Monitoring Spread Spectrum Comms

By Tom Filecco

Having an interest in unusual and "exotic" communications equipment, I recently acquired a frequency hopping spread spectrum (FHSS) transceiver. FHSS is used as a means of combating jamming and signal interception in a few communications systems. The biggest one that comes to mind is SINCGARS (Single Channel Ground/Air Communications System) used by the U.S. Military. I wanted to see just how secure it is against commonly available commercial off-the-shelf equipment. The unit I acquired operated in the VHF-high band, and when not in "comsec mode" was a single channel frequency agile transceiver operating in the 163-173 Mhz. Range. The following pieces of equipment were used in evaluating the transceiver:

- Information Security Associates ECR-1 TSCM receiver/spectrum analyzer.
- Optoelectronics R-10 Interceptor near field receiver.
- Icom R-10 communications receiver.
- Aceco FC3002 frequency counter (reaction tune capability with Icom receiver).

The objectives of this exercise were to determine how easily it would be to detect the FHSS signal, and to see if it were possible to actually hear the transmitted audio while in FHSS mode.

The first step was to fire the thing up in single channel mode, make sure it worked, and make sure the test equipment worked. The transceiver was attached to a dummy load, and keyed up in single channel mode. It was a stock VHF-high FM transceiver. The ECR-1 showed a nice spike on the screen, the Opto Interceptor locked on the signal, and the Aceco frequency counter registered a hit and tuned the Icom R-10 to the frequency. No problem. Now for things to get interesting.

I flipped the "comsec mode" switch to "on", and keyed the thing up. The first thing I noticed was that the frequency counter and Icom receiver reaction-tune combo did not detect a signal. That was no surprise. The FHSS signal hopped too quickly for the counter to get a lock, yet alone tune a receiver via a 9600 baud TTL serial link. Optoelectronics is currently selling a "Digital Scout" that allegedly has the capability to measure TX frequency on FHSS signals. Since I don't have one handy to evaluate, it remains to be seen how well it would work. Taking the Aceco out of "capture mode" and using it as a regular frequency counter however would result in the frequency display showing a signal within 500 KHz.-1 MHz. The counter had to be within a foot of the transmitter (keying into a dummy load though) to get this reading however.

The next piece of test equipment I checked was the ECR-1. The spectrum display clearly showed a nice FHSS signal. One could even narrow the display down to the 10 MHz. of spectrum the transceiver operated on, and make out individual frequencies in the hopping pattern. The receiver's sweep speed, however was not quick enough to make out the audio of the transmitter while it was in FHSS mode. All one heard was a "popping" sound above the squelch noise. A FHSS signal makes a distinguishable pattern on a spectrum display, provided one is looking at a wide enough chunk of the spectrum. If I went down to too narrow a display, I wound up "missing" parts of the hopping sequence, and an unskilled operator may overlook the signal. Interestingly enough, on a wide enough sweep range, I could make out the second harmonic of the transmitter hopping in time to the fundamental frequency.

Finally there was the surprise of the experiment. The Optoelectronics R-10 Interceptor continually locked on to, and followed the FHSS signal. The sweep speed of the R-10 was quick enough to allow one to hear the transmitted audio! It wasn't perfect. The audio sounded "clipped" as the Interceptor was still playing catch-up. The Interceptor near field receiver would lock onto any strong local signal, and this would result in losing the FHSS signal. Upon hitting the skip button on the Interceptor however, it would shortly reacquire the signal. The evaluation was done in a rural area where there were few "near field" signals, which meant there was little for the Interceptor to lock onto. This technique would probably be less effective in an urban area with more radio traffic. The lack of a delay period before resuming its sweep proved to be a handy feature for tracking the FHSS signal well enough to hear the transmitted audio. The Interceptor is a neat piece of equipment that many hobbyists didn't understand, but the pros knew better. It harks back to the days before the cellular phone companies managed to pay off enough congressmen to declare 54 MHz. of spectrum "private" (as if passing a law would do that).

In conclusion, FHSS is readily detectable and even able to be monitored under certain circumstances depending on available equipment and other factors. There are few things a skilled operator with a spectrum analyzer cannot detect; which is probably why it is the number one piece of equipment used for RF sweeps by TSCM pros. The transceiver I used for the evaluation only operated in a small 10 MHz. piece of RF spectrum. SINCGARS transceivers have 58 MHz. of operating space, so I suspect monitoring more modern FHSS equipment would be more difficult. Additionally, encrypting the signal with a good cryptographic system would prevent communications from being monitored (but not detected); which is the case with the latest SINCGARS units. Frequency hopping spread spectrum in itself does offer security against the casual listener, and others using less sophisticated monitoring equipment and techniques.