REVERSE ENGINEERING A CONSUMER WIRELESS DEVICE

GNU Radio Conference 2024

Jason Bonior

Red Wire Technologies

WHO IS THIS FOR?

- People who:
  - are new to GNU Radio;
  - are new to analyzing a wireless signal; or
  - are not directly interested in SDR but utilize data taken from them.

OUTLINE

1. Documentation
2. Frequency
3. Modulation
4. Coding
5. Packet Structure
6. Checksum
7. Final Flowgraph
8. Displaying our Data

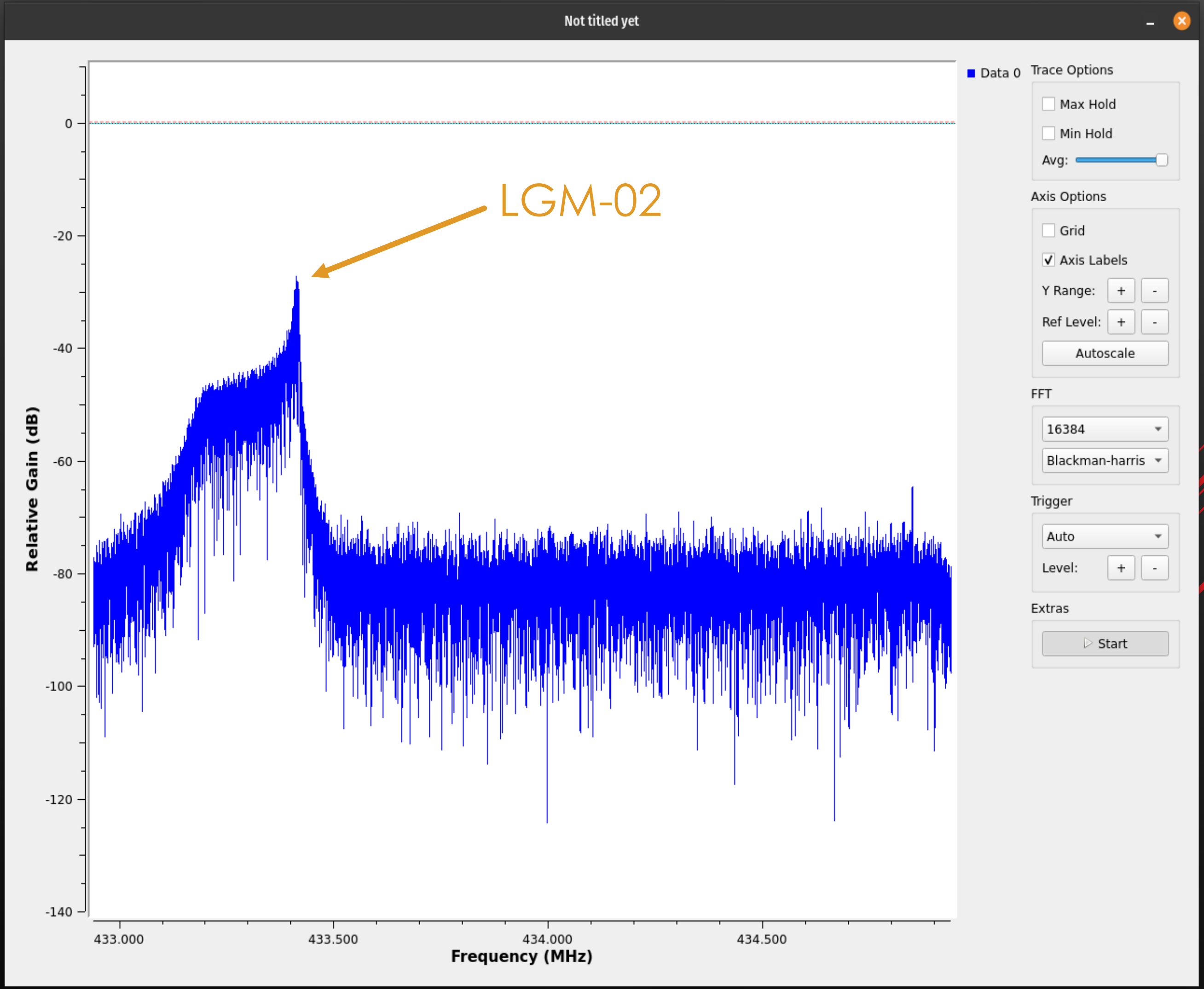
DOCUMENTATION

- Has someone else already done this?
  - Does an OOT Module already exist (CGRAN)?
  - Do other libraries exist (RTL 433)?
  - Wireless tools (Flipper Zero)?
- FCCID
  - Operating frequency and operational descriptions
  - Testing reports
  - Schematics, BOM, Block Diagrams (If you are lucky)

FREQUENCY

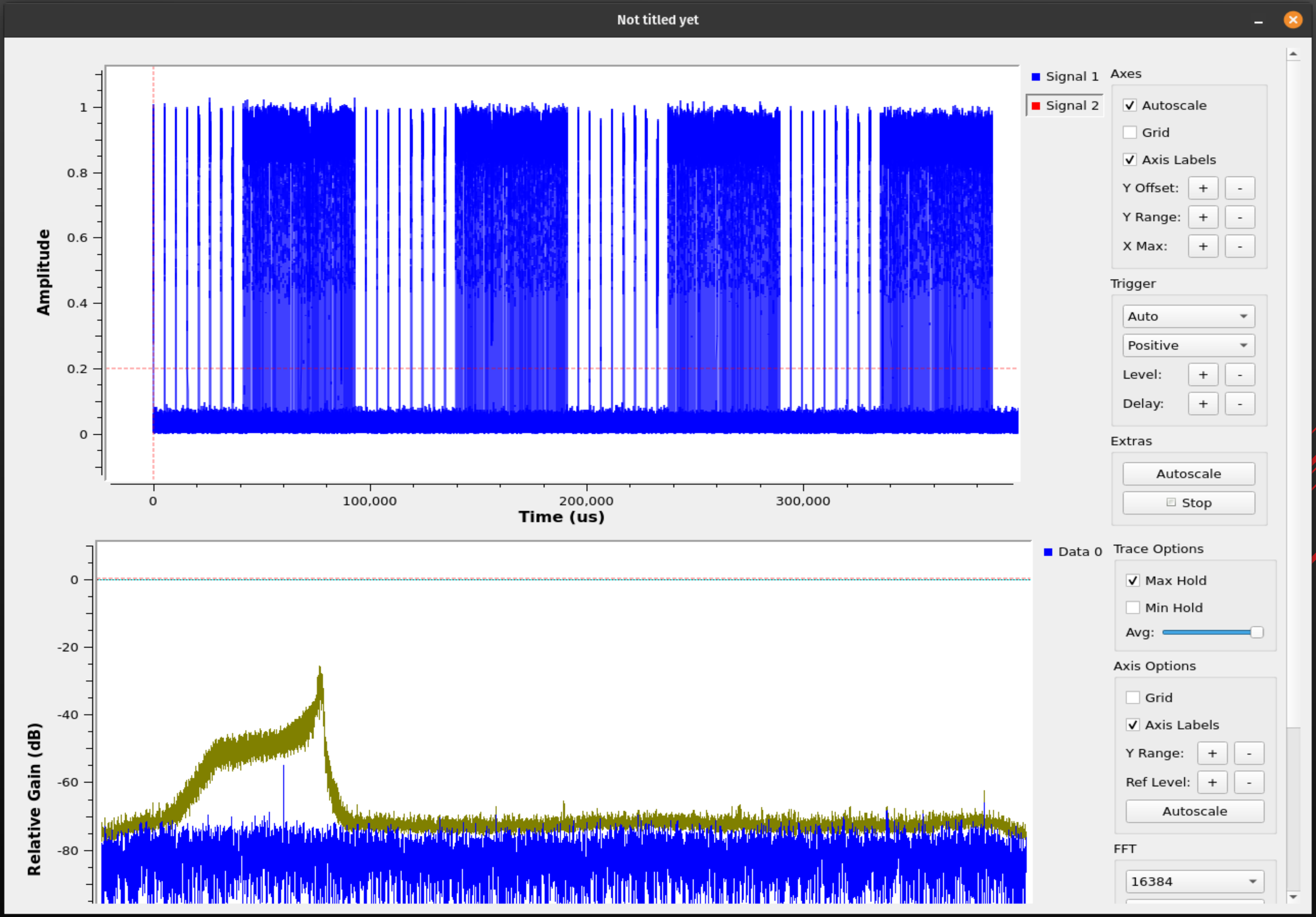
- If you can't find any easy solutions start with finding the operating frequency:
  1. QT Sinks in GNU Radio
  2. Spectrum Analyzer

- Start with common frequency bands:
  - 433.05-434.79 MHz
  - 902-928 MHz (865-880 MHz in Europe)
  - 2.4-2.5 GHz



MODULATION

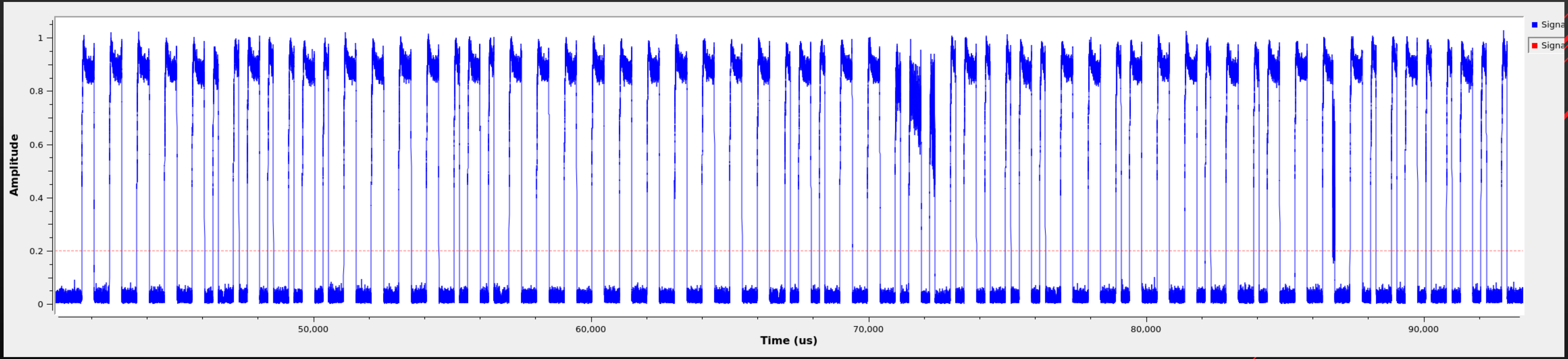
Complex to Mag Time Domain Plot looks like ASK



PACKET ENCODING

We see symbol widths that are multiples of 1 and 2 but not 3 or more:

- Probably Manchester Encoding



COLLECT AND COMPARE PACKETS

- We are lucky, we can vary the value of our sensors!
  - Change temperature of the two probes and look for variations in the packets:

172/72:	A6 65 56 65 A5 66 56 66 5A 59 69 59
171/72:	A6 65 56 65 A5 5A 56 66 55 95 A6 59
167/72:	A6 65 56 65 9A AA 56 66 59 A6 99 9A
162/109:	A6 65 56 65 9A 96 56 AA A9 96 66 95
162/90:	A6 65 56 65 9A 96 56 99 55 6A 59 66
160/84:	A6 65 56 65 9A 6A 56 95 A9 5A A6 A9

PACKET STRUCTURE

- Only 0x5, 0xA, 0x9, 0x6 looks like Manchester?
  - Double check the plots, is the Manchester decoder working properly?
  - Try applying it again?
    - Now we have something that looks more reasonable!

A6 65 56 65 A5 66 56 66 5A 59 69 59

$\downarrow$

2B EB 3A EA CD 9D

HYPOTHETICAL PACKET STRUCTURE

- Packet: 0x28AA2EE5D8

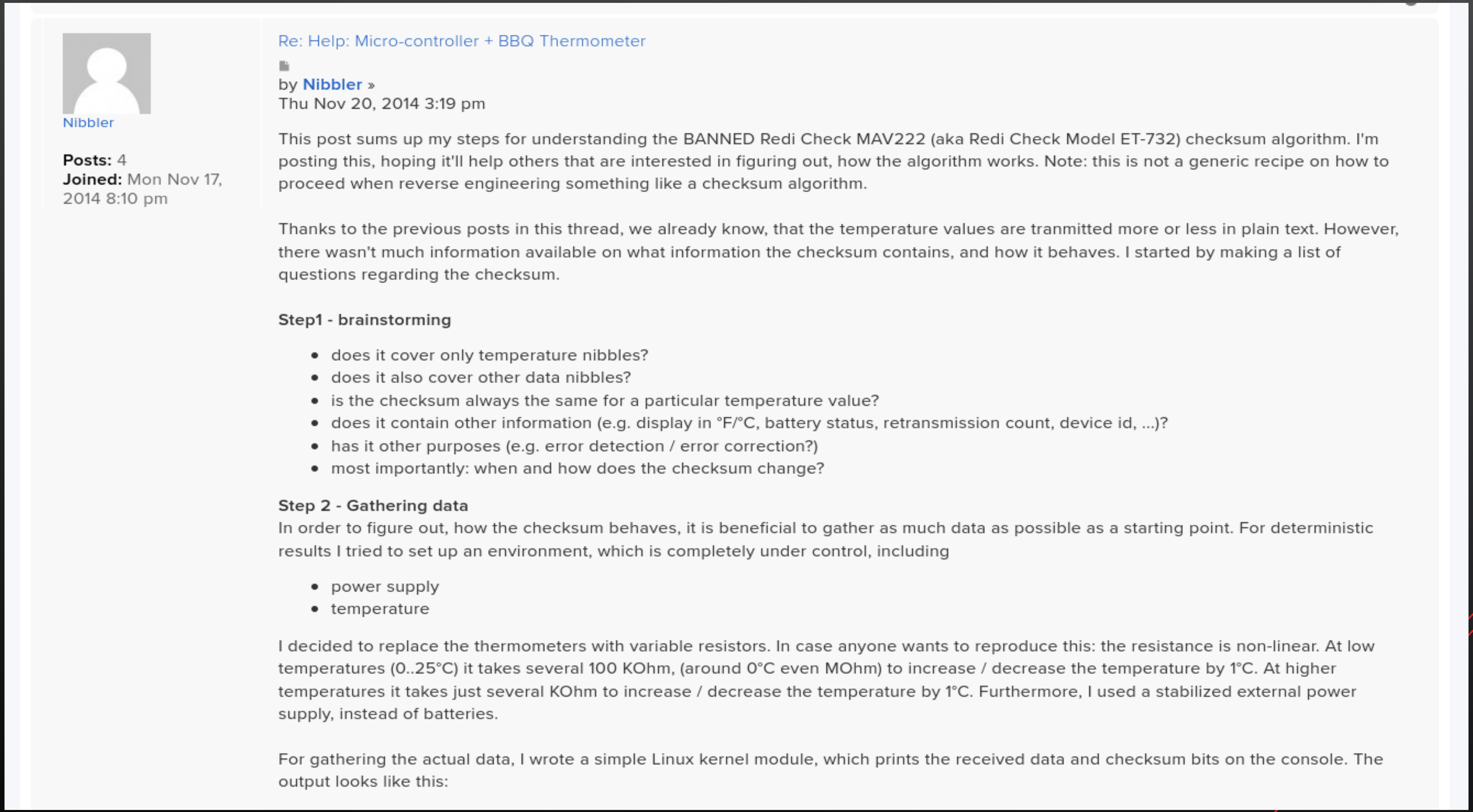
Packet Type:	0x2
Temperatures:	0x8AA2E
Checksum:	0xE5D8

CHECKSUMS

- Changes in single bits result in large changes in the checksum, looks like a CRC...
  - CRC RevEng didn't yield results.

- Same data, different checksums?
    - 0x28CA32CBF3
    - 0x28CA3270C8
    - If we push the sync button, the checksums change?!

CHECKSUM



Re: Help: Micro-controller + BBQ Thermometer

Nibbler

Posts: 4
Joined: Mon Nov 17, 2014 8:10 pm

by Nibbler »
Thu Nov 20, 2014 3:19 pm

This post sums up my steps for understanding the BANNED Redi Check MAV222 (aka Redi Check Model ET-732) checksum algorithm. I'm posting this, hoping it'll help others that are interested in figuring out, how the algorithm works. Note: this is not a generic recipe on how to proceed when reverse engineering something like a checksum algorithm.

Thanks to the previous posts in this thread, we already know, that the temperature values are tranmitted more or less in plain text. However, there wasn't much information available on what information the checksum contains, and how it behaves. I started by making a list of questions regarding the checksum.

Step1 - brainstorming

- does it cover only temperature nibbles?
- does it also cover other data nibbles?
- is the checksum always the same for a particular temperature value?
- does it contain other information (e.g. display in °F/°C, battery status, retransmission count, device id, ...)?
- has it other purposes (e.g. error detection / error correction?)
- most importantly: when and how does the checksum change?

Step 2 - Gathering data
In order to figure out, how the checksum behaves, it is beneficial to gather as much data as possible as a starting point. For deterministic results I tried to set up an environment, which is completely under control, including

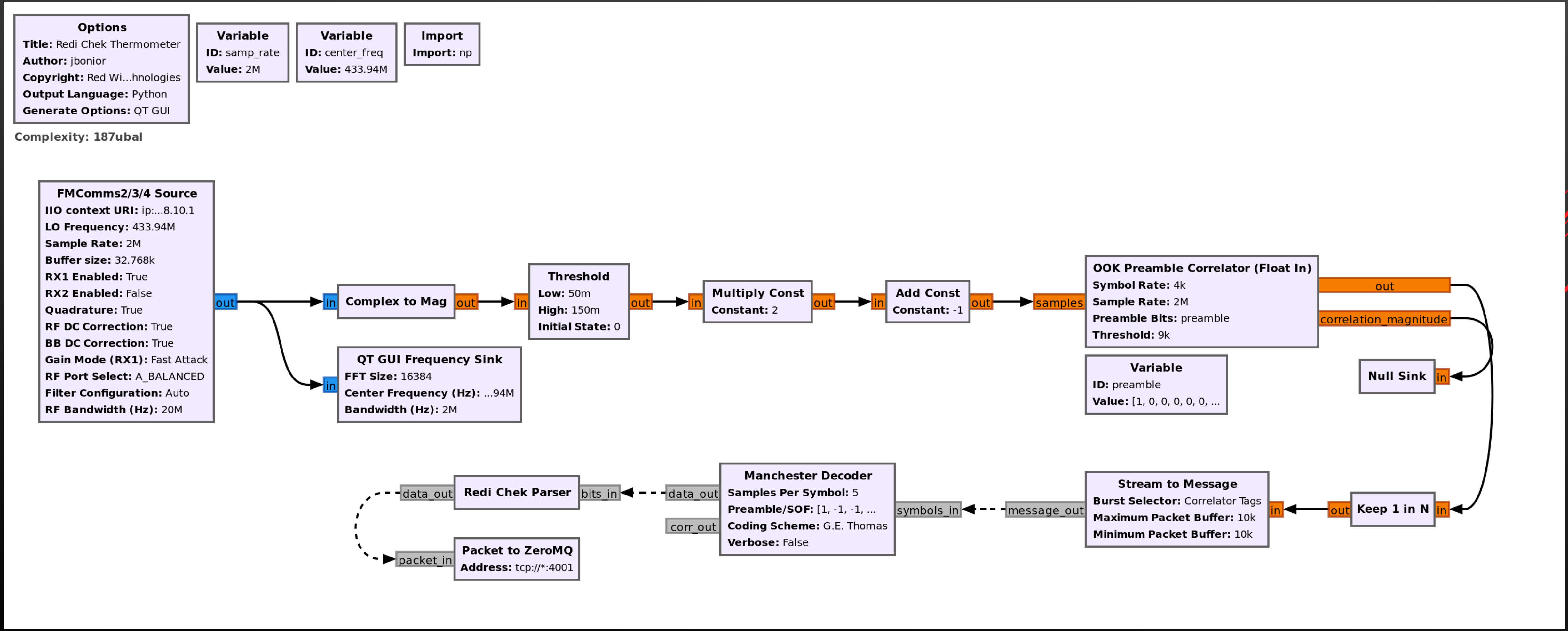
- power supply
- temperature

I decided to replace the thermometers with variable resistors. In case anyone wants to reproduce this: the resistance is non-linear. At low temperatures (0..25°C) it takes several 100 KOhm, (around 0°C even MOhm) to increase / decrease the temperature by 1°C. At higher temperatures it takes just several KOhm to increase / decrease the temperature by 1°C. Furthermore, I used a stabilized external power supply, instead of batteries.

For gathering the actual data, I wrote a simple Linux kernel module, which prints the received data and checksum bits on the console. The output looks like this:

Nibbler. "Re: Help: Micro-controller + BBQ Thermometer." Adafruit Forums. https://forums.adafruit.com/viewtopic.php?f=8&t=25414&sid=e1775df908194d56692c6ad9650fdfb2&start=15#p322178 (Accessed August 30, 2024)

OUR FINAL FLOWGRAPH



Options
Title: Redi Chek Thermometer
Author: jbonior
Copyright: Red Wi...hnologies
Output Language: Python
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 2M

Variable
ID: center_freq
Value: 433.94M

Import
Import: np

Complexity: 187ubal

FMComms2/3/4 Source
IIO context URI: ip:...8.10.1
LO Frequency: 433.94M
Sample Rate: 2M
Buffer size: 32.768k
RX1 Enabled: True
RX2 Enabled: False
Quadrature: True
RF DC Correction: True
BB DC Correction: True
Gain Mode (RX1): Fast Attack
RF Port Select: A_BALANCED
Filter Configuration: Auto
RF Bandwidth (Hz): 20M

Complex to Mag

QT GUI Frequency Sink
FFT Size: 16384
Center Frequency (Hz): ...94M
Bandwidth (Hz): 2M

Threshold
Low: 50m
High: 150m
Initial State: 0

Multiply Const
Constant: 2

Add Const
Constant: -1

OOK Preamble Correlator (Float In)
Symbol Rate: 4k
Sample Rate: 2M
Preamble Bits: preamble
Threshold: 9k

Variable
ID: preamble
Value: [1, 0, 0, 0, 0, 0, ...

Null Sink

Keep 1 in N

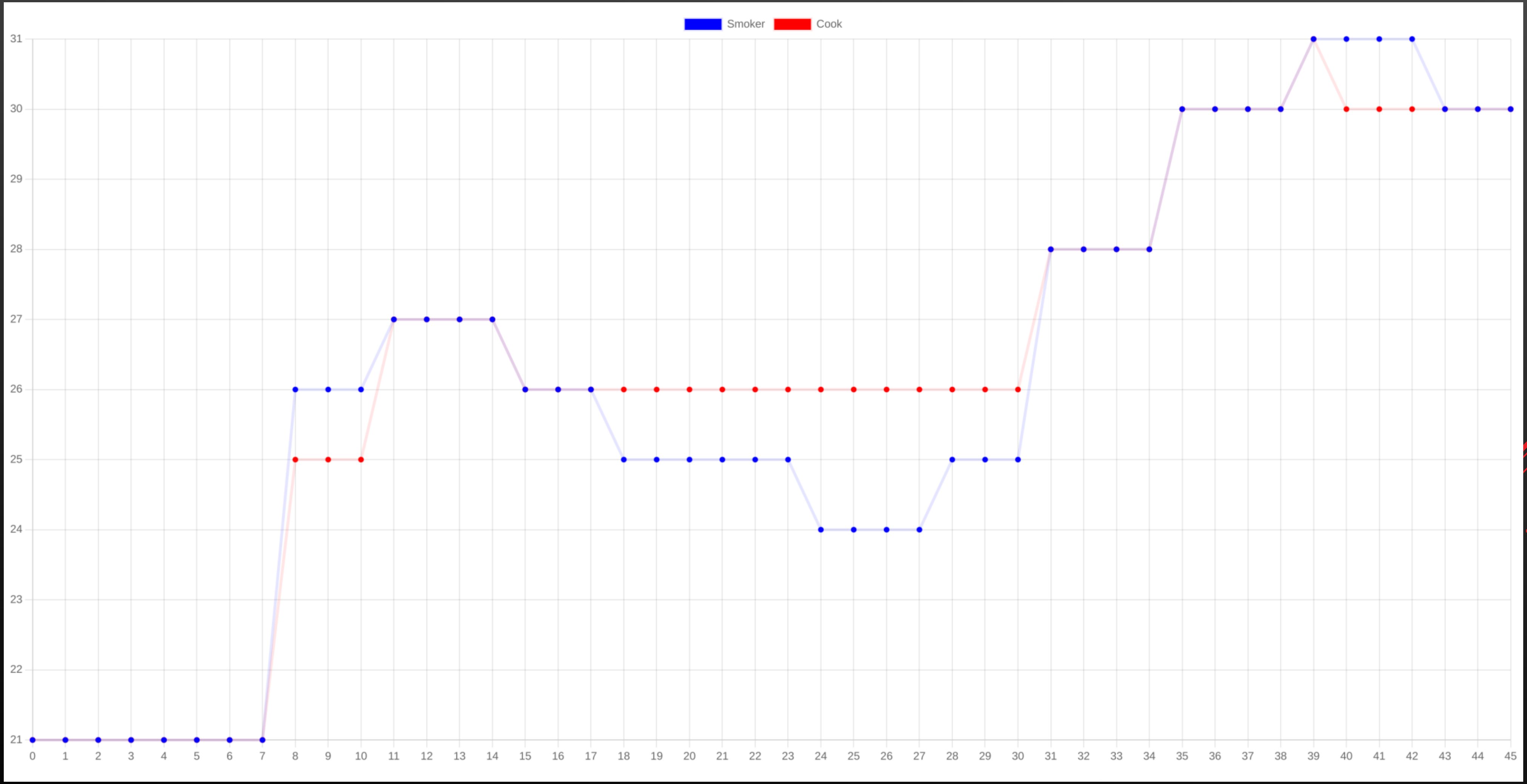
Stream to Message
Burst Selector: Correlator Tags
Maximum Packet Buffer: 10k
Minimum Packet Buffer: 10k

Manchester Decoder
Samples Per Symbol: 5
Preamble/SOF: [1, -1, -1, ...
Coding Scheme: G.E. Thomas
Verbose: False

Redi Chek Parser

Packet to ZeroMQ
Address: tcp://*:4001

DISPLAYING OUR DATA



QUESTIONS?

RedWire TECHNOLOGIES

We are Hiring!

jbonior@redwiretechnologies.us

https://github.com/redwiretechnologies/gr-bbq

https://github.com/redwiretechnologies/gr-rwttools2

https://forums.adafruit.com/viewtopic.php?f=8&t=25414&sid=e1775df908194d56692c6ad9650fdfb2&start=15#p322178