• Watch Chris Popp’s tutorial of content distribution:
  – http://www.youtube.com/watch?v=gZz87tOLNGQ

• Any questions on course content?
Token Bucket Filters

Data

Token Bucket Capacity, B

r tokens/sec

Each byte needs a token in order to pass

Dropping Filter: drops packets if token is not available

Buffered Filter: buffers data until tokens become available
Token Bucket Operation

- **Tokens**
  - Overflow
  - Buffer tokens up to capacity of bucket

- **Tokens**
  - Packet
  - Enough tokens $\rightarrow$ packet goes through, tokens removed

- **Tokens**
  - Packet
  - Not enough tokens $\rightarrow$ wait for tokens to accumulate
Token Bucket Filters

- **Question**
  - Given a finite length data stream, will it be affected by a token bucket filter?

  Not if during every time interval, the number of bytes is less than or equal to $B + rt$, where $t$ is the length of the interval.

- Given a token rate $r$ and a finite data trace, how can the minimum token bucket size $B$ be found such that there is no packet loss?
Token Bucket Filters

- Given a token rate $r$ and a finite data trace, how can the minimum token bucket size $B$ be found such that there is no packet loss?

  - Simply observe the maximum buffer size
    - If the buffer is truncated to size $B$, then the number of empty buffer positions is equivalent to the number of tokens in an $(r, B)$ token bucket filter
Token Bucket Filters

- The number of empty buffer positions for buffer size $B$ and a constant rate server is equivalent to the number of tokens in an $(r,B)$ token bucket filter.

![Graph showing units of traffic over time and queue length for constant rate server with tokens left in bucket if $B = 500$.]
Token Bucket Filters

- $r = 15$ kbps

- What is the minimum size of $B$ required so that the filter lets the stream pass with no loss or delay?
Token Bucket Filters

- \( r = 15 \text{ kbps} \)

- \( \text{Min } B = (40 - 15) \times 20 + (50 - 15) \times 10 - (15 - 10) \times 20 + (20 - 15) \times 40 = 950 \text{ bits} \)
Token Bucket Filters

- What is the minimum $B$ needed for arbitrary $r > 0$
  - If $r \geq 50$
    $B = 0$
  - If $50 > r \geq 40$
    $\text{Min } B = (50 - r) \times 10$
  - If $40 > r \geq 20$
    $\text{Min } B = (40 - r) \times 20 + (50 - r) \times 10$
  - If $20 > r \geq 10$
    $\text{Min } B = (40 - r) \times 20 + (50 - r) \times 10 - (r - 10) \times 20 + (20 - r) \times 40$
  - If $10 > r \geq 0$
    $\text{Min } B = (40 - r) \times 20 + (50 - r) \times 10 + (10 - r) \times 20 + (20 - r) \times 40$
Wireless Networking

CS/ECE 438: Communication Networks
Prof. Matthew Caesar
May 5, 2010
Wired Communication

• Pros
  – Very reliable
    • For Ethernet, medium HAS TO PROVIDE a Bit Error Rate (BER) of $10^{-12}$ (one error for every 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 physical 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)
• Multihop Wireless Networks
  – Sensor 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 6.2 ♦ Link characteristics of selected wireless network standards
Other Wireless Link Characteristics

• 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 Amoeboed “cell”
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
- APs (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 APs
  - 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
• 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
Exposure 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!)
Since we can’t detect collisions, we try to avoid them.

When medium is 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.
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 responds 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
• If other nodes hear RTS, but not CTS: send
  – Presumably, destination for first sender is out of node’s range...
• 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)
RTS / CTS Protocols (MACA)

- MACA = Multiple Access with Collision Avoidance
- Overcome exposed/hidden terminal problems with contention-free protocol
  1. B stimulates C with 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
### 802.11 Stack View

<table>
<thead>
<tr>
<th>MAC</th>
<th>CSMA/CA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PHY</strong></td>
<td><strong>802.11</strong></td>
</tr>
<tr>
<td>2 Mbps</td>
<td>11 Mbps</td>
</tr>
<tr>
<td>S-Band ISM FHSS</td>
<td>S-Band ISM DSSS</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

*Figure 6.10* 802.11 uses link-layer acknowledgments.
Channelization of spectrum

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

- Frequency Spectrum partitioned into several channels
  - Nodes within interference range can use separate channels
  - Now A can send to 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

(Assume ideal world...)

1 2 3 4 5 6 7 8 9 10 11 12

S A B C D R
Multi-Hop Wireless Ad Hoc Networks
Multi-Hop Wireless Ad Hoc Networks

(Reality check...)

Problem 1: node A can’t use both of these links at the same time
- shared wireless channel
- transmit or receive, but not both
Multi-Hop Wireless Ad Hoc Networks

Problem 2: can’t use both of these links at same time
- range overlap at A
- “hidden node” problem
- “exposed node” problem
Multi-Hop Wireless Ad Hoc Networks

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
Multi-Hop Wireless Ad Hoc Networks

Problem 4: TCP uses ACKS to indicate reliable data delivery
- bidirectional traffic (DATA, ACKS)
  - even more contention!!!
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
Final Words
What Remains

• Final Exam
  – May 10, 7-10pm, rooms 1105 and 1111 SC

• Homework 7
  – Due at final exam
Where to go from here?

- CS 425: Distributed systems
  - Focus on applications, distributed algorithms

- CS 538 (listed as CS 598: Advanced Networking)
  - Graduate version of this class

- Undergraduate research
  - Hands-on experience, show you can complete a major project
  - Create your own innovations!
Where to go from here?

- CS 461/463
  - Computer security (including network security)

- Chat with me anytime