DUKING IT on the wireless network

WIRELESS COMMUNICATION CAN BE A BITTER BATTLE, AND IEEE 802.11 IS WELL-ARMED FOR THE JOB. BUT WITH MULTIPLE VERSIONS OF THE STANDARD AND A TURF FIGHT OVER THE 11G EXTENSION, YOU MIGHT WONDER WHETHER CHIP MAKERS ARE STRUGGLING TO DOMINATE THE STANDARD OR TO FORM FLEXIBLE NETWORKS. PUT UP YOUR DUKES AND LOG IN.
IEEE 802.11 does not specify a single method of implementing wireless data communications. Rather, it comprises a family of standards—some ratified and others working their way through the ratification process. The 802.11 Working Group is just one of 16 under the IEEE LMSC’s (LAN/MAN Standards Committee’s) Project 802 (see sidebar “802.map”). The 802.11 WLAN (Wireless LAN) Working Group originally proposed a single MAC (media-access controller) and three PHYs (physical-layer) controllers—two for RF and one for IR. The standard has evolved as a result of lessons learned during early commercialization efforts. The prominent issues that the market feedback stresses are operating range, throughput rate, channel count, security, robustness, and cost. In response, 802.11 has expanded beyond its original 2.4-GHz spectrum and has considered a wider range of modulation schemes than were originally contemplated.

WORKING OUT

Robust wireless-data-communication systems must contend with a number of media-related challenges. Interference is a ubiquitous concern for RF wireless communication—particularly so in unlicensed spectra, such as the 2.4-GHz region that 802.11 and its “b” and “g” extensions target. Additionally, typical WLANs operate in strong multipath environments (Reference 1). Unlike other limitations on a channel, such as bandwidth, transmitting power, or media losses, interference and multipath fading vary significantly as functions of location and time in as little as 1 ft. or tens of milliseconds. Mitigating techniques available to land-line channels, such as controlled impedance links, electrically balanced feeds, cable shields, and twisted pairs, don’t apply to wireless. Instead, network-management protocols and modulation schemes based on statistical methods allow communications channels to operate in the presence of multipath interference and hash-talking contenders for the spectrum. Those contenders comprise like systems—the multiple nodes in an 802.11 network—and unlike systems, such as Bluetooth devices, high-frequency cordless telephones, microwave...
CSMA allows a peer-to-peer multipoint network to manage its own traffic as long as all nodes can sense each other.

802.MAP

The IEEE LAN/MAN (local-area-network/metropolitan-area-network) standards committee, IEEE project 802, comprises 16 working groups, the best known being 802.3—Ethernet and 802.11—Wireless LANs (Table A).

The workgroups develop LAN and MAN standards for the data link and PHYs (physical layers)—the last two layers in the OSI (open systems interconnection) reference model.

Project 802 started 22 years ago as the “Local Network Standards Committee,” with the goal of defining one LAN standard for speeds of 1 to 20 MHz (Reference A). The project defined a PHY, a MAC (media-access control), and a high-level interface, using a bus topology and access method similar to that for Ethernet.

Since then, working groups within project 802 have added other PHYs and MACs. The MACs share a common upper interface to the logical-link-control sublayer. The project also expanded to include MANs, LAN security, and higher data rates. The project is now called the “LAN/MAN standards committee” to reflect its broader scope.

TABLE A—WHO’S WHO IN 802

<table>
<thead>
<tr>
<th>Group number</th>
<th>Working group</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1</td>
<td>High-level interface</td>
</tr>
<tr>
<td>802.2</td>
<td>Logical link control</td>
</tr>
<tr>
<td>802.3</td>
<td>Ethernet CSMA/CD</td>
</tr>
<tr>
<td>802.4</td>
<td>Token bus</td>
</tr>
<tr>
<td>802.5</td>
<td>Token-ring-access method and physical-layer specification</td>
</tr>
<tr>
<td>802.6</td>
<td>MAN (metropolitan-area network)</td>
</tr>
<tr>
<td>802.7</td>
<td>Broadband technical advisory</td>
</tr>
<tr>
<td>802.8</td>
<td>Fiber-optic technical advisory</td>
</tr>
<tr>
<td>802.9</td>
<td>Isochronous LAN</td>
</tr>
<tr>
<td>802.10</td>
<td>Standards for interoperable LAN/MAN security</td>
</tr>
<tr>
<td>802.11</td>
<td>WLAN (wireless LAN)</td>
</tr>
<tr>
<td>802.12</td>
<td>Demand priority</td>
</tr>
<tr>
<td>802.13</td>
<td>Not used</td>
</tr>
<tr>
<td>802.14</td>
<td>Cable-TV-based broadband-communications network</td>
</tr>
<tr>
<td>802.15</td>
<td>WPAN (wireless personal-area network)</td>
</tr>
<tr>
<td>802.16</td>
<td>Broadband wireless access (WMAN)</td>
</tr>
<tr>
<td>802.17</td>
<td>Resilient-packet-ring study group</td>
</tr>
</tbody>
</table>

REFERENCE

When, say, Node C is communicating with Node A, Node B must know to remain silent, even though it cannot properly detect C’s transmissions. However, the simple CSMA listen-before-speaking protocol does not prevent Node B from transmitting during Node C’s payload-frame interval.

The hidden-node problem substantially raises the probability of collisions by generating false idle detections in the CSMA protocol. The network could use a collision-detection method, but at a cost to the data-throughput rate of several tens of percentage points in simple networks. Instead, 802.11 wireless networks depend on collision avoidance, which solves the problem at the cost of a predictable increase in the transaction overhead born by each payload packet.

Using CSMA/CA, a node with a payload frame ready to transmit listens for traffic on the channel as in the previous example. When the node senses that the channel is idle, it sends a short RTS (request-to-send) frame to the receiver (Figure 3). The RTS frame includes a duration field corresponding to the time required to transmit the payload frame. The receiver sends a short CTS (clear-to-send) packet in response. After the transmitter sends the payload frame, the receiver responds with an ACK (acknowledgment), as before. This handshaking routine reserves the channel for the transmitter. Any hidden third node that could interfere with the transmission can detect either the transmitter’s RTS frame that contains the reservation interval or the short CTS and ACK frames that precede and follow the payload, respectively. CSMA/CA still allows a nonzero probability of collisions due to hidden nodes, but, with short RTS and CTS frames, that probability is low.

CSMA/CA allows 802.11 networks to assume multiple topologies. Because each node can negotiate frame times with every other node within its reach, nodes operating autonomously can form ad hoc networks. These casual peer-to-peer networks allow, for example, people to connect laptops for file sharing during a meeting. Such arrangements relieve participants from the overhead of registering for guest privileges on an enterprise’s main network when access to the enterprise server is unnecessary.

More formal BSS (basic-service-set) networks use an access-point node that bridges the wireless network to a wired LAN (Figure 4). You can form an ESS (extended-service set) with multiple overlapping BSS regions. Unlike ad hoc networks, a BSS is not a peer-to-peer network. Instead, BSS networks operate in so-called infrastructure mode, in which all communication between nodes flows through the access point. Infrastructure mode simplifies the collision-avoidance problem, because no wireless nodes are hidden from the access point. Access points can operate the BSS in a polled mode, which eliminates the collision-avoidance problem at the cost of further network overhead.

The access point at the center of a BSS can provide a range of other network services. The access points that combine to define an ESS can coordinate service handoffs as wireless nodes move between adjacent BSS regions. With the wireless-network communications flowing through the access point, mobile nodes can “ snooze” to reduce their battery current while the access node queues low-priority messages. Scheduled events and system-broadcast or other high-priority messages can trigger a wake-up message from the access point.

**Looking Like a Contender**

In the wired world, the PHY implements a network’s signaling protocol and couples to a medium with essentially constant attributes. Although noise sources can couple into copper feeds, the design of those lines—the characteristic impedance and I/O topology—minimizes such disturbances. Fiber-optic media are, of course, even more...
impervious to interference signals within the environment.

Wireless networks, by contrast, don’t operate over private media. For them, the fight against interferers for a clear and reliable communications channel is ever ongoing—an issue that goes to the heart of the PHY design. In the case of freespace optical, the transmission’s limited propagation characteristics eases the problem. That same propagation trait limits optical wireless communications from most LAN applications, albeit with some intriguing exceptions, in favor of the more geographically restricted PAN (personal-area network).

In RF WLANs, the shared medium can be particularly problematic in the 2.4-GHz ISM band that 802.11 uses. In addition to broadband interference, wireless networks share their piece of the spectrum with many other radiating systems, including wireless telephones, microwave ovens, and systems such as Bluetooth and the short-range communications for which the FCC first allocated the ISM band. Of these systems, the press most often cites microwave ovens. But, according to chip-set manufacturers, they are far from the most worrisome interference source because they operate only during comparatively small intervals during a day, they are more likely farther away than other interference generators from wireless network nodes, and regulatory agencies require that they exhibit low electromagnetic leakage.

Although the 2.4-GHz ISM band is unlicensed, it is not unregulated. The FCC mandates maximum power levels and allowable modulation methods to minimize the mutual interference caused by multiple devices operating in the same band with geographic overlaps. When the IEEE ratified 802.11, it included definitions for three MACs. One MAC supported optical wireless; one, FHSS (frequency-hopping spread spectrum); and one, DSSS (direct-sequence spread spectrum). The 802.11b extension defines a DSSS-modulated PHY that raises the signaling rate to 11 Mbps from the original 1- and 2-Mbps standard.

The original 802.11 DSSS PHY uses a two-stage modulation scheme. Depending on the data rate, the PHY modulates the data stream using either BPSK (binary phase-shift keying) or QPSK (quadrature-phase-shift keying). BPSK allows a 1-Mbps bit rate to map onto a 1M-sample/sec symbol rate. QPSK can code two bits per symbol, which gives 802.11’s original top speed of 2 Mbps on the same carrier (Reference 3).

The PHY then mixes the PSK modulated signal with an 11-chip Barker code—an 11-bit sequence representing a spreading signal—by XORing the two streams (Figure 5). A DSSS modulator could use other pseudonoise sequences, but the 802.11 standard specifies the 11-chip Barker code because it exhibits attractive properties in a short sequence (Reference 4). The resultant spread signal has a low power spectral density and high interference immunity despite operating in a shared spectrum (Figure 6).

The ratio of the chip rate RC to the data rate RB gives the DSSS processing gain:

\[ G_p = 10 \log \left( \frac{R_C}{R_B} \right) \]

In the case of 802.11, the processing gain is

\[ G_p = 10 \log \left( \frac{11 \text{ Mbps}}{1 \text{ Mbps}} \right) = 10.4 \text{ dB} \]

This equation expresses the SNR advantage of spread-spectrum signals over a narrowband representation of the same bit signal. The SNR advantage manifests itself as the same demodulation process that “unspreads” the DSSS signal also spreads uncorrelated interfering signals and broadband noise (references 5, 6, and 7).

TAKIN’ IT TO THE STREET

The road to 802.11’s successful commercialization reached a major milestone with the advent of the first high-speed PHY extension, which 802.11 defines. The 11b PHY supports 5.5- and 11-Mbps bit rates using CCK (complementary-code keying) in place of the Barker code. CCK codes are polyphase-complementary 8-bit sequences that result in sharp autocorrelation responses. You can observe the behavior of a simplified example in the form of a pair of biphase-complementary 8-bit sequences. If you start with the sequences

\[ a = \{-1, -1, -1, 1, 1, -1, 1, -1\} \]

and

\[ b = \{-1, -1, 1, 1, -1, -1, -1, -1\} \]

...
the autocorrelative vectors are given by
\[
c_j = \sum_{i=1}^{n-j} a_i \cdot a_{i+j},
\]
and
\[
d_j = \sum_{i=1}^{n-j} b_i \cdot b_{i+j}.
\]

A characteristic of complementarity codes is that their autocorrelative vectors sum to zero everywhere except for where the shift index is zero—a trait that enhances channel discrimination in the presence of multipath interference:
\[
c_j + d_j = \begin{cases} 
2n & j = 0 \\
0 & \text{otherwise}
\end{cases}
\]

(Reference 8).

The CCK codes differ from this simple biphase-complementary example in that the sequences are formed of eight values on the complex plane. The combination of CCK and QPSK modulations encodes eight bits per symbol, allowing 802.11b to transmit at an 11-Mbps data rate with only a moderate increase of the underlying symbol rate from 1 to 1.375M samples/sec. A fallback data rate of 5.5 Mbps is available to 802.11b systems operating under suboptimal RF conditions by encoding 4 bits per symbol. Implementations of 802.11b also maintain backward compatibility with vanilla 802.11 at 1 and 2 Mbps. In addition to packing 5.5 times the data rate as 802.11’s original DSSS modulation method, CCK’s superior discrimination in multipath environments is an important factor in enterprise installations.

In these first two versions of the standard, transmissions have been limited to three nonoverlapping channels in the 2.4-GHz ISM band. Though the transmission bit rates are as great as 2 and 11 Mbps for 802.11 and 802.11b, respectively, the actual throughput rates are approximately half the data bit rate. This situation is due to the fact that the 802.11 protocol carries a fairly large transaction overhead with relatively small payload packets, so when collisions occur, they affect small amounts of data.

DIVVYING UP THE TURF

Three nonoverlapping channels allow for some flexibility in how customers deploy 802.11b networks. For example, customers may start with a single access point for a small network installation in areas free of structural obstructions. If a sufficient number of users demand more bandwidth than a single shared channel can provide, the network design may collocate as many as two additional access points with the first.

Networks that must service large areas or areas with obstructions require more complicated layouts. A common design that simplifies network planning and expansion uses a tile map (Figure 7). The object of a tiled design is to keep access points operating on the same channel as far from each other as possible without leaving coverage gaps. The cell size you choose is always a compromise. If you select a large cell, you minimize the incidence of cell-to-cell interference but risk reducing the client’s throughput rate by forcing more users to share a channel. Large cells can also increase the fraction of users who operate at less than top speed, due to signal attenuation over the distance to their access point.

Enterprise WLANs and WCANs (wireless-campus-area networks) can pose greater challenges than do residential and SOHO (small-office/home-office) applications. WLAN and WCAN applications tend to serve many more clients operating over a comparatively large area. Enterprise-based wireless networks often operate alongside fast wired networks, so its clients’ throughput expectations are proportionately higher than the SOHO clients’ whose wired network may likely operate at one-tenth the speed. In these larger applications, three nonoverlapping 11-Mbps channels may saturate before the network satisfies the demands on its bandwidth.

PACKIN’ MORE PUNCH

The second PHY extension to the 802.11 family substantially increases the cell bandwidth. Operating in the 5.2- and 5.3-GHz UNII (unlicensed national-information-infrastructure) bands, 802.11a offers eight independent channels operating as fast as 54 Mbps. The FCC has also allocated a third 5.7-GHz UNII band, intended for outdoor applications.

The 5-GHz version of 802.11 uses OFDM (orthogonal-frequency-division multiplexing) instead of DSSS. The OFDM transmitter generates multiple modulated narrowband subcarriers. An inverse FFT and an FFT, respectively, encodes and decodes data in the frequency domain (Reference 9).

At first glance, 802.11a looks like it’s fighting an uphill battle. The FCC limits the radiated power in the lowest UNII band to 50 mW and in the second band to 250 mW—respectively, −13 and −6 dB below 802.11b’s 1W. The propagation attenuation at 5 GHz is also greater by several decibels than at 2.4 GHz. The instantaneous power dissipation of 802.11a radios is also greater than the 11b’s.

Working in its favor, 11a is not sharing spectrum with a large number of competing devices, as is 11b. However, 11a does not have the UNII spectrum to itself. It shares this space with certain radars, which can lead to disparities in performance, depending on geography, and prevents the band’s consistent use worldwide.

For nodes operating within 100 ft of
their access points, corresponding to a cell area of more than 30,000 sq ft, 11a’s throughput rate can range from 3 to 4.5 times that of 11b in a typical enterprise environment. The 5-GHz radio’s instantaneous power dissipation may be greater while transmitting, but the energy required to transmit a given block of data can be as little as one-third of an 11b radio, because the transmission time is much shorter. The larger channel count allocated for 11a allows network designers to separate cells sharing a common channel by a greater distance, which reduces co-channel interference (Figure 8).

If you’re concerned about interoperability between sites worldwide, 11a does have a serious limitation. Operation by 802.11a in the UNII bands is licensed only in North America. The 2.4-GHz ISM band, by contrast, is commonly available for 802.11b in North America, Europe, and Asia. Several companies are working on dual-mode PHY chips so that, for example, a PCMCIA card in your laptop can communicate with an 802.11a network in the United States and operate just as easily, if a bit more slowly, with an 802.11b network overseas.

THE STRUGGLE WITHIN

The lack of a single worldwide band for WLANs other than the admittedly crowded 2.4-GHz ISM band has motivated the LMSC to add a faster PHY for the original 802.11 spectrum. The High-rate 802.11b Study Group formed two years ago to determine the feasibility of extending 2.4-GHz services to 20 Mbps or more. This initiative has since evolved into the TGg (task group G), charged with defining a third extension to the basic standard. During the course of its work, TGg has considered a broad range of modulations schemes. Several criteria exist for the candidates, including backward compatibility with 11b and compatibility with the existing MAC. As it approached its November 2001 meeting, the TGg had converged on a few modulation methods, including 11a’s OFDM, a combination of CCK and OFDM supported by Intersil, and PBCC (packet binary convolutional code) supported by Texas Instruments.

A variation on the OFDM theme solves the handshaking problem. CCK-OFDM uses CCK modulation for the packet’s header, and OFDM for the payload. This arrangement provides compatibility for mixed 11b and 11g, but at the cost of throughput. The combination remains significantly faster than 11b at all ranges but not faster than PBCC. A dual-band radio for CCK-OFDM in 2.4 GHz and OFDM in 5.2 GHz is simpler to implement than are other dual-band systems. Mixed 11b/11g installations can evolve toward pure OFDM as network managers replace older 11b equipment with combinations of 11a and 11g. This path leads to the highest throughput of any combination of these three technologies, but that benefit is deferred as long as 11b nodes are in the network.

Like CCK-OFDM, PBCC uses a CCK header for compatibility with 11b systems. PBCC enjoys a 20 to 25% greater throughput than CCK-OFDM, depending on range. It also offers a 3-dB improvement in process gain over 11b’s CCK modulation (Reference 12). But dual-band radios that support PBCC in the ISM band must decode three modulated waveforms, not two.

The unratified 11g draft standard contains all of the above, distributed between mandatory and optional modes (Table 1). The optional modes may represent opportunities to differentiate OEM equipment, or they may add to the market confusion and suboptimal throughputs unless customers take the trouble to learn about the optional modes supported by each node they buy.

THE MAIN EVENT

Many of the discussions about 802.11 stress the operating range the various modulation schemes provide for a given throughput. The throughput, however, may be a stronger function of multipath fading and the presence of interferers than of distance alone. Throughput and distance are easier to measure than are interfering mechanisms. But the ease of making a measurement does not address its relevance. The raw throughput in either a fixed or an idealized environment, such as a free field, doesn’t tell you about matters such as which modulation scheme is most resilient in the presence of the various interfering signals.

In enterprise LAN and CAN applications, node spacing may be dense enough that network operators are more concerned with channel count, capacity, and reuse than with operating range. In
such cases, 11a becomes more attractive for its high channel count and high throughput. Its lower operating radius may actually prove to be an advantage in installations that sector the networks along a building’s architectural features and boundaries. For example, if one part of a building is laid out as an engineering laboratory and another houses accounts payable, a high-speed wireless network technology that offers a moderate operating radius may serve each department well without generating strong interfering signals for the other.

References
5. Fakatselis, John, “Processing gain in spread spectrum signals,” Harris Semiconductor (now Intersil), undated.