

CELL2.TXT

CELLULAR TELEPHONE PHREAKING PHILE

VOL 2 by "The Mad Phone-man"

Some terms you should understand:

Control Channel- The channel the phone and cell base first communicate on.

Reverse Control Ch- The opposite frequency, 45 mhz lower than the control channel. This is where the mobile unit is.

Voice channel- The channel you are assigned by the switch to commence the call on after the exchange of subscriber data.

Reverse voice channel- Again 45mhz lower.

Cell Site- The base station that talks to the mobile.

Switch- The computer that places the calls, and takes and receives data from the subscriber or from PSTN. (public switched tel netwk)

OK that should get things started. A subscriber picks up his handset to place a call.

The phone has already been locked onto the strongest control ch in the area by a computerized scanner in the phone. As he drives thru the service area the computer constantly picks out the strongest control ch and stays on it, altho more than one cell site can actually be heard. The subscriber enters the number to call on the keypad, and presses the "send" button. At this time the following data is transmitted to the cell site by the mobile. The caller's electronic serial number (ESN), his home system number (two digits) his mobile's area code and phone number, and the number he wants. The cellular switch now picks up an outgoing line, places the call for him and tells the mobile to switch to a voice channel. The two ends are linked in the central switch and viola! A complete phone call, in about 3 seconds.

I have purposely over-simplified the whole process to point out the moment of truth. The mobile's ESN and phone number and the data in the switch must match or no go. This is how the billing is figured out. If one had the ESN and the mobilephone number, you could call anytime anywhere without fear of trace, let alone bill. The ideal setup would let you listen to the reverse control channel, record and display heard working numbers and ESN's and recall them at your discretion to make calls. This would be tits! We're not quite there yet. But some hard work has already been done for us. All the aforementioned codes are sent in hex, in NRZ code (phancy term for phase shift keying) but the phone already has, for example a NRZ receiver and transmitter built right in. All that has to be done is to have a receiver on the reverse control channel, recover the other subscribers data and save it or at least print it out. The mobile radio data books show some good technical stuff on the systems used and chip part numbers for the NRZ stuff. I know there is a mfgr using the lowley 8085 chip for the control head functions, seems like there's room for experimentation here.

More to come!... "The Mad Phone-man"

CELL2.TXT

Downloaded From P-80 International Information Systems 304-744-2253