IEEE 802.11 Wireless LANs

Shyam Parekh & Pravin Varaiya
EECS 228A
October 2, 2003
Personal Information

- Background
- shyam@eecs.berkeley.edu
- Office Hours:
  - 463 Cory Hall
  - Tu-Th 4:00-5:00 PM
Gameplan for Remaining Semester

- Shift focus to Networking & Communication Issues
  - IEEE 802.11 Wireless LANs
  - Sensor Networks
  - Congestion Control
  - Traffic Models
- Updated schedule at
  [http://www-inst.eecs.berkeley.edu/~ee228a/228A03/228A03syllabus.htm](http://www-inst.eecs.berkeley.edu/~ee228a/228A03/228A03syllabus.htm)
References

- **802.11 Wireless Networks: The Definitive Guide**, M. Gast, O'Reilly, 2002
- ANSI/IEEE Std 802.11, 1999 Edition
- ANSI/IEEE Std 802.11b-1999
- ANSI/IEEE Std 802.11a-1999
- **Reading suggestions** on the Syllabus page

* The lectures will make liberal use of drawings from the references
IEEE 802 Standards & OSI Model

- Observe 802.11 MAC is common to all 802.11 Physical Layer (PHY) standards
- 802.11 PHY is split into Physical Layer Convergence Procedure (PLCP) and Physical Medium Dependent (PMD) sublayers
Related Standards

- **Bluetooth**
  - Originally intended for interconnecting computing and communication devices

- **HIPERLAN**
  - European standard for Wireless LANs

- **IEEE 802.16 Broadband Wireless**
  - Addresses needs of fixed broadband wireless access replacing fibers, cables, etc.
## 802.11 Standards and Spectrum

<table>
<thead>
<tr>
<th>Key Standards</th>
<th>Max Rate</th>
<th>Spectrum (U.S.)</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>2 Mbps</td>
<td>2.4 GHz</td>
<td>1997</td>
</tr>
<tr>
<td>802.11a</td>
<td>54 Mbps</td>
<td>5 GHz</td>
<td>1999</td>
</tr>
<tr>
<td>802.11b</td>
<td>11 Mbps</td>
<td>2.4 GHz</td>
<td>1999</td>
</tr>
<tr>
<td>802.11g</td>
<td>54 Mbps</td>
<td>2.4 GHz</td>
<td>2003</td>
</tr>
</tbody>
</table>

- 2.4 - 2.5 GHz for all above except 802.11a (referred to as C-Band Industrial, Scientific, and Medical (ISM))
  - Microwave ovens and some cordless phones operate in the same band
- 802.11a uses Unlicensed National Information Infrastructure bands
  - 5.15 - 5.25 GHz
  - 5.25 - 5.35 GHz
  - 5.725 - 5.825 GHz
Basic Service Sets (BSSs)

- Independent BSSs are also referred to as Ad Hoc BSSs
- Observe that the AP in an Infrastructure BSS is the centralized coordinator and could be a bottleneck
Extended Service Set (ESS)

- BSSs in an ESS communicate via Distribution System
- A DS has to keep track of stations within an ESS
- Inter Access Point protocol (IAPP) is not yet standardized
Network Services

- Distribution
- Integration
- Association
- Reassociation
- Disassociation
- Authentication
- Deauthentication
- Privacy
- MAC Service Data Unit (MSDU) delivery
Seamless Transition

- Seamless transition between two BSSs within an ESS
- Between ESSs, transitions are not supported
802.11b: HR/DSSS* PHY

- Use Complementary Cod Keying (CCK) instead of Differential Quadrature Phase Shift Keying (DQPSK) used at low rate (2Mbps) DS
- CCK Primer:
  - Two finite sequences of equal length are complementary if number of pairs of like elements at a given separation in one sequence is equal to the number of pairs of unlike elements at the same separation in the other sequence
  - Such sequences have a property that sum of their autocorrelation sequences is positive for lag 0 and 0 for all other lags
  - This helps in combating multipath interference

*High Rate Direct-Sequence Spread Spectrum
802.11b: HR/DSSS PHY - 2

- 4-bit (for 5.5 Mbps) or 8-bit (for 11 Mbps) symbols form MAC layer arrive at 1.375 million symbols per second
- Each symbol is encoded using CCK code word
  - \{e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_4)}, -e^{j(\phi_1+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_3)}, e^{j(\phi_1+\phi_3)}, -e^{j(\phi_1+\phi_2)}, e^{j\phi_1}\}
  - \phi_1, \phi_2, \phi_3, \text{ and } \phi_4 \text{ are decided by symbol bits}
802.11b: HR/DSSS PHY - 3

- Uses same channels as by the low rate DS
- In US, channels 1-11 (with center frequencies at 2.412 - 2.462 GHz and 5 MHz distance) are available
- For 11 Mbps, Channels 1, 6, and 11 give maximum number of channels with minimum interference
802.11b: HR/DSSS PHY - 4

- Long PLCP format

- Optional Short PLCP format is offered for better efficiency
802.11a: 5 GHz OFDM PHY

- Fundamental Orthogonal Frequency Division Multiplexing (OFDM) work was done in 1960s, and a patent was issued in 1970.
- Basic idea is to use number of subchannels in parallel for higher throughput.
- Will 802.11a be a success?
  - Denser Access Point deployment needed due to higher path loss?
  - Will higher power need be a hindrance?
OFDM is similar to Frequency Division Multiplexing except it does not need guard bands
- But need guard times to minimize inter-symbol and inter-carrier interference
- Relies on “orthogonality” in frequency domain
802.11a: 5 GHz OFDM PHY - 3

- In U.S., there are 12 channels, each 20 MHz wide

- Spectrum layout
802.11a: 5 GHz OFDM PHY - 4

- Each channel is divided into 52 subchannels: 48 are used for data
- PLCP Protocol Data Unit (PPDU) format

- PHY uses rate of 250K symbols per second
- Each symbol uses all 48 channels
- Convolution code is used by all subchannels
Preamble and Frame start
802.11a: 5 GHz OFDM PHY - 6

- **Rate dependent parameters:**

- **64-QAM Constellation**

<table>
<thead>
<tr>
<th>Data rate (Mbits/s)</th>
<th>Modulation</th>
<th>Coding rate (R)</th>
<th>Coded bits per subcarrier (N_{bpsc})</th>
<th>Coded bits per OFDM symbol (N_{bps})</th>
<th>Data bits per OFDM symbol (N_{dps})</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>BPSK</td>
<td>1/2</td>
<td>1</td>
<td>48</td>
<td>24</td>
</tr>
<tr>
<td>9</td>
<td>BPSK</td>
<td>3/4</td>
<td>1</td>
<td>48</td>
<td>36</td>
</tr>
<tr>
<td>12</td>
<td>QPSK</td>
<td>1/2</td>
<td>2</td>
<td>96</td>
<td>48</td>
</tr>
<tr>
<td>18</td>
<td>QPSK</td>
<td>3/4</td>
<td>2</td>
<td>96</td>
<td>72</td>
</tr>
<tr>
<td>24</td>
<td>16-QAM</td>
<td>1/2</td>
<td>4</td>
<td>192</td>
<td>96</td>
</tr>
<tr>
<td>36</td>
<td>16-QAM</td>
<td>3/4</td>
<td>4</td>
<td>192</td>
<td>144</td>
</tr>
<tr>
<td>48</td>
<td>64-QAM</td>
<td>2/3</td>
<td>6</td>
<td>288</td>
<td>192</td>
</tr>
<tr>
<td>54</td>
<td>64-QAM</td>
<td>3/4</td>
<td>6</td>
<td>288</td>
<td>216</td>
</tr>
</tbody>
</table>
OPNET Overview

- Original work at MIT, now maintained and marketed by OPNET Inc.
- Discrete event simulator
- Hierarchical modeling that mimics real life architecture: Network, Node, and Process Layer modeling
- At Process Layer, a finite state machine representation is used for modeling, where state behavior is dictated by C code
- Process models are supplied (open code) for many popular communication protocols
- Decent capabilities for animation, GUI, analysis, debugging, etc.
OPNET Setup

- Installed on Windows machines in 199 Cory
- One modeling and one run-time license available from scotland.cs.berkeley.edu and port_a
- Preferable if individual installations are done on own machines (with remote license server)
  - Installation CDs are available at `\\filestore\software\Opnet`
- For 199 Cory setup or license server issues, contact inst@cory.eecs.berkeley.edu (please keep me in the loop)