Lecture 17 Overview

- Project discussion
- Intro to 802.11 WiFi
- Jigsaw discussion
Project update

- Second checkpoint due Tonight
  - 1-2 page summary of your progress since last checkpoint

- Project presentations Thursday 3/21
  - Sign up for a 25-minute slot between 8:00am and 3:05pm
    - 20 minute presentation (including all project members)
    - 3-4 minutes for questions
  - You will be expected to attend at least 3 presentations and actively participate in discussion

- Reports due Friday 3/22 by midnight
IEEE 802.11 Infrastructure

mobile terminal

fixed terminal

application
TCP
IP
LLC
802.11 MAC
802.11 PHY

access point

infrastructure network

application
TCP
IP
LLC
802.3 MAC
802.3 PHY
802.3 MAC
802.3 PHY
802.11 Physical Layers

- **802.11b - 2.4 GHz ISM band**
  - FHSS (Frequency hopping spread spectrum); deprecated
  - DSSS (Direct sequence spread spectrum)
  - Up to 11 Mbps

- **802.11a/g - 2.4 GHz ISM band / 5.0 GHz UNII band**
  - OFDM (Orthogonal frequency domain multiplexing)
  - Up to 54 Mbps

- **802.11n – 2.4/5.0 GHz bands**
  - Adds MIMO and other tricks to 802.11g
  - Up to 300-500 Mbps!

- Each backwards compatible with the previous ones
IEEE 802.11b

- Data rate
  1, 2, 5.5, 11 Mbit/s
  User data rate max. approx. 6 Mbit/s

- Transmission range
  300m outdoor, 30m indoor
  Max. data rate ~10m indoor

- Frequency
  Free 2.4 GHz ISM-band
**CSMA:** listen before transmit

- If channel sensed idle: transmit entire packet
- If channel sensed busy, defer transmission
  - Persistent CSMA: retry immediately with probability $p$ when channel becomes idle (may cause instability)
  - Non-persistent CSMA: retry after random interval

- But what about collisions?
CSMA/CA

- Impossible to hear collision w/half-duplex radio

- Wireless MAC protocols often use collision avoidance techniques, in conjunction with a (physical or virtual) carrier sense mechanism

- Collision avoidance
  - Nodes negotiate to reserve the channel.
  - Once channel becomes idle, the node waits for a randomly chosen duration before attempting to transmit.
Hidden Terminal Problem

- B can communicate with both A and C
- A and C cannot hear each other

**Problem**
- When A transmits to B, C cannot detect the transmission using the **carrier sense** mechanism
- If C transmits, collision will occur at node B

**Solution**
- Hidden sender C needs to defer
When A wants to send a packet to B, A first sends a Request-to-Send (RTS) to B.

On receiving RTS, B responds by sending Clear-to-Send (CTS), provided that A is able to receive the packet.

When C overhears a CTS, it keeps quiet for the duration of the transfer.

Transfer duration is included in both RTS and CTS.
Backoff Interval

- **Problem:** With many contending nodes, RTS packets will frequently collide

- **Solution:** When transmitting a packet, choose a backoff interval in the range $[0, CW]$
  - $CW$ is contention window

- Wait the length of the interval when medium is idle
  - Count-down is suspended if medium becomes busy
  - Transmit when backoff interval reaches 0

- Need to adjust $CW$ as contention varies
Jigsaw: What Really Happens

- Measure real large wireless networks
  - Collect every possible information
    » PHY/Link/IP/TCP/App layer trace
    » Collect every single wireless packet
  - Need many sniffers for 100% coverage
- Automatically merge traces
  - Global view of wireless networks across time, locations, channels, and protocol layers
  - Enables manual and automatic diagnosis
Our lab: EBU3b

- 150k square feet
  - 4 floors
- 500+ occupants
  - 150 faculty/staff
  - 350 students
- Building-wide WiFi
  - 39 access points
  - 802.11b/g
    » Channel 1, 6, 11
  - 10 – 90 active clients anytime
  - Daily Traffic ~5GB

CSE 222A – Lecture 17: Wireless Networking
Jigsaw Deployment

- Overlays existing WiFi network
  - Series of passive sniffers
  - Blanket deployment over 4 floors
- 39 sensor pods (156 radios)
  - 4 radios per pod, cover all channels in use
  - Captures all 802.11 activities
    - Including CRC/PHY events
  - Stream back over wired network to centralized storage
Frames carry TSF time-stamps
Need a global clock
Estimate the offset between TSF and the global clock for each sniffer
Synchronization

- Create a virtual global clock
  - To keep unification working
  - Critical evidence for analysis
    » If A and B are transmitting at the same time they could interfere
    » If A starts transmitting after B has started then A can’t hear B

- Require fine time-scales (10-50us)
  - NTP is +100 usec accuracy
  - 802.11 HW clocks (TSF) have 100PPM stability

CSE 222A – Lecture 17: Wireless Networking
Ideal Unification

CSE 222A – Lecture 17: Wireless Networking
Real Unification

CSE 222A – Lecture 17: Wireless Networking
Challenge: sync at large-scale

● How to bootstrap?
  ◆ Goal: estimate the offset between TSF and the global clock for each sniffer
  ◆ Time reference from one sniffer to the other

● Sync across channels
  ◆ Dual radios on same sniffer slaved to same clock (creates a de facto time linkage)

● Manage TSF clock skews
  ◆ Continuously re-adjust offsets when merging frames
Jigsaw in Action

- Jigsaw merges 156 traces into one global trace
- Covers 99% of AP frames, 96% of client frames

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Starts</td>
<td>Jan 24, 2006 (Tuesday)</td>
</tr>
<tr>
<td>Duration</td>
<td>24 hr</td>
</tr>
<tr>
<td>Total APs</td>
<td>107 (39 CSE)</td>
</tr>
<tr>
<td>CSE Clients</td>
<td>1026</td>
</tr>
<tr>
<td>Active CSE clients anytime</td>
<td>10 - 90</td>
</tr>
<tr>
<td>Total Events</td>
<td>2,700M</td>
</tr>
<tr>
<td>PHY/CRC Errors</td>
<td>48%</td>
</tr>
<tr>
<td>Valid Frames</td>
<td>52%</td>
</tr>
<tr>
<td>JFrames</td>
<td>530M</td>
</tr>
<tr>
<td>Events per Jframe</td>
<td>2.97</td>
</tr>
</tbody>
</table>

CSE 222A – Lecture 17: Wireless Networking
Jigsaw syncs 99% frames < 20us

- Measure sync. quality by max dispersion per Jframe

- 20 us is important threshold
  - 802.11 back-off time is 20us
  - 802.11 inter frame time is 50 us
  - Sufficient to infer many 802.11 events

CSE 222A – Lecture 17: Wireless Networking
Hidden Terminals

![Graph showing the relationship between % (s, r) Pairs and Interference Loss Rate.](image-url)
Multi-hop routing

- Identify a route, forward over links
- Abstract radio to look like a wired link
For Next Class...

- Read ExOR paper
- Submit checkpoint by tonight!