HIGH SPEED MULTIMEDIA (HSMM) RADIO

By John Champa, K8OCL

Any discussion of High Speed Multimedia radio must start with a special communication mode known as *spread spectrum.* Its origins are unusual, to say the least. Rather than springing from the mind of a career scientist or engineer, spread spectrum was the 1940s brainchild of Hollywood movie actress Hedy Lamarr and composer George Antheil. In fact, they were granted a patent for spread spectrum.

In its most basic form, the idea behind spread spectrum is ingenious, yet simple. Instead of a signal appearing on a single frequency, the signal is spread throughout a range of frequencies. In the original frequency hopping spread spectrum design, the signal rapidly switched from one frequency to the other. Spread spectrum turned out to be ideal for military communications (the kind Hedy Lamarr and George Antheil had in mind) because the wide bandwidth signals are difficult to detect using conventional AM/SSB and FM receiving gear. With wide signal bandwidth and low power densities, if anything at all is heard, it is simply perceived as an increase in the background noise level.

Although HSMM has spread spectrum at its heart, HSMM is not a specific mode *per se.* In Amateur Radio it means any VHF/UHF/SHF/EMF digital mode with a raw data rate above 56 kilobits per second (kbps). Accordingly, the D-STAR system discussed earlier in this book is one form of HSMM radio. With existing technology the HSMM data rate provides enough signal capacity to operate more than one mode at the same time. Usually it uses an IP-based transport infrastructure that makes it completely compatible with personal computer (PC) technology.

Despite the fact that John Costas, W2CRR, published a paper on nonmilitary applications of spread spectrum communications in 1959, spread spectrum was used almost solely for military purposes until the late 1970s. In 1981, the Federal Communications Commission (FCC) granted the Amateur Radio Research and Development Corporation (AMRAD) a Special Temporary Authorization (STA) to conduct Amateur Radio spread spectrum experiments.

In June 1986, the FCC authorized all US amateurs to use spread spectrum above 420 MHz. These FCC grants were intended to encourage the development of spread spectrum, which is an important element in commercial wireless systems. An example of such commercial wireless products are wireless local area networks (WLAN) using the Institute of Electrical and Electronics Engineers (IEEE, pronounced "I triple E") radio standards 802.11. In their traditional fashion, radio amateurs have been quick to adapt these commercial products to their needs in radio experimenting.

SPREAD-SPECTRUM TRANSMISSIONS

A transmission can be called "spread spectrum" if the RF bandwidth used is (1) much larger than that needed for traditional modulation schemes and (2) independent of the modulation content. Although numerous spread spectrum schemes are in existence, amateurs can use any of them as long as the modulation scheme has been published, for example, on the ARRLWeb. By far, direct-sequence spread spectrum (DSSS) and orthogonal frequency domain modulation (OFDM) are the most popular forms within the Amateur Radio community. The older frequency hopping spread spectrum (FHSS) has fallen into disuse as cheap used commercial gear becomes less available.

The Global Positioning System (GPS) is an excellent example of the use of DSSS. The average signal at the GPS receiver's antenna terminals is approximately –160 dBw. Since most sources of interference are relatively narrowband, spread-spectrum users will also benefit, as narrowband interfering signals are rejected automatically during the despreading process. These benefits are obtained at the cost of fairly intricate circuitry: The transmitter must spread its signal over a wide bandwidth in accordance with a certain prearranged code, while the receiver must somehow synchronize on this code and recombine the signal.

This technical complexity is offset by several important advantages:

- *Interference rejection.* If the interference is not synchronized with the original spread spectrum signal, it will not appear after despreading at the receiver.
- *Security.* The length and sophistication of the pseudo-random codes used can be such as to make unauthorized recovery difficult, if not impossible.
- *Power density.* Low power density makes for easy hiding of the RF signal and a resulting lower probability of detection.

For the Amateur Radio community particular benefit is derived from the interference rejection, since it offers both robustness and reliability of transmissions, as well as a low probability of interference to other users.

Additionally, spread spectrum has the potential to allow better utilization of the RF spectrum allocated to amateurs. There is a limit as to how many conventional signals can be placed in a given band before serious transmission degradation takes place. Additional spread spectrum signals will not cause severe interference, but may instead only raise the background noise level. This becomes particularly important in bands shared with other users and in our VHF and UHF bands increasingly targeted by commercial users. The utilization of a channel by many transmitters is essentially the concept behind CDMA (Code Division Multiple Access), a system in which several DSSS transmissions can share the same RF bandwidth, provided they utilize orthogonal pseudo-random sequences.

Amateur Radio Spread Spectrum

In 1989, in a paper titled *License-Free Spread Spectrum Packet Radio,* Al Broscius, N3FCT, suggested the use of Part 15 spread spectrum wireless local area network (WLAN) devices be put to use in Amateur Radio.

Then in late 1999, the FCC considerably relaxed the Amateur Radio service rules regarding the use of spread spectrum. These changes allowed amateurs to use commercial off-the-shelf (COTS) Part 15 spread spectrum devices used under § 97.311 of the FCC rules. The stage was now set for amateur HSMM.

HSMM AND THE EMERGENCE OF COMMERCIAL PART 15 EQUIPMENT

Just as military surplus radio equipment fueled Amateur Radio in the 1950s, and commercial FM radios and repeaters snowballed the popularity of VHF/UHF amateur repeaters in the 1960s and 1970s, the availability of commercial wireless LAN (WLAN) equipment is driving the direction and popularity of Amateur Radio use of spread spectrum in the 2000s.

FCC Part 15 documents the technical rules for commercial spread-spectrum equipment. The IEEE has provided the standards under which manufacturers have developed equipment for sale commercially for unlicensed use. You'll recognize this equipment in the form of wireless routers, access points and more. IEEE 802.11 standardized DSSS (802.11b) and OFDM (802.11g) for the 2.4 GHz band provide data rates of 11 to 54 Megabits per second (Mbit/s), half-duplex. 802.11g, which does not use spread spectrum but uses OFDM for data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbit/s, is backward compatible with 802.11b. 802.11a addresses the use of OFDM in certain parts of the 5 GHz band, but unfortunately most of the equipment presently made in the US operates outside the Part 15 shared portion of 5 GHz Amateur Band. 802.11a provides the same data rates as 802.11g. The currently unreleased 802.11n standard promises data rates in excess of 108 Mbit/s.

The Wireless Fidelity (WiFi) organization certifies compliance of manufactures equipment with these FCC Part 15 requirements. Recently, radio amateurs have started to investigate the use of ZigBee (802.15.4) devices for mesh networking capabilities. By trading bandwidth for power output, the ranges of these devices are surprising good. Increasing the power output beyond the Part 15 restrictions may lead to some significant opportunities for radio experimenting under Part 97 of the regulations. That is the reason radio amateurs refer to our use of this equipment under Part 97 as HSMM radio rather than "WiFi", "WiMax" etc. because we, as a licensed radio service, are not bound by such restrictions. However, we have other restrictions which will be mentioned later.

MULTIMEDIA MODES

In HSMM radio we have the opportunity to operate several different modes at the same time, and usually do. Being generally IP-based, and given enough bandwidth, radio amateurs have the capability to do the same things with HSMM radio that are done on the Internet...

AUDIO: Although technically digital voice, since it is two-way voice over an IP (VoIP) network similar to EchoLink and IRLP networks used to link many Amateur Radio repeaters over the Internet.

VIDEO: Motion and color video modes are called amateur digital video (ADV). This is to distinguish it from Digital Amateur Television (DATV). DATV uses hardware digital coder-decoders (CODEC) to achieve relatively high-definition video similar to *entertainment quality TV.* The usual practice in HSMM radio is to use a far less expensive (often free) PC-based software video CODEC such as Microsoft *Netmeeting* to achieve *video communications quality* signals in much smaller bandwidths.

TEXT: Text exchanges via a keyboard are often used in HSMM radio, but they are similarly called by their Internet or packet radio name: *Chat mode.* If a server is available on the network, e-mail can also be exchanged.

IMAGE: File transfers using file transfer protocol (FTP) e.g., JPEG, can also be done, just as on the Internet.

MOTION VIDEO: FTP of MPEG files can provide one-way video streaming of short video clips. Alternatively, if your Hinternet has an I-Gateway or server, you can simply send a link (URL).

REMOTE CONTROL (RC): Individual devices or even complete stations can be remotely controlled.

WARNING: Do not use two computers in ad hoc mode for remote station operation. This method is completely insecure. You must use an AP/wireless router for the host and a wireless client adaptor in the far end PC as a client. This will allow for implementation of various network infrastructure security measures to protect the link. More on this later.

MESH NETWORKS: A main emphasis in HSMM radio is a dramatic shift in emphasis within Amateur Radio from traditional analog point-to-point radio connections and toward *networked digital radios.* This has resulted in many amateurs nick naming HSMM radio *The Hinternet.* Although the name may imply an under-dog status, the intent is to provide a radio amateur based network completely independent of the Internet. Is this really possible? Won't it always be necessary to use the Internet for at least part of any high-speed radio amateur networking infrastructure? Not necessarily. Already we are seeing trends in Automatic Position Reporting Systems (APRS), Automatic Link Establishment (ALE), etc. in which all the radios are networked together most of the time.

HSMM RADIO APPLICATIONS

By far the most intense application of HSMM radio technology has been in Field Day activities. Field Day presents a special challenge since the event is intended to simulate emergency operating. Field Day stations are usually outdoors and operate with limited resources.

Field Day HSMM applications generally fall into two easy and economical areas, but there undoubtedly are many others:

- Providing a radio local area network (RLAN) covering several acres of radio stations.
- Providing a high-speed (HS) data link back to another amateur's house where there is a DSL line or cable modem for an HSMM Internet Gateway.

In the more sophisticated Field Day operations, we see both applications being served. Why? With the RLAN logging can be instantaneous and, for example, duplicate contacts can be immediately identified and eliminated. With access to an RLAN server, ongoing scoring can be accomplished. This allows the leadership to frequently analyze the group's performance. They can then quickly re-direct resources and activities on the run to better achieve the club's objectives.

Having an HS data link to the outside world from a remote Field Day location allows sending e-mail, photos, and other material to other club members joining the Field day after the start-up or wanting to watch and learn. Also, supporting individuals and family members can be kept informed of needed supplies and situational changes complete with images, etc.

Shared High-Speed Internet Access

Sharing high-speed Internet access (cable, DSL, etc) with another radio amateur is not a frequent application for HSMM radio, but there is an occasional call for it, usually not for routine use, but for special events. Remember that half of the US population is restricted to slow dial-up Internet connections (usually around 20 to 40 kbit/s) over regular analog telephone lines. Getting a high-speed Internet connection, even a shared one, can dramatically change the surfing experience! Just remember that if you use an HSMM radio to share HS access to the Internet, Amateur Radio has content restrictions. For example, you cannot use the link to run your business, transmit music, etc.

What about pop-up ads? These can be effectively blocked, but if one slips through it is analogous to an amateur television station (ATV) transmitting an outdoor scene (e.g., Memorial Day parade) and inadvertently picking-up a billboard in the station camera. Such background sources are merely incidental to your transmission and can be ignored. They are not the primary purpose of your communications, plus they are not intended for rebroadcast to the public, making them totally unrelated to your transmissions.

Remember when sharing Internet access that some cable and DSL companies do not permit such sharing of their services. Other companies seem not to care. It is better to check out the customer agreement situation first. Different ISPs (Internet Service Providers) have different agreements. The control operator of the host HSMM radio node or I-Gate (Internet gateway), is responsible is responsible for ensuring compliance with the user agreement.

Security for all HSMM radios and their associated computer needs to be emphasized here:

- All PCs must have an individual or personal firewall, either software or hardware.
- All PCs must have an active and updated anti-spyware/anti-virus software program(s).
- Always be a safe computer user whether you are on the Internet or the Hinternet. Protect your system!
- This topic is covered in additional detail in the section on Information Security that follows.

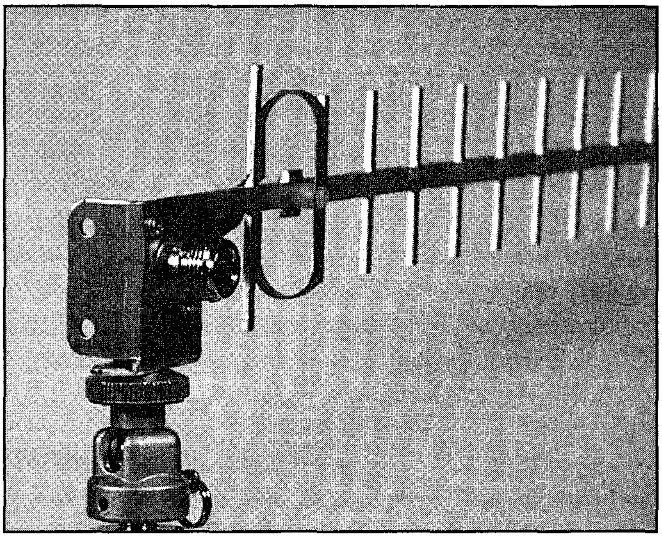

Figure 7-1—The MFJ-1800 is an inexpensive Yagi antenna designed for HSMM on 2.4 GHz.

Gaming Over HSMM Radio

Just as on the Internet, it is possible to do such things as playing interactive games using HSMM radio. Currently individuals play chess via CW (continuous wave telegraphy) on the HF (high frequency/shortwave) ham bands. The big difference is, with HSMM radio the game can come complete with sound effects and full-motion animation. This can be lots of fun for new and old hams alike. Further, it can attract others in the "Internet Generation" to become interested in Amateur Radio and perhaps become new radio club members. In the future it is easy to imagine entire radio amateur clubs based on gaming technology much as clubs presently are often focused on contesting. In the commercial gaming world these activities are called "WLAN Parties." Such e-games are also an excellent method for testing the true speed of your station's Hinternet link capability.

HSMM Radio in Emergency Communications

There are a number of significant reasons and exciting new examples why HSMM radio might be the way of the future for many Emergency Communications (EmComm) situations.

These may or may not be under ARES, RACES, or MARS auspices.

1. 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.

2. EmComm organizations increasingly need high-speed radio networks that can simultaneously handle voice, video, data and text traffic.

3. The cost of a commercially installed HS data network can be more than emergency organizations and communities can collectively afford. The volunteers and HSMM radio operators can be a stop gap measure to provide such community assistance until a commercially available solution can be provided.

4. EmComm managers also know that they need to continuously exercise any emergency communications system and have trained operators for the system in order for it to be dependable.

Being able to communicate what is taking place at a disaster site to everybody on the HSMM radio network can be invaluable in estimating the severity of the situation, planning appropriate responding resources and other reactions. The Emergency Operations Center (EOC) can actually see what is happening

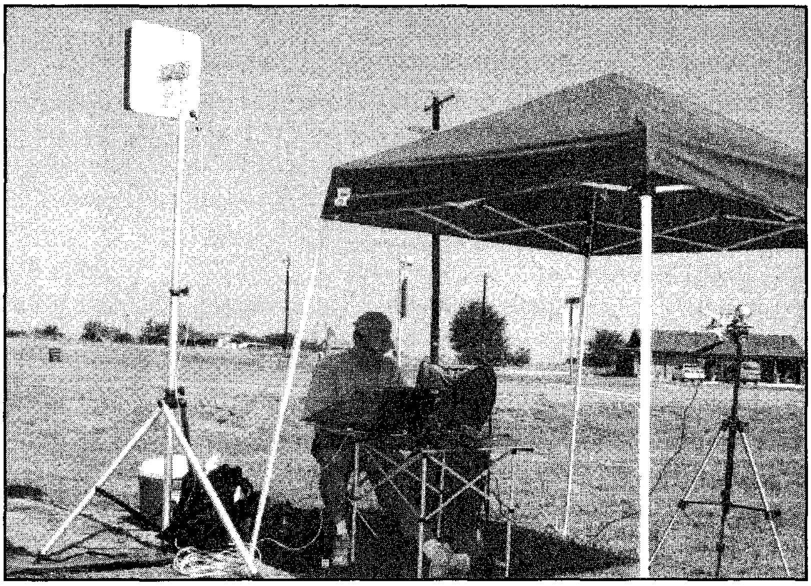

Figure 7-2--N5OOM and the North Texas Microwave Society have used RooTenna-based systems for public service activities. The RooTenna is the square housing atop the support mast.

while it is happening. Submitting a written report while simultaneously talking to the EOC using Voice over IP (VoIP) would provide additional details.

Prior to connecting any HSMM radio device to any EOC internal data network, however, the control operator must coordinate with and get approval from the appropriate EOC officials. All EOCs and other governmental facilities (National Guard, etc.) have strict security policies regarding the connection of any wireless devices to their wired data network.

With HSMM radio, often all that is needed to accomplish such immediacy in the field is a laptop computer equipped with a wireless local area network card (PCMCIA) with an external antenna jack, a small directive 2.4 GHz antenna such as the MFJ-1800 (see **Figure 7-1**), an antenna stand, and an inexpensive webcam or even the video output from a digital camera. Other creative approaches are possible, such as the Pacific Wireless RooTenna (**www.pacwireless.com**), a small radio housing with a built in 19 dB antenna. N5MOO and the North Texas Microwave Society have used RooTenna-based systems for public service activities (see **Figure 7-2**.)

HSMM RADIO RELAYS

There are a number of ways to extend an HSMM radio link. The most obvious means would be to run higher power (at both ends of the link) and to place the antennas as high as possible (**Figure 7-3**), as is the case with VHF/UHF FM repeaters. Even in 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 non-licensed other users. Although the law states that such uses must tolerate interference from licensed users of the band, it is best to avoid it. Radio amateurs should always strive to be good neighbors.

There are several simple means of accomplishing non-interference with Part 15ers. First, is by doing an RF site survey of the area and the route you wish to cover. NetStumbler (**www.netstumbler.com**) is an excellent a free radio tool that can be used for this purpose. You will also need some quality topographical maps of the route. Secondly, avoid channels already in use as much as possible, remembering that only channels 1 through 6 are within the amateur band. Thirdly, use highly directive antennas at both ends of the link. Follow good radio amateur operating practices and use the minimum power necessary to complete the link. When running high power (anything over a few hundred milliwatts) use adequate filtering to avoid splattering by suppressing the signal sidebands of the channel you are using, etc.

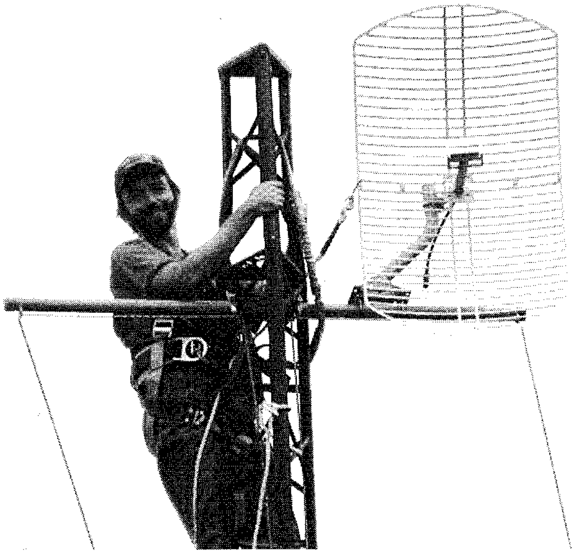

Figure 7-3—Height is important for any HSMM installation. In this photo, Daryl, KG4PRR, is installing an HSMM parabolic dish antenna at the home of K4RBZ.

There is a quick short cut to conducting the ranging portion of an RF site survey. You want to see beforehand see if the path you have in mind might be suitable. Try using two 1.2 GHz handheld transceivers. If possible, get at the same height as the directive antennas you are going to use, and see if any contact whatsoever is possible. Chances are fair that if the 1 or more Watts of 1.2 GHz FM signal does not get through, then neither will the 2.4 GHz link signal without some special attention to design.

Other means of getting greater distances using 802.11 on 2.4 GHz or other amateur bands should also be considered. One approach we have already mentioned: Use highly directive, high-gain antennas, or what is called the directive link approach.

Another approach used by some HSMM radio networks is what is called a low-profile radio network design. They depend on several low power sources and radio relays of various types. For example, two HSMM radio repeaters (known commercially as *access points (AP) or wireless routers*) 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. Using a series of such radio relays on a series of amateur towers between the end-points of the link, it is possible to cover greater distances with relatively low power. Although the data throughput will suffer to some extent using this approach, the link will still move lots of multimedia data.

A BASIC HSMM RADIO STATION

How do you set up an HSMM radio base station? It is really very easy. HSMM radio amateurs can go to any electronics outlet or office supply store and buy commercial off the shelf (COTS) Wireless LAN gear, either IEEE 802.11b (now more or less obsolete and usually sold for very low prices) or IEEE 802.11g.

The favorite location for radio amateurs to shop is Freeman, Anderson, and Bird (FAB Corp) where most of the personnel are radio amateurs and if you identify yourself as an HSMM radio buff you can get a 10% discount (**www.fab-corp.com**). More importantly, being radio amateurs, they can give you technical advice on how to most economically and effectively accomplish your HSMM radio experimenting objectives.

The most popular model in use in Amateur Radio by far is the Linksys WRT54GL wireless router (**Figure 7-4**). It is a combination unit consisting of a wireless access point (AP) or hub coupled with a router. As with other routers, your host PC or laptop connects directly to it using a standard Ethernet cable. If the PC is also connected to the Internet, then it may also perform the function of a *gateway*. If further, this PC is loaded with appropriate server software, it may also perform a network server function such a se-mail management.

This HSMM radio popular wireless router is a *Linux* based model that supports firmware upgrades to distros such as DD-WRT and Tomato (see this URL for more details: **www.youtube.com/watch?v=No_NyW2Ug9o**).

The WRT54GL Router

Linksys released the WRT54GL in 2005 to support third-party firmware based on *Linux*, after the original WRT54G line was switched from *Linux* to VxWorks. See **Table 7-1**.

The first step in configuring your router for HSMM is to disconnect both rubber duck antennas that came with the unit and put them in your parts box or nearest trash container! To connect any outside antenna or a small field antenna such as the MFJ-1800 mentioned earlier, you are going to be become familiar with RP (reverse polarity) connectors. These are connectors that may appear to be male connectors on the outside. However, a close examination of the interior of the connector will reveal that there is no pin. Instead it will be equipped with a socket. Confusing? Not really. These RP connectors are used by the manufacturers to discourage Part 15 owners from using the equipment in ways for which it was not WiFi certified. Being licensed radio amateurs; we are not bound by such certification and can modify the system to accomplish our specific requirements.

Figure 7-4--The Linksys WRT54GL wireless router.

How do you get around this situation so you can connect your coaxial cable for the long run out to the tower, mast pipe, roof, etc? There are two common approaches. (1) use a TNC RP to female N-series adaptor, or (2) construct or purchase a pig tail adaptor with a TNC RP connector on one end and a female N-series connector on the other end.

There are often two antenna ports on wireless devices. These are used for *receive* space diversity. The wireless device will normally automatically select whichever antenna is receiving the best signal at any specific moment. Which do you connect to?

The transmitted signal from the wireless router always goes out the same antenna port. It does not switch. In other words, except for some Cisco models, most wireless devices have *only receive space diversity*. They do not have transmit space diversity. Some access points/wireless routers will allow you to manually (via software) select the antenna port that is used for transmission. When it does not allow such a choice, you will need to find some means of detecting which antenna is the transmit antenna port with RF output power present. That is the port to be used for the pig tail or feed line connection to your exterior antenna. Space diversity is discussed in more detail later.

Now you are ready to connect your wireless router to the length of low-loss coaxial cable (often Times LMR-400, equivalent or better) running to the tower, mast pipe, or roof mounted directive antenna outside. You now have the host end of the link.

Software Configuration

Linksys is the most popular 802.11 modulation AP/wireless router presently used in HSMM radio; the comments here apply generally to that brand and similar units from other manufacturers. If you use another brand of AP/wireless router, follow the instructions from that manufacturer. The usual practice is to use the supplied Linksys CD as a nice Frisbee to play with your puppy. Most people just use the wireless network configuration tool that comes with their PC's OS (operating system), especially if it is *Microsoft XP*, which works particularly well.

Table 7-1
LinkSys WRT54GL Routers Supporting Third-Party Firmware

Version	*CPU Clock*	*RAM*	*Flash Memory*	*Prefix S/N*	*Notes*
1.0	200 MHz	16 MB	4 MB	CL7A	New model line, released after the version 5 WRT54G, which returns to a *Linux*-based OS as opposed to the VxWorks firmware. SpeedBooster is not enabled in stock firmware; however, third-party firmware will enable the feature. The hardware is essentially the same as the WRT54G version 4.0. One alteration is that the internal numbering scheme of the 4-port switch changed in this model, from 1 2 3 4, to 3 2 1 0.
1.1	200 MHz	16 MB	4 MB	CL7B CL7C	In June 20, 2006, this version was shipping with firmware revision 4.30.7. This pre-loaded firmware allows the user to upload a 4MB firmware image, whereas the pre-loaded firmware on version 1.0 limited the image to 3MB. Firmware version 4.30.11 is now available for both hardware versions. Fully supported by Tomato, openwrt, and DD-WRT.
1.1	200 MHz	32 MB	8 MB	CO61	This T-Mobile SPECIAL EDITION is a WRT-54GL (Renamed WRT54G-TM). Uses BCM5352EKPBG Chipset, SpeedBooster technology, & *Linux* OS. Fully supported by Tomato, openwrt, and DD-WRT. It requires a jtag cable to flash a wrt54gl 1.1 cfe to it as its stock cfe will reject non t-mobile/linksys firmware images. Build the cfe from scratch with your router's MAC address using "skynet repair kit." after flashing the cfe to it you can download the Linksys stock firmware for a wrt54gl 1.0 and then use the Linksys Web page update tool to flash the 3rd party firmware onto it. the IP address will go from 192.168.0.1 (t-mobile firmware) to 192.168.1.1(wrt54gl 1.0-1.1 firmware); other third-party firmware unknown

However, I recently installed a Linksys Wireless Print Server on my network so that all the other stations could share my printer without anyone, including me, being physically connected to the device (with the price of ink cartridges you'd better exercise care here!). In that case, the Linksys CD worked perfectly, so you must be your own judge. The point is, be prepared to use other drivers when needed and available, just as you might with any other electronic device in your PC network, wired or wireless. Some of these have the newest drivers and some have the original that came with the unit years ago. They all probably still work to a certain extent.

SSID: The AP/wireless router host software is provided with an *SSID* (Service Set Identifier) that many Part 15 stations turned off for somewhat higher security. But radio amateurs should leave it ON. Enter your call sign as the SSID and use it for the station identification. It constantly broadcasts your call, thus providing automatic and constant station identification. There are 32 characters available for use in this field so more information such as your group's name can be entered too, including spaces and punctuation. If the router asks if you want to enable the broadcast, click **YES**. (Note that SSID in the HSMM world has a somewhat different meaning than SSID in the packet radio community. Among packet users, SSID is defined as Secondary Station Identifier.)

ESSID: Some manufacturers use this term in place of SSID to put emphasis on the fact that the SSID is the name for your *network,* not for a specific wireless AP/router.

ACCESS POINT NAME: When this field is made available (by default it is blank) it is for you to enter a description. This may be handy if you have deployed more than one AP in your network all with your call sign as the SSID. It would allow you to tell them apart. Otherwise, just leave it blank.

CHANNEL: To be as non-interfering with other services as possible, we need to also look at channel selection. The channels provided under Part 15 are only 5 MHz wide. However, the 802.11b/g bandwidth is approximately 20 MHz wide resulting in considerable frequency overlap. Consequently, there are only three totally non-overlapping channels: 1, 6 and 11. Channel 7 and above are outside the Amateur Radio band, so we will focus our discussion only on channels 1 through 6.

After you have completed a site survey of 802.11 activities in your area, you will be in a much better position to select an appropriate channel for your HSMM radio link. In the interim, here are some general guidelines: Avoid channel 6. It is the most common manufacturer default channel setting and 80% or more of your neighbors will be using it for their household wireless LAN. Channel 1 is used by most of the remaining manufactures as their default channel, so that should probably be avoided also. The result is most radio amateurs use channels 3 or 4 depending whether there is a WISP (wireless Internet service provider) operating in their area. Often a WISP will use one of these intermediate channels with a highly directive antenna for

HSMM Glossary

Ad Hoc Mode—An operating mode of a wireless client that allows it to associate directly with any other wireless client without having to go through an Access Point (AP)/Router. See *Infrastructure Mode.*

AP—Access Point (most often now combined with an IP router).

Association—The service used to establish access point/ station mapping and enable station use of the WLANs services in the infrastructure mode.

Authentication—The Process by which the wireless communications system verifies the identity of a user attempting to use a WLAN prior to the user associating with the AP.

COTS—Commercial Off The Shelf equipment.

DHCP—Dynamic Host Configuration Protocol. A protocol used by a client computer to obtain an IP address for use on a network.

HSMM (High Speed Multimedia)—A digital radio communication technique often using spread spectrum modes primarily to simultaneously send and receive video, voice, text and data.

IEEE—Institute of Electrical and Electronic Engineering

IEEE 802.11—An IEEE standard specifying FHSS, DSSS, and OFDM modulation in the 2.4 GHz band

IEEE 802.11a—An IEEE standard specifying OFDM in the 5.8 GHz band at 6, 12, 16, 24, 36, 48, and 54 Mbit/s data rates.

IEEE 802.11b—An IEEE standard specifying DSSS in the 2.4 GHz band at 5.5 and 11 Mbit/s data rates in addition to being backward compatible with DSSS at 1 and 2 Mbit/s specified in 802.11.

IEEE 802.11g—An IEEE standard specifying OFDM in the 2.4 GHz band 6, 12, 16, 24, 36, 48, and 54 Mbit/s data rates in addition to being backward compatible with DSSS at 1, 2, 5.5, and 11 Mbit/s specified in 802.11b.

IEEE 802.11n—An IEEE standard specifying data rates up to 250 Mbit/s and being backward compatible with 802.11a and 802.11g.

IEEE 802.16—An IEEE standard specifying wireless last-mile broadband access in the Metropolitan Area Network (MAN). Also known as WiMax.

ISM—Industrial, Scientific, and Medical. Specific frequency bands authorized by Part 18 rules for non-communication equipment such as microwave ovens, RF lighting, etc. The ISM spectrum where spread spectrum is allowed is located at 2.4 – 2.5 GHz and 5.725 – 5.875 GHz band.

Infrastructure Mode—An operating mode of a client station that requires all communications to go through an Access Point.

OFDM—Orthogonal Frequency Division Multiplexing. A modulation method in which the communication channel is divided into multiple subcarriers each being individually modulated. While not meeting the Part 2 definition of spread spectrum the FCC has given specific authorization for OFDM systems.

Orthogonal—A mathematical term derived from the Greek word *orthos*, which means straight, right or true. In terms of RF, orthogonal applies to the frequencies of the subcarriers which are selected so that at each one of these subcarrier frequencies, all the other subcarriers do not contribute to the overall waveform. In other words, the subcarrier channel is independent of the other channels.

PCMIA—Personal Computer Manufacturer Interface Adaptor. In wireless configurations this is the radio transceiver. This device is now most often simply called the PC card.

Pigtail—A short piece of small diameter, very flexible, low-loss coaxial cable with appropriate connectors on the end(s) to match the PC card antenna port to an external antenna system such as a small dish, etc.. Also called a strain relief cable. Sometimes these are also used for supplying a 2.5 or 5 GHz antenna connection.

RLAN—Radio Local Area Network. These are generally much larger than a WLAN, for example covering an entire Field Day site over many acres, but smaller than a RMAN which might cover an entire town.

RMAN—Radio Metropolitan Area Network

RWAN—Radio Wide Area Network. Regional or even national coverage.

Spread Spectrum (SS)—An information bearing communications system in which: (1) Information is conveyed by modulation of a carrier by some conventional means, (2) the bandwidth is deliberately widened by means of a spreading function over that which would be needed to transmit the information alone.

SSID—Service Set Identifier. A unique alphanumeric string used to identify a WLAN. In HSMM radio this is most often the individual call sign and perhaps the name of the Amateur Radio club or repeater group.

ESSID—See SSID above. The name of your network, not just the device.

UNII—Unlicensed National Information Infrastructure. The UNII spectrum is located at 5.15 - 5.35 GHz, 5.725 - 5.825 GHz, and the recently added 5.470-5.725 GHz band.

USB—Universal Serial Bus.

VPN—Virtual Private Network.

WEP—Wired Equivalent Privacy. An encryption algorithm used by the authentication process for authenticating users and for encrypting data payloads over a WLAN.

WEP Key—An alphanumeric character string used to identify an authenticating station and used as part of the data encryption algorithm.

Wi-Fi—Wireless Fidelity. Refers to products certified as compatible by the Wi-Fi Alliance. See **www.wi-fi.org**. This term is also applied in a generic sense to mean any 802.11 capability operated under FCC regulations Part 15.

WiMax—Familiar name for the IEEE 802.16 standard.

WISP—Wireless Internet Service Provider

WLAN—Wireless Local Area Network.

WPA—WiFi Protected Access methodology used to enhance the network protection issues of encryption and authentication over the use the older WEP algorithm.

back-haul or other purposes. If so, you may wish to coordinate with the WISP and arrange to use some other channel rather than the one specifically used by the WISP. It is not a perfect solution because of all the overlap, but it is a good faith effort to keep most of your stronger signal out of anyone's home, business or governmental WLAN traffic. Yes, we are licensed and they are not, but the political reality is we must learn how to share the band. Radio amateurs have done it successfully on other bands such as 60 meters. We can learn to do it here, too.

WEP: This stands for Wired Equivalent Privacy. In spite of all the horror stories you may have read in the press, this encryption method is more than adequate means to economically achieve authentication and thus keep the vast majority of free-loaders off your network. If you live in the country you may not need to enable this capability. However, in an urban environment, it is probably a good thing to do so that you need not constantly monitor every bit of traffic coming over the network to ensure that it originates from an Amateur Radio station. Mixing traffic with another service that shares the same frequency band is not a generally accepted practice except in times of emergency. Therefore it is often necessary for HSMM radio stations to encrypt their transmissions. *This is not to obscure the meaning of the transmission because the encryption algorithm is standardized and published, and the encryption key is available at any time from the transmitting station. The purpose of the encryption is for authentication and protection of the Part 97 network, not obscuring the meaning. Other forms of authentication often involve a level of complexity that is alien to HSMM radio networks. Most of these networks at this time do not have servers on them. In addition other methods of authentication involve an actual exchange (pass word, user id, etc.) with the Part 15 in order to operate. As mentioned earlier, under normal circumstances (non-emergencies) different services are not intended by the FCC to communicate with one another.*

Why use encryption when the primary purpose is authentication, these are two separate network protection issues? HSMM radio networks, at this stage in the development of the *Hinternet* (the radio amateur version of the Internet) are very simple networks.

Using the onboard encryption to also provide authentication is a readily available, economic and easy way for radio amateurs to protect their HSMM radio network, much as in the manner of FM repeater codes used to protect that type of system. Often clubs handle the WEP/WPA keys in the same manner as PL (Private Line, a Motorola term for limiting access to a repeater by requiring a sub-audio tone code on the incoming transmissions in order to activate the repeater's receiver). See the sidebar "Authentication and HSMM Networks" by Nate Duehr, WYØX, for a fuller explanation as to why radio amateurs often need to use encryption to achieve the one function that is actually needed, i.e., authentication.

However, because we are operating licensed HSMM radio, not unlicensed WiFi, and we have much greater communications capability in terms of antenna design, output power (up to 100 W for spread spectrum modulation), we must follow certain

HSMM Radio References

- Use of HSMM radio within Amateur Radio is a developing story. You can keep up with developments by visiting the Web site of the North Texas Microwave Society: **ntms-hsmm@yahoogroups.com**
- For more details about using HSMM radio for remote control of stations, see the article "Remote-Control HF Operation over the Internet," by Brad Wyatt, K6WR, *QST*, November 2001 p 47-48.
- For guidelines on using e-games on-the air in Amateur Radio, see the HSMM column titled "Is (*sic*) All Data Acceptable Data" by Neil Sablatzky, K8IT, in the Fall 2003 issue of *CQ VHF*.
- For more information regarding HSMM radio on future OSCAR satellites, visit **www.amsat.org**.
- Burger, Michael W, AH7R, and John J. Champa, K8OCL, "HSMM in a Briefcase," *CQ VHF*, Fall 2003, p 32.
- Champa, John, K8OCL, and Ron Olexa, KA3JIJ, "How To Get Into HSMM," *CQ VHF*, Fall 2003.
- Duntemann, Jeff, K7JPD, *Jeff Duntemann's Wi-Fi Guide*, 2nd Ed, Paraglyph Press, 2004.
- Flickenger, Rob, *Building Wireless Community Networks*, 2nd Ed, O'Reilly, 2003. (Available from the ARRL Book Store).
- Fordham, David, KD9LA, "802.11 Experiments in Virginia's Shenandoah Valley," *QST, July 2005.*
- Gast, Matthew S., *802.11 Wireless Networks, The Definitive Guide*, O'Reilly, 2002. (Available from the ARRL Book Store).
- Mraz, Kris I, N5KM, "High Speed Multimedia Radio," *QST*, April 2003, pp 28-34.
- Olexa, Ron, KA3JIJ, "Wi-Fi for Hams Part 1: Part 97 or Part 15," *CQ*, June 2003, pp 32-36.
- Olexa, Ron, KA3JIJ, "Wi-Fi for Hams Part 2: Building a Wi-Fi Network," *CQ*, July 2003, p 34-38.
- Rinaldo, Paul L., W4RI, and Champa, John J., K8OCL, "On The Amateur Radio Use of IEEE 802.11b Radio Local Area Networks," *CQ VHF*, Spring 2003, p 40-42.
- Rotolo, Don, N2IRZ, "A Cheap and Easy High-Speed Data Connection," *CQ*, February 2003, p 61-64.
- Rotolo, Don, N2IRZ, "Computers & Internet, Building a Decent RF Network", *CQ* 2005, October, p. 66.
- Rotolo, Don, N2IRZ, "Computers & Internet, Digital Connection: Wireless Local Area Network (LAN) Design", *CQ* 2006, December, p. 52.
- Rotolo, Don, N2IRZ, "Packet/Digital, Can HSMM Find a Real Home In Ham Radio? Plus More On RSQ", *CQ* 2005, April, p. 72.
- Rotolo, Don, N2IRZ, "Packet/Digital, Digital Connection: Data encryption is legal!" *CQ* 2006, August, p. 50.

Authentication and HSMM Networks

By Nate Duehr, WYØX

In Amateur Radio digital networks, we often find ourselves in the difficult situation of needing to meet FCC law stated in Part 97.113: Prohibited Transmissions. Where "messages encoded for the purpose of obscuring their meaning except as otherwise provided herein" are not allowed, we are also trying to keep non-Amateur-licensed users from accessing our networks, either accidentally or maliciously.

What amateurs need is a secured form of authentication (likely using encryption keys to encrypt the authentication headers on each packet/ frame of data), but not "payload/message encryption".

Amateurs in recent on-line discussions have pointed out that the IPSec standard allows for this type of partially encrypted packet structure which leaves the packet's payload unencrypted, while encrypting the packet header, but IPSec is not widely deployed in most IPv4 networks today. There are also no consumer-grade inexpensive 802.11 devices which can authenticate based solely on received IPSec packets.

To describe one of the dissenting viewpoints, many amateurs believe that the header information of the packet is still part of the overall "message" intended to be sent by the originating Amateur station. They believe that since part of the transmitter's signal is encrypted, the meaning of the overall message being sent is partially obscured.

Amateurs have debated numerous methods of keeping non-amateurs from joining their 802.11 networks accidentally or maliciously, and thus causing their stations to transmit under indirect control of an unlicensed person.

Many amateurs rely on filtering or blocking non-amateur traffic from unknown MAC addresses. This is ineffective since MAC addresses are sent in the clear in unsecured modes, and they can easily be "spoofed" by anyone to gain access to your amateur-based network. It offers no security at all from packet-sniffing/ snooping technology, available for free on the Internet.

Hash algorithms have also been recommended in online forums as a way to authenticate sessions using passphrases or other information to feed through the hash, producing a mathematically significant outcome that's reproducible using the same passphrase later on. The passphrase would only known to the two station operators, but again hashes are insecure because they're transmitted "in the clear" and are capable of being spoofed, once received.

Some have recommended only accessing things via HTTPS, not fully understanding that HTTPS is just HTTP (the main protocol that Web browsers utilize), which has been encapsulated inside of SSL/TLS (Secure Sockets Layer), a fully-encrypted streaming protocol, thus obscuring the entire message.

In all cases I've seen so far, there are no proposals that work with off-the-shelf equipment, and that don't have to rely on some form of encryption during at least some portion of the on-air packet sequences. Some portion of every packet must still be encrypted.

Since the security/encryption protocols in modern 802.11 APs already exist, are standardized, well-tested, and work between vendors, many HSMM Amateur Radio operators believe it is simply easier to encrypt the entire session.

Part 97.305(c)(3) appears to give us a way to use encrypted sessions, if we're willing to store the transmitted packets from our station. Packet capture of all transmitted traffic and storage of our digital station transmissions is relatively simple today, with the relatively low prices of computer media storage devices and recordable media.

It also seems reasonable to provide a copy of the network encryption key(s) to FCC on-demand, or to any other licensed radio amateur who wishes to monitor and/or join the network, for monitoring purposes, can be done immediately in real-time. If a station refuses to offer up their network key, they could be asked to cease transmission or restrict operation, as described in 97.305(c)(1) and (2).

The encryption debate will continue as long as radio amateurs continue to experiment. Realistically, the only high-confidence method of authenticating nodes or users participating in any on-air digital systems on an untrusted "public" network is via the utilization of modern encryption technology.

practices before using any encryption:

- Use only frequencies above 50 MHz
- Permit no international traffic
- Station identification must be at required times and always in the clear (not encrypted)
- The encryption algorithm used (WEP, WPA, etc.) must be a published algorithm
- Specific key(s) used by the HSMM radio station must be recorded in the station logbook
- All other restrictions regarding the nature of the Amateur Radio traffic apply (no music, etc.)

Most wireless routers will allow for the use of multiple WEP keys, typically up to four. This will allow you to configure the device so that different client stations have different access authority. For example, club members may have one level of access, while visiting radio amateurs may be given a lesser access. Most HSMM radio groups have just one WEP key and everybody gets that one. It is treated in the same fashion, and for much the same purpose, as a repeater's PL tone.

Remember that when it comes to the length of the WEP or other key used, our main purpose is to provide a simple and economical means of authentication already available on the wireless devices. In other words, it is to ensure that only Part 97 stations and not Part 15 stations auto-associate or auto-connect with our

HSMM radio node. The shorter the WEP key, the better! This makes it easy to use and remember. During early HSMM radio experimenting at the turn of the century the shortest possible key (5 characters) was used: HSMM-

AUTHENTICATION TYPE: Some routers will ask for the type of authentication you want to use such as *shared key, open system*, and *both*. Click on **shared key** because you will be sharing the WEP/WPA key with any and all radio amateurs who wish to access your HSMM radio node.

DHCP: Some routers will ask if you want Dynamic Host Configuration Protocol enabled. This is the function that assigns IP addresses. Unless you have another source of the DHCP function on your network, you will want to **ENABLE** this function.

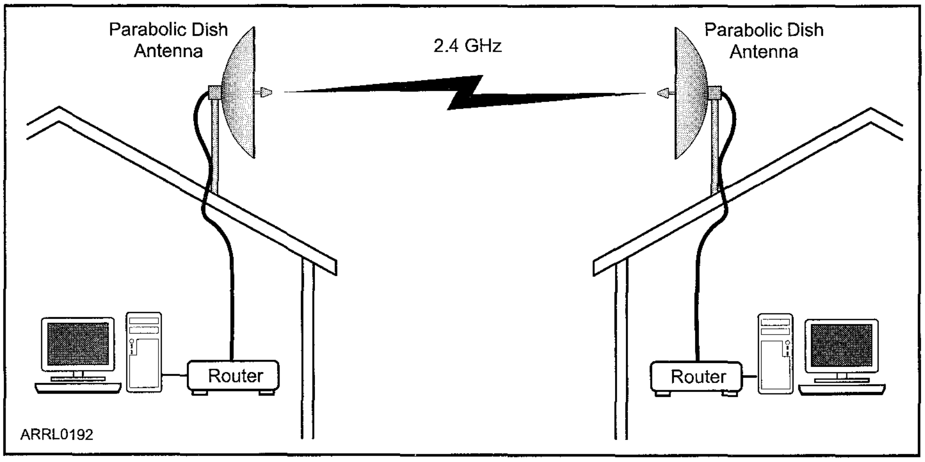

Figure 7-5—This is a simplified diagram of a typical HSMM link between two stations. Note that high gain parabolic dish antennas are being used in this example.

ANTENNA SELECTION: A few wireless routers with dual antennas will ask you select an antenna. The default is normally receive space diversity. Because we are going to connect an outside gain antenna, you want to make a selection. Otherwise, you will need to identify which antenna is the actual transmit antenna and connect the feed line to that port.

MAC ADDRESS FILTER: Some wireless routers will allow for this security measure, but it is troublesome to administer it, so it is recommended that you not bother enabling this function. Use WEP or some other method of encryption using the guidelines discussed previously.

OUTPUT POWER: Some wireless routers will allow you to set this power level, often up to 100 mW. As with all other radio amateur operations use only the minimum power needed to accomplish your mission.

If you have selected the Linksys WRT54GL as your host computer's device, this link will help talk you through the set-up: **www.youtube.com/watch?v=No_NyW2Ug9o.**

The Far End of the Link

Next we will address the client end of the link. See **Figure 7-5**. The core of the other end of the HSMM radio link is a computer-operated HSMM 2.4 GHz radio transceiver or simply a PC client adapter. It will probably cost well under $80, especially if you are able to find some older 802.11b cards. A friend of mine, Randy Dunning, KC5QHH, recently purchased one of these PC card transceivers at a flea market for only $5, yet it runs a mighty 200 mW of RF transmitter output power and has a reasonably good quality receiver.

These transceivers/wireless adapter cards usually come in three forms:

(1) One form is called a PC cards as described above. Earlier these were called PCMCIA cards, but more recent terminology is to simply call them laptop PC cards.

(2) Another type of transceiver/adaptor comes with a USB interface. This is often considered a superior interface for most HSMM stations. The reason for this has nothing to do with the quality of the transceiver, but rather the fragile nature of the tiny connectors (MMCX, etc.) that are found on the PC cards. They are not really designed for frequent plugging and unplugging. Without extreme care, they can be easily torn out. An example of a wireless USB adapter is shown in **Figure 7-6.**

(3) Linksys and other manufactures also produce similar cards for the expansion slot on the rear of your desktop PC too. For example, the Linksys Wireless-G PCI Adapter WMP54G shown in **Figure 7-7.**

Just make certain that regardless of which model client card or type of USB or expansion port interface you purchase has an antenna that is removable or has an external antenna port of some type!

(4) If you are not afraid to modify your laptop, you can access the wireless adaptor built into many new laptops and add a small SMA connector. See **http://repair4laptop.org/wireless_lan_antenna.html.**

Figure 7-6—This 802.11 b/g Wireless LAN USB Adapter features an external RP-SMA female connector if you wanted to extend its range with an optional antenna. Transmit power is a standard 15dBm It is perfect to travel with and it is the size of a removable USB Thumb Drive, so you can keep it in your pocket!

To connect to the AP/wireless router in an HSMM radio network the wireless computer user(s) at the far end must 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 (the host station call sign), so set your computer station to recognize the SSID you assigned to the AP/wireless router to which you wish to connect.

You may need to use either an adaptor or a short pigtail to connect the card's MMCX antenna port or the interface's RP antenna connector to the N-series connector on the coaxial cable run to the antenna. Fortunately at the other end, most 2.4 GHz antennas come with a female N-series connector.

Team up with a nearby radio amateur to test. Do your initial testing in the same room together making sure the link-up is working. Then as you increase distances going toward your separate station locations, you can coordinate using a suitable local FM simplex frequency. You will increasingly need this communication to assist with directional antenna orientation as you get further apart.

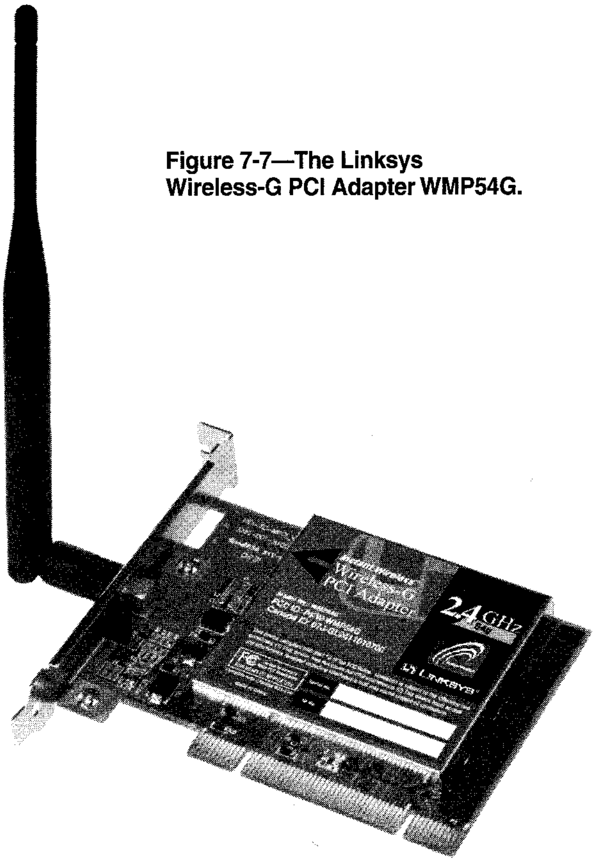

Figure 7-7—The Linksys Wireless-G PCI Adapter WMP54G.

MOBILE HSMM OPERATING

When hams use the term "mobile HSMM station" what they are 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 would be very dangerous and possibly make you immediately eligible for the Silent Keys list in *QST* magazine! So unless you have someone else driving the vehicle, keep your eyes on the road and not on the computer screen!

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

- A portable computer, such as laptop or mini-computer. A PDA might be made to work but software for such devices may be problematic. The operating system can be *Microsoft Windows*, *Linux*, or *Mac OS*, although *Microsoft XP* offers some better WLAN functionality.
- PC Card wireless client adaptor card with at least one external antenna port.
- Pig tail assembly as described earlier, with a short length of low-loss coaxial cable.
- Topographic maps or mapping software of the area.
- A small power inverter (~200W) to convert your vehicle's 13.8 Vdc to 115 Vac to keep the laptop battery charged. Running the laptop plus a small transceiver drains the onboard battery fairly quickly.
- Two antennas. One omnidirectional magnet mount on the roof of the vehicle, and another directional antenna that can be clip mounted on a window edge or placed outside the vehicle on a small tripod or portable mast.

Some type of radio software hams 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 for Windows* or *NetStumbler*. All operating systems have monitoring programs that are available. *Linux* has *Kismet*; *MAC OS* has *MacStumbler*. Marius Milner has a version for the PocketPC, which he calls *MiniStumbler*. Whichever monitoring utility you use, make certain it supports the specific PC card you are using too.

While operating your HSMM mobile station, if you monitor an unlicensed Part 15 station (non-ham), most types of WiFi equipment will automatically associate or link to such stations. 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 various steps you can take to prevent Part 15 stations from automatically linking with HSMM stations. So in like manner, except in the case of a communications emergency, we recommend that you do not use a Part 15 station's Internet connection for any radio amateur purpose.

HSMM AREA SURVEYS

Area or site surveys were mentioned earlier. Exactly how should these be conducted?

Both licensed amateurs (FCC Part 97 Regulations) and unlicensed (FCC Part 15 Regulations) stations use the 2.4-GHz band. To be a good neighbor, find out what others are doing in your area before designing your community HSMM radio network or long range link. This is easy to do using IEEE 802.11 modulation. Unless it has been disabled, an access point/router is constantly sending out an identification beacon known as its SSID. In HSMM practice this is simply the radio amateur station call sign (and perhaps the local radio club name) entered into the software configuration supplied on the CD that comes with the device.

An area or site survey using appropriate monitoring software, for example the free *NetStumbler* software downloaded and running on your PC (**www.netstumbler.com/index.php**), is recommended prior to starting up any HSMM operations. Slew your station's directional antenna through a 360-degree arc, and drive your HSMM mobile station (described earlier) around your local area. This HSMM area survey will identify and automatically log most other 802.11 station activity in your area. There are many different ways to avoid interference with other users of the band when planning your HSMM operations. Moving your operating frequency 2-3 channels away from the other stations is often sufficient.

RUNNING HIGH POWER

It is tempting for some radio amateurs to think that if they run higher power they will get better range out of their HSMM radio station. This is not always the case. There are many factors involved in range determination when operating UHF or microwave frequencies. The first and most significant of these is the lay of land (topology) and path obstructions. Running additional power is unlikely to correct for either of these impediments.

Second, running higher power to improve signal link margins often requires that this be done at both ends of the link to obtain meaningful results.

Third, most RF amplifiers for use with 802.11 modulations are of the BDA (bi-directional amplifier) type. They amplify both the incoming signal and the outgoing signal using a HS switch, with perhaps some AGC (automatic gain control) function in more sophisticated models. That means to get maximum effectiveness out of such devices they must be mounted as close as possible to the antenna.

Fourth, 802.11 signals from such inexpensive broadband devices often come with significant sidebands. This is not prime RF suitable for amplification! A tuned RF channel filter should be added to the system to reduce these sidebands and to avoid splatter.

Also, if your HSMM radio station is next door to an OSCAR satellite ground station or other licensed user of the band, you may need to take extra steps in order to avoid interfering with them, such as moving to channel 4 or even channel 5. In this case a tuned output filter may be necessary to avoid not only causing QRM, but also to prevent some of your now amplified sidebands from going outside the amateur band, which stops at 2450 MHz.

Nonetheless, achieving the network design objectives, especially in the case of EMCOM, may require the use of high-power to overcome the noise and Part 15 interference on the band. Higher power output may be needed to improve the reliability of the link. Generally when speaking of "high-power" HSMM radio amateurs mean 1-3 W of RF output power. Beyond that level becomes very expensive and the additional signal strength can be more economically and appropriately obtained with the use of higher gain, more directive antennas arrays.

Only after an HSMM radio link analysis (see **logidac.com/gfk/80211link/pathAnalysis.html**) clearly indicates that additional RF output power is required to achieve the desired path distance and a thorough RF area survey has been conducted, should more RF power output be considered. Even then, do not use higher power as a substitute for higher antenna gain at both ends of the link. Only after all reasonable efforts have been taken to get the highest possible antenna system gain and directivity, and the link is still not meeting requirements, should higher power be employed. At that point in the analysis showing that higher power is required, what is needed is called a *bi-directional amplifier.* It is usually mounted at the end of the antenna pig-tail near the top of the tower or mast for maximum efficiency. See **Figure 7-8**.

The importance of the RF area survey cannot be over emphasized. The control operator needs to be continually aware of the Part 15 surrounding activities and sources, especially along the directional path of the RF beamed signal from their station.

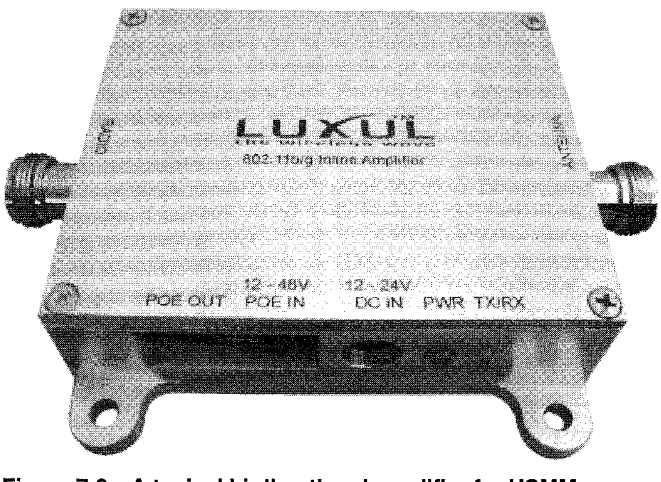

Figure 7-8—A typical bi-directional amplifier for HSMM applications. This unit delivers 1 W output.

To date radio amateurs have never been attributed to being the source of a library, school, police station's etc. WLAN being ground to a halt by being in the path of a strong Part 97 station signal running 1-3 W output. That may not sound like a lot of power, but it is much higher than normal Part 15 power. You don't want to be the first! Run higher power with care and only as a last resort. As radio amateurs we have the right, and the FCC has always supported that right against Part 15 objections, but the political reality is that Part 15 stations out number us by 100,000 to 1, if not more. Be careful, please!

Automatic Power Control

It should be noted that the existing FCC Amateur Radio regulations covering spread spectrum 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 modulations for various reasons. As a result the FCC has communicated to the ARRL that the APC provision of the existing spread spectrum regulations are therefore not applicable to 802.11 emissions under Part 97.

However, using higher than normal output power in HSMM 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 path conditions and the existing 802.11 activity in your area. Using the minimum power necessary for the communications is the law and has always been a good operating practice for hams.

HSMM ANTENNA SYSTEMS

There are a number of factors that determine the best antenna design for a specific HSMM radio application. Most commonly, HSMM stations use horizontal instead of vertical polarization. It seems to work better than vertical polarization. In addition, most Part 15 stations are vertically polarized, so this is sometimes thought to provide another small barrier between the two different services sharing the band. With multipath propagation is it doubtful how much real isolation this polarization change actually provides.

More importantly, most HSMM radio 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 modulations means higher rate data throughput. Higher data throughput, in turn, translates into more multimedia radio capability. Look at **Figure 7-9**. The Valley ARA and the Massanutten ARA set up an elaborate HSMM network on Field Day, using high-gain directional antennas on mountaintops to span as much as 17 miles!

Highly directional antennas also have many other advantages. Such antennas can allow two radio amateurs to shoot their narrow beam width signals over, or shoot around, or even shoot between, other wireless stations on the band. However, the nature of 802.11 modulations coupled with the various configurations of many COTS devices allows hams to economically experiment with many other fascinating antenna designs. Such unique antenna system designs can be used to simply help avoid interference, or to extend the range of the station. For example, much more experimenting needs to be done with the use of circularly polarized (CP) antennas instead of liner polarized

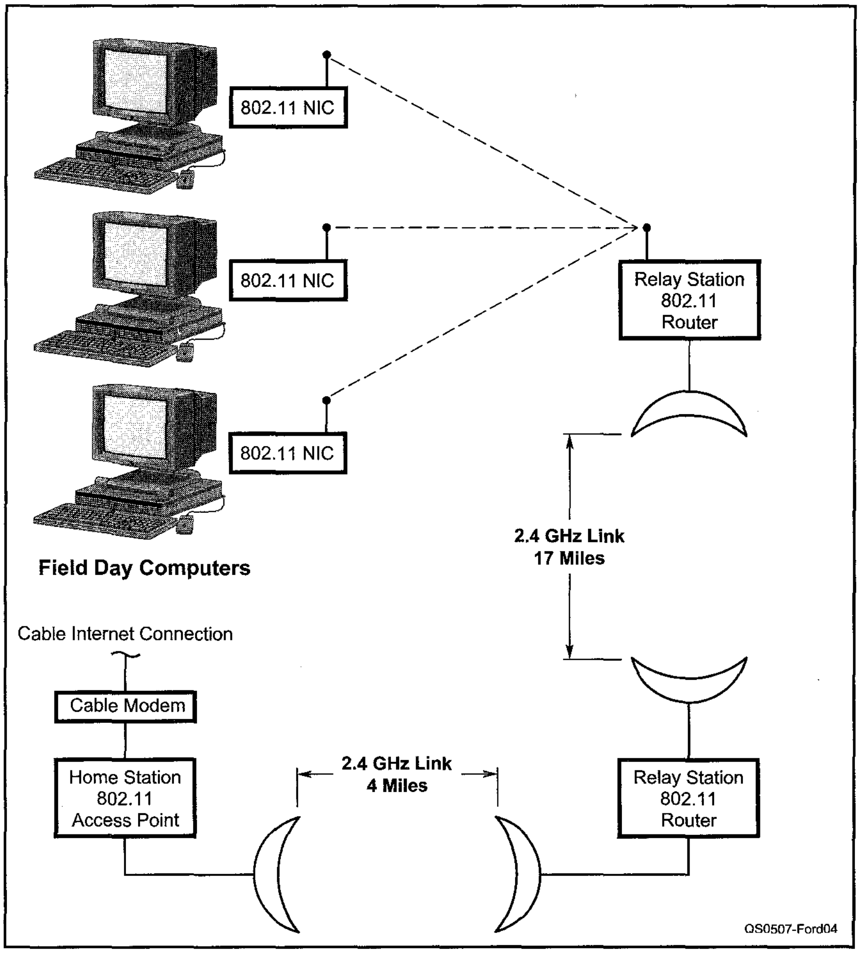

Figure 7-9—The Valley ARA and the Massanutten ARA set up this complex HSMM network for their Field Day operations. Note the long links supported by parabolic dish antennas, as well as the final link to the Internet.

antennas. What about the isolation provided between left-handed CP and right-handed CP? Would using two antennas of different handiness for receive space diversity produce significantly better reception? These are questions for which we don't have answers at this time.

Space Diversity

Some AP/wireless routers have space diversity capability built-into their design. However, as mentioned previously, it is not always operated in the same fashion, so check the literature or the Web site of your particular device manufacturer to be certain how the dual antenna ports are used. Many APs come equipped with two rubber ducky antennas and two antenna ports. One antenna port may be the primary and the other port the secondary input to the transceiver. Which signal input is used may depends on which antenna is providing the best S/N ratio at that specific instant.

The antenna spacing on the back panel of the AP provides a very minimum antenna separation to achieve space diversity. Try experimenting with two outside high-gain antennas spaced 10 or more wavelengths apart (that is only about one meter on the 2.4-GHz band). It may be very worthwhile in improving the quality of the link and the resulting speed of data throughput, especially on long links. Such extended radio paths tend to experience more multipath signal distortion. This multipath effect is caused by multiple signal reflections off various objects in the path of the linking signal. The use of space diversity techniques helps reduce this effect and thus improve the data rate throughput on the link. The higher the date rate means that more multimedia (MM) capability is built into radio link.

Circular Polarization

Another technique that warrants further investigation is the use of circular polarization. Radio amateurs have used such antennas for year in satellite communications. They are easily home-made devices. See **Figure 7-10**.

The use of circular polarization (CP) using helical antennas, patch feedpoints on dish antennas or other means, warrants further study by radio amateurs. Remember this is HS digital radio. The use of CP antennas may help avoid symbol errors. Circularly polarized antennas should be used at both ends of the link. Also, be certain that the antennas are of the same *handedness*, for example, right-hand circular polarization (RHCP). The ability of circular polarization to enhance propagation of long-path HSMM radio signals should not be overlooked.

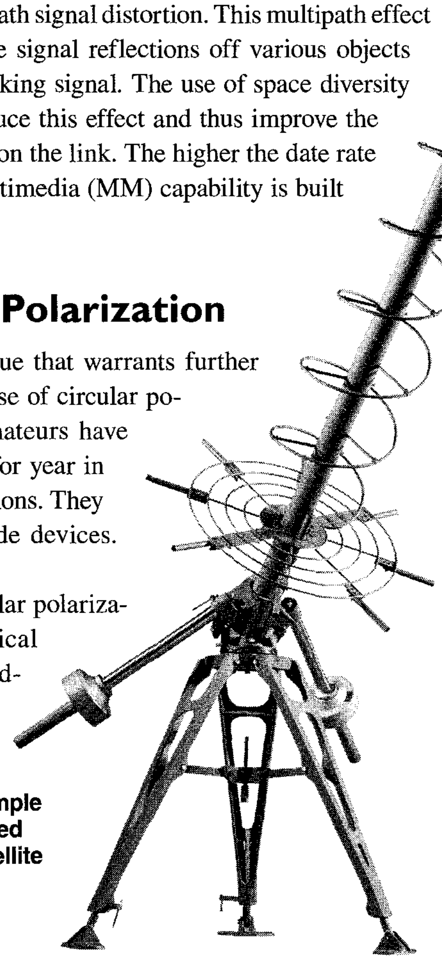

Figure 7-10—An example of a circularly polarized antenna used for satellite communications.

Circularly Polarized Space Diversity

A combination or hybrid antenna design combining both circularly polarized antennas and space diversity could yield some extraordinary signal propagation results. For example, it has been suggested that using an RHCP for one antenna and LHCP for the other antenna, plus using antenna spacing greater than 10 wavelengths, could provide a nearly "bullet-proof" design. Only actual field testing of such designs under different terrain features would reveal such potential.

Mixed Antenna Design Issue

In conventional wide-bandwidth analog radio antennas systems, so long as both antennas at both ends of a radio link have broad bandwidths and the same polarization, all is fine.

While this may be true for wide bandwidth analog signals, such as amateur television VSB (vestigial sideband) signals or FM ATV signals, it may not be true for broad bandwidth high-speed digital signals.

802.11 signals produce very broadband signals, typically 20-22 MHz. There is evidence to date that indicates the use of a same polarized antenna with one type of feed point at one end of the link and the use of a same polarized antenna with a different type of feed point at the other end of the link, may introduce a problem with HS digital signals. A common example of this potential mixed-antenna issue would be if one HSMM radio station uses a horizontally polarized linear Yagi, while the other HSMM radio station at the opposite end of the link uses a horizontally polarized loop Yagi.

Here is another typical situation. Let us say the ham at one end of the radio path uses a dish antenna with a horizontal dipole feed point. The other ham at the opposite end of the path uses a horizontally polarized loop Yagi. Both antennas have gain, both antennas are broad bandwidth designs, and both antennas are horizontally polarized. Nonetheless, the radio amateur experimenters may experience higher BER (bit error rate) because of symbol errors caused by the different manner in which the two antennas manipulate the digital radio signal wave front.

Further radio amateur experimentation with HSMM radio signals is warranted to determine the full impact on the radio link of using mixed antenna types.

INFORMATION SECURITY

An HSMM radio station can be considered a form of software defined radio (SDR). Your computer running the appropriate software combined with the wireless adaptor or router creates a single unit, which is now your station's HSMM radio transceiver. Unlike other radios, your HSMM radio is now a networked radio device. It could be connected directly to other computers (ad hoc mode) and to other radio networks (infrastructure mode) and even to the Internet. So each HSMM radio station needs to be protected.

There are at least two basic steps that should be taken with regards to all HSMM radios:

(1) The PC should be provided with a current antivirus/antispyware program(s). This software must be regularly updated to remain effective. Such programs may have come with the PC when it was purchased. If that is not the case, reasonably priced and even free anti-virus programs are readily available from a number of sources, e.g. AVG (**http://free.grisoft.com/**).

(2) It is important to use a firewall software program or hardware on your HSMM radio. The firewall should be configured to allow all outgoing traffic, but to restrict all incoming traffic without specific authorization. Commercial personal computer firewall products are available from Symantec, ZoneLabs and McAfee Network Associates. Check this URL for a list of freeware firewalls for your personal computer: **www.webattack.com/freeware/security/fwfirewall.shtml**. Check this URL for a list of shareware firewalls for your personal computer: **www.webattack.com/Shareware/security/swfirewall.shtml**.

HSMM ON OTHER BANDS

Up to this point all the discussion has been regarding HSMM radio operations on the 2.4-GHz amateur band. However, 802.11 signals can be used on any amateur band above 902 MHz.

FM repeaters may not have a problem with sharing the frequency with 802.11 operations, since they would likely just hear an 802.11 modulated signal as weak background noise, and the 802.11 modulation, especially the OFDM channels used by 802.11g, would simply work around the FM interference with little negative impact.

There is some older 802.11 gear (FHSS) available on the surplus market for amateur experimentation. Alternatively, some form of frequency transverter may be used to take 2.4 GHz to the 902-MHz band.

The 1.2-GHz band has some potential for 802.11 experimenting. Some areas have several FM voice repeaters and even ATV FM repeaters on the band. But again these relatively narrow bandwidth signals would likely hear any 802.11 modulations as simply background noise.

Looking at the potential interference from the HSMM radio perspective, even in the case of the FM ATV, it is unlikely the signal would significantly disrupt the 802.11 modulation unless the two signals were on exactly the same center frequency or at least with complete overlap in bandwidth. Keep in mind that the FM ATV signal is only several megahertz wide, but the 802.11 modulation is 20 - 22 MHz wide. For the analog signal to wipe out the spread spectrum signal, it would need to overpower or completely swamp the 802.11 receiver's front end.

The 3.5-GHz band offers some real possibilities for 802.11 developments. Frequency transverters are available to get to the band from 2.4 GHz and there is little other activity on the band at this time. Developments in Europe of 802.16 with 108 Mbit/s data throughput may make 3.5-GHz gear available for amateur experimentation in the US. Radio amateurs are investigating the feasibility of using such gear when it becomes available in the US for providing a RMAN or *radio metropolitan area networks*. The RMAN would be used to link the individual HSMM radio repeaters (AP/wireless routers) or RLANs together in order to provide county-wide or regional HSMM radio coverage, depending on the Amateur Radio population density.

The 5-GHz band is also being investigated. Some US manufactured COTS 802.11a modulation gear has OFDM channels that operate in this Amateur Radio band. The 802.11a modulation could be used in a HSMM RLAN operating 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 MAN links. This band is also being considered by AMSAT for what is known as an ADX (Advanced Digital Transponder). This would be an HSMM radio transponder onboard a Phase-3 high orbit satellite (HOS), or even a high-altitude or a Phase-4 geostationary OSCAR. Another form of modulation such as TDMA (time division multiple access) would likely have to be used because of signal timing issues and other factors, but the concept is at least being seriously discussed.

RMAN link alternatives are also being tested by radio amateurs. One of these is the use of *virtual private networks* (VPN) similar to the method currently used to provide worldwide FM voice repeater links via the Internet.

Acknowledgements

The author would like to express his appreciation to the following individuals for their intellectual contributions to this chapter: Nathan Duehr, WYØX; Tim Gorman, ABØWR, Douglas Kilgore, KD5OUG and Les Rayburn, N1LF.