## EE 122: Wireless Networks

Ion Stoica  
TAs: Junda Liu, DK Moon, David Zats  
[http://inst.eecs.berkeley.edu/~ee122/fa09](http://inst.eecs.berkeley.edu/~ee122/fa09)  
(Materials with thanks to Vern Paxson, Jennifer Rexford, and colleagues at UC Berkeley)

---

### Announcements

- Project 2, part 1 (checkpoint) due Monday (November 16) by midnight
- No lecture Wednesday, November 11

---

### Wired Communication

**Pros**
- Very reliable
  - For Ethernet, medium **HAS TO PROVIDE** a Bit Error Rate (BER) of $10^{-12}$ (one error every one trillion bits!)
  - Insulated wires; wires placed underground and in walls
  - Error Correction Techniques
- Very high transfer rates
  - Up to 100-Gbit/s or more
- Long distance
  - Up to 40km (~25 miles) in 10-Gbit/s Ethernet (cutting edge)

**Cons**
- Expensive to set up infrastructure
- **Infrastructure is fixed once set up**
- No mobility

---

### Wireless Communication

**Pros**
- Allows mobility
- **Much cheaper and easier to deploy, change, and upgrade!**

**Cons**
- Exposed (unshielded) medium
- Susceptible to physical phenomena (interference)
- Variable BER -- Error correction may not suffice in all cases
- Slower data rates for wider distances
- OSI layered stack designed for wired medium
- Difficult to “hide” underlying behavior
- Security: anyone in range hears transmission
Goals for Today’s Lecture

- Characteristics of Wireless Media
- 802.11 Architecture and Media Access Control Protocol
- Collision Detection vs. Collision Avoidance
  - Hidden Terminal and Exposed Terminal Problem
  - Request To Send (RTS) / Clear To Send (CTS) mechanism
- Multihop Wireless Networks
  - TCP over Multihop Networks
- Wireless Security

Wireless Communication Standards (Alphabet Soup)

- Cellular
  - 2G: GSM (Global System for Mobile communication), CDMA (Code Division Multiple Access)
  - 3G: CDMA2000
- IEEE 802.11
  - A: 5.0Ghz band, 54Mbps (25 Mbps operating rate)
  - B: 2.4Ghz band, 11Mbps (4.5 Mbps operating rate)
  - G: 2.4Ghz, 54Mbps (19 Mbps operating rate)
  - Other versions to come
- IEEE 802.15 – lower power wireless
  - 802.15.1: 2.4Ghz, 2.1 Mbps (Bluetooth)
  - 802.15.4: 2.4Ghz, 250 Kbps (Sensor Networks)

Wireless Link Characteristics

(Figure Courtesy of Kurose and Ross)

- Path loss
  - Signal attenuation as a function of distance
- Signal-to-noise ratio (SNR—Signal Power/Noise Power) decreases, make signal unrecoverable
- Multipath Propagation
  - Signal reflects off surfaces, effectively causing self-interference
- Interference from other sources
  - Internal Interference
    - Hosts within range of each other collide with one another’s transmission (remember Aloha)
  - External Interference
    - Microwave is turned on and blocks your signal
**Path Loss**

- Signal power attenuates by about $\sim r^2$ factor for omni-directional antennas in free space
  - Where $r$ is the distance between the sender and the receiver
- The exponent in the factor is different depending on placement of antennas
  - Less than 2 for directional antennas
  - Faster Attenuation
    - Exponent greater than 2 when antennas are placed on the ground
    - Signal bounces off the ground and reduces the power of the signal

**Multipath Effects**

- Signals bounce off surface and interfere with one another
- What signals are out of phase?
  - Orthogonal signals cancel each other and nothing is received!

---

**A Wireless Link?**
(courtesy of Gilman Tolle and Jonathan Hui, ArchRock)

---

**A Wireless Link!**
(courtesy of Gilman Tolle and Jonathan Hui, ArchRock)
The Amoeboid “cell” (courtesy of David Culler, UCB)

Wireless Bit Errors

- The lower the SNR (Signal/Noise) the higher the Bit Error Rate (BER)
- How can we deal with this?
  - Make the signal stronger
- Why is this not always a good idea?
  - Increased signal strength requires more power
  - Increases the interference range of the sender, so you interfere with more nodes around you
- Error Correction schemes can correct some problems

802.11 Architecture

- Designed for limited geographical area
- AP’s (Access Points) are set to specific channel and broadcast beacon messages with SSID and MAC Address periodically
- Hosts scan all the channels to discover the AP’s
  - Host associates with AP (actively or passively)

Ethernet vs 802.11

- Wireless MAC design
  - Why not just use Ethernet algorithms?
    - Ethernet: one shared “collision” domain
  - It’s technically difficult to detect collisions
    - Collisions are at receiver, not sender
  - … even if we could, it wouldn’t work
    - Different transmitters have different coverage areas
  - In addition, wireless links are much more prone to loss than wired links
  - Carrier Sense (CSMA) is OK; detection (CD) is not
Hidden Terminals

- A and C can both send to B but can’t hear each other
  - A is a hidden terminal for C and vice versa
- CSMA/CD will be ineffective – need to sense at receiver

Exposed Terminals

- Exposed node: B sends a packet to A; C hears this and decides not to send a packet to D (despite the fact that this will not cause interference)!

CSMA/CA: CSMA w/ Collision Avoidance

- Since we can’t detect collisions, we try to avoid them
- When medium busy, choose random interval (contention window)
  - Wait for that many idle timeslots to pass before sending
- When a collision is inferred, retransmit with binary exponential backoff (like Ethernet)
  - Use ACK from receiver to infer “no collision”
  - Use exponential backoff to adapt contention window

5 Minute Break

Questions Before We Proceed?
Multiple Access with Collision Avoidance (MACA)

- Before every data transmission
  - Sender sends a Request to Send (RTS) frame containing the length of the transmission
  - Receiver respond with a Clear to Send (CTS) frame
  - Sender sends data
  - Receiver sends an ACK; now another sender can send data
- When sender doesn’t get a CTS back, it assumes collision

MACA, con’t

- If other nodes hear RTS, but not CTS: send
  - Presumably, destination for first sender is out of node’s range …
- … Can cause problems when a CTS is lost
- When you hear a CTS, you keep quiet until scheduled transmission is over (hear ACK)

MACA = Multiple Access with Collision Avoidance
Overcome exposed/hidden terminal problems with contention-free protocol

1. B sends to C Request To Send (RTS)
2. A hears RTS and defers (to allow C to answer)
3. C replies to B with Clear To Send (CTS)
4. D hears CTS and defers to allow the data
5. B sends to C
1. B sends to A Request To Send (RTS)
2. C hears RTS and defers (to allow A to answer)
3. A replies to B with Clear To Send (CTS); C doesn’t hear
4. C sends to D Request To Send (RTS); B sends to A
5. D replies to C with Clear To Send (CTS)
6. C sends to D

---

**802.11 Stack View**

<table>
<thead>
<tr>
<th>MAC</th>
<th>802.11</th>
<th>802.11b</th>
<th>802.11a</th>
<th>802.11g</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHY</td>
<td>2 Mbps S-Band ISM FHSS</td>
<td>11 Mbps S-Band ISM DSSS</td>
<td>54 Mbps C-Band ISM OFDM</td>
<td>54 Mbps S-Band ISM OFDM</td>
</tr>
</tbody>
</table>

- CSMA/CA runs over the 802.11 physical layer
- Link-level acknowledgements for every frame sent

---

**Link-Layer Acknowledgements**

- Receiver acks every data packet
- If ACK is lost, source tries again until a maximum retransmission number is reached

---

**Channelization of spectrum**

- Typically, available frequency spectrum is split into multiple channels
- Some channels may overlap

<table>
<thead>
<tr>
<th>26 MHz</th>
<th>100 MHz</th>
<th>200 MHz</th>
<th>150 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>915 MHz</td>
<td>2.45 GHz</td>
<td>5.25 GHz</td>
<td>5.8 GHz</td>
</tr>
<tr>
<td>250 MHz</td>
<td>500 MHz</td>
<td>1000 MHz</td>
<td></td>
</tr>
<tr>
<td>24.125 GHz</td>
<td>61.25 GHz</td>
<td>122.5 GHz</td>
<td></td>
</tr>
</tbody>
</table>
Preventing Collisions Altogether

- Frequency Spectrum partitioned into several channels
  - Nodes within interference range can use separate channels
  - Now A can send B while C sends to D without any interference!
  - Aggregate Network throughput doubles

Using Multiple Channels

- 802.11: AP’s on different channels
  - Usually manually configured by administrator
  - Automatic Configuration may cause problems
- Most cards have only 1 transceiver
  - Not Full Duplex: Cannot send and receive at the same time
- Multichannel MAC Protocols
  - Automatically have nodes negotiate channels
  - Channel coordination amongst nodes is necessary
  - Introduces negotiation and channel-switching latency that reduce throughput

Wireless Multihop Networks

- Vehicular Networks
  - Delay Tolerant (batch) sending over several hops carry data to a base station
- Common in Sensor Network for periodically transmitting data
  - Infrastructure Monitoring
    - E.g., structural health monitoring of the Golden Gate Bridge
- Multihop networking for Internet connection sharing
  - Routing traffic over several hops to base station connected to Internet
  - E.g., Meraki Networks

Large Multihop Network
(courtesy of Sanjit Biswas, MIT)
Multi-Hop Wireless Ad Hoc Networks
(Courtesy of Tianbo Kuang and Carey Williamson University of Calgary)

Multi-Hop Wireless Ad Hoc Networks

Multi-Hop Wireless Ad Hoc Networks
(Assume ideal world.)

Multi-Hop Wireless Ad Hoc Networks
Multi-Hop Wireless Ad Hoc Networks

Problem 1: node A can’t use both of these links at the same time
- shared wireless channel
- transmit or receive, but not both
(Reality check…)

Problem 2: S and B can’t use both of these links at the same time
- range overlap at A
- “hidden node” problem
- “exposed node” problem

Problem 3: LOTS of contention for the channel
- in steady state, all want to send
- need RTS/CTS to resolve contention

RTS: Request-To-Send
CTS: Clear-To-Send
Problem 4: TCP uses ACKS to indicate reliable data delivery.
- bidirectional traffic (DATA, ACKS)
- even more contention!!!
Multi-Hop Wireless Ad Hoc Networks

73

Multi-Hop Wireless Ad Hoc Networks

74

Multi-Hop Wireless Ad Hoc Networks

75

Multi-Hop Wireless Ad Hoc Networks

76
Summary

- Wireless connectivity provides a very different set of tradeoffs from wired
  - Much greater ease of deployment
  - Mobility
  - But: unprotected physical signaling
  - Complications due to interference, attenuated range
  - Leading to much more frequent loss
- Hidden terminal and Exposed terminal problems motivate need for a different style of Media Access Control: CSMA/CA
- Multihop provides applications to sensornets, citynets
  - But additional complications of routing, contention
- Wireless devices bring new security risks
- Next lecture: Quality of Service