Lecture 5: The 802.11 Standard

October 7, 2004
Today's Lecture

All about 802.11

CSMA/CD MAC and DCF

WEP and 802.1x Security
IEEE working group 802.11 formed in 1990

- Now the most popular and pervasive Wireless LAN standard
Infrastructure vs. Independent Mode

**Infrastructure mode:**
All communications must be relayed by access point

**Independent mode:**
Nodes communicate directly with each other
Extended Service Set Model

Entire ESS looks like a single virtual LAN!

Create association

Propagate association information

Distribution system
Extended Service Set Model

Entire ESS looks like a single virtual LAN!

Distribution system

Transmit to node B
Distributed Coordination Function

802.11 uses a variant of CSMA

- Called the Distributed Coordination Function (DCF)
- Access point controls when nodes can transmit.
- No collision detection – rather, collision avoidance (CSMA/CA)

Recall CSMA:

- Before a node transmits, it listens for activity on the network
- If medium is busy, node waits to transmit
- After medium is clear, don't immediately start transmitting...
  - Otherwise all nodes would start talking at the same time!
- Instead, delay a random amount of time (random backoff)
DCF Illustrated

Interframe space (IFS)

Sender
- Channel busy
- Wait
- Backoff
- Transmit
- Backoff
- Transmit

Receiver
- ACK
- ACK

time
Exponential Backoff

ACK-based scheme for reliability

- Receiver sends ACK after each successful transmission
- Sender will retransmit if no ACK is heard, after waiting for a random interval

Binary exponential backoff

- First backoff interval between $[0 \ldots 31]$ time slots
- If collision occurs, new backoff interval chosen between $[0 \ldots 63]$ slots
- Repeat until backoff interval reaches $[0...1023]$ slots.

Why increase the backoff interval each time???
802.11 provides four different interframe spacing times

- Provide different traffic “priorities”

Standard IFS time is the “Distributed IFS” (DIFS)

“Short IFS” (SIFS) used for higher priority frames

- e.g., ACK packets from AP back to a node
  - Allows ACKs to “sneak in” before contention period begins
Long messages broken into multiple *frames*

- Node can transmit next frame in a sequence **immediately** after receiving ACK
- But, must do backoff before sending next *message*

Transmitter “reserves the channel” using request to send (RTS)

- Receiver transmits clear to send (CTS) to initiate transmission of long message
Node C is not aware of Node A's transmissions!

- Collisions can occur at Node B

Solution: Network Allocation Vector (NAV)

- Each message includes length of time other nodes must wait to send
- Node B's CTS to Node A can be heard by Node C
  - *CTS will prevent Node C from transmitting before Node A is done*
# 802.11 Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Frequency</th>
<th>Data rate</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b</td>
<td>2.4 Ghz, DSSS</td>
<td>11 Mbps</td>
<td>~300 feet,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>~100' indoors</td>
</tr>
<tr>
<td></td>
<td><em>Widely deployed and inexpensive</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4 Ghz, O-FDM</td>
<td>54 Mbps</td>
<td>&lt; 802.11b</td>
</tr>
<tr>
<td></td>
<td><em>Backwards compatible with 802.11b</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11a</td>
<td>5 Ghz, O-FDM</td>
<td>54 Mbps</td>
<td>~80 feet</td>
</tr>
<tr>
<td></td>
<td><em>Uses UNII band, products emerging now</em></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
802.11b PHY

Original 802.11 standard used Frequency Hopping, G-FSK
- Divide 2.4 Ghz band into 78 channels, 1 MHz wide
- Dwell time of 390 ms per channel
- 26 different, fixed (globally known) hop sequences

802.11b standardized on DSSS with Q-PSK modulation
- 8-bit Complementary Code Keying (previous lecture)
- Band divided into 14 channels, 5 MHz wide each
  - *However, DSSS energy spread over a 22 MHz band!!!*

- This means that not all channels can be used simultaneously.
802.11 Security: WEP

Wireless networks are inherently a broadcast medium!
- It is easy to intercept transmissions between end hosts
- Compare to wired systems: Must physically tap into the wires
  - *Nightmare for companies: Hacker in the parking lot with a laptop*

Wired Equivalent Privacy (WEP)
- Rather than provide 802.11 with a truly robust security solution, goal was to prevent “casual” snooping
- Problem: WEP was developed from scratch by a closed committee, standard not readily accessible for review by researchers

WEP relies on a secret key being shared by end hosts and APs
- Traffic between nodes is encrypted using this key
- Requires key to be distributed in some fashion by system admins
  - *Makes it very difficult to change the key later!*
WEP Weaknesses

In 2001, researchers at UC Berkeley demonstrated that WEP was vulnerable to a range of attacks

- 40-bit encryption keys are susceptible to brute force attacks
- WEP reuses portions of the random “keystring” making analysis possible
- Attackers can modify contents of frames without necessarily decrypting them

Not long afterwards, WEP cracking software was demonstrated

- Adam Stubblefield, Rice undergrad doing internship at AT&T, wrote the code in less than a week on a Linux laptop
- Open source AirSnort software now widely available
  - Can recover a WEP key after intercepting 5-10 million packets

Bottom line: Don't depend on WEP!

- “WEP is so flawed that it is not worth using in many cases.” -- Matthew S. Gast,
  802.11 Wireless Networks: The Definitive Guide
What to do?

Industry is working on solutions based on new 802.1x standard
• This is not without its problems, however

Better solution: End-to-end security
• Don't depend on underlying network infrastructure to ensure security
• Rather, perform authentication and encryption at the application level

Common solution: SSL/TLS protocol
• Same protocol used by Web browsers to talk to secure Web servers
• Provides a range of authentication and encryption options
• No assumptions about security of the underlying network
Next Lecture

Bluetooth and 802.15.4

Reading: Stallings Chapter 15
  • (No required reading on 802.15.4)