HSMM Radio Equipment

Readily available computer oriented Wi-Fi equipment can be used to form the basis for high speed data transport at 2.4 GHz and above. This article shows you how it’s done and how it works.

By John Champa, K8OCL; and John B. Stephensen, KD6OZH; With input from Dave Stubb, VA3BHF

Introduction

This is the first article to discuss what is known in Amateur Radio as High-Speed Multimedia (HSMM) radio in technical detail. HSMM Radio is a form of Amateur Packet Radio that starts at speeds of 56 kbps and goes up from there up to 5000 times faster than conventional packet radio. This capability enables multimedia, or simultaneous digital video, digital voice, data, and text. Initial HSMM Amateur Radio research has been based on readily available, inexpensive commercial gear designed for WiFi or wireless local area networking (WLAN). HSMM is not a specific mode—it is, instead, a direction or a driving force within Amateur Radio to develop high-speed digital networking capability under Part 97 regulations.

Military surplus radio equipment fueled Amateur Radio in the 1950s. Commercial FM radios and repeaters snowballed the popularity of VHF/UHF amateur repeaters in the 1960s and 70s. In the same way, current availability of commercial wireless LAN (WLAN) equipment is driving the direction and popularity of Amateur Radio use of spread spectrum in the early 2000s.

The Institute of Electrical and Electronics Engineers (IEEE) has provided the standards under which manufacturers have developed WLAN equipment for sale commercially and hams have adapted this equipment to outdoor use. The IEEE 802.11 series of standards defines a series of RF modems similarly to the way that the International Telecommunications Union (ITU) defined a series of telephone modems in the past. The term “WiFi” is short for wireless fidelity and indicates that the subject equipment has been tested to ensure that it fully complies with the applicable IEEE 802.11 standard.

Accordingly, the first part of this article describes existing 802.11 equipment for the 13-cm and 5-cm amateur bands. The second part of this article describes a proposed communication protocol for HSMM operation that will fit into the existing ARRL band plans from 219 to 2400 MHz. The initial implementation will make use of the DCP-1 hardware module described in an article by John Stephensen, KD6OZH.

Existing Products—High Speed Multimedia Radio

In early 2002 the ARRL Technology Task Force (TTF) established the High Speed Multimedia (HSMM) Working Group with John Champa, K8OCL, as its chairman. John moved quickly to identify two initial goals for the new working group to immediately begin the development of such high-speed digital Amateur Radio networks:

• Encourage the amateur adoption and modification of COTS IEEE 802.11 spread spectrum hardware and software for Part 97 uses.
• Encourage or develop other high-speed digital radio networking techniques, hardware, and applications.

These efforts were rapidly dubbed HSMM Radio. Although initially dependent on adaptation of COTS 802.11 gear to Part 97, the emphasis is on simultaneous voice, video, data, and text modes.

Applications

HSMM radio has some unique ham
radio networking applications and operational practices that differentiate it from normal WiFi hotspots at coffeehouses and airports as described in the popular press. HSMM radio techniques are often used for system RC (remote control) of Amateur Radio stations.

In this day of environmentally sensitive neighborhoods, one of the greatest challenges, particularly in high-density residential areas, is constructing ham radio antennas; particularly high tower-mounted HF beam antennas. Such amateur installations also represent a significant investment in time and resources. This burden could be easily shared among a small group of friendly hams, a radio club or a repeater group.

Implementing a link to a remote HF station via HSMM radio is easy to do. Most computers now come with built-in multimedia support. Most Amateur Radio transceivers are capable of PC control. Adding the radio networking is relatively simple. Most HSMM radio links use small 2.4 GHz antennas mounted outdoors or pointed through a window. These UHF antennas are relatively small and inconspicuous when compared to a full-size 3-element HF Yagi on a tall steel tower.

A ham does not have to have an antenna-unfriendly homeowners association or a specific deed restriction problem to put RC via HSMM radio to good use. This system RC concept could be extended to other types of Amateur Radio stations. For example, it could be used to link a ham’s home to a shared high performance Amateur Radio DX station, EME station, or OSCAR satellite ground station for a special event or even on a regular basis.

Shared Internet Access

Sharing high-speed Internet access (Cable, DSL, etc.) with another ham is a popular application for HSMM radio. As long as it is not done for profit, it is entirely legal in the US under Part 97 rules. However be careful to read the terms of service supplied by your service provider. Many have restrictions against sharing your service with another party. If you violate the terms and conditions of your service agreement, the provider can (and will) disconnect your service. Pop-up ads, although a nuisance, are not illegal and can readily be controlled by the proper browser configuration. Just as on the Internet, it is possible to do such things as playing interactive games, complete with sound effects and full motion animation, with HSMM radio. This can be lots of fun for new and old hams alike, plus it can attract others in the “Internet Generation” to get interested in Amateur Radio and perhaps become new radio club members. In the commercial world these activities are called “WLAN Parties”. Such e-games are also an excellent method for testing HSMM radio link speed.

Emergency Communications

There are a number of significant reasons why HSMM radio is the wave of the future for many Emergency Communications Support (RACES, ARES, etc.) situations.

• The amount of digital radio traffic on 2.4 GHz is increasing and operating under low powered, unlicensed Part 15 limitations cannot overcome this noise.

Fig 1—OFDM carrier interleaving. Fig 2—Encoding complementary code frequency sequence.
EmComm organizations increasingly need high-speed radio networks that can get out of the disaster area and into an area where ADSL, cable modem, satellite or other broadband Internet access is available. With HSMM radio often all that would be needed to accomplish this in the field is a laptop computer with a headset, and perhaps an attached digital camera. The laptop must be equipped with a special wireless local area network card (PCMCIA) with an external antenna jack. In HSMM radio jargon such a card is simply called a RIC (radio interface card). Then connect the RIC to a short Yagi antenna (typically 18 inches of antenna boom length), or perhaps a small dish antenna mounted on a tripod weighted with a sandbag. Connection is established by pointing the antenna toward the HSMM repeater back at the EOC. More details are provided further into this paper.

Radio Relay for the 21st Century

There are a number of ways to extend the HSMM link. The most obvious means would appear to be to run higher power and place the antennas as high as possible, as is the case with VHF/UHF FM repeaters. In some densely populated urban areas of the country this approach with 802.11, at least in the 2.4 GHz band, may cause some interference with other users. Other means of getting greater distances using 802.11 on 2.4 GHz or other amateur bands should be considered. One approach is to use highly directive, high-gain antennas, or what is referred to as a “point to point” or ad-hoc link approach. Another method used by some HSMM radio networks is what is called a low-profile radio network design. It depends on several low power sources and radio relays of various types. For example, two HSMM radio repeaters (known commercially as access points, or APs, about $100 devices) may be placed back-to-back in what is known as bridge mode. In this configuration they will simply act as an automatic radio relay for the high-speed data. It is possible to cover greater distances with in the 2.4 GHz band, but still get move lots of multimedia data.

A Basic HSMM Radio Station

How does one set up an HSMM radio base station? It is really very easy. HSMM radio amateurs will just need to go to any electronics outlet or office supply store and buy commercial off-the-shelf (COTS) Wireless LAN gear, either IEEE 802.11b or IEEE 802.11g. Then they connect external outdoor antennas. That is all there is to it.

There are some purchasing guidelines to follow. First, decide what interfaces you are going to need to connect to your computer. Equipment is available for all standard computer interfaces: Ethernet, USB, and PCMCIA. If you use a laptop in your station, get the PCMCIA card. Make certain it is the type that has a removable rubber duck antenna or external antenna port! Finally, compare the RF performance of the devices you are contemplating. Unfortunately, there is little performance consistency across brands. Better cards can be purchased with up to 200-mW power output and –97 dBm receive sensitivity. Poor performers (while useful for covering a room in a home or office) have power outputs of less than 30 mW and receive sensitivities in the mid–80s dBm range. Buying the best performing card you can afford will assure the best performance. Also make sure the hardware selected for both ends of the link have equivalent performance. The overall link will be limited by the worst performing device. The included directions will explain how to accomplish the installation of these devices in your computer or network. These devices have two operating modes: ad-hoc and Infrastructure. Infrastructure mode is used to communicate with an access point (AP—more on this later). Ad-hoc mode allows these client cards to communicate together and form an “ad-hoc” network (thus the name). Setting two or more cards into ad-hoc mode is the easiest way to get started experimenting with HSMM.

These client devices are the core of any HSMM radio station. They become a computer-operated HSMM 2.4 GHz radio transceiver and will probably cost about $20 to $80, depending on the performance of the hardware (better cards cost more). Start off your experimentation by teaming up with a nearby ham radio operator and setting each device in the ad-hoc mode and on a common channel. Channels 1 through 6 fall inside the Part 97 frequency allocation. However, channel 1 has output that falls within the AO-40 channel assignment, and channel 6 is commonly used by part 15 devices as the default channel. Using channels 2 through 5 limits the interference you may cause to other operators or have caused to you. Do your initial testing in the same room together. Then as you increase distances going toward your separate station locations, you can coordinate using a suitable local FM simplex frequency. Frequently hams will use 146.52 MHz or 446.00 MHz, the National FM Simplex Calling Frequencies for the 2m and 70-cm bands, respectively, for voice coordination. More recently, HSMM radio operators have tended to use 1.2 GHz FM transceivers and handheld transceivers. The 1.2 GHz amateur band more closely mimics the propagation characteristics for the 2m and 70-cm bands. The rule of thumb being, if you can not hear the other station on the 1.2 GHz FM radio, you probably will not be able to link up the HSMM radios.

HSMM Repeaters

What hams would call a repeater, and in the wired LAN world, computer buffs would call a hub, the WiFi industry refers to as a radio access point, or simply AP. This is a device that allows several Amateur Radio stations to share the radio network and all the devices and circuits connected to it. An 802.11b AP will sell for about $80 and an 802.11g AP for about $100. The AP acts as a central collection point for digital radio traffic, and can be connected to a single computer or to another radio or wired network. Remember to select an AP with performance similar to the performance of the other 802.11 hardware you’re using.

The AP identifies itself to its users by means of a station ID or SSID. Each AP is provided with an SSID, which is the station identification it constantly broadcasts. For ham purposes, the SSID can be set to your call sign, thus providing automatic, and constant station identification. To use an AP in a radio network the wireless computer users have to exit ad-hoc mode and enter what is called the infrastructure mode, in their operating software. Infrastructure mode requires that you specify the radio network your computer station is intended to connect to, so set your computer station to recognize the SSID you assigned to the AP (yours or another ham’s AP) to which you wish to connect.

Point-To-Point Links: The AP can also be used as one end of a radio point-to-point network. If you wanted to extend a radio network connection from one location to another, for example in order to remotely operate an HP station, you could use an AP at the network end and use it to communicate to a computer at the remote station location.

An AP allows for more network fea-
tures and improved information security than provided by ad-hoc mode. Most APs provide DHCP service, which is another way of saying they will automatically assign an Internet (IP) address to the wireless computer network, limited to the radio network. In addition, they can provide MAC address filtering which allows only known users to access the network.

**Mobile Operating**

When hams use the term mobile HSSM station what they are normally talking about is a wireless computer set-up in their vehicle to operate in a stationary portable fashion. Nobody is suggesting that you try to drive a vehicle and look at a computer screen at the same time. That could be very dangerous, and is illegal in some states. So under no circumstances do I ever recommend that you drive a very fast moving vehicle and listen to radio bands of interest. The vehicle keeps your eyes on the road and not on the computer screen. Additionally, 802.11 was not designed for mobile use and is intolerant of the Doppler shift and signal fades associated with mobile operations.

**What sort of equipment is needed to operate an HSSM mobile station?**

Some type of portable computer, such as a laptop. Some hams use a PDA, notebook, or other small computing device. The operating system can be Microsoft Windows, Linux, or Mac OS, although Microsoft XP offers some new and innovative WLAN functionality. Some type of radio software hams would call an automatic monitor, and computer buffs would call a sniffer utility. The most common type being used by hams is Marius Milner’s Network Stumbler, or “NetStumbler.” All operating systems have monitoring programs available. Linux has Kismet; MAC OS has MacStumbler. Marius Milner has a version for the Pocket PC called “MiniStumbler.”

- A RIC (Radio Interface Card or PCMCIA WiFi computer adapter card with external antenna port) supported by the monitoring utility you are using. The most widely supported RIC is the Orinoco line. The Orinoco line is inexpensive and fairly sensitive.
- An external antenna attached to your RIC. This is often a magnetically mounted omnidirectional vertical antenna on the vehicle roof, but a small directional antenna pointed out a window or mounted on a small tripod are also frequently used. Be aware of the length and type of cable used to connect the antenna. The small diameter flexible coax often used can exhibit 6 dB of loss per 10 feet! If the antenna needs to be mounted more than 5 feet from the receiver, use LMR 400 or better coax so as to minimize line losses. A pigtail or short strain relief cable will be needed to connect from the RIC antenna port to the N-series, RPTNC or other type connector on the external antenna.
- A GPS receiver that provides NMEA formatted data and computer interface cable will allow the monitoring utility to record where HSSM stations are located on a map just as in APRS. GPS capability is optional, but just as with APRS, it makes the monitored information much more useful since the station’s location is provided.

While operating your HSSM mobile station, if you monitor an unlicensed Part 15 station (non-ham), some types of WiFi equipment will automatically associate or link to such stations if they are not encrypted, and many are not (i.e., WEP is not enabled). Although Part 15 stations share the 2.4 GHz band on a non-interfering basis with hams, they are operating in another service. In another part of this section we will provide a port a non overlapped 802.11 carrier.

**Commercial users often recommend moving 5 channels away from the nearest AP to completely avoid interference.**

There are six channels within the amateur 2.4 GHz band, but there are problems for hams with two of them. Channel 1 centered on 2412 MHz overlaps into OSCAR satellite downlink frequencies. Channel 6 centered on 2437 MHz is by far the most common out-of-the-box default channel for the majority of WLAN equipment sold in the US, so that often is not the best choice. Subsequently, most HSSM radio groups end up using either channel 3 or channel 4, depending on their local situation. Again, an area survey is recommended before putting anything on the air.

Because of the wide sidebands generated by these inexcusively broadband 802.11 devices, even moving 2 or 3 channels away from such activity may not be enough to totally avoid interference, especially if you are running what in HSSM is considered high power (typically 1800 mW RF output—more on that subject later). You may have to take other steps. For example, you may use a different polarization with your antenna system. Many HSSM stations use horizontal polarization because much of the non-ham 802.11 activity in their area is primarily vertically polarized.

**Special Antenna Systems**

There are a number of factors that determine the best antenna design for a specific HSSM radio application.
Most commonly, HSSM stations use horizontal instead of vertical polarization. Furthermore, most HSSM stations use highly directional antennas, instead of omnidirectional antennas. Directional antennas provide significantly more gain and thus better signal-to-noise ratios, which in the case of 802.11 modulation, means higher rate data throughput. Higher data throughput, in turn, translates into higher data throughput. Higher data throughput brings better data packet throughput. This does nothing to help reject multi-path reflections from the desired path distance, should more power be considered. 

Increasing the effective radiated power (ERP) of an HSSM radio link also provides for more robust signal margins and consequently a more reliable link. These are important considerations in providing effective emergency communications services and accomplishing other important public service objectives in a band increasingly occupied by unlicensed stations and other noise sources.

It should be noted that the existing FCC Amateur Radio regulations covering spread spectrum (SS) at the time this is being written were implemented prior to 802.11 being available. The provision in the existing regulations calling for automatic power control (APC) for RF power outputs in excess of 1 W is not considered technologically feasible in the case of 802.11 modulation for various reasons. As a result the FCC has communicated to the ARRL that the APC provision of the existing SS regulations are therefore not applicable to 802.11 emissions under Part 97.

Using higher than normal output power in HSSM radio, in the shared 2.4 GHz band, is also something that should be done with considerable care, and only after careful analysis of link power conditions and the existing 802.11 activity in your area. Using the minimum power necessary for the communications has always been a good operating practice for hams as well as a regulatory requirement. There are also other excellent and far less expensive alternatives to running higher power when using 802.11 modes. For examples, amateurs are also allowed to use higher gain directional antennas. Such antennas increase both the transmit and the receive effective gain of the antenna as possible, a common amateur practice. Also providing for more robust signal margins and consequently a more reliable link. These are important considerations in providing effective emergency communications services and accomplishing other important public service objectives in a band increasingly occupied by unlicensed stations and other noise sources.
the top of the tower or mast. As mentioned before, this is a two-way system, and the link will communicate only as far as the weakest link direction. A BDA needs to be used on both ends of the link in order to achieve greater communication distances. A system with a BDA on only one end may be heard by the far end station, but the BDA equipped station will probably not hear the weaker signal of the “barefoot” far end station. A reasonably priced 2.4 GHz 1800 mW output BDA is available from the FAB Corporation (www.fab-corp.com). It is specifically designed for amateur HSMM radio experimenters. Be certain to specify “HSMM” when placing your order. Also, to help prevent unauthorized use by unlicensed Part 15 stations, the FAB Corp may request a copy of your amateur license to accompany the order, and they will only ship the BDA to your licensee address as recorded in the FCC database.

This additional power output of 1800 mW should be sufficient for nearly all amateur operations. Even though many experimenters using EmComm, which may require more robust signal margins than normally needed by amateurs, seldom will require more power output than this level. If still greater range is needed, there are other less expensive ways to achieve such ranges (see the section HSMM Radio Relays).

When using a BDA and operating at higher than normal power levels on the channels 2 through 5 recommended for Amateur Radio use (these channels are arbitrary channels intended for Part 15 operation and are not required for Amateur use, but they are hard-wired into the gear so we are stuck with them). You should also be aware of the sidebands produced by 802.11 modulation. These sidebands are in addition to the normal 22 MHz wide spread spectrum signal. Accordingly, if your HSMM radio station is next door to an OSCAR repeater or other amateur-remote station, you may need to take extra steps in order to avoid interfering with them. The use of a tuned output filter may be appropriate in order to avoid causing QRK. Even when operating on the recommended channels in the 2-5 range, whenever you use higher than normal power, some of your now amplified sidebands may go outside the amateur band, which stops at 2450 MHz. So from a practical point of view, whenever the use of a BDA is required to achieve a specific link objective, it is a good operating practice to install a tuned filter on the BDA output. Such filters are not expensive and they are readily available from several commercial sources. It should also be noted that most BDAs currently being marketed, while suitable for 802.11b modulation, are often not suitable for the newer, higher speed 802.11g modulation.

There is one further point to consider. Depending on whether 802.11 operating may be taking place in your area, it may be a good practice to only run higher power when using directional or sectoral antennas. Such antennas allow hams to operate “over and around” other licensed amateur stations. For example, in the case of 802.11 modulation, the 2.4 GHz band is shared with Part 15 unlicensed 802.11 stations. How do you keep these unlicensed stations from automatically associating (auto-associate) with your licensed ham radio HSMM network?

Many times the steps taken to avoid interference with other stations also limit those other stations’ capability to auto-associate with the HSMM repeater, and improve the security of the HSMM station. For example, operating with a directional antenna oriented toward the desired coverage area rather than using an omnidirectional antenna, etc.

The most effective method to keep unlicensed Part 15 stations off the HSMM repeater is to simply enable the Wired Equivalent Protection (WEP) already built into the 802.11 equipment. The WEP encrypts or scrambles the digital code on the HSMM repeater based on the instruction or “key” given to the software. Such encryption makes it impossible for unlicensed stations not using the specified code to accidentally auto-associate with the HSMM repeater.

The primary purpose of this WEP implementation in the specific case of HSMM operating is to restrict access to the ham network by requiring all stations to authenticate themselves. Ham stations do this by using a WEP implementation with the appropriate ham key. Hams are permitted by FCC regulations to encrypt their transmission in specific instances; however, actually at the time of this writing, this is not one of them. Accordingly, for hams to use WEP for authentication and not for encryption, the key used to implement the WEP must be published. The key must be published in a manner accessible by most of the Amateur Radio community. This fulfills the traditional ham radio role as a self-policing service. The current published ham radio WEP key is available at the home page of the ARRL Technology Task Force High Speed Multimedia Working Group: www.arrl.org/hsmm/.

Before implementing WEP on your HSMM repeater be certain that you have checked the Web site (www.arrl.org/hsmm/) to ensure that you are using the current published WEP key. The key may need to be changed occasionally.

The HSMM Working Group is cur-
rently investigating the feasibility of obtaining a waiver or station temporary authorization (STA) for selected Amateur Radio HSMM experimental stations. The purpose of the waiver would be to allow us to experiment with a variety of wireless content security measures such as virtual private networking (VPN). Our research would be restricted to frequencies above 50 MHz and apply only to domestic amateur digital computer-to-computer networking experiments.

**Commercial Part 15 Equipment**

The IEEE standards for WLAN equipment have evolved from low speeds to high speeds, increasing the spectrum efficiency with each new version. IEEE 802.11 standardized frequency-hopping spread spectrum (FHSS) for the 2.4 GHz ISM band to operate at data rates of 1 and 2 Mbps. Next came the release of 802.11b which provided additional data rates of 5.5 and 11 Mbps but only for DSSS. The purpose of using FHSS and DSSS modulation techniques is to avoid inter-symbol interference (ISI) due to multipath propagation. In FHSS the receiver is on the next frequency when the delayed version of the last symbol arrives on the previous frequency. In DSSS the delayed version no longer matches the spreading code.

This was followed by 802.11g which provided standardization using Orthogonal Frequency Division Multiplexing (OFDM) for data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps as well as backward compatibility with 802.11b. The FHSS radio can operate at data rates of 1 and 2 Mbps. The currently unreleased 802.11n standard promises data rates in excess of 108 Mbps. Of course, none of these increases in capacity come for free. With each increase in capacity comes the need for more complex modulation to support it. As Claude Shannon theorized in 1948, increasing the bandwidth of a fixed-size channel leads to the need for more power in order to discern the intelligence from the channel noise. In other words, increasing modulation complexity reduces receiver sensitivity. For example, an 802.11b link operating at 1 MBPS uses BPSK and has a receive sensitivity of around –94 dBm. For an 802.11g link operating at 54 Mbps the modulation is 64QAM, and the receive sensitivity drops to –68 dBm because of the additional signal to noise ratio required to retrieve the information from 64 possible modulation points rather than the 2 points associated with BPSK.

Note that the power increase is non-linear as doubling the number of states per transmitted symbol increases the number of bits transmitted by an ever-decreasing amount.

**Frequency Hopping Spread Spectrum**

FHSS radios, as specified in 802.11, hop among 75 of 79 possible non-overlapping frequencies in the 2.4 GHz band. A complete hop sequence occurs approximately every 400 ms with a hop time of 224 µs. Since these are Part 15 devices the radios are limited to a maximum peak output power of 1 W and a maximum bandwidth of 1 MHz (at –20 dB) at any given hop frequency. The rules allow using a smaller number of hop frequencies at wider bandwidths (and lower power: 125 mW) but most manufacturers have opted not to develop equipment using these options. Consequently, off-the-shelf equipment with this wider bandwidth capability is not readily available to the amateur.

The hopping sequences are well defined by 802.11. There are three sets of 26 such sequences (known as channels) consisting of 75 frequencies each. The ordering of the frequencies is designed as a pseudo-random sequence hopping so that no two channels are on the same frequency at the same time. Channel assignment can be coordinated among multiple colocated networks so that there is minimal interference among radios operating in the same band.

**Direct Sequence Spread Spectrum**

DSSS uses digital modulation to accomplish signal spreading. That is, a well-known pseudo-random digital pattern of ones and zeros is used to modulate the data at a very high rate. In the simplest case of DSSS, defined in 802.11, an 11-bit pattern known as a Barker sequence (or Barker code) is used to modulate every bit in the input data stream. The Barker sequence is 10110111000. Specifically, a “zero” data bit is modulated with the Barker sequence resulting in an output sequence of 10110111000. Likewise, a “one” data bit becomes 01001000111 after modulation (the inverted Barker code). These output patterns are known as “chipping” streams; each bit of the stream is known as a “chip". It can be seen that a 1 Mbps input data stream becomes an 11 Mbps output data stream.

The DSSS radio, like the FHSS radio, can operate at data rates of 1 and 2 Mbps. The chipping stream is used to phase modulate the carrier via phase shift keying. Differential Binary Phase Shift Keying (DBPSK) is used to achieve 1 Mbps and Differential Quadrature Phase Shift Keying (DQPSK) is used to achieve 2 Mbps.

---

**Table 1**

<table>
<thead>
<tr>
<th>Data Rate, Mbps</th>
<th>CCK encoded bits</th>
<th>DQPSK encoded bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>

**Table 2**

<table>
<thead>
<tr>
<th>Data Rate, Mbps</th>
<th>Modulation</th>
<th>Coding Rate, (R)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>BPSK</td>
<td>1/2</td>
</tr>
<tr>
<td>9</td>
<td>BPSK</td>
<td>3/4</td>
</tr>
<tr>
<td>12</td>
<td>QPSK</td>
<td>1/2</td>
</tr>
<tr>
<td>18</td>
<td>QPSK</td>
<td>3/4</td>
</tr>
<tr>
<td>16</td>
<td>QAM</td>
<td>1/2</td>
</tr>
<tr>
<td>36</td>
<td>16QAM</td>
<td>3/4</td>
</tr>
<tr>
<td>48</td>
<td>64QAM</td>
<td>3/8</td>
</tr>
<tr>
<td>54</td>
<td>64QAM</td>
<td>3/4</td>
</tr>
</tbody>
</table>
The higher data rates specified in 802.11b are achieved by using a different pseudo-random code known as a Complementary Sequence. Recall the 11 bit Barker code can encode one data bit. The 8 bit Complementary Sequence can encode 2 bits of data for the 5.5 Mbps data rate or 6 bits of data for the 11 Mbps data rate. This is known as Complementary Code Keying (CCK). Both of these higher data rates use DQPSK for carrier modulation. DQPSK can encode 2 data bits per transition. Table 1 shows how 4 bits of the data stream are encoded to produce a 5.5 Mbps data rate and 8 bits are encoded to produce an 11 Mbps data rate. There are 64 different combinations of the 8 bit Complementary Sequence that have the mathematical properties that allow easy demodulation and interference rejection. At 5.5 Mbps only four of the 64 combinations are used. At 11 Mbps all 64 combinations are used. See Fig 2.

As an example, for an input data rate of 5.5 Mbps, four bits of data are sampled at the rate of 1.375 million samples per second. Two input bits are used to select 1 of 4 eight-bit CCK sequences. These 8 bits are clocked out at 250 kbaud. The 802.11a and 802.11g specify 20 MHz wide channels with 52 carriers spaced every 312.5 kHz. Of the 52 carriers, four are non-data pilot carriers that carry a known bit pattern to synchronize demodulation. The remaining 48 carriers are modulated at 250 kbaud. The state of all 48 data carriers is known as a symbol. Thus, at any given instant in time 48 bits, or more, of data are being transmitted.

The term “orthogonal” is derived from the fact that these carriers are positioned such that they do not interfere with one another. The center frequency of one carrier’s signal falls within the nulls of the signals on either side of it. Figure 1 illustrates how the carriers are interleaved to prevent intercarrier interference. OFDM avoids ISI by making the symbol period much longer than the multi-path delay. A gap is then placed between each symbol to occupy the time consumed by multi-path reflections. The gap is 0.8 microseconds in 802.11a & g.

OFDM radio can be used to transmit data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps as specified by both 802.11a and 802.11g. In order to transmit at faster and faster data rates in the same 20 MHz channel different modulation techniques are employed: BPSK, QPSK, 16QAM and 64QAM. In addition, some of the bits transmitted are used for error correction so the raw data rates could be reduced by up to half of what they would be without error correction. For instance, assuming BPSK (1 bit per carrier) and assuming ½ the bits are used for error correction (known as the coding rate, R), the resulting data rate would be 6 Mbps.

48 carriers × 1 bit per carrier × 1/2 R = 24 bits (effective)
24 bits × 250 kilo transitions per second = 6 Mbps

Table 2 shows a complete list of the modulation methods and coding rates employed by 802.11 OFDM. The higher data rates will require better signal strength to maintain error free reception due to using fewer error correction bits and more complex modulation methods.

**Frequencies for HSMM**

Up to this point all the discussion has been regarding HSMM radio operations on the 2.4 GHz amateur band. However, 802.11 modulation can be used on any amateur band above 902 MHz, so we can research each of these options.

AM ATV on the 902-928 and 1240-1300 MHz bands is very susceptible to interference (~50 dBc can be seen) so it is would probably be difficult to find a good spot for 802.11 operation in major cities on either of these bands. The 902 MHz band is just 26 MHz wide so 802.11 modulation would occupy almost the entire band. The 1240 MHz band has ATV channels every 12 MHz so it is impossible to avoid interference. Luckily, ATV at 2400 MHz and above is 16 MHz wide and is much more immune to interference.

The 3.3-3.5 GHz band offers some real possibilities for 802.11, or the newer 802.16 standard. Activity is centered in three bands at 3.37-3.39 (FM ATV), 3.4-3.41 (European weak-signal modes and U.S. satellite sub-band), 3.456-3.458 (U.S. weak-signal modes) and 3.472-3.474 (FM ATV). There is lots of unused spectrum and frequency transverters could be used to get to this band from 2.4 GHz. Development in Europe of 802.16 with 108 Mbps data throughput may make 3.5 GHz gear available for amateur experimentation in the U.S. In the U.S., the 802.16 development is above the amateur 3.5 GHz band, while the European frequencies used are within the US amateur band. Hams are investigating the feasibility of using such gear when it becomes available in the US for providing a RMAN or radio metropolis area networks. The RMAN would be used to link the individual HSMM repeaters (AP) or RLANs together in order to provide countywide or regional HSMM coverage, depending on the ham radio population density.

The 5.65-5.925 GHz band is also being investigated. The COTS 802.11a modulation gear has OFDM channels that operate in this Amateur Radio band. The 802.11a modulation could be used in a ham radio satellite much as 802.11g is in the 2.4 GHz band. It is also being considered by some HSMM groups as a means of providing RMAN links. This band is also being considered by AMSAT for what is known as a C-34-C transponder. This would be an HSMM transponder on the Advanced Motion Picture 3 high-altitude OSCAR with uplink and downlink pass-band in the satellite sub-bands at 5.65-5.67 and 5.83-5.85 GHz. Some other form of modulation other than 802.11 would likely have to be used because of timing issues and other factors, but the concept is at least being seriously discussed.

The 10 GHz band could also host HSMM activity via transverters. Activity is currently limited to the 10.22-10.28 (WBFM), 10.368-10.37 (weak-signal) and 10.39-10.41 (FM ATV) GHz segments and 10.45-10.5 GHz is reserved for amateur satellites. The bottom 200 MHz of the band would be ideal for HSMM, perhaps in conjunction with ICOM DSTAR systems.

Other RMAN link alternatives are also being tested by hams. One of these is the use of wired networks for linking and the technique known as virtual private networks (VPN). This is similar to the method currently used to provide worldwide FM voice repeater links via the Internet, except that it would be broadband and multimedia. Mark Williams, ABSLN, of the HSMM Working Group is leading a team to test the use of various VPN technologies for linking HSMM repeaters. Mark recently made a presentation on this research at the 2004 Dayton Hamvention during the Technology Task Force (TTF) Forum. This forum is an annual event conducted by the ARRL TTF Chairman, Howard “Howie” Huntington, K9KM. The forum also involves our brothers in the two other TTF working groups: The Software Defined Radio (SDR) Working Group and the Digital Voice (DV) Working Group.

There are also commercial products being developed such as the ICOM D-STARSAT system which could readily be integrated into a RMAN infrastruc-
OFDM in Broadcasting

The latest additions to the 802.11 series standardize RF modems using orthogonal frequency division multiplexing or OFDM. This technology provides a bandwidth-efficient method of transmitting digital signals over long distances. OFDM is not only being applied to wireless computer networking but also to broadcasting on frequencies from 150 kHz to 3 GHz. The basic technology is the same, but certain parameters are modified to fit the characteristics of the radio channel. Table 3 shows several OFDM broadcasting standards. Digital Radio Mondiale (DRM) is a standard for the long wave, medium wave and short wave broadcasting bands\(^1\). It is designed to tolerate the long multi-path delays caused by ionospheric propagation and therefore uses very low symbol rates. The inter-symbol guard band is 2.7-7.3 ms long and can therefore tolerate multi-path delays due to path length differences of up to 700 miles. The Digital Audio Broadcasting (DAB) standard is a European standard for terrestrial broadcasting on VHF and UHF bands\(^2\). Multi-path delays are 1/10th to 1/100th of those in short wave radio and 4 modes of operation are specified. 1 kHz carrier spacing is used for VHF broadcasting and 2 or 4 kHz spacing for broadcasting up to 1500 MHz. 8 kHz spacing may be used up to 3 GHz. This system is designed for bands that have no existing analog broadcast stations. IBOC (in-band on channel) AM and IBOC FM are systems marketed by Ibiquity that have been accepted by the FCC for use in the U.S. medium wave and VHF broadcast bands. Multi-path tolerance is similar to DAB but the bandwidth is narrower. This system is optimized to fit in bands with existing analog broadcasting.

OFDM in Amateur Radio

In the amateur bands, OFDM is being used in the HF bands for digital voice transmission. A 36-carrier OFDM modem was developed by G4GUO and is being marketed by AOR. It has characteristics similar to DRM but uses less than half the bandwidth. When used with an AMBE vocoder with rate 2/3 convolutional coding it has a throughput of 2400 BPS.

For high-speed data transmission, amateurs have been using IEEE 802.11 compliant products in the 13-cm band.\(^3\) Most activity has been with DBSS equipment at a data rate of 11 MBPS. However OFDM modems are now available which operate in the 13-cm and 9-cm amateur bands with data rates up to 54 MBPS. This series of standards were designed for short-range (a few thousand feet) use and therefore tolerate a multi-path differential of only 400 feet. However, they can and are being used over longer distances by using directional antennas to suppress multi-path propagation. Transverters can be constructed to convert 13 cm 802.11 equipment to the 9, 3 and 1.2-cm bands.

There is a gap between the capabilities of the 802.11 and G4GUO modems that needs to be filled. The VHF and UHF amateur bands are ideal for multi-point local communication, as path losses are low with omnidirectional antennas. An OFDM RF modem with high data rates and longer multi-path delay tolerance would allow operation in urban areas over both line-of-sight (LOS) and non-line-of-sight (NLOS) paths.

In the effort to research various alternatives to linking Amateur Radio 802.11-based repeaters together, the HSMM Working Group has established several Radio Metropolitan Area Network (RMAN) project teams.
Table 4. OFDM Modems for the Amateur Radio Service

<table>
<thead>
<tr>
<th>Standard</th>
<th>G4GUO</th>
<th>RAMAN-UHF Draft Standard</th>
<th>IEEE 802.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling Rate</td>
<td>50 baud</td>
<td>937.5 baud</td>
<td>7500 baud</td>
</tr>
<tr>
<td>Carrier Spacing</td>
<td>62.5 Hz</td>
<td>1171.875 Hz</td>
<td>9375 Hz</td>
</tr>
<tr>
<td>IS Gap</td>
<td>4 ms</td>
<td>213.3 µs</td>
<td>26.7 µs</td>
</tr>
<tr>
<td>Multi-path</td>
<td>750 miles</td>
<td>40 miles</td>
<td>5 miles</td>
</tr>
<tr>
<td>Frequency (MHz)</td>
<td>1.8–30</td>
<td>219–450</td>
<td>902–2400</td>
</tr>
<tr>
<td>FFT Sample Rate</td>
<td>4 ksps</td>
<td>150</td>
<td>1200</td>
</tr>
<tr>
<td>Pilot Carriers</td>
<td>50</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Data Carriers</td>
<td>4</td>
<td>128</td>
<td>512</td>
</tr>
<tr>
<td>Chan. Spacing</td>
<td>100</td>
<td>200</td>
<td>750</td>
</tr>
<tr>
<td>Bandwidth (kHz)</td>
<td>2.3</td>
<td>78</td>
<td>603</td>
</tr>
<tr>
<td>Low Rate (ksps)</td>
<td>2.4</td>
<td>120</td>
<td>960</td>
</tr>
<tr>
<td>Modulation</td>
<td>DQPSK</td>
<td>DQPSK</td>
<td>D8PSK</td>
</tr>
<tr>
<td>FEC Rate</td>
<td>2/3</td>
<td>2/3</td>
<td>2/3</td>
</tr>
<tr>
<td>High Rate (ksps)</td>
<td>240</td>
<td>480</td>
<td>1920</td>
</tr>
<tr>
<td>Modulation</td>
<td>64QAM</td>
<td>64QAM</td>
<td>64QAM</td>
</tr>
<tr>
<td>FEC Code Rate</td>
<td>2/3</td>
<td>2/3</td>
<td>2/3</td>
</tr>
</tbody>
</table>

*Under ARRL proposed regulations based on signal bandwidth.

OFDM Modem Physical Layer

The UHF amateur bands fall into 2 categories. The FCC limits the bandwidth available for data transmission in the 219-220 MHz and 420-450 MHz bands to 100 kHz, but there is no limit for the bands at 902 MHz and above. There is a practical limit of 6 MHz in the 902-928 MHz, 1240-1300 MHz, 2300-2305 MHz and 2390-2450 MHz bands because they are shared with existing users of analog modes. The goal is to develop a series of modems that operate above 56 KBPS and span the range of bandwidths available within the ARRL band plans. Table 4 shows the characteristics of OFDM modems being used in the amateur bands today and the proposed standard described in this document. The bandwidths for the modems were chosen to fit off-the-shelf SAW filters used in GSM, CDMA and cable TV equipment.

The modem design was strongly influenced by the DAB standard as it operates in the same frequency range and supports both mobile and fixed users. Radio propagation in an urban area is characterized by strong multi-path propagation. Propagation measurements indicate that multi-path delay ranges from 0.4 to 10 µs typically and up to 90 µs worst case for LOS and NLOS paths in an urban environment. The modems defined in the middle seven columns of Table 4 use either 7500-Baud symbol rates with 9.375 kHz carrier spacing or 937.5-baud symbol rates with 1172-Hz carrier spacing. This results in an active symbol time of Ts = 106.7 or 853.3 µs with a guard band of Tg = 26.7 or 213.3 µs between adjacent symbols. The guard band is filled with a copy of the last ¼ of the OFDM symbol as shown in Figure 3.

The lowest speed modem is designed to fit in a 100-kHz channel and uses 64 data carriers plus a pilot carrier as shown in Figure 4. The pilot carrier is transmitted at 3 dB above the level of the data carriers and is placed in the center of the channel. Half of the data carriers are placed on each side of the pilot carrier and enumerated 1 through 64 from the lowest frequency to the highest frequency. The major lobes of the data carriers occupy 78 kHz. Extending beyond that limit on either side are the minor lobes of these carriers. Since the first minor lobe is at –13 dB and the amplitude decreases at only 6 dB/ octave, additional filtering is required. A FIR filter with flat group delay must be used to attenuate minor lobes to –34 dB at ±50 kHz.

Eight-phase differential phase shift keying (8DPSK) is used for the low data rate to allow mobile operation. As the station moves, the absolute phase varies as the strength and delay of multi-path rays vary so a fixed phase reference cannot be used. In...
stead the difference between the phase of the current symbol and the previous symbol is used to determine the value transmitted. Three coded bits are transmitted per symbol per carrier as shown in Table 5.

**Trellis-Coded Modulation**

Since the transmission channel will corrupt the transmitted data due to noise and fading, a forward error correcting (FEC) code must be used to provide adequate performance at reasonable signal to noise ratios (SNR). A plain block convolutional code could be used for FEC but it is much more efficient to use an error correcting code that is integrated with the modulation method. This is called trellis-coded modulation or TCM and we will use a rate 2/3 trellis-code where 2 data bits (x1 and x2) are converted into a 3-bit code word (y0, y1 and y2).

In TCM the signal constellation is partitioned into subsets as shown in Figure 5. Each partitioning increases the distance between constellation points. A convolutional coding of xn-1, as shown in Figure 6, generates y0 and y1, which are used to select between the subsets C0, C1, C2, and C3 at the receiver. The data bit x2 = y2 then selects the final value.

The coding decreases the error rate because it increases the sequential distance between codes. The coded bits, y0, y1, may assume only certain sequences of values that are dependent on the state of the convolutional encoder, S0-1, and the input, x1, as shown in Figure 6.

**Viterbi Decoding**

The receiver can use this information to find the allowed sequence of symbols that is closest in Euclidean distance to the received sequence of symbols and determine the state of the convolutional coder in the transmitter. This is usually done using the Viterbi algorithm with a soft-decision input.

The input is not a 3-bit vector, but a set of eight probabilities that the transmitted signal matches each of the eight signal constellation points shown in Fig 7. The algorithm associates a distance metric with each possible sequence of received signals and selects the maximum-likelihood path. The selection is made by tracing back the possible signal sequences and detecting segments that are common, as shown in Figure 8 (ML segment).

After determining the transmitter’s state, the uncoded bit, x2/y2, is decoded by selecting the closest point in the remaining subset of the signal constellation. This is equivalent to decoding a BPSK data stream so the ultimate error rate for trellis-coded 8PSK is the same as for BPSK data. This results in a considerable coding gain, as the number of data bits actually received is double what BPSK would deliver. Figure 9 shows the gain provided by trellis-coded 8PSK compared to QPSK.

Since the outer Reed-Solomon code works on symbols, the event error rate curve is the one that is relevant.

### Higher Data Rate

When the SNR is high, and the transmission path characteristics are stable, transmitting 4-bits per carrier results in a rate twice the basic data rate. This can be done in fixed stations where the phase of the received signal does not change rapidly. 64QAM modulation is used with a rectangular constellation as shown in Figure 10. The in-phase (I) and quadrature (Q) components of the signal are orthogonal and are treated separately in the encoding and decoding process. Two data bits are converted to three coded bits as was done for 8PSK. One set of bits modulates the I carrier and another modulates the Q carrier as shown in Table 6. The maximum I and Q amplitude is limited to 0.7 so that the vector sum will not exceed 1.0.

---

**Table 5**

<table>
<thead>
<tr>
<th>Tribit</th>
<th>Carrier Phase Shift</th>
</tr>
</thead>
<tbody>
<tr>
<td>y2 = 1  y1 = 0  y0 = 0</td>
<td>0°</td>
</tr>
<tr>
<td>0 0 0</td>
<td>45°</td>
</tr>
<tr>
<td>0 0 1</td>
<td>90°</td>
</tr>
<tr>
<td>0 1 0</td>
<td>135°</td>
</tr>
<tr>
<td>1 0 0</td>
<td>180°</td>
</tr>
<tr>
<td>1 0 1</td>
<td>225°</td>
</tr>
<tr>
<td>1 1 0</td>
<td>270°</td>
</tr>
<tr>
<td>1 1 1</td>
<td>315°</td>
</tr>
</tbody>
</table>
Symbol Synchronization

To properly demodulate the 8DPSK or 64QAM encoded information, the receiver must maintain proper symbol synchronization as shown in Figure 11. This causes the inter-symbol interference (ISI) to be ignored when the fast Fourier transform (FFT) is calculated to demodulate the individual carriers.

Two special symbols are used for synchronization. Since the phase of the incoming carriers is in flux during the first part of the OFDM symbol period, the total amplitude of all carriers is used to delimit the symbol period. A special maximum amplitude symbol, called the reference (REF) symbol is defined, where the absolute phase of each carrier is set according to the formula:

\[ q = 3.6315 k^2 \]

where \( k \) is the carrier index by frequency. This pattern minimizes amplitude distortion due to selective fading. In addition, the crest factor of the REF symbol waveform is less than 5 dB so that the reference symbol can be transmitted at 3 dB above normal power levels to improve amplitude and phase estimation.

The second special symbol is the null (NUL) symbol, which consists of the pilot carrier and no data carriers. The sequence REF-NUL-REF is present at the beginning of each data frame. The receiver normally uses a moving average filter with a time constant of one symbol period to detect the end of the NUL symbol, as shown in Figures 12 and 13.

The REF-NUL-REF sequence is inserted into the transmitted data stream every 125 symbols. This reduces the required symbol clock accuracy to ±100 PPM. The REF symbol after the NUL is then used as an amplitude and phase reference for demodulating the following symbols.

Protocol Control Information

The PHY-PDU begins with 8 PIL symbols. The PIL symbol is a full amplitude pilot carrier with no data carriers.

The high amplitude single carrier (PIL symbols) allows the receiver to acquire carrier frequency lock more easily. This is followed by the REF-NUL-REF sequence and a 1 to 125-symbol data block. If more than 125 symbols are to be transmitted, all blocks but the last have 125 data symbols. The PHY-PDU ends with a PIL symbol.

MAC Sublayer Error Correction

The physical layer provides forward error correction to compensate for errors due to Gaussian noise. However, the radio communications channel is also subject to fading and/or impulse noise that may introduce errors in bursts. The error correction provided in the physical layer may be overwhelmed and bytes containing errors may be delivered to the MAC sublayer. Reed-Solomon codes are particularly good at correcting bursts of errors and one is used in the MAC sublayer to alleviate this problem. This type of code operates on symbols m-bits wide, taking a block of \( k \) symbols and adding parity bits to form a block of \( n \) symbols where \( n = 2^m - 1 \). The encoded block consists of the \( k \) original symbols plus \( n-k \) parity symbols, as shown in Figure 15, and is capable of correcting \( t = (n-k)/2 \) symbol errors.

The code used is an RS (255,223) code that operates on 8-bit symbols and will correct errors in up to 16 symbols per block with an overhead of 12.6%. When 223 data bytes are available for transmission, an encoded block of 255 bytes is generated. The parity symbols are created by dividing a polynomial represented by the \( k \) data symbols by the RS generator polynomial. The symbols in the remainder are the parity symbols. If the end of the PHY-SDU is reached and the number of data bytes to be transmitted is less than 223, a shortened code block is generated.

At the receiver, the process of detecting an error is fairly simple, but correcting errors requires a lot of computation, as shown in Figure 16. As
the data and parity symbols are received, they are divided by the generator polynomial and the remainder, called the syndrome, is zero if there are no errors. If the syndrome is not zero, the syndrome is processed to locate the errors. There are 2t simultaneous equations to be solved with the unknowns being the t locations of errors. The solution can be found in two steps. First the equations are solved using an iterative algorithm, such as Euclid’s algorithm or the Berlekamp-Massey algorithm. This generates an error polynomial whose roots are the locations of the corrupted symbols. The error polynomial is then evaluated to find its roots using an exhaustive search, such as the Chien search. The error values are then calculated using the syndromes and the error polynomial roots. This is usually done using the Forney algorithm, which performs a matrix inversion. The error values are then exclusive-ORed with the received data to correct the errors.

**MAC Service**

This MAC entity is designed to provide a standard IEEE 802.3-style MAC service to the user. The user sends and receives service data units up to 1,536 bytes in length. The sender identifies by the source MAC address and the receiver is identified by the destination MAC address. Addresses are 48 bits in length and may be either individual or group addresses. Individual addresses consist of a six-character amateur-radio-service call sign plus a one-character extension. Group addresses are arbitrary 7-character strings. Characters are encoded in 6-bit ASCII.

Since the physical layer transmits up to 128 bytes per OFDM symbol, each station will accumulate multiple MAC protocol data units (MPDUs) for transmission in one PHY-SDU whenever possible. Each MPDU consists of MAC protocol control information (MPCI) and, optionally, a MAC service data unit (MSDU). Figure 17 shows an example with five MPDUs with three containing MSDUs. The maximum PHY-SDU length is 5,184 bytes.

**MPDU Formats**

There are three types of MPDUs defined. A Data MPDU transports a complete MSDU. It consists of 21-bytes of MPCI containing the address and type fields followed by a variable-length user-data field as shown in Figure 18. The MPCI fields are the intermediate address (IA), destination address (DA), source address (SA) and length (L). DA, SA and L are obtained from the MAC service user while IA is generated by the MAC entity. IA is the next destination address while DA is

---

**Table 6**

<table>
<thead>
<tr>
<th>Tribit</th>
<th>I &amp; Q Amplitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>y_2 y_1 y_0</td>
<td></td>
</tr>
<tr>
<td>0 0 0</td>
<td>−0.7</td>
</tr>
<tr>
<td>0 0 1</td>
<td>−0.5</td>
</tr>
<tr>
<td>0 1 0</td>
<td>−0.3</td>
</tr>
<tr>
<td>0 1 1</td>
<td>−0.1</td>
</tr>
<tr>
<td>1 0 0</td>
<td>+0.1</td>
</tr>
<tr>
<td>1 0 1</td>
<td>+0.3</td>
</tr>
<tr>
<td>1 1 0</td>
<td>+0.5</td>
</tr>
<tr>
<td>1 1 1</td>
<td>+0.7</td>
</tr>
</tbody>
</table>
the ultimate destination address. A secondary station may be set IA to the primary station address to cause it to forward data to another secondary station that it cannot reach directly.

Access is controlled by a primary station that polls multiple secondary stations for traffic. It transmits a token that confers the right to transmit to the addressed secondary station. The secondary station then transmits any accumulated traffic and gives the token back to the primary station. The Token MPDU contains the address of the primary station (PA) and the next secondary station (SA) to transmit as shown in Figure 19.

Stations exchange received signal strength indication (RSSI) reports to determine what other stations are reachable in a network. The primary station periodically transmits an RSSI MPDU to each secondary station and the secondary stations respond by broadcasting RSSI MPDUs. Each station builds up a database of neighbor stations with the strength of its signal at each neighbor and the transmission capabilities of each neighbor. This can be used to select the modulation method and number of carriers to use when transmitting to adjacent stations.

The RSSI MPDU reports the received signal strength (SNR) for one or more transmitting stations (TA) at a particular receiving station (RA) as shown in Figure 20. The TA and RSSI fields are repeated N times. The C and M fields indicate the transmitter capabilities at the reporting station. C is the maximum number of data carriers supported divided by 4. M is the maximum number of bits transmitted per data carrier.

### OFDM Modem Hardware

The OFDM modem described here is being implemented on the DCP-1 digital signal processing board. The DCP-1 uses an Xilinx Spartan-3 FPGA to implement the physical layer of the modem and an Oki Semiconductor ML67Q5000 MCU to implement the MAC sublayer. The received signal is digitized at the IF frequency by a 14-bit ADC at 19.2 Msps and transmitter I and Q baseband signals are generated by a dual 14-bit DAC at 9.6 Msps. The DCP-1 connects to its host via RS-232 or RS-485 up to 230.4 kbps or via USB at 12 Mbps or 480 Mbps. This hardware will be made available to amateurs by one of the authors, KD6OZH.

To allow the widest possible software compatibility, the modem will emulate an IEEE 802.11 LAN controller. For point-to-point operation, individual LAN addresses would be Amateur Radio service call signs. The net control stations call sign or an alphanumeric multicast address could be used for multi-point operation. Station identification is automatic, as the transmitting station’s call sign is always the source address. Since the DCP-1 has an RS-232 interface, an interface that would emulate either a dial-up modem or a TNC in KISS mode is also being considered. This may be useful at low data rates for compatibility with older computers or legacy software is also being considered.

### Conclusion

We expect to have OFDM modems using 8DPSK modulation operational and being tested in the field this year.

---

**Fig 11—ISI Rejection using Guard Band**

**Fig 12—Synchronization with Normal REF Symbol**
The source code will be made public and interested amateurs can modify or improve it as desired. The full specification is available from the HSMM working group. OFDM will allow a number of new applications in the UHF amateur bands and should provide much higher reliability than older technologies such as AFSK and FSK without FEC.

A 937.5-Baud OFDM modem can support data rates up to 240 Kbps in the 219-220 MHz band and up to 1.92 Mbps in the 420-450 MHz band. Operation in the 219 and 420 MHz bands is interesting because 100-W and higher-power amplifiers are available and the path loss is low. This allows the exploitation of paths with high losses. The low baud rate allows a wide (213.3-ms) guard band to suppress ISI for operation over NLOS paths that would be impossible with other types of equipment. The transmission characteristics should be ideal for mobile operation. Pure data transmission would be limited to 240 kbps by the current FCC regulations, but compressed video could be transmitted at the higher data rates as it would be classified as digital ATV. Since the modems will be implemented in software, the occupied bandwidth and data rate can be changed to accommodate FCC regulations and the current propagation conditions.

OFDM could enable mobile ATV, which is impossible with analogue techniques. You could turn on a video camera and the operator on the “talk-in” frequency at a hamfest could see where you are and provide better directions. This capability could prove invaluable in emergency situations. At the home station, applications such as NetMeeting could be used to allow radio club meetings to take place over the air. Presentations could be relayed over the video link. This would be very useful for members with physical disabilities. These data rates are also useful for linking clusters of computers where the main source of traffic is email or facsimile or where the Internet connection is a temporary dial-up link. The 120 or 240 kbps data rates should be adequate for forwarding health and welfare traffic at Red Cross shelters. This type of link also provides some level of security, as the general public won’t have compatible equipment.

The 7500-baud modems can provide higher data rates and may be used on the 33, 23 and 13-cm bands. They are ideal for 802.11 AP linking as they can accommodate T1 data rates for applications that require database access or video. The ability to operate in the 23-cm band eliminates the interference present on 13-cm and allows longer paths to be accommodated when compared to 802.11 modems. This is ideal for linking 802.11 APs serving clusters of computers at remote sites. There are probably many other applications that haven’t been thought of yet—Amateur Radio operators will always find new uses for state-of-the-art technology.

Notes
3. Supplement to IEEE Standard for informa-
Fig 17—PHY-SDU with Multiple MPDUs

Fig 18—Data MPDU

Fig 20—RSSI MPDU with one signal report

Fig 19—Token MPDU

Maximize Microwave Performance

Model 1152
PLL for DEMI Transverters

Model 5112
PLL for DB6NT Transverters

Model M10K
5 to 10GHz Multiplier-LO/Beacon Use

Model SEQ-1
Micro-Controlled Sequencer

Model 10224
PL Dielectric Resonate Oscillator


John Champa, K8OCL, is Chairman of the ARRL HSMM Working Group. John B. Stephensen, K6DOZH, is the RMAN-UHF Project Leader of the ARRL HSMM Working Group.