share the same bandwidth in Code Diversity Multiple Access (CDMA) systems. Frequency Hopping Spread Systems (FHSS) also exhibit some degree of immunity to multipath. Because a FHSS transmitter is continuously changing frequencies, it will always hop to some frequencies which experience little or no multipath loss. In a severe fading environment, throughput of an FHSS system will be reduced, but it is unlikely that the link will be lost completely. The performance of DSSS systems in the presence of multipath is described further in a separate section below.

Modulation Technique

Modulation technique is a key consideration. This is the method by which the analog or digital information is converted to signals at RF frequencies suitable for transmission. Selection of modulation method determines system bandwidth, power efficiency, sensitivity, and complexity. Most of us are familiar with Amplitude Modulation (AM) and Frequency Modulation (FM) because of their widespread use in commercial radio. Phase Modulation is another important technique. It is used in applications such as Global Position System (GPS) receivers and some cellular telephone networks.

For the purposes of link budget analysis, the most important aspect of a given modulation technique is the Signal-to-Noise Ratio (SNR) necessary for a receiver to achieve a specified level of reliability in terms of BER. A graph of $E_b/N_0$ vs BER is shown in Figure 4. $E_b/N_0$ is a measure of the required energy per bit relative to the noise power. Note that $E_b/N_0$ is independent of the system data rate. In order to convert from $E_b/N_0$ to SNR, the data rate and system bandwidth must be taken into account as shown below:

$$\text{SNR} = (E_b/N_0) \times (R/B_T)$$

where:

- $E_b$ = Energy required per bit of information
- $N_0$ = thermal noise in 1Hz of bandwidth
- $R$ = system data rate
- $B_T$ = system bandwidth

Spread Spectrum Radios

The term “spread spectrum” simply means that the energy radiated by the transmitter is spread out over a wider amount of the RF spectrum than would otherwise be used. By spreading out the energy, it is far less likely that two users sharing the same spectrum will interfere with each other. This is an important consideration in an unlicensed band, which why the regulatory authorities imposed spread spectrum requirements on radios which transmit over 1dBm (about 0.75mW) in the following bands:

![Graph of Probability of Bit Error for Common Modulation Methods](image)
Variable Bit Rates

- 802.11b supports 1, 2, 5.5, and 11Mbps
- 2, 5.5Mbps and 11Mbps are QPSK
- To support this, the signal field says what the data rate is
  - 00001010: 1Mbps (11 chips/bit, barker code)
  - 00010100: 2Mbps (11 chips/bit, barker code)
  - 00110111: 5.5Mbps (2 chips/bit, CCK)
  - 01101110: 11Mbps (1 chip/bit, CCK)
- So the header is still at 1Mbps, even if the data is at 11Mbps
Collisions are not so simple

- If A transmits first, B can still decode its packet
- If C transmits first, A will corrupt its packet and B can’t decode C’s packet
- What if AB and BC are both -60dB?
- Signal strength matters: this is the RF capture effect
802.11 Packet Loss Rates
802.11 Packet Loss Rates (at 11Mbps)

- How does this affect TCP?
Wireless PHY Summary

• Can’t control or limit the channel
• Need to deal with weak signals, interference, etc.
• Signal strength affects collisions
• Many different kinds of modulation: amplitude, frequency, phase
• Use robust encodings when needed, use fast speeds when possible
• Lots of intermediate packet delivery ratios
2 minute break
Wireless Link Layers
MAC Layer Responsibilities

- Arbitrate control of the channel
- One node should be able to use 100%
- Multiple nodes should get a fair share
- Want high utilization under contention
CA versus CD

- Collision detect (CD) is hard in wireless
- Local signal is much stronger than anything received
- Protocols use collision avoidance (CA) by sensing the channel
Simple MAC: CSMA/CA

• 1) Wait a small random period, check the channel
• 2) If the channel is busy, go to 1 (maybe longer wait)
• 3) Transmit packet
802.11b MAC: CSMA/CA

- Maintain a waiting counter $c$
- For each time step channel is idle, $c --$
- When $c = 0$, transmit
- If packet is not acknowledged (layer 2), pick a new, larger $c$
  - Use lack of layer 2 ack as collision detect
Problems with CSMA/CA

• Want to know state of channel at receiver, not transmitter

• But wireless is not transitive!
  - A hears B
  - A hears C
  - B and C may not hear each other
  - B and C can only sense their channel, but need to know if A’s channel is clear
Hidden Terminal Problem

- B and C can’t hear each other, A can hear both
- B and C sense a clear channel, transmit, and collide at A
- B is a *hidden terminal* to C, and C is a *hidden terminal* to B
Exposed Terminal Problem

- A transmits to B
- C hears the transmission, backs off, even if it wants to transmit to D
- C is an *exposed* terminal to A’s transmission
RTS/CTS

- Request-to-send, Clear-to-send (RTS/CTS)
- Allows transmitter to check availability of channel at receiver
- Transmitter sends an RTS
- If it hears a CTS, sends data
- If not, retries RTS some time later
- If you hear a CTS for someone else, don’t transmit
RTS

B  RTS  A

C
Data

B \rightarrow A

\not C
Network Allocation Vector (NAV)

- 802.11b supports RTS/CTS
- NAV is data structure node uses to know when channel may be clear
- NAV is in terms of *time*: variable bit rates, RTS, etc.
RTS/CTS Benefits

• Solves the hidden terminal problem (assuming CTS not corrupted)
  - In practice, not true: a node’s CTS can collide with another node’s RTS
  - In practice, can reduce but not solve the hidden terminal problem on data
  - Control packets still collide

• Improves data packet delivery ratio

• Does it solve the exposed terminal problem? What about ACKs?
RTS/CTS Drawbacks

- 3 packets per packet: RTS/CTS/DATA (4-22% overhead in 802.11b)
- RTS still go through CSMA: they can be lost
- CTS losses cause lengthy retries
- 33% of IP packets are TCP ACKs: is it worth it?
- In practice, WiFi doesn’t use RTS/CTS
802.11 Association

- Terminal hears beacon from AP (scan channels), or sends a probe request
- Terminal sends an authentication request, AP sends authentication response
  - If security is enabled, use keys
  - Also “null” authentication
- Terminal sends association request, AP sends association response
Installing the PTK, and where applicable the GTK keys, causes the MAC to encrypt and decrypt all subsequent MSDUs irrespective of their path through the controlled or uncontrolled ports.

Upon successful completion of the 4-Way Handshake, the Authenticator and Supplicant have authenticated each other; and the IEEE 802.1X Controlled Ports are unblocked to permit general data traffic. See Figure 5-13.

Figure 5-11—Establishing the IEEE 802.11 association

Figure 5-12—IEEE 802.1X EAP authentication
2.4GHz Band
Wireless Routing
Wireless Routing

- Network is much more dynamic
- Not constrained by physical topology
- Discovering and estimating links to neighbors
- Discovering and maintaining routes to nodes
- Rich area of study: we’ll just touch on link cost
Hopcount Considered Harmful

- Minimizing hopcount causes protocol to choose long links

- Links are more likely to be on edge of SNR/PRR curve
  - Less stable
  - Require more maintenance

- One way wireless routing is different

- OLSRv2 adds the concept of link metrics
DSDV and Hopcount on Roofnet

- From DeCouto et al., “A High-Throughput Path Metric for Multi-Hop Wireless Routing.”
Variations Across Hopcounts

- From DeCouto et al., “A High-Throughput Path Metric for Multi-Hop Wireless Routing.”
Expected Transmissions (ETX)

- Proposed by DeCouto et al.
- Alternative metric: ETX, number of transmissions until you receive an ACK

**Cost of link is** \[ \frac{1}{PRR_{AB} \cdot ARR_{BA}} \]

- \( PRR_{AB} = 75\% \), \( ARR_{BA} = 66\% \), \( ETX_{AB} = 2.0 \)
- \( PRR_{AB} = 50\% \), \( ARR_{BA} = 50\% \), \( ETX_{AB} = 4.0 \)

- **Cost of route is sum of ETX values of links on route**
ETX Benefits

- From DeCouto et al., “A High-Throughput Path Metric for Multi-Hop Wireless Routing.”
ETX Is Not Enough

- 802.11b supports four different bit rates
- ETX can select the route, but not the bitrate
- One packet at 11Mbps $\neq$ one packet at 1Mbps

Solution: Estimated Time of Transmission (ETT)

- Probe at different bit rates
- Choose link bit rate based on minimum cost
Link Metrics Today

• Rough consensus that ETX/ETT is the right metric
  - Addresses intermediate links
  - Can be used across link layers

• No consensus on how to estimate the value
  - Several proposals
  - Still an active area of research

• Issue: conflates hopcount and link quality, making loops very easy (100% → 33% can look like 2 more hops)

• Issue: minimizes delay, does not maximize throughput
Throughput Dropoff

- Only every third node can transmit, or you get the hidden terminal problem
- In TCP, data and ack packets cause the hidden terminal problem
Wireless Routing

- Maintaining consistent, distributed state on a dynamic system
- Preventing loops via serialization or source routing
- On-demand versus continuous
- ETX/ETT better metric than hopcount
WiFi Today

• Faster and faster data rates (with high SNR): 802.11n supports 600Mbps

• But control sequence and timing remains slow for backwards compatibility: 91% of packet time at 600Mbps

• Amdahl’s Law: if data is only 9% of a packet, faster data rates won’t help much
Wireless Capacity Problem

- Shannon: **Channel capacity** $C = B \log_2(1 + S/N)$
  - $B$ is bandwidth of line
  - $S$ and $N$ are average signal & noise power

- **To make wireless faster, need higher B, higher S, or lower N**
  - Higher $B$ constrained by FCC: 83.5MHz for 2.4GHz, 100MHz for 5GHz
  - Higher $S$ constrained by FCC and batteries: no cooking please
  - Lowering $N$ much is hard

- **How can we make wireless keep pace with wired?**
Wireless Horizon: 60GHz

- 60GHz band: 1mm wavelength
- 7GHz of bandwidth (could be super-fast!)
- But power is tiny: received power proportional to antenna size
- Antenna size needs to match 1/4 wavelength: circuit sizes matter!
- Lots of hard problems: Ada Poon and Tom Lee in EE researching topic