HOMING IN

Number 19 on your Feedback card

Radio Direction Finding

Joe Moell P.E. KØOV
PO Box 2508
Fullerton CA 92633

Testing Motron's Transmitter Fingerprinter

According to many hams, Southern California has a reputation for being the repeater-jamming capital of the world. As someone who has traveled and talked to many repeater owners and users, I think that reputation is undeserved. The sad truth is that you can find examples of illegal repeater use in big cities and small towns everywhere.

With hundreds of coordinated 2 meter repeaters between Santa Barbara and the Mexican border, hams here can be proud that only a handful have ongoing problems with jamming, bootleggers, and unidentified transmissions. The rest are full of friendly and helpful hams who seldom face these problems.

Of course, there are occasions when nets and round tables on even our "cleanest" repeaters are brought to a halt by carriers, tones, and cuss words. When a phone call goes out to a radio direction finding (RDF) team, the job is not easy if there are many perpetrators in scattered locations. It would be a huge help to be able to separate and identify which transmissions come from which source.

Just Like Snowflakes

We all know that every human is unique and can be identified from all others by differences in the skin patterns on the fingertips and DNA in the cells. These methods require the person to submit to examination or testing. When this is not possible or desired, a voiceprint can be done from a distance, without the knowledge of the subject, at the cost of greater uncertainty.

Similarly, every radio transmitter is unique. You cannot read the serial number on its nameplate from a distance, but you can identify it by analyzing, with sufficient precision, the characteristics of its signal. Differences in signals, however slight, are always present due to differences in individual parts and the randomness in factory testing and tuning techniques.

You may have heard reports of unique transmitter "signatures" and a technique called "fingerprinting" to identify rigs used for illegal activities and to apprehend their owners. What these reports usually leave out is the fact that this technique was invented by a ham and such equipment is now available for purchase.

A Sleepless Experimenter

When I spent nine months on assignment in Seattle back in 1972, the city's most popular repeater was run by Phil Ferrell W7PUG, an engineer at The Boeing Company. Today, this repeater is as popular as ever, Phil is K7PF, and he has retired to work on his own pet projects.

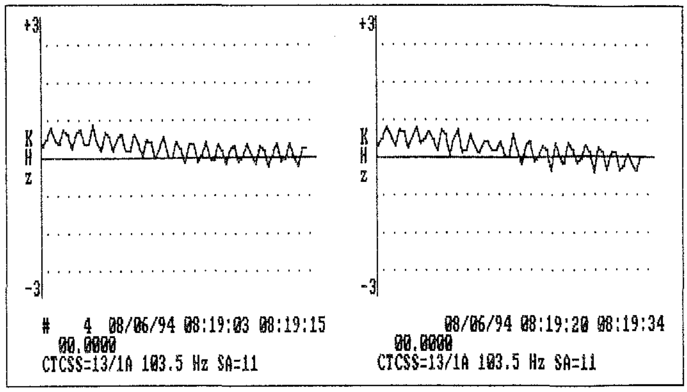

Figure 1. Two consecutive transmissions from a crystal-controlled repeater transmitter. Subaudible tone modulation (CTCSS) is plainly visible. TxID-1 computes and displays the CTCSS frequency below the trace.

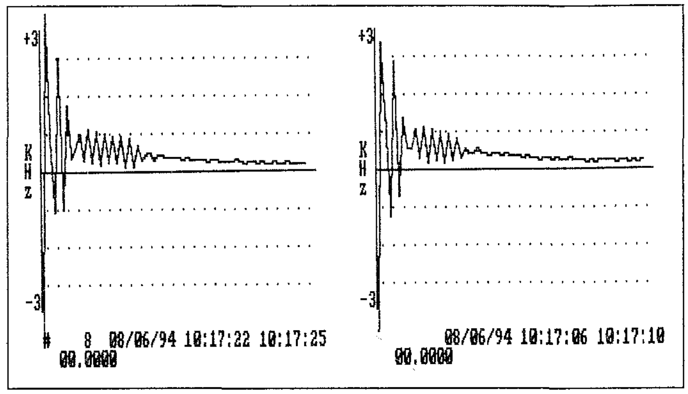

Figure 2. Two consecutive transmissions from the same FT-530 handie-talkie on the same frequency. Except for the ringing duration, the fingerprints are almost identical.

In the mid '80s, when unidentified signals appeared on the Seattle repeater Phil decided to fight back by using his knowledge of signal analysis. He reasoned that most of the offending transmitters were owned by licensed hams and could be identified by comparing their signals to those of regular and occasional repeater users.

The first design challenge was to figure out what signal characteristics to look at. "I had heard FM transmitters come on the air on top of one another," says Phil. "There would be a heterodyne with a chirp or quickly warbling tone at the beginning, as the phase-locked loop (PLL) settled on frequency. I researched PLL theory, which goes into a branch of math involving Gilbert transforms. That wasn't helpful, so I tried looking at it as a low-bandwidth FM phenomenon."

After some experimentation, his transmitter fingerprinting scheme took shape. It takes 2,048 instantaneous frequency samples at 100 microsecond intervals at the beginning of a transmission, then averages and filters this data to display and record 64 super-samples of frequency versus time.

"Amplitude and multipath don't have much effect," says K7PF. "It's a robust technique and works under almost all conditions. Even on signals of -120 or -125 dBm, when the audio is almost unintelligible, the low bandwidth of the system gives a pretty decent fingerprint."

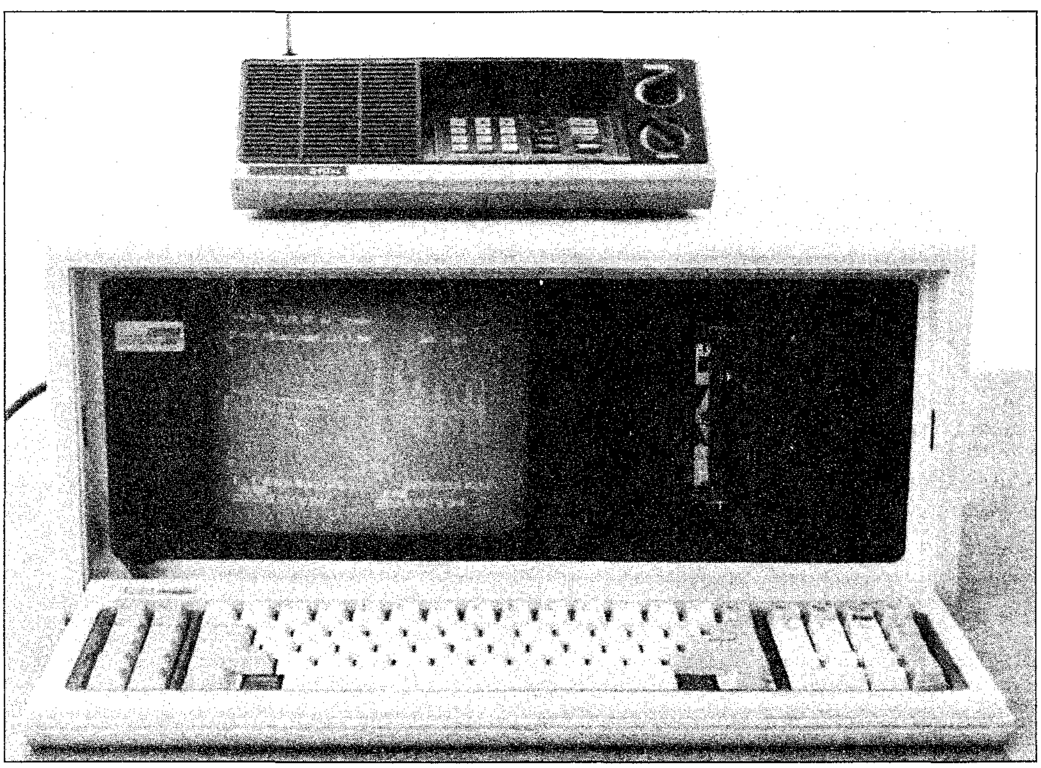

Photo A. All you need to take transmitter fingerprints is a suitable receiver and a computer with the TxID-1 hardware and software installed. Not shown is an optional tape recorder for documenting audio and fingerprints simultaneously.

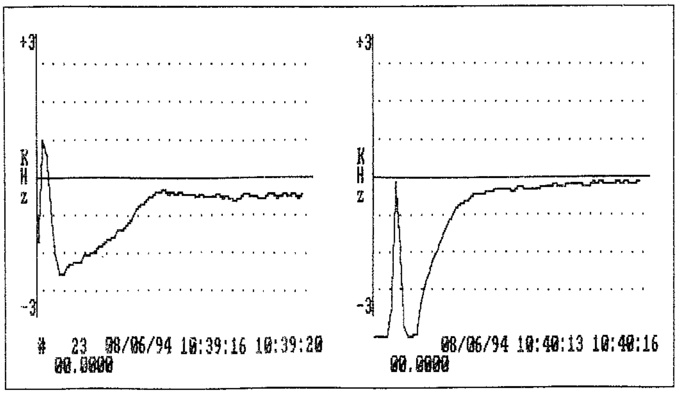

Figure 3. These two HTX-202 transceivers were bought at the same time, but have distinctly different fingerprints. They were set for the same power level on the same frequency.

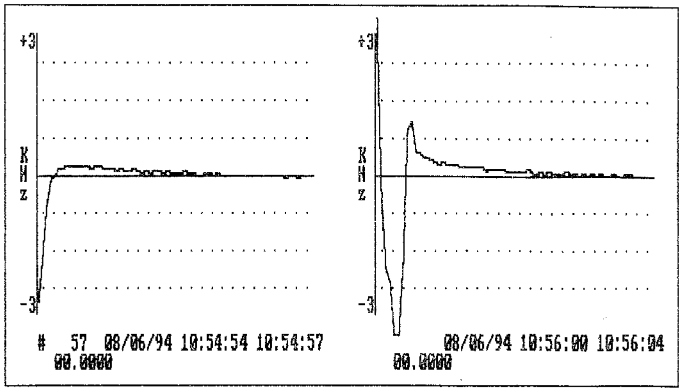

Figure 4. In a rapid-exchange QSO, this TH-78A produces consistent fingerprints like the one at left. If the rig sits for a few moments until the battery-saver feature activates, the next transmission looks like the trace at right.

There were distinctive characteristics on every radio he tested, even those of the same model. "I was showing the system at a club meeting and a husband and wife stood up," he goes on. "They both had brand-new Alinco handhelds with adjacent serial numbers. He told me flat out he thought they would have identical fingerprints. I was standing there kinda sweating and said, 'Well, I don't think so, but we'll take a look.' I finished the talk and got to the demonstration time and they immediately leaped to their feet. We checked the rigs and they were like chalk and cheese, totally different.

"A small percentage of rigs have two or more fingerprints. Theoretically, there are two predictable routes for PLL lockup. It's unlikely a given radio would be set up so it could take both routes, but it can happen." A rig's fingerprint may change slightly as you tune different parts of the same ham band. Dual- and multiband VHF/UHF rigs have completely different prints on each band.

K7PF soon realized he had a marketable signal identification system. "In a rare moment of greed, I ran it past the Boeing patent staff," he says with a chuckle. "That turned out to be a good move." Transmitter fingerprinting is now patented and assigned to Boeing, who sees to it that nobody makes commercial use of this idea without compensating Boeing and K7PF for it.

Next, FCC heard about fingerprinting and asked for some of Ferrell's equipment to evaluate. About this time, Don Moser AA7Y of Motron Electronics heard about the system at the Sea-Pac ham convention. K7PF showed AA7Y his breadboard and they worked out a deal for Motron to manufacture the circuit boards for Ferrell's FCC contract and to market the finished product, called the TxID-1, to the public.

Dozens of 78s

Phil's description fingerprinting made sense to me, but I was a bit skeptical at first about just 64 super-samples providing positive identification of like-model transmitters. For a rigorous test, I decided to take TxID-1 to a meeting of the 78's Amateur Radio Club. This group was formed to teach the arcane art of programming the

Kenwood TH-78A handheld to new purchasers. Dozens of TH-78s and other HTs would be there. Could TxID-1 display the unique features of many rigs of the same type?

Motron's TxID-1 system consists of the data acquisition and control board that plugs into the expansion slot of an IBM PC or compatible computer, an interface board, and a PC software program written by George Hadley N7SNI. TxID-1 connects directly to the receiver's discriminator and includes its own fast squelch circuit for uniform timing.

For this experiment, I mounted the main board in WB6UZZ's Compaq Portable 286 PC and connected it to a Bearcat BC210XL scanner (Photo A). The interface board (Photo B) plugs into the TxID-1 main board and has connections for receiver discriminator (mandatory) and AGC (optional). The BC210 is easy to adapt to TxID-1. There is plenty of room inside, RCA jacks mount readily on the steel rear panel, and its discriminator tap-off point is easy to locate.

Discriminator polarity and voltage swing differ among receiver models. To ensure that TxID-1 accurately displays the instantaneous frequency, you must calibrate the discriminator frequency-versus-voltage curve in 1 kHz steps. I used a TS-700A VFO-controlled rig and a VHF frequency counter to get the data for the BC21ØXL passband in about 10 minutes.

With this data, running OPAMP.EXE (supplied on the program disk) calculates values of two resistors to set gain and polarity of the input operational amplifier on the TxID-1 board to match your receiver. I ran the program, found the resistors in my junkbox, and soldered them to the supplied component header in less than 15 minutes. Note that the whole procedure must be done over if you change receivers.

I tested version 1.15, the current software revision, which is menu-driven with single-character commands. It supports the Microsoft Mouse, but not Windows. A 486 with fast hard drive and VGA/EGA monitor provides best performance, but a compatible with 512K memory, CGA graphics, and a floppy drive will do.

I tried to enter the frequency to be displayed in the fingerprint disk file, but the entry was not accepted. AA7Y says this is a software bug that will be fixed in the next revision. That is why all the plots in this review show 00.0000 on the frequency line. The first signal I fingerprinted was a crystal-controlled repeater output (Figure 1). Most repeaters have continuously running oscillator stages, so there is no PLL hunting.

Immediately following the 200 millisecond sample period, the program displays the fingerprint on the left side of the screen, along with the detected CTCSS frequency, if any, and the signal amplitude, if receiver AGC input is provided. From that point until the transmission ends, it decodes and displays any DTMF digits received and determines the maximum deviation of voice and DTMF modulation. The display also includes the date and exact time of transmission start and stop.

A new fingerprint is produced each time a transmission begins. Of course, prints of repeater users must be made on the input frequency, as fingerprint data does not pass through the repeater. If you accidentally set the receiver to the output frequency, you will see the print of the repeater transmitter, not the user.

With the MOVE command, you can put the fingerprint of your choice on the right side of the screen for comparison with incoming prints on the left (Figure 2). The COMPARE command (not shown in the figure) overlays the print from the right side onto the print on the left, in different colors if you have a color monitor.

When COMPARE is commanded, the program automatically calculates a figure of merit for the difference in the two overlaid prints. "It subtracts the corresponding values of each supersample, with a maximum allowable difference value of 2 kHz each," says N7SNI. "The 64 difference values are each squared, then all are averaged."

Perfect correlation would give a mean-square difference of zero. That rarely happens, but most rigs have only small differences between transmissions, whereas prints of non-identical rigs usually show much higher difference numbers. The difference value is 4 for the two transmissions of Figure 1, and 9 for those of Figure 2.

By selecting the appropriate program mode, some or all fingerprints can be stored on disk. They can also be recorded on audio tape. Using a stereo tape deck, you can simultaneously log user fingerprints and audio on the left and right channels. The manual says the program will turn on your recorder at the start of a transmission and delay the audio until it comes up to speed, but I did not test this feature.

I spent much time using the ANALYZE feature, which allows comparison of fingerprints stored in one or more disk files. You can also put an annotation line on the prints and edit them down into a master file. The MOVE and COMPARE functions work perfectly with disk-stored prints, but there are minor program bugs in storing and display of the DTMF and deviation data.

The Acid Test

So how did TxID-1 do with different rigs of the same model? Very well! Most times, the differences were obvious, as shown in Figure 3. The mean-square numeric value in the COMPARE mode for these two prints is 179.

TH-78s and other Kenwood rigs settle on frequency much faster than other brands, so they were harder to tell apart. But it was still possible to find differences, usually in the final frequency after PLL settling. (Of course, this value might be affected by such factors as temperature fluctuations in the transmitter and/or receiver, so care must be used.)

For fast-settling rigs, it would be desirable to eliminate the 2 millisecond delay between squelch activation and start of the print. Phil says he is working on a firmware upgrade that will store data to allow "looking back" before the squelch opens, to the exact start of transmissions.

A few HTs had wild variations in consecutive-transmission fingerprints, which turned out to be caused by near-dead batteries. Features such as a rig's battery saver also cause changes in its fingerprint (Figure 4). Then there was one rig at the meeting that seemed to have an unlimited number of prints that were similar, but with definite differences. I compared 10 prints from this rig and found only 7 out of the 45 possible comparisons had mean-square difference numbers less than 100. To avoid giving aid and comfort to potential troublemakers, I will not reveal the make and model. Fortunately, other rigs of this type at the meeting did not have these variations.

Parting Shots

Learning to use the TxID-1 is fairly easy and intuitive, but I can only give the manual a grade of C. It has plenty of detail to help you connect to receivers and recording gear. There are advanced topics such as command-line parameters and script files. But information on how to analyze and compare your prints is hard to find. For instance, there is no help in interpreting the mean-square difference function in the COMPARE mode and no explanation why the CTCSS frequency readout often gives false indications.

Motron's telephone support was very good, and I was able to get some added information on the program by reading the large (50K) help file on the program disk. Don Moser of Motron says a new manual is coming, along with Revision 2 of the software. It will fix all the known bugs. Also in the works is a remote access feature. You will be able to put TxID-1 on the receiver at your mountaintop repeater and downlink fingerprints via phone or packet radio.

I would like to see some other improvements in the software, such as a hard copy printout function. For the figures in this article, I used the computer's "PRINT SCREEN" key with a dot matrix printer after running the "GRAPHICS" command from DOS. There should also be an faster and easier way to start and stop the fingerprinting function without exiting to the MONITOR menu.

It would also be great if TxID-1 could be programmed to automatically search your database of known user transmitters and select the closest print or prints in it when your repeater is keyed up. This would be a faster way to identify "kerchunkers." Also, how about a way to automatically alert the operator when a particular rig comes on the air? This would be especially valuable when someone's transceiver is stolen. Don, Phil, and George say they are working on such features.

At $699 plus $8 shipping for the complete TxID-1 hardware and software package plus the cost of the computer and receiver, the Motron fingerprint system won't find its way into the average ham shack. However, it is well within the budget of many repeater clubs and is certainly a worthwhile addition to the arsenal of repeater councils and interference committees.

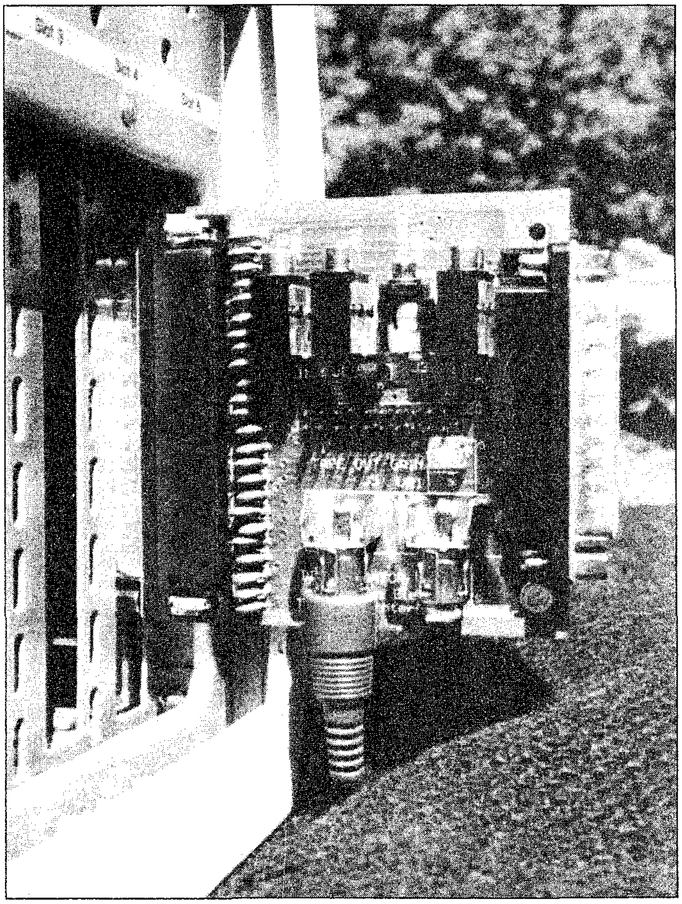

Photo B. The IA-1 Interface Adapter board has jacks for receiver discriminator and S-meter input, plus tape recorder on/off and audio. It attaches to the TxID-1 Transmitter Identifier board mounted inside the computer. The unused DB25 connector is for optional RS-232 control of AR-3000 receivers.

From its introduction, TxID-1 has had steady sales to government, amateur, and commercial purchasers. But according to AA7Y, many customers don't want the fact that they own TxID-1 to be public knowledge. "Nonsense!" says K7PF. "A system like fingerprinting does no good unless people know about it. A ham from Victoria, British Columbia tells me that the TxID-1 is like having a shotgun by the door. It never needs to be used, but everybody knows its there just in case."

TxID-1 is not sold at ham stores. It is available only from Motron Electronics, 310 Garfield Street, Suite 4, PO Box 2748, Eugene OR 97402, (503) 687-2118. 73