How to Get into the AT&T Network by Building Your own Mobile Phone.

by THE RESEARCHER

This article is presented for entertainment and academic study only. It is a violation of Federal laws to operate an unlicensed transmitter or make fraudulent telephone calls. It is not intended nor expected that anyone actually build the devices described. The article is simply a detailed and factual description of something that could be done.

I wrote a file in collaboration with another telephone experimenter of high repute on IMTS (Improved Mobile Telephone Service) posted elsewhere on this board under the title of "Feature Article". This file was downloaded and posted on another BBS in the Midwest. From there it fell into the hands of the Chief of Security of Southwestern Bell. His words to the Sysop, who had been busted for Blue Boxing were, "A person with a knowledge of electronics could use the information in that file to build his own mobile telephone".

I am going to explain in this article how you can build your own mobile phone. If you haven't figured it out already, you will soon see why the security man was concerned.

This article presupposes that you have a working knowledge of two-way radio. If you don't possess this knowledge, get a copy of "The Radio Amateur's Handbook" (readily available from libraries and book stores) and study up on narrow band FM and 2-Meter transmitters. To get everything you will need in one file, I am reprinting the IMTS article here:

Signaling Used in IMTS (Improved Mobile Telephone Service)

Each mobile telephone channel consists of two frequencies; one for the land base station and one for the mobile phone. The base station uses two tones for signaling:

Idle	2000 Hz
Seize	1800 Hz

The mobiles use three tones:

Guard	2150 Hz
Connect	1633 Hz
Disconnect	1336 Hz

The land base station marks the idle channel by placing the idle tone on it. All the mobiles search for the channel with the 2000 Hz idle tone and lock on to it.

Each mobile phone is assigned a standard telephone number consisting of area code + 7 digits. When a land customer dials a mobile number, the idle tone

(2000 Hz) changes to seize (1800 Hz). The number pulsed to the mobile phone contains 7 digits consisting of the area code and last 4 digits of the number. The digits are made up of 50 ms pulses of 2000 Hz separated by 50 ms of 1800 Hz.

If there is a mismatch between the digits sent and the wired ID in the mobile, the mobile drops off and hunts for the idle channel. If the number matches, the mobile will send back an acknowledgement tone of 750 ms of guard (2150 Hz). The base station waits 3 to 4 seconds for this tone. If not received in that time, the calling party gets a recording. If the tone is received, the mobile phone will ring for up to 45 seconds. Ringing is composed of 1800 Hz and 2000 Hz shifting at 25 ms for two seconds then four seconds of 1800 Hz. When the mobile phone is picked up it sends a connect tone of 1633 Hz for 400 ms to tell the base station it has answered. When the mobile hangs up, it sends disconnect, which is 750 ms of 1336 Hz. When the base receives the disconnect tone, it will drop carrier for about 300 ms and go off. If it is the only available channel, it will return to idle.

Now I will describe what happens when a call is originated by a mobile. When the mobile goes off hook, it sends 350 ms of guard (2150 Hz) followed by 50 ms of connect (1633 Hz). When the base station hears the connect tone, it removes the idle tone and stays quiet for about 250 ms. It then transmits 250 ms of seize (1800 Hz). The mobile then sends 190 ms of guard and starts transmitting the ID sequence at 20 pulses per second. The ID is the area code and last four digits of the mobile's number. The pulses are marked by 25 ms of connect (1633 Hz) followed by 25 ms of either silence or guard tone (2150 Hz). If the pulse is odd, it is followed by silence. If even, it is followed by guard tone. This is used for parity checking. The interdigit time is 190 ms and will be either silence or guard tone depending on whether the last pulse was odd or even. If the last pulse of the last digit in the ID is even it will be followed by 190 ms of guard tone.

When a number is dialed from a mobile phone, 2150 Hz is sent continuously as soon a the dial goes off normal (when the dial is moved from its resting position). Dial pulses representing breaks are marked by 1633 Hz and are sent at 10 pulses per second. A pulse is 60 ms of 1633 Hz with 40 ms of 2150 Hz between pulses.

The most popular mobile telephone channels are located in the VHF high band. More cities are equipped with these channels than any other band. They are listed below.

Mobile Telephone Frequencies

Channel	Base	Mobile
JL	152.51	157.77
YL	152.54	157.80
JP	152.57	157.83
YP	152.60	157.86
YJ	152.63	157.89
YK	152.66	157.92

JS	152.69	157.95
YS	152.72	157.98
YR	152.75	158.01
JK	152.78	158.04
JR	152.81	158.07

****

This is a list of the components you will need to build your own mobile phone:

1. Cassette Tape Recorder.
2. Radio Scanner (Like those used to receive police calls).
3. Mobile phone dialer (build your own).
4. Low Power Transmitter (Modified 2-Meter transmitter 1 - 5 watts).

How to Build a Mobile Phone Dialer

Build a Wien-Bridge oscillator. These are commonly used in red boxes. If you don't have a red box schematic, look up Wien-Bridge in an electronics textbook. Where you would normally connect a frequency adjustment pot, use two multi-turn pots connected in series. Power for the oscillator will be supplied by a 9 volt battery.

Obtain a rotary dial of the type used on rotary telephones. The dial will have four wires coming out of it; two white, one blue, and one green. The two white wires make a connection when the dial is off normal (moved from its resting position). Connect the two white wires in series with one of the leads from the 9 volt battery. The oscillator will be running only when the dial is moved off normal. It works like this: Dial is moved off normal. Circuit is completed between oscillator and battery. Dial goes back to resting position. Circuit is opened.

The blue and green wires go to a normally closed contact in the dial. This contact opens once for each pulse in a dialed digit. For example it opens three times for the digit "3". Connect these two wires (blue & green) across one of the pots in the oscillator. With the dial in its resting position, adjust the other pot for a frequency of 2150 Hz (Guard tone). Move the dial until the contact opens and adjust the pot with the blue and green wires going to it for a frequency of 1633 Hz (Connect tone).

When the dial is moved off normal, power will be applied to the oscillator, and it will begin running at 2150 Hz. When the dial is released the short across the second pot will be removed each time the contacts open for a dial pulse. During these pulse times the frequency will shift down to 1633 Hz. When the dial gets back to its resting position, power will be removed from the oscillator. This will exactly duplicate the dial pulsing of a mobile telephone.

The Transmitter

Antennae used by mobile phone base stations are located on high towers.

This allows line-of-sight transmission to and from the mobiles. If you are within a few miles of a base station very little power is needed to establish contact. 1 to 5 watts should be completely adequate. The less power you use, the less your chances of getting caught. More on this later.

2-Meter transmitters, used in amateur radio, operate in the range of 144 to 148 Mhz. With a change of crystals and a little retuning, you have your transmitter.

How to use Your Home brew Mobile Telephone

With your scanner, locate the base station frequency which currently has the idle tone on it. Switch to the mobile frequency on that same channel and monitor it with the cassette recorder running continuously. What you want is a clean recording of a mobile unit broadcasting its ID sequence. You also want a recording of the disconnect tone when he hangs up. Once you have these, rewind the tape to the start of the sequence. Now you are ready to make a call.

The procedure For Placing a Call

1. Set your scanner to the base station frequency with the idle tone and leave it there. Monitor with earphones to avoid audio feedback through the transmitter.

2. Set the transmitter to the corresponding mobile frequency. Turn it on and leave it on.

3. Play the taped ID sequence.

4. Use your dial pulser to call the desired number. If all has gone well, you will hear your dial pulses in the earphones. You can use this method to call one of the special 800 numbers and whistle off with 2600 Hz; then MF to anywhere in the world. This technique will reduce your visibility on the bill for the ID you are using.

5. When you are ready to hang up, play the disconnect tone and switch off the transmitter.

A Few Notes About Your Own Security

You should use only as much transmitter power as necessary to maintain a reliable contact. If you do much of this kind of experimenting, the FCC is going to be after you with direction finding equipment. These use directional antennae and a process of triangulation to locate illegal transmitters. If you keep your power down, stay mobile, and avoid establishing a pattern of calling at the same time every day, it will be nearly impossible to track you down.

This file is presented by: P-80 Systems

Scan Man