

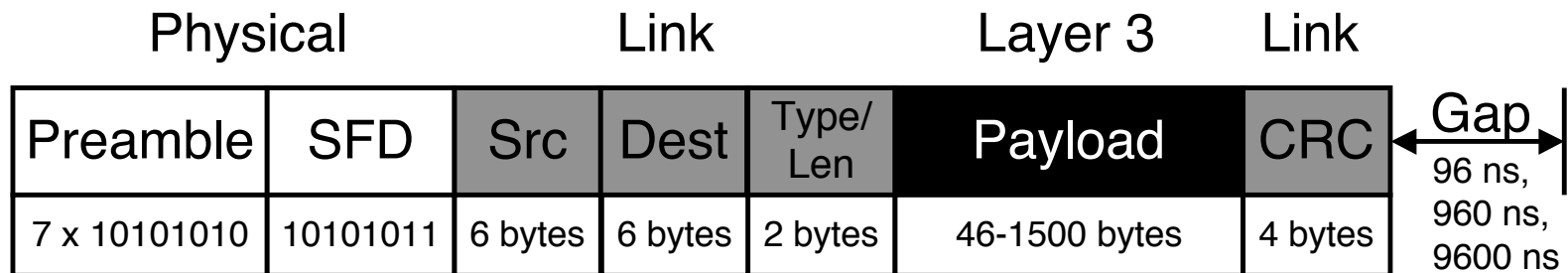
Lecture 11: Wireless Networking

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**

Ethernet: 802.3

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



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)**

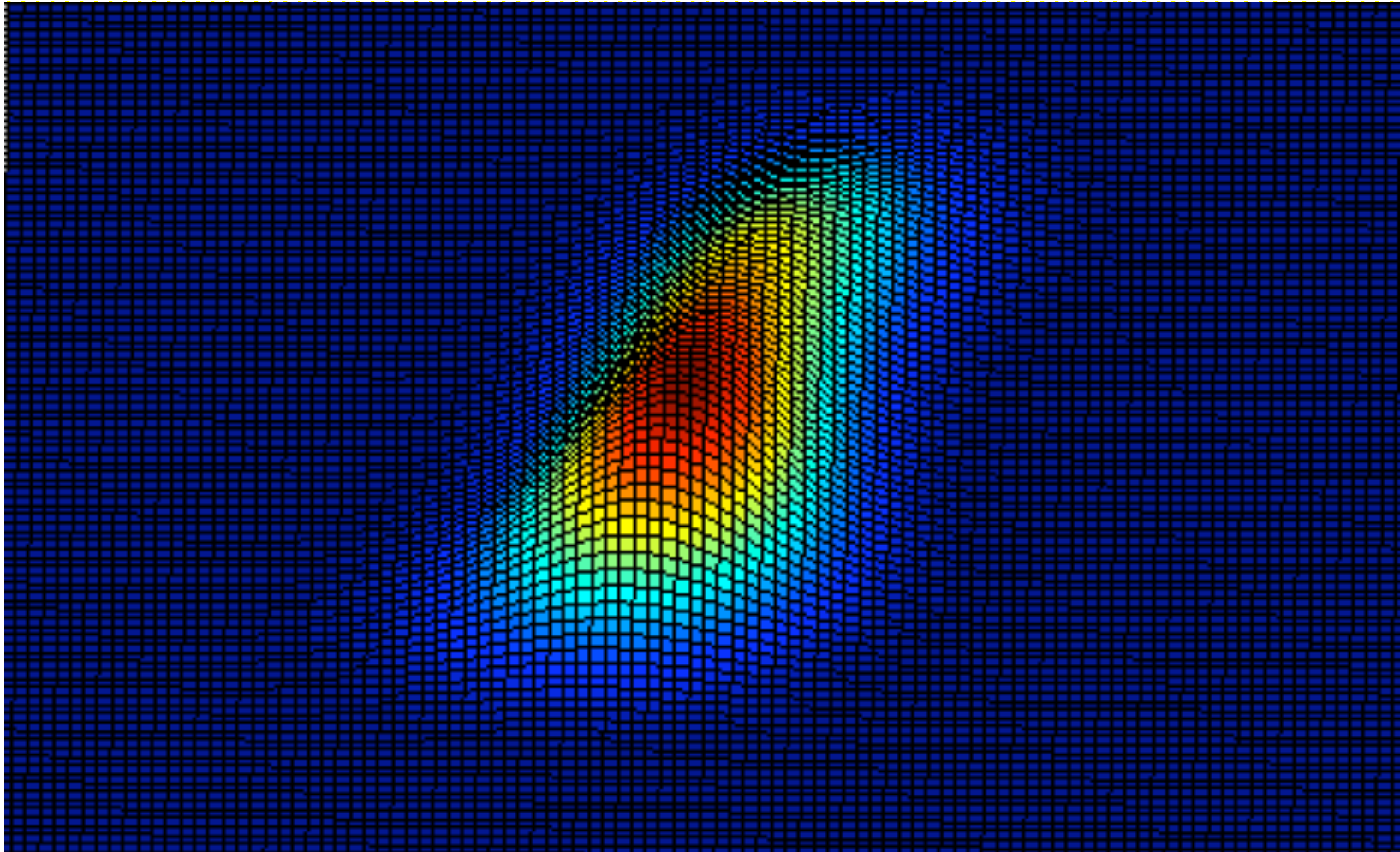
Wireless is Different

- **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

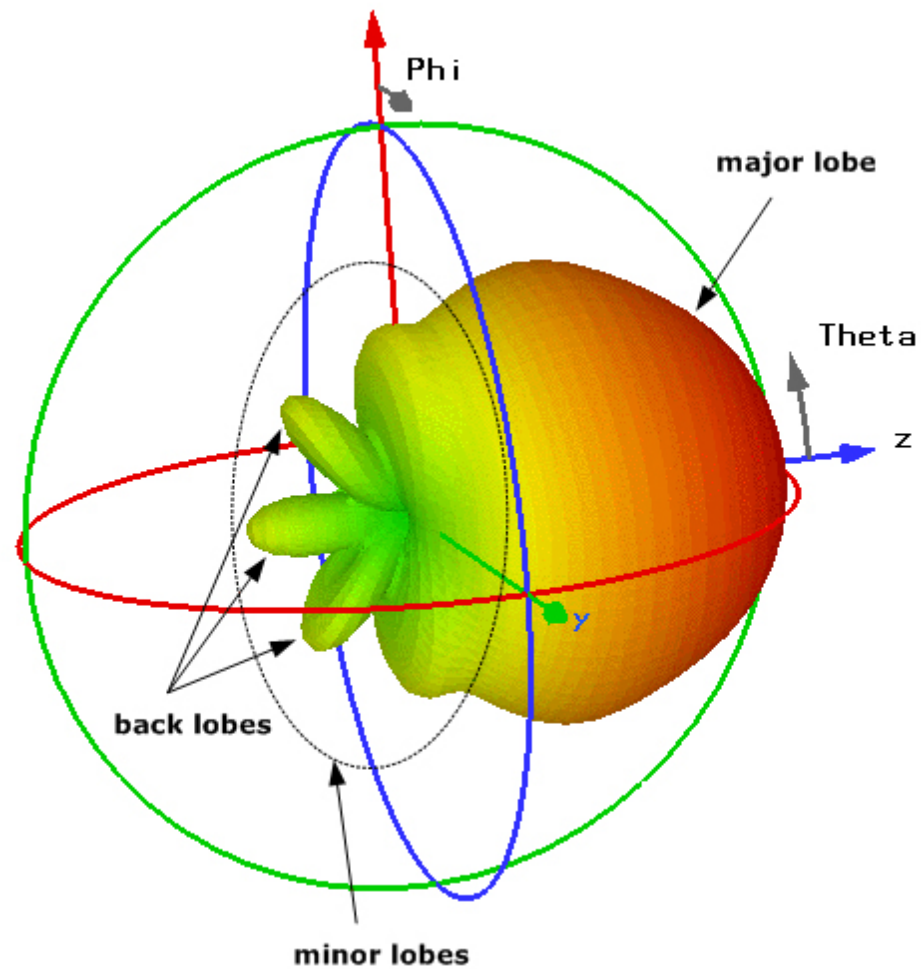
Attenuation Over Space

- 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



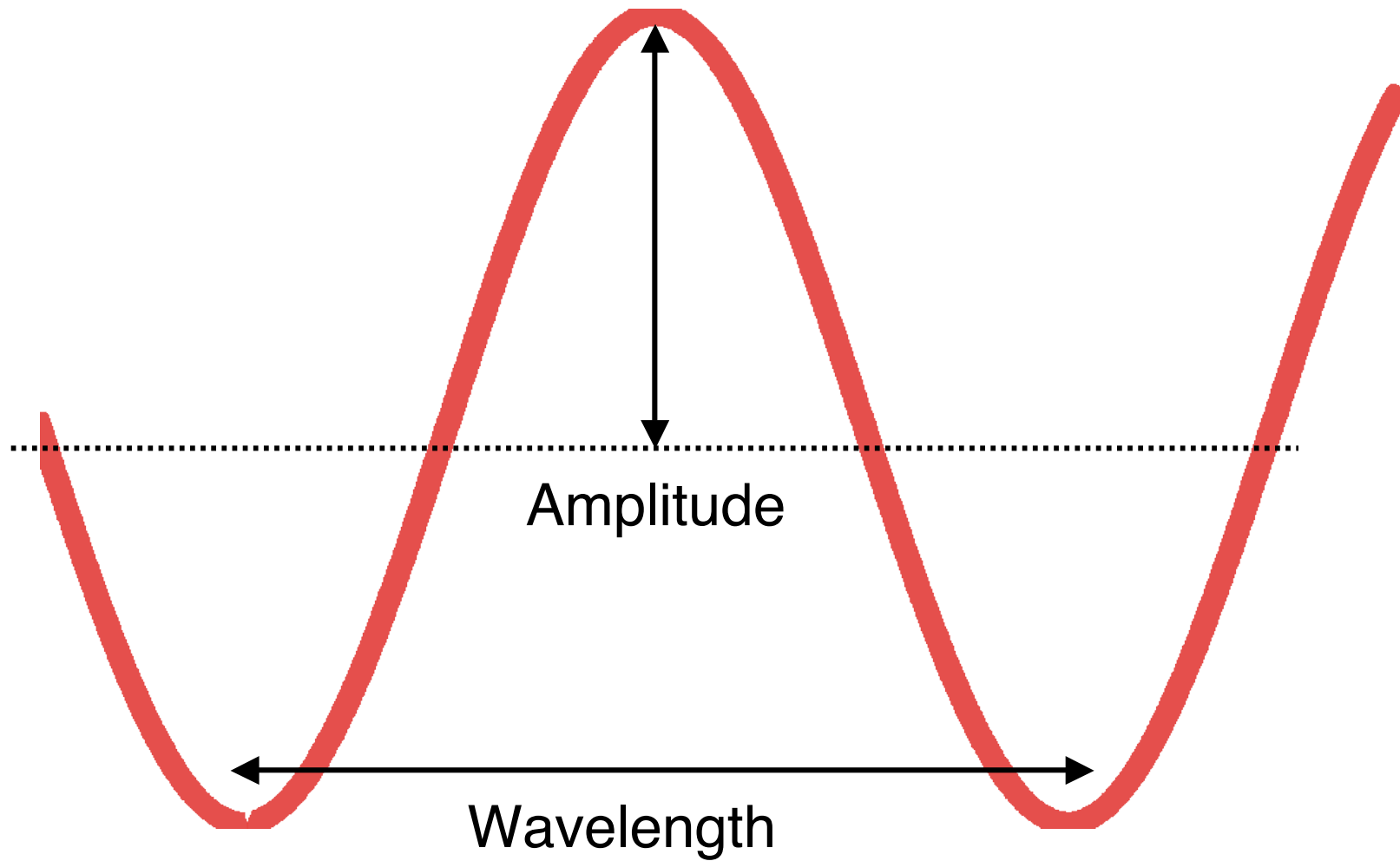
Directional Antennas



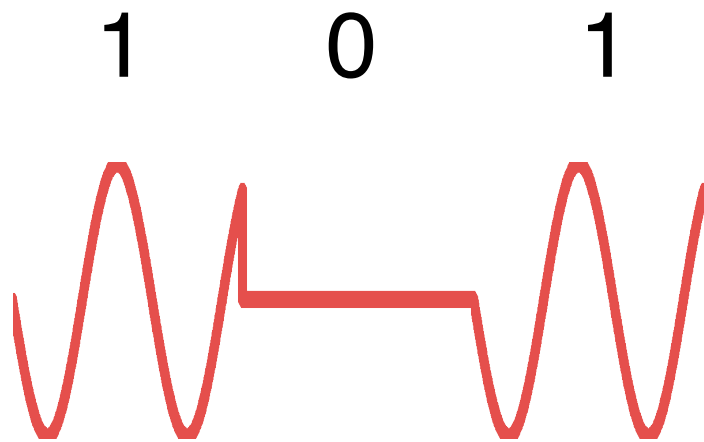
Interference

- **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**

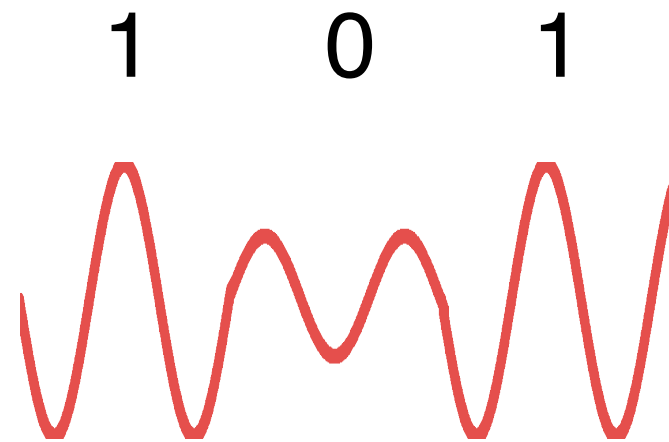
Analog Signals



Specifying the Signal: Modulation



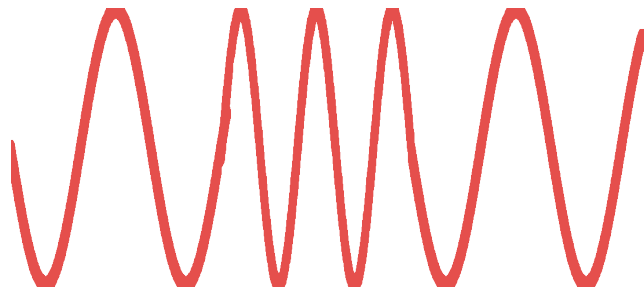
On-Off Keying
(OOK)



Amplitude Shift
Keying (ASK)

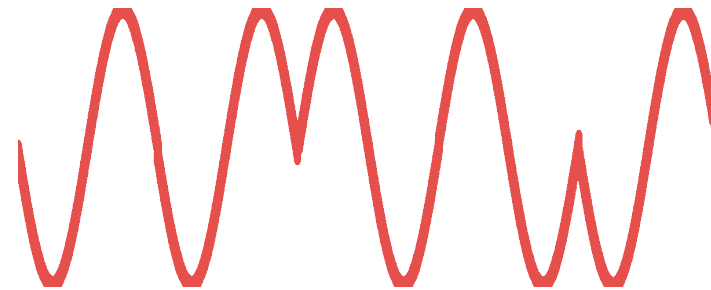
Modulation, Continued

1 0 1



Frequency Shift
Keying (FSK)

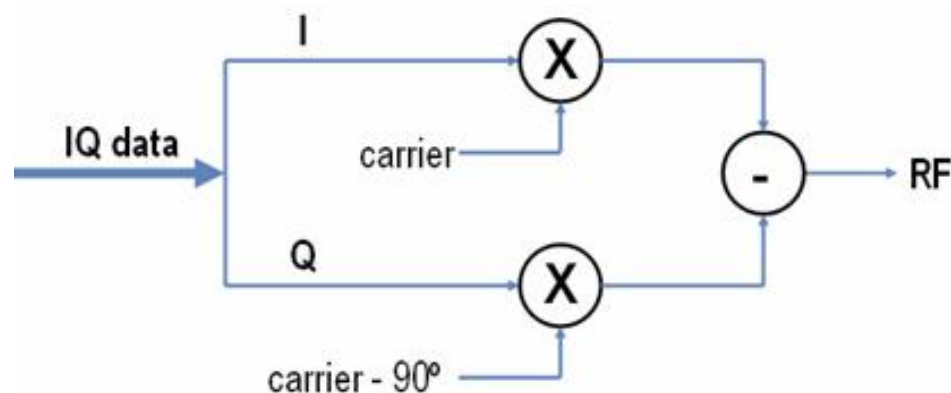
1 0 1



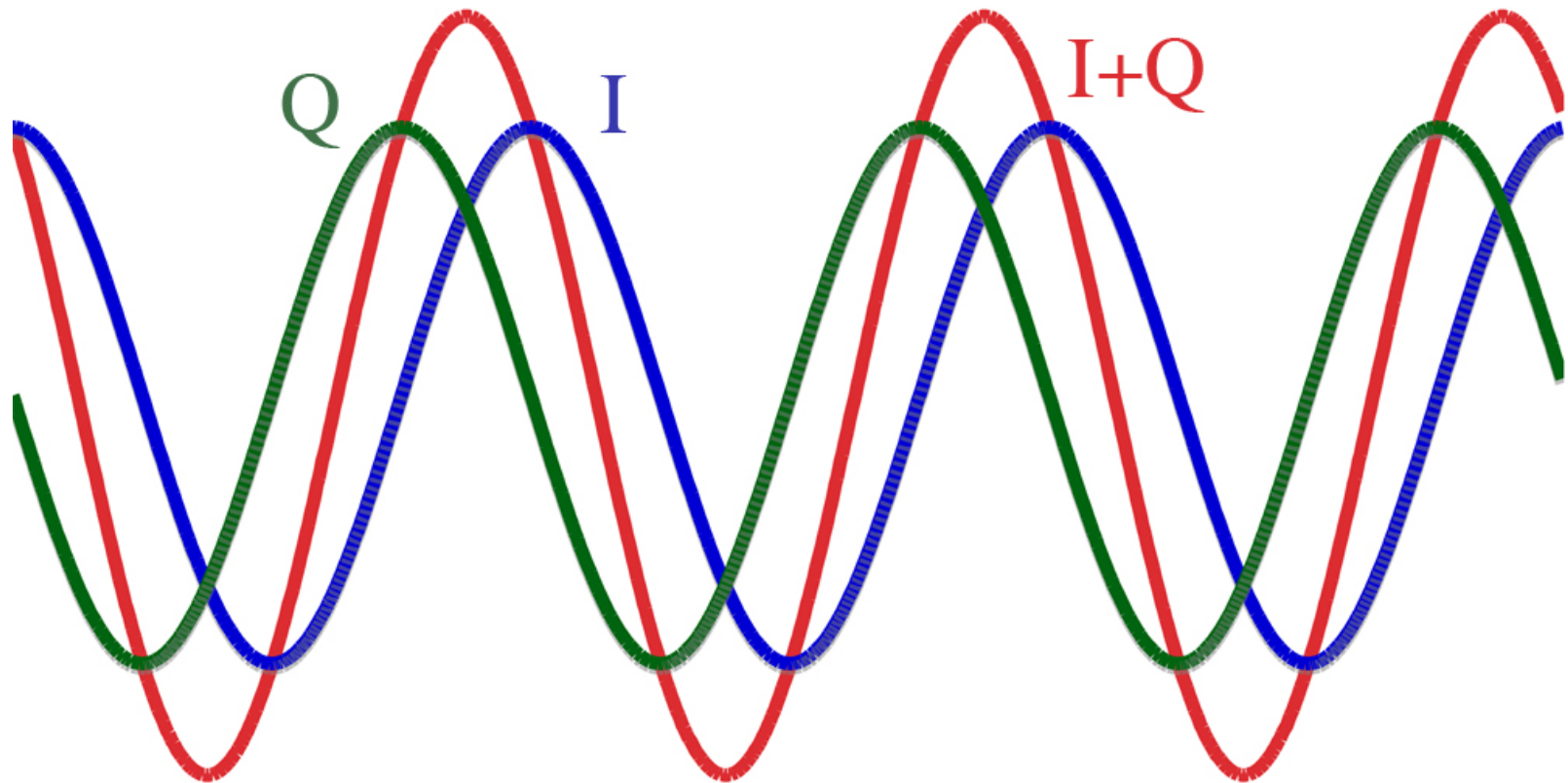
Phase Shift
Keying (PSK)

I/Q Modulation

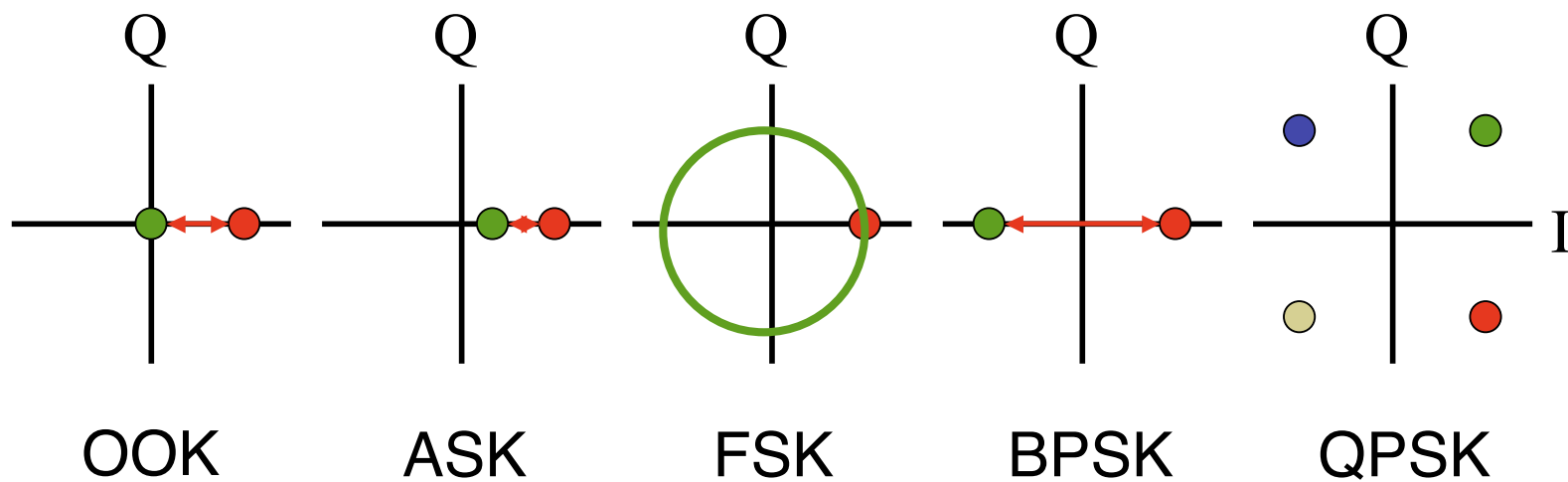
- I: in-phase, Q: quadrature
- Sum of two sines is a sine
- Show what the carrier looks like compared to a simple, unmodulated signal
- Use I/Q because this is how it's actually done in hardware



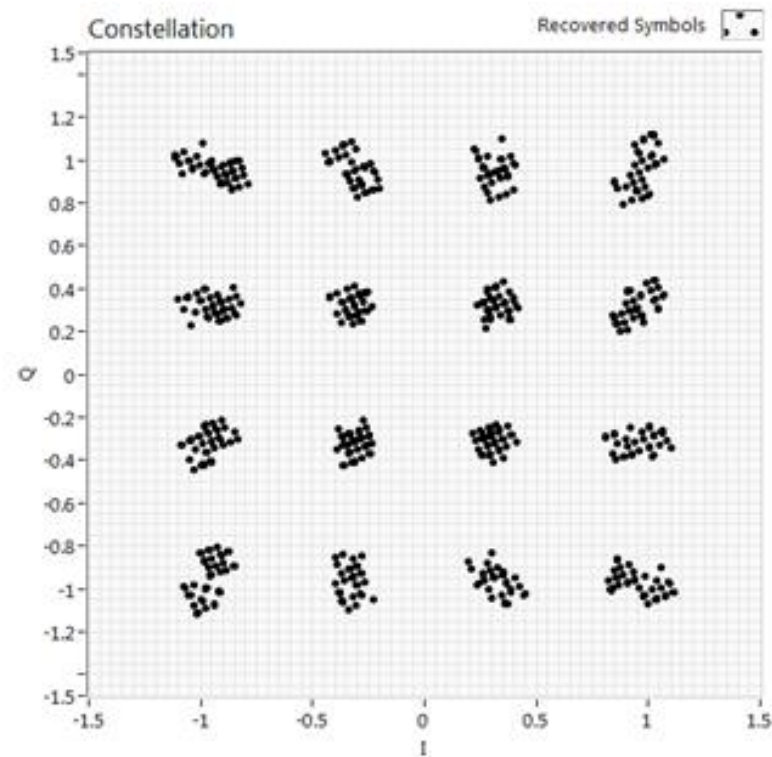
$I+Q$



Modulation in I/Q Plots



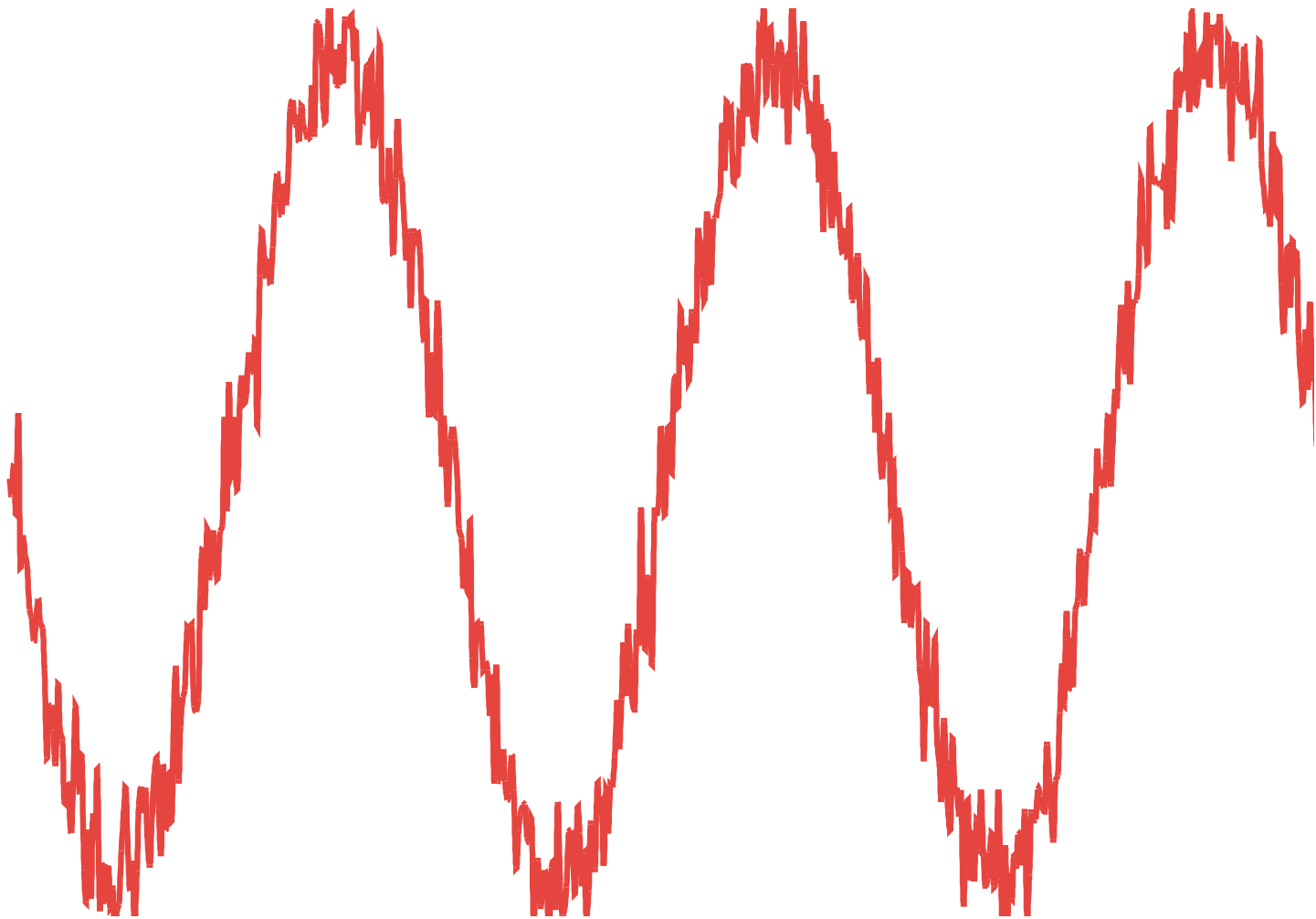
Example measurements from 16-QAM



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



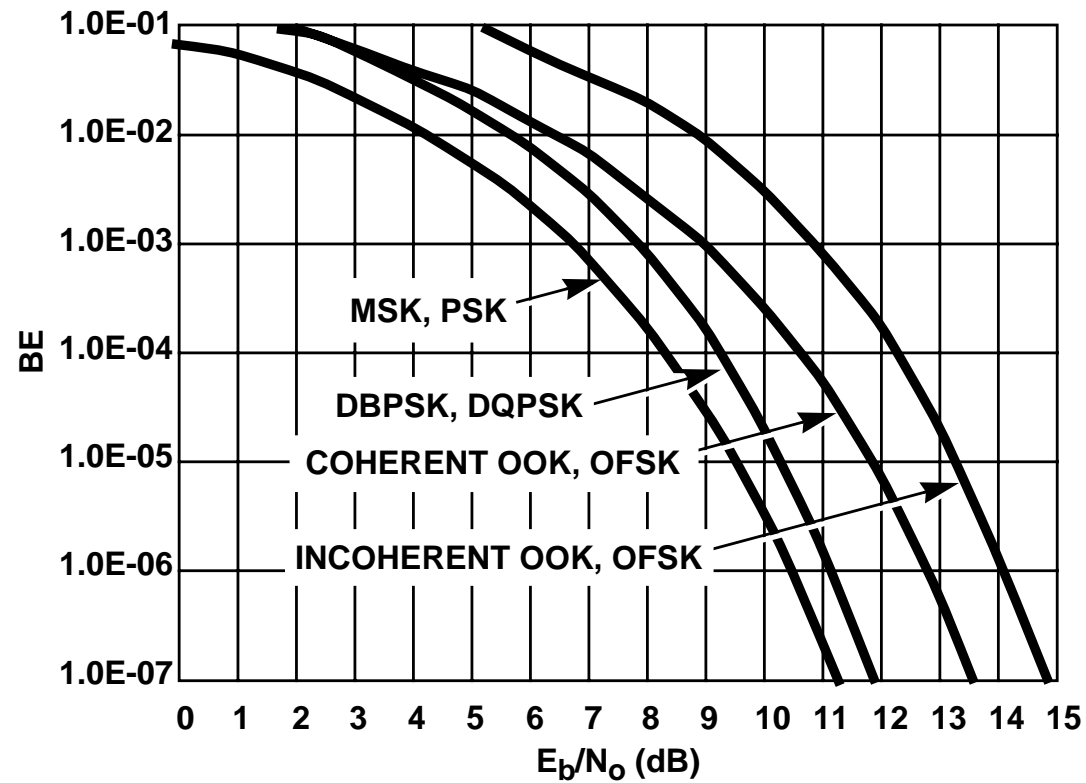
SINR

- **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

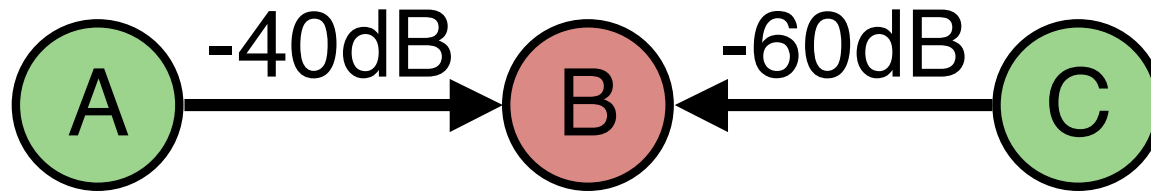
Example Theoretical Bit Error Rates



Variable Bit Rates

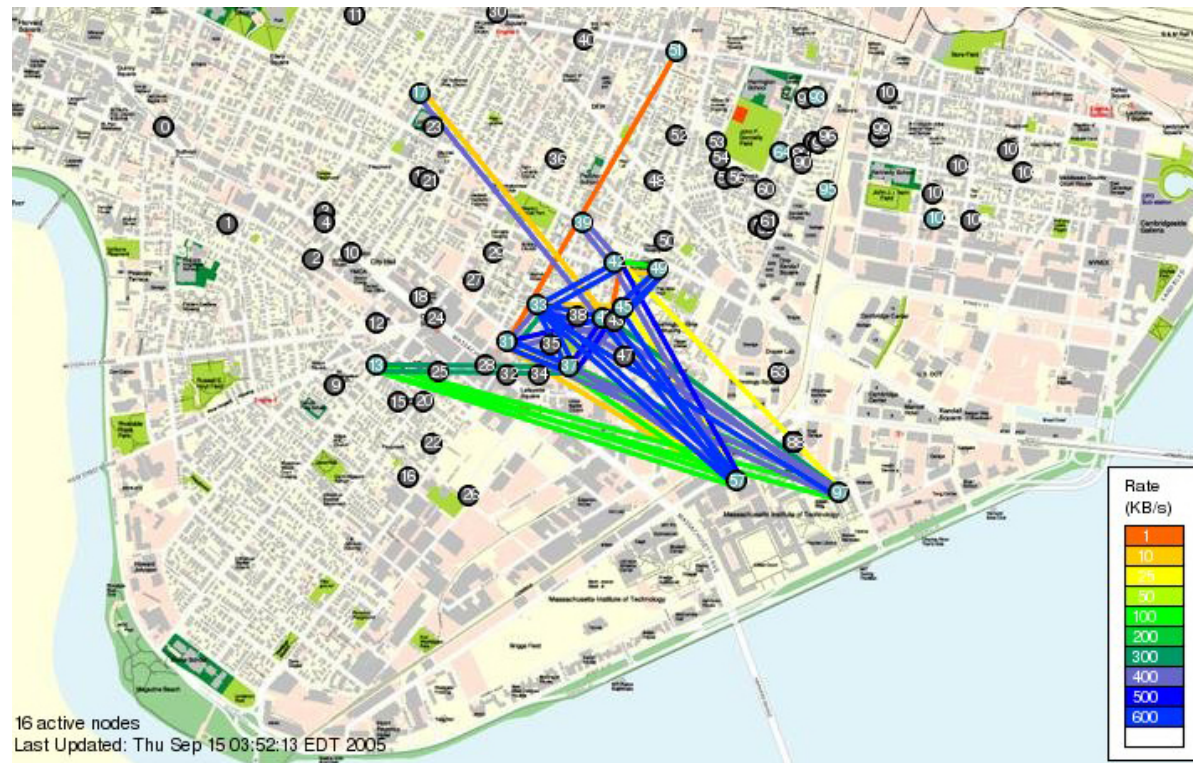
- 802.11b supports 1, 2, 5.5, and 11Mbps
- 2, 5.5Mbps and 11Mbps are QPSK
- To support this, the signal field says what the data rate is
 - 00001010: 1Mbps (11 chips/bit, barker code)
 - 00010100: 2Mbps (11 chips/bit, barker code)
 - 00110111: 5.5Mbps (2 chips/bit, CCK)
 - 01101110: 11Mbps (1 chip/bit, CCK)
- So the header is still at 1Mbps, even if the data is at 11Mbps

Collisions are not so simple

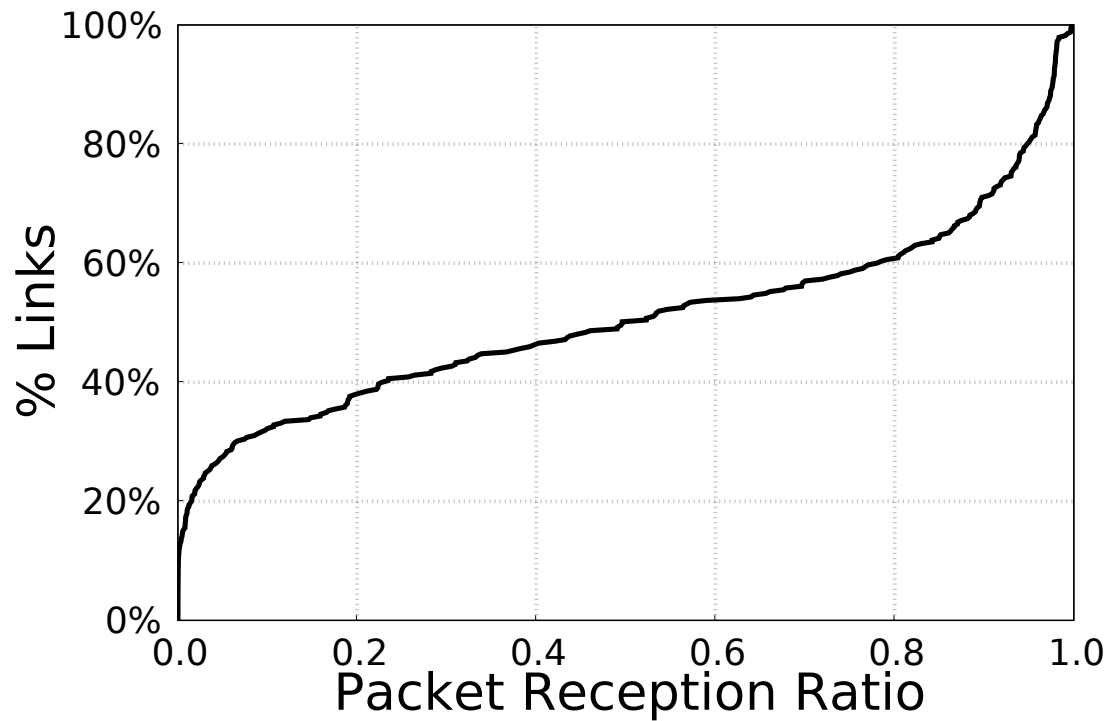


- If A transmits first, B can still decode its packet
- If C transmits first, A will corrupt its packet and B can't decode C's packet
- What if AB and BC are both -60dB?
- Signal strength matters: this is the RF capture effect

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

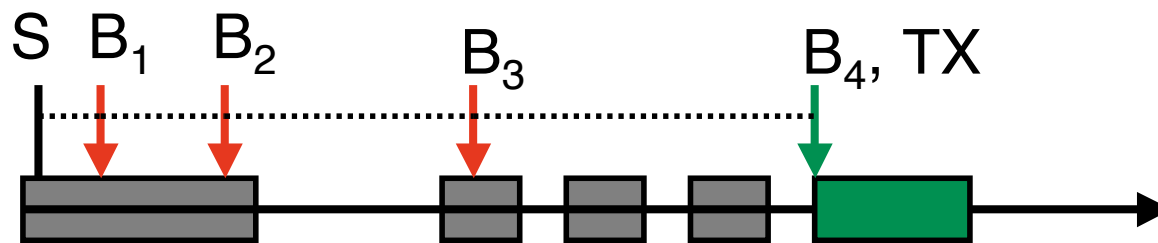
- Arbitrate control of the channel
- One node should be able to use 100%
- Multiple nodes should get a fair share
- Want high utilization under contention

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**

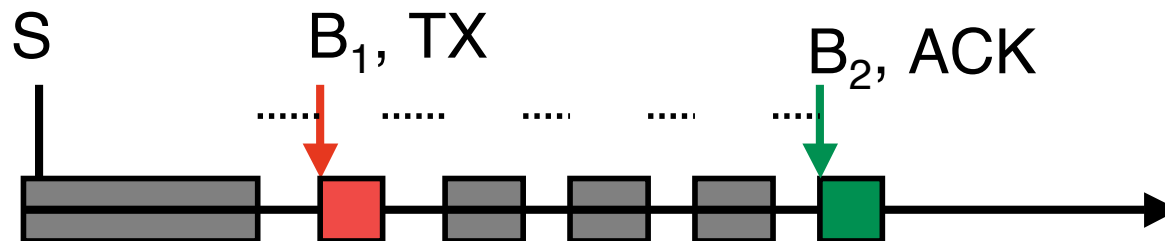
Simple MAC: CSMA/CA

- 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

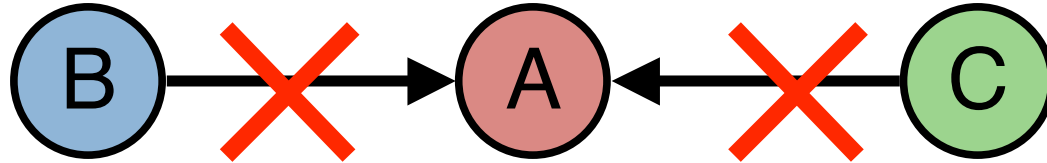
- Maintain a waiting counter c
- For each time step channel is idle, $c - 1$
- When $c = 0$, transmit
- If packet is not acknowledged (layer 2), pick a new, larger c
 - Use lack of layer 2 ack as collision detect



Problems with CSMA/CA

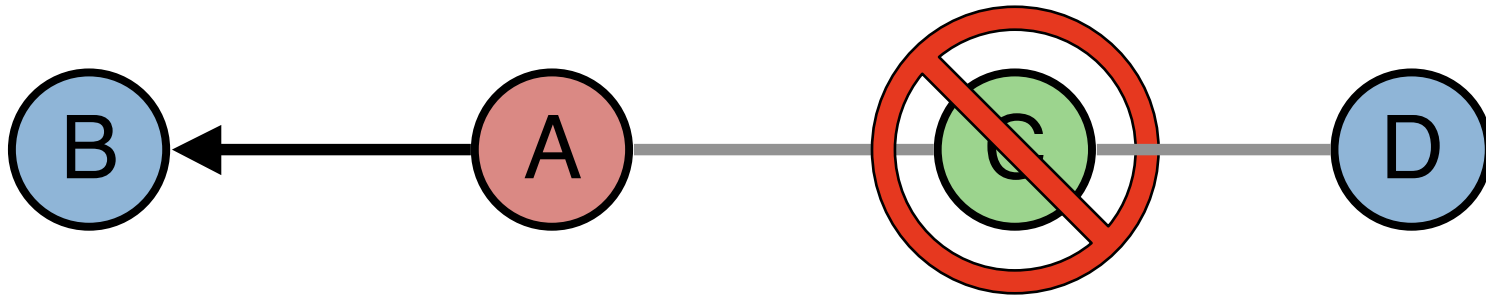
- **Want to know state of channel at receiver, not transmitter**
- **But wireless is not transitive!**
 - A hears B
 - A hears C
 - B and C may not hear each other
 - B and C can only sense their channel, but need to know if A's channel is clear

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

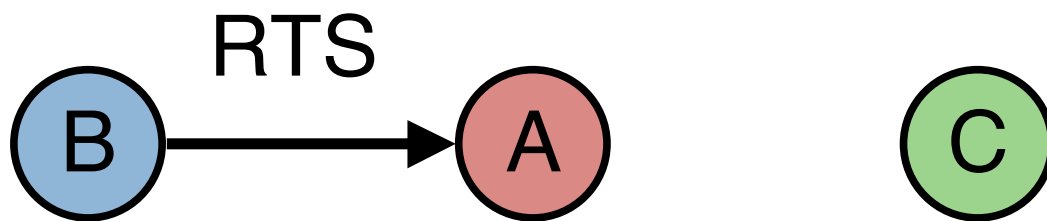


- A transmits to B
- C hears the transmission, backs off, even if it wants to transmit to D
- C is an *exposed* terminal to A's transmission

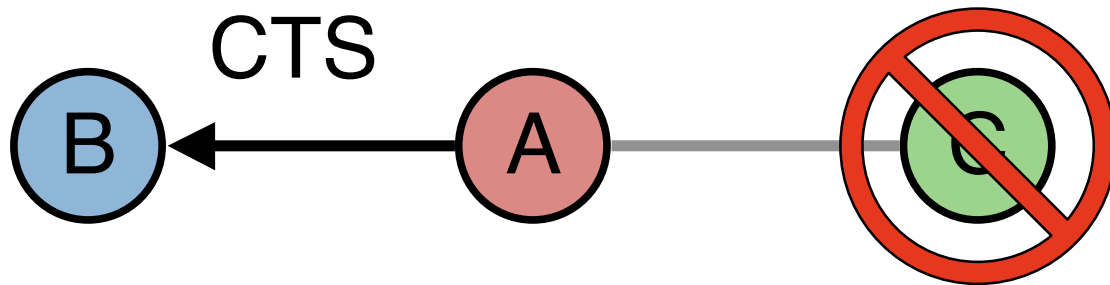
RTS/CTS

- 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

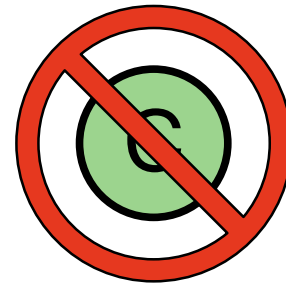
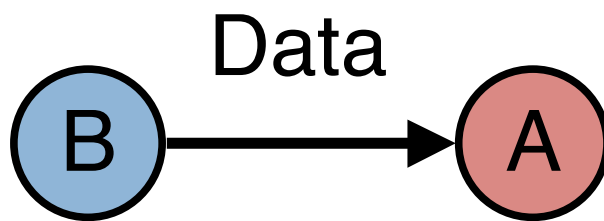
RTS



CTS



Data

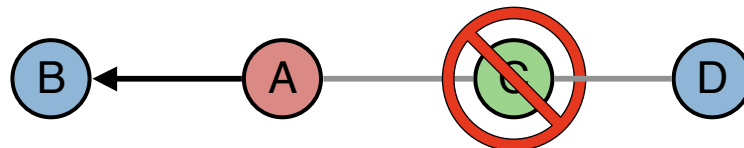


Network Allocation Vector (NAV)

- 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***

Association Continued

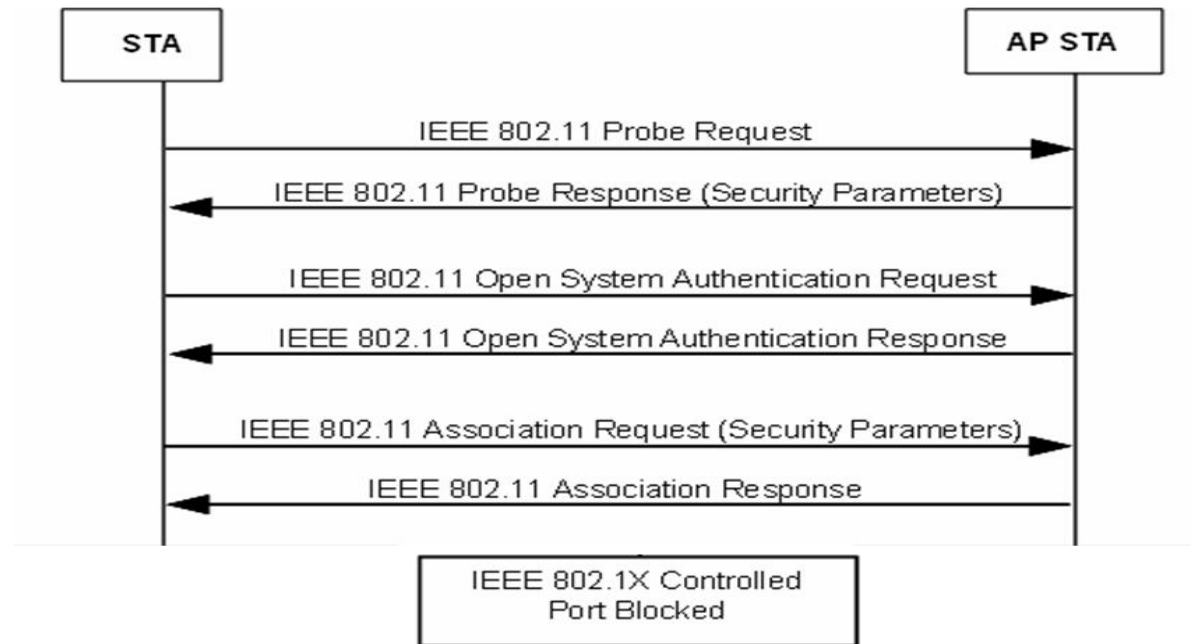
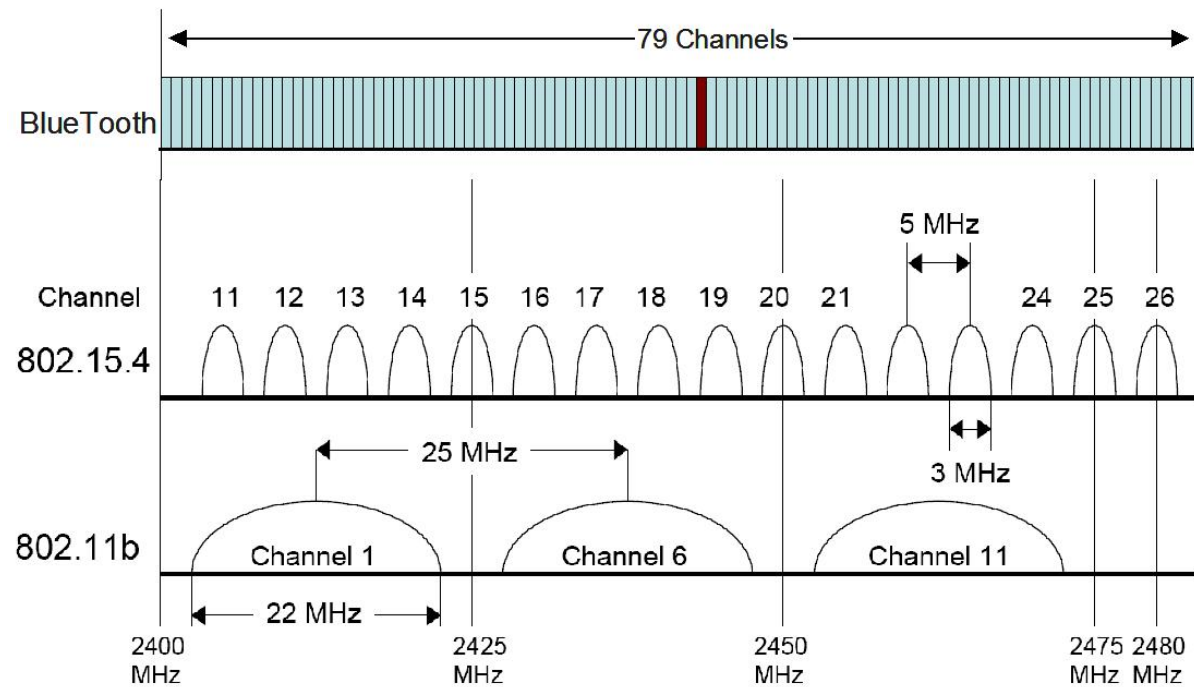


Figure 5-11—Establishing the IEEE 802.11 association

2.4GHz Band



Wireless Routing

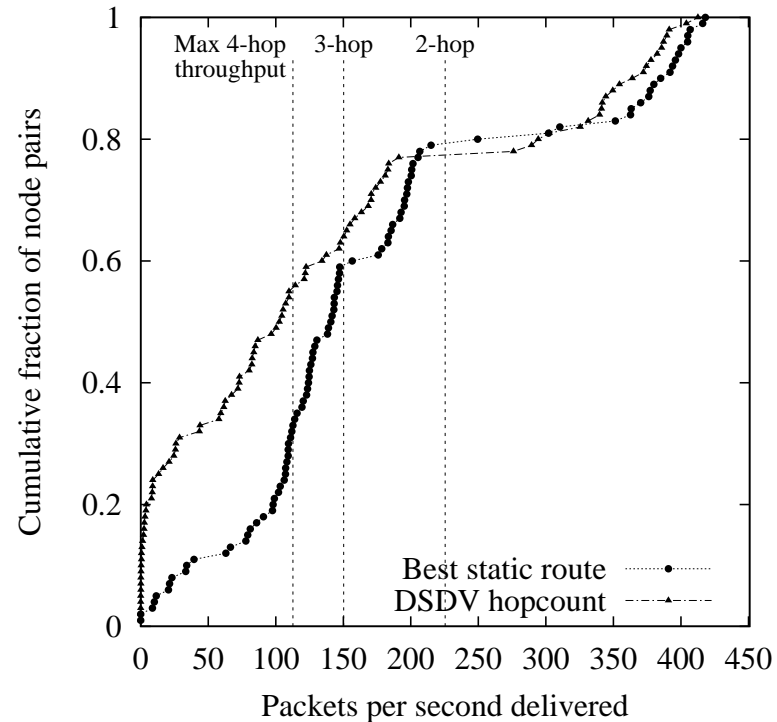
Wireless Routing

- 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

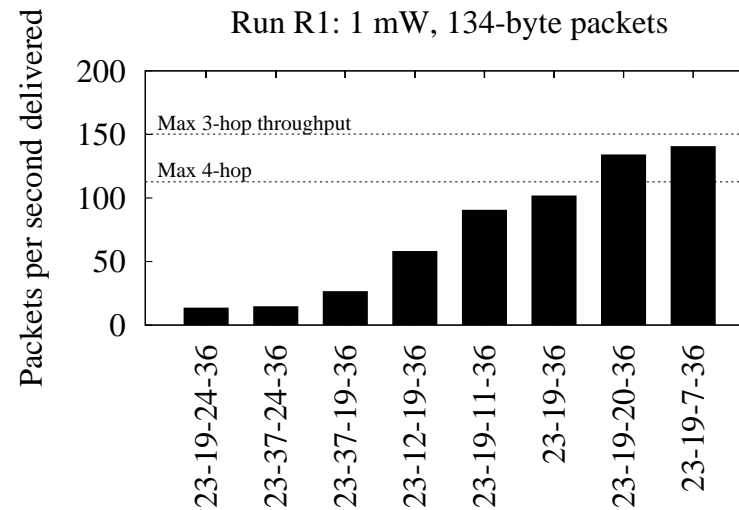
- **Minimizing hopcount causes protocol to choose long links**
- **Links are more likely to be on edge of SNR/PRR curve**
 - Less stable
 - Require more maintenance
- **One way wireless routing is different**
- **OLSRv2 adds the concept of link metrics**

DSDV and Hopcount on Roofnet



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

Variations Across Hopcounts

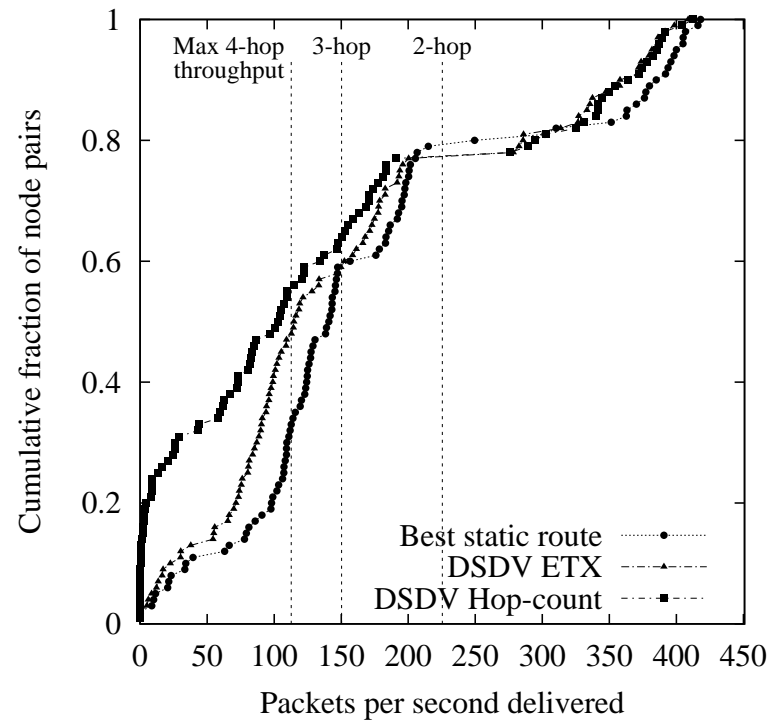


- From DeCouto et al., “A High-Throughput Path Metric for Multi-Hop Wireless Routing.”

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

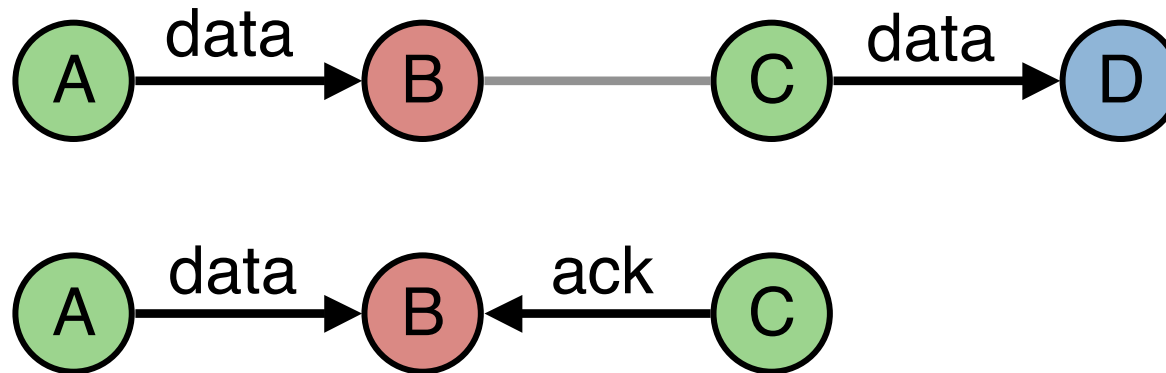
- 802.11b supports four different bit rates
- ETX can select the route, but not the bitrate
- One packet at 11Mbps \neq one packet at 1Mbps
- **Solution: Estimated Time of Transmission (ETT)**
 - Probe at different bit rates
 - Choose link bit rate based on minimum cost

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