Decoding POCSAG using Gqrx & RTL-SDR

Noë Flatreaud

Noë Flatreaud

Follow

4 min read

·

Oct 6, 2024

Listen

Share

More

Recent events, involving Hezbollah, Mossad and the explosion of thousands of trapped pagers, sparked my interest in learning more about the POCSAG protocol and its decoding process.

In this article we’ll find out POCSAG pager protocol specifications, behaviour and how to sniff it.

POC-what ?

POCSAG (Post Office Code Standardisation Advisory Group) also known as Radio Paging Code №1 or RPC1 is a one-way 2FSK paging protocol that supports 512, 1200, and 2400 bps speed. Transmissions can include tone, numeric, and alphanumeric data. The protocol uses FSK modulation with a ±4.5 kHz shift on the center carrier, where a +4.5 kHz shift represents a 0 and a -4.5 kHz shift represents a 1. You can find POCSAG signals on the VHF or UHF band and 12.5 or 25 kHz channel spacing.

Typical 2 & 4 FSK Power Spectrum you’d find

Press enter or click to view image in full size

Here is an example POCSAG signal waterfall (right) and it’s decoded messages (left)

Frequencies

POCSAG pagers operate on various frequencies depending on the region. Here are some common frequency ranges:

HF-High/VHF-Low Band: 25 MHz — 54 MHz

VHF Mid Band: 66 MHz — 88 MHz

VHF High Band: 138 MHz — 175 MHz

UHF: 406 MHz — 422 MHz

UHF High: 435 MHz — 512 MHz

‘900’ Band: 929 MHz — 932 MHz

You can find each specific frequency by region and service on <https://www.sigidwiki.com/wiki/POCSAG>

Required Hardware and Software

RTL-SDR Dongle: A USB dongle capable of receiving frequencies from 500 kHz up to 1.75 GHz.

In principle, any software defined radio (SDR) covering a frequency range up to 800 MHz should be suitable to monitor POCSAG communication. This also includes cheap RTL-SDR USB sticks. The RTL-SDR was initially produced as DVB-T tuner and is available for around 25€.

Gqrx: An open-source software-defined radio receiver.

Sox: A command-line audio processing tool.

Multimon-ng: A tool for decoding various digital radio protocols, including POCSAG.

For this tutorial, I am using Dragon OS, an all-in-one GNU/Linux distribution dedicated to radio hacking and wireless activities, but you can install it standalone.

Setting Up Gqrx

Launch Gqrx: Open the Gqrx application.

Configure the RTL-SDR Dongle: Select your RTL-SDR device from the input controls.

Press enter or click to view image in full size

Make sure that your Audio output is sampled at 48 kHz.

Enable UDP Server: Go to the “Input Controls” tab and enable the UDP server. Set the port to 7355.

The remote host and port number are configurable.

Once configured, you can start streaming signals.

Press enter or click to view image in full size

<https://www.cemocom.de/tag/pocsag/>

You can verify the data is coming through at the opposite end using netcat:

$ nc -l -u 7355

You should see a lots of symbols scroll through the terminal that you can pipe to the next tool.

Capturing and Decoding the Signal

You task now is to capture the signal received from the RTL-SDR in Gqrx piped through the UDP Socket on port 7355.

Multimon-ng helps us identify and decode the POCSAG signals in various speeds (512,1200 and 2400 bps), sox resamples our audio signal from 44100 to 48000 bauds for signal processing.

Use the following command to capture the signal from Gqrx and decode it using Multimon-ng:

$ nc -l -u localhost 7355 | sox -t raw -esigned-integer -b16 -r 48000 - -t raw -esigned-integer -b16 -r 22050 - | multimon-ng -t raw -a POCSAG512 -a POCSAG1200 -a POCSAG2400 -f alpha -e --timestamp –

You’d normally be able to receive plaintext messages from nearby emergencies & firefighters

Press enter or click to view image in full size

Hooray, you just sniffed and decoded paging activity ❤