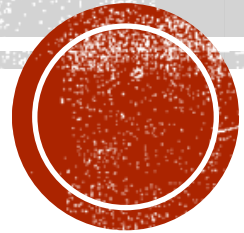
HOW TO HACK WIRELESS SCADA

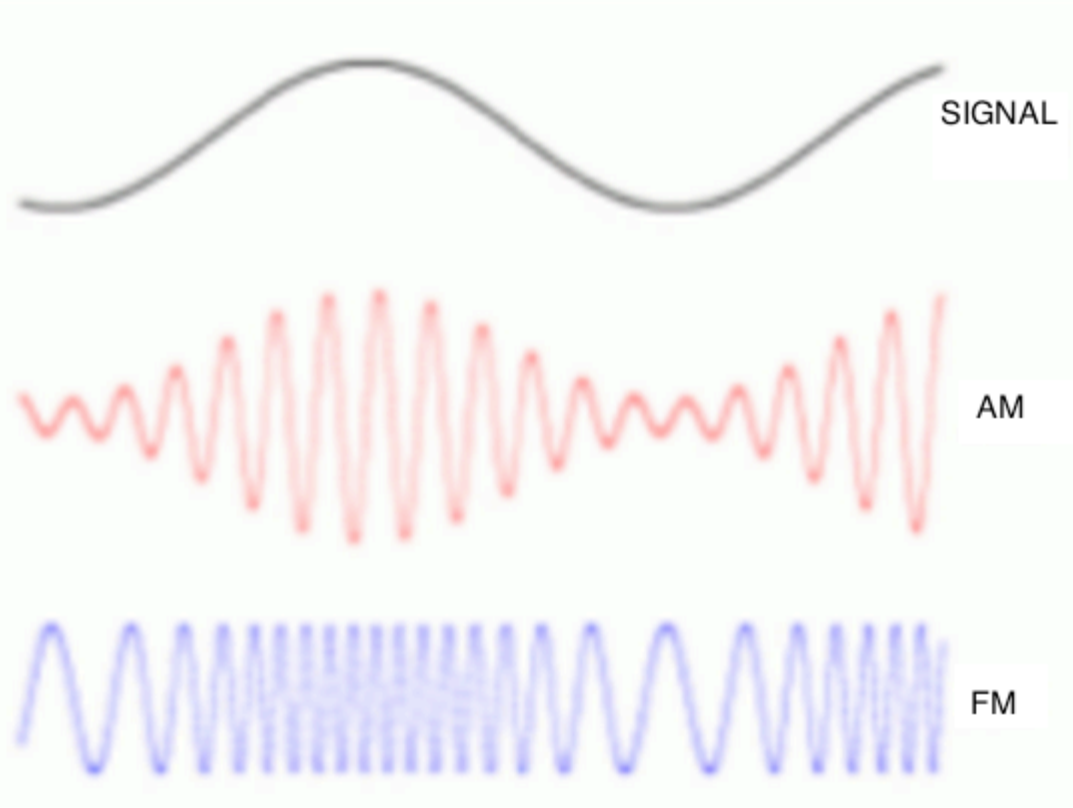


Elena Feldman. Chelyabinsk State University.
Department of computer security and applied algebra.

AGENDA

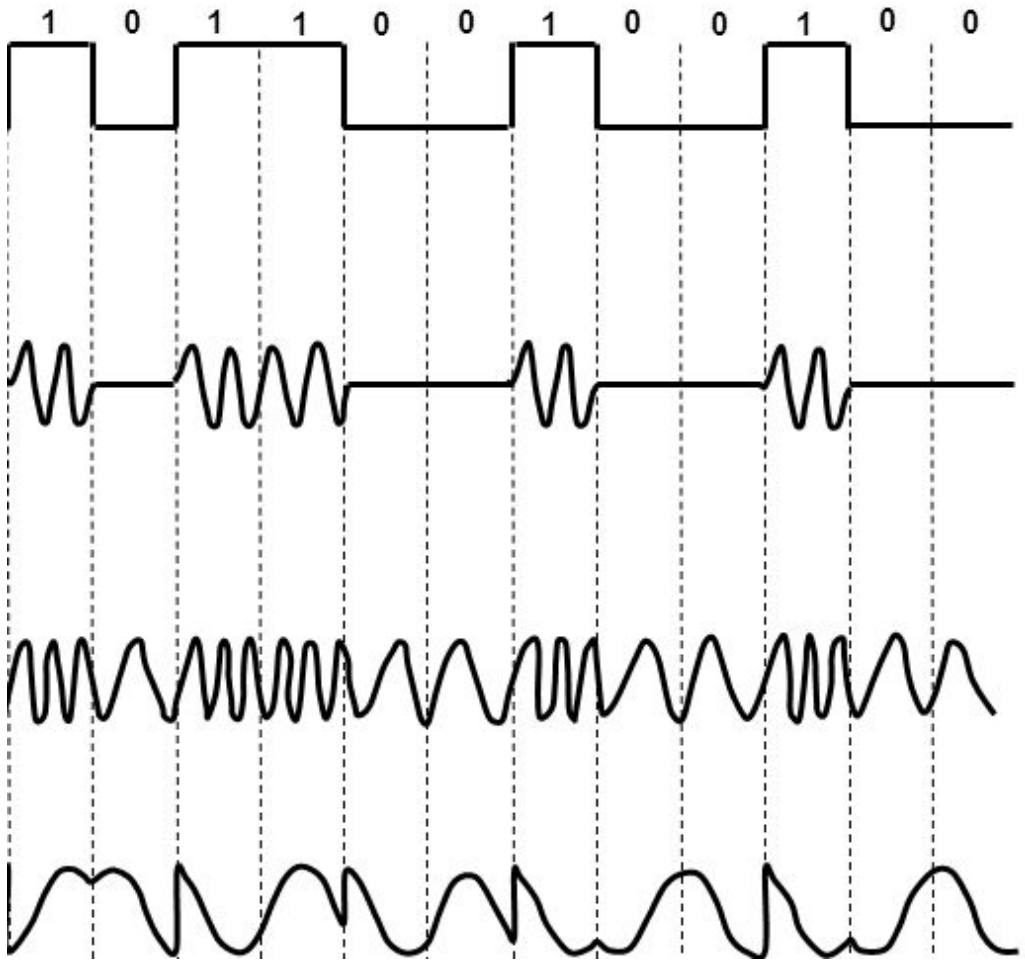
- Signals basics
- Modulation schemes
- Receiving data
- Digital receiver
- Z-Wave protocol
- Digital transmitter

SIGNAL AND MODULATION



TYPES OF MODULATION

- Data
- ASK
- FSK
- PSK



RECEIVING DATA

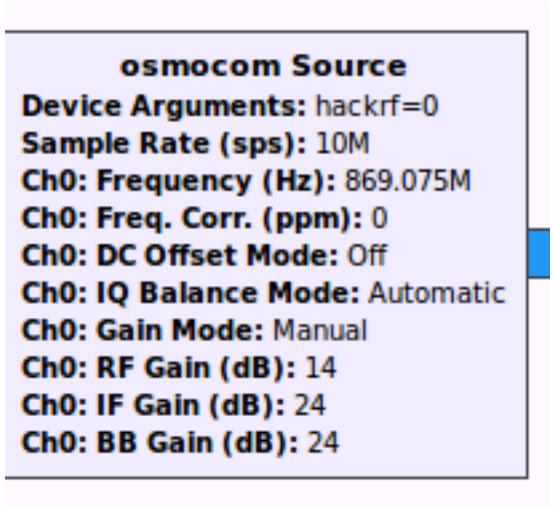
- Software Defined Radio

- GNU Radio

DIGITAL RECEIVER

- Configure the GNU Radio environment
- Configure the receiver source (Osmocom block)
- Debug the signal
- Signal identification, Centring the signal with Frequency Xlating FIR filter.
- Filtering
- Demodulating
- Data recovery

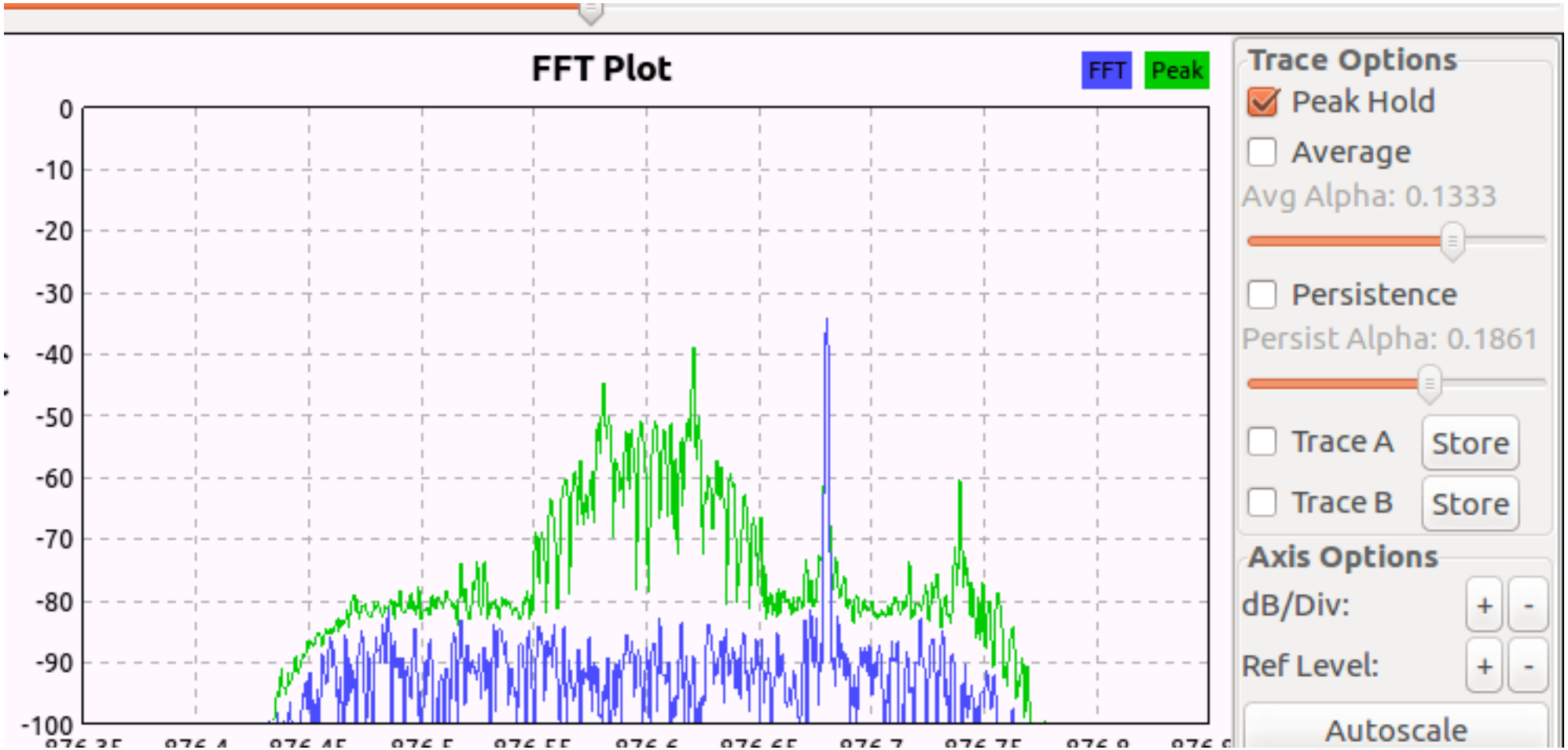
OSMOCOM BLOCK



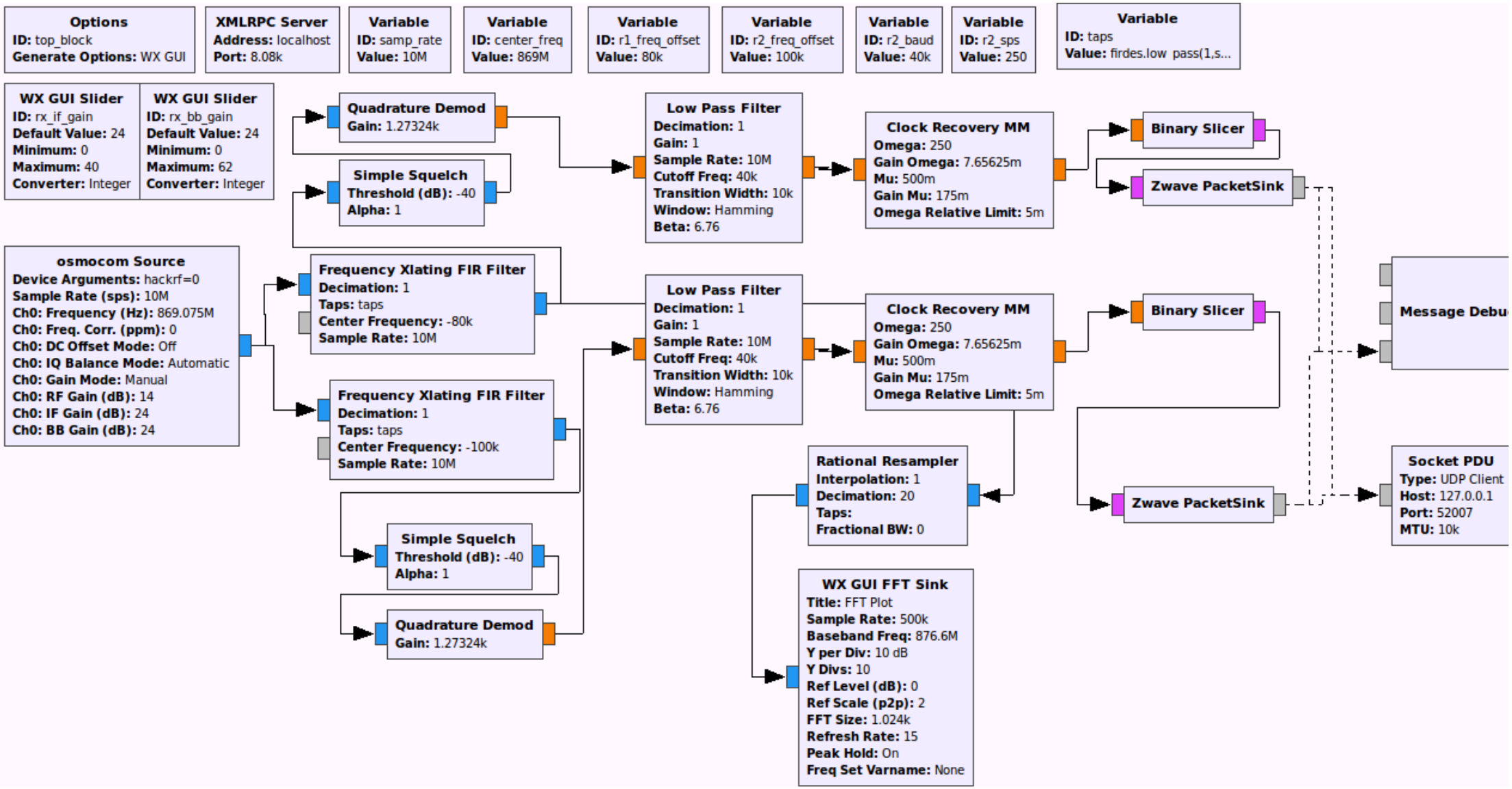
Device: hackrf (first)
Sample rate: 10M
Frequency: 869.075M
Gain parameters

DEBUG?

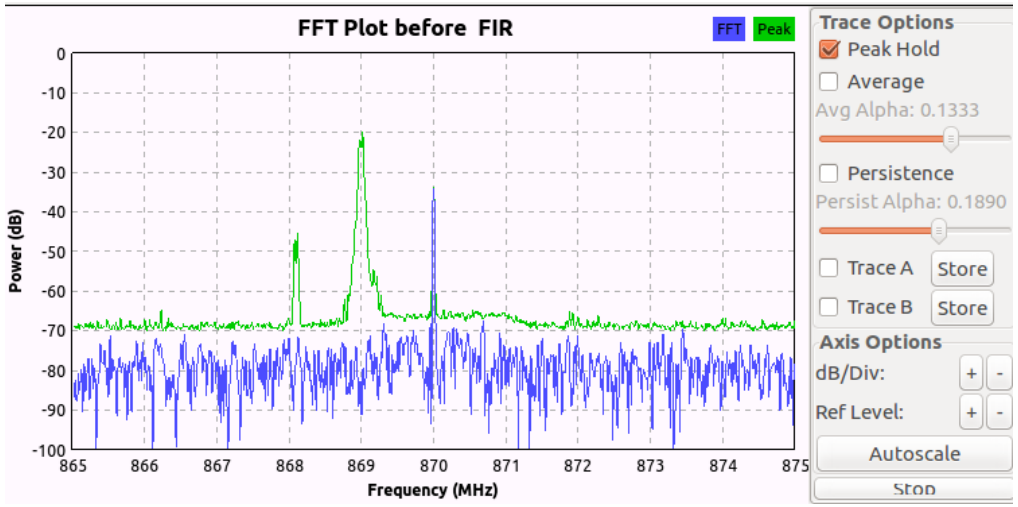
- First – watch signal

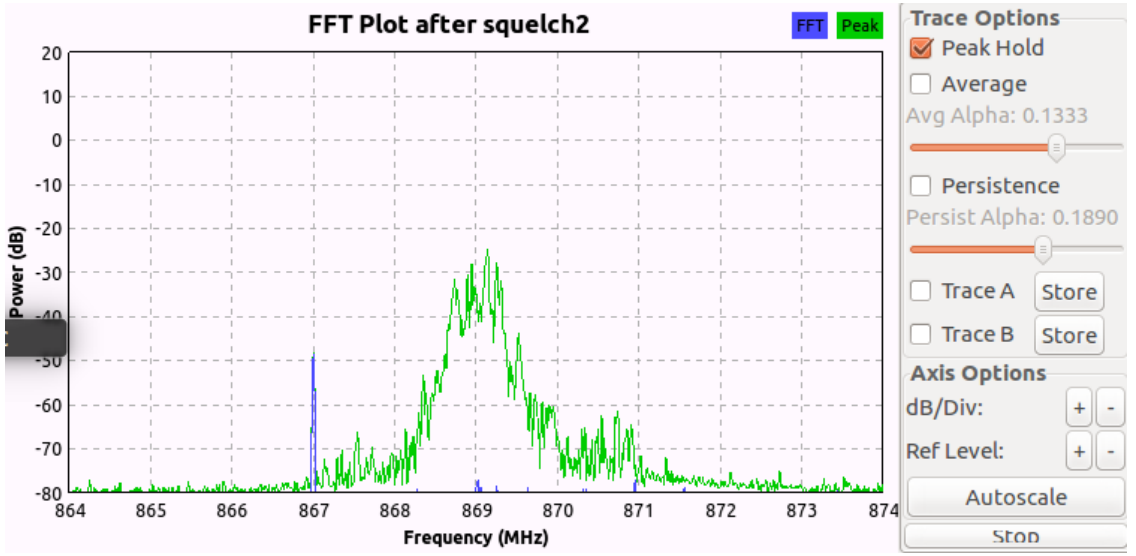


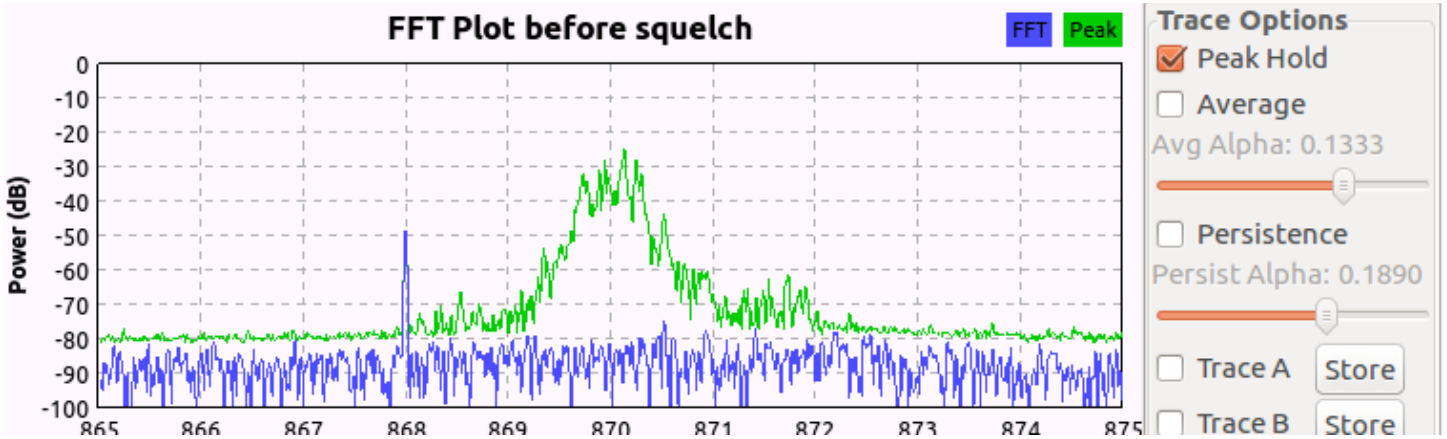
DEBUG: SEE SIGNAL GRAPH



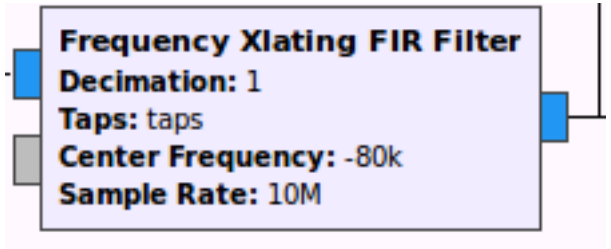
DEBUG: ADD PLOTS BEFORE AND AFTER

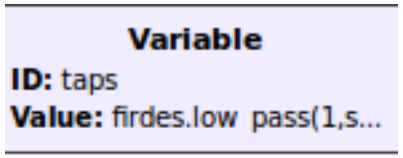


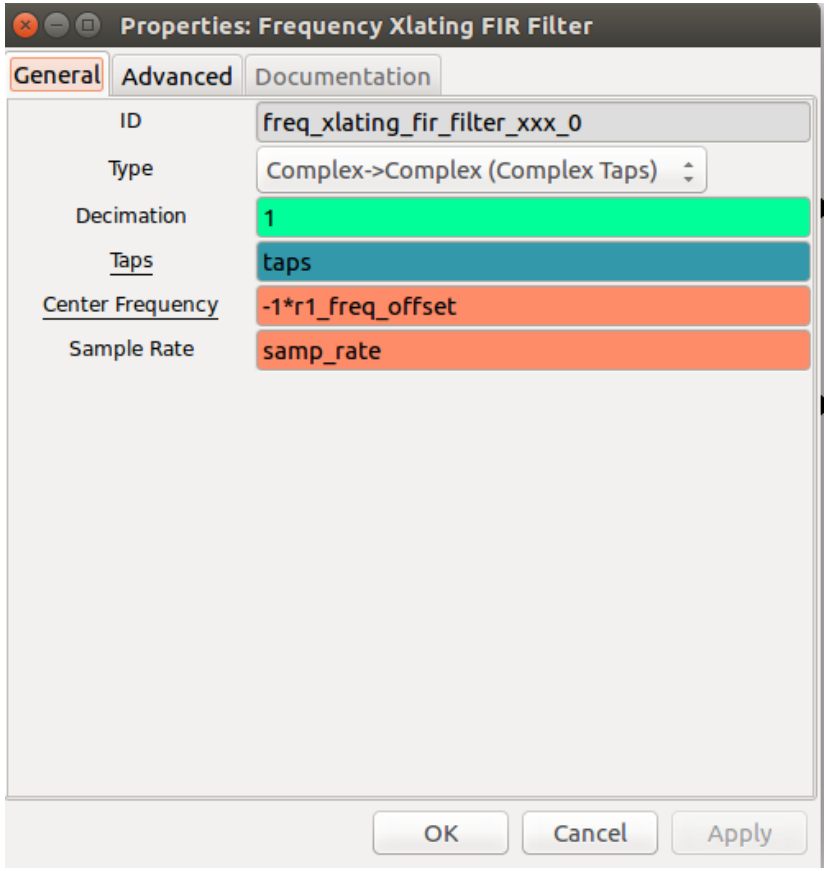


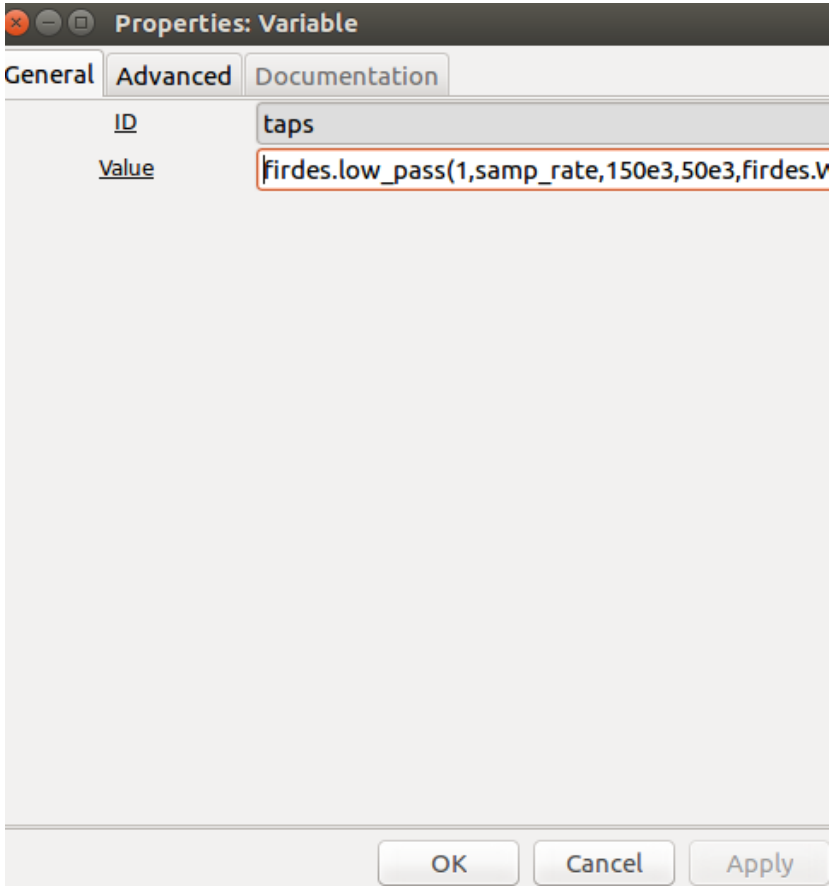


CENTERING SIGNAL – XLATING FIR FILTER

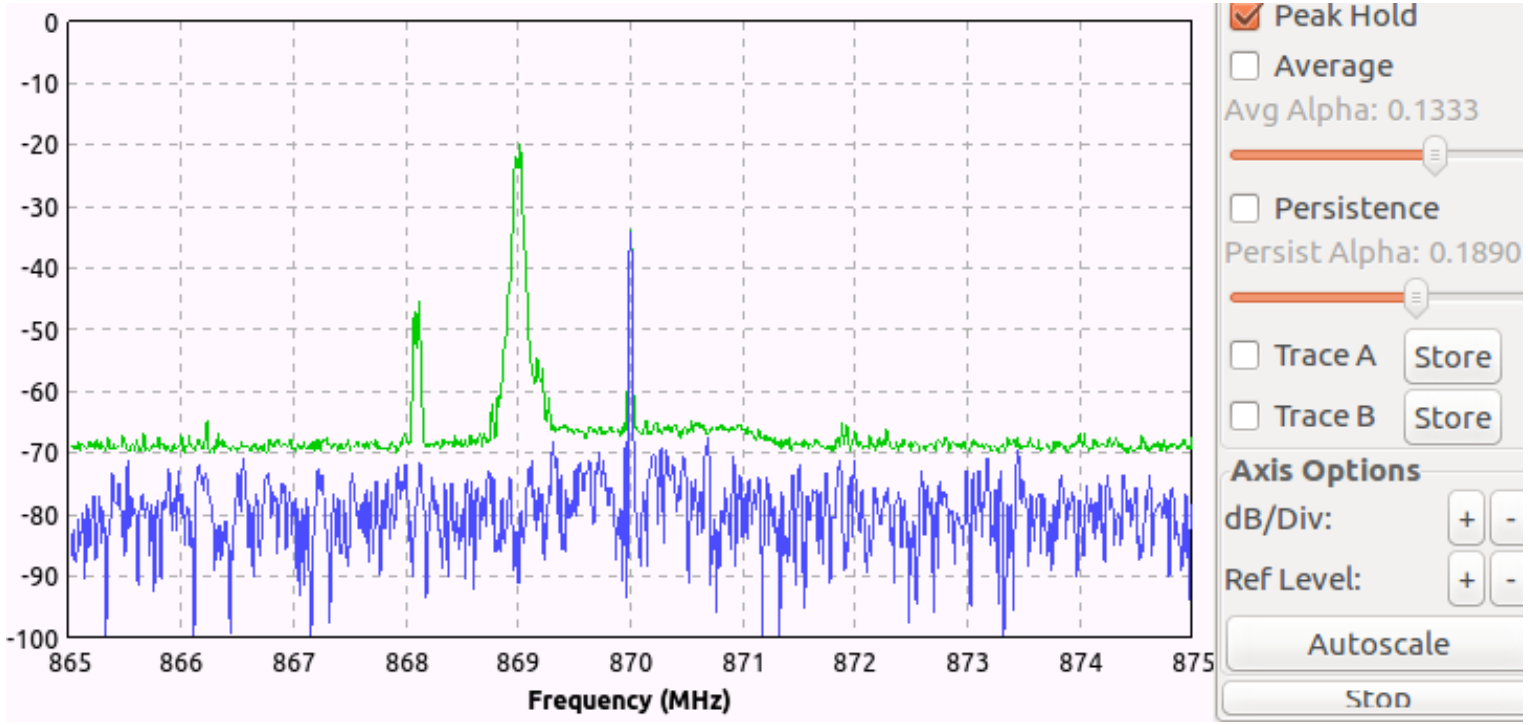


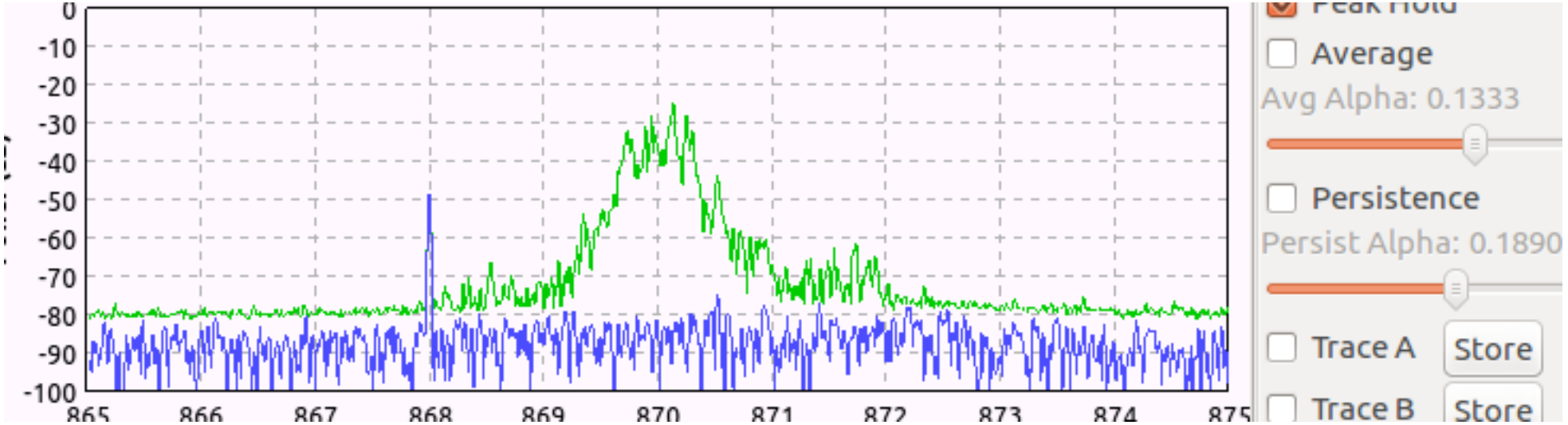






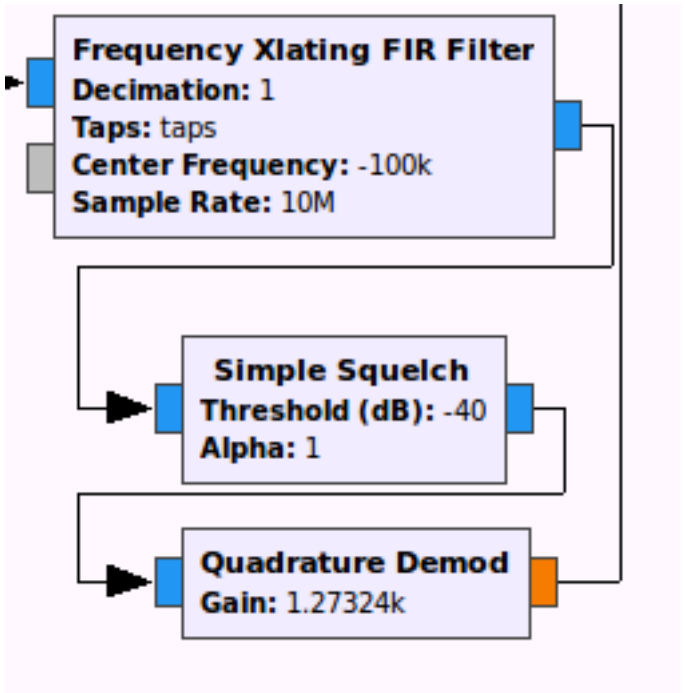
XLATING FIR FILTER



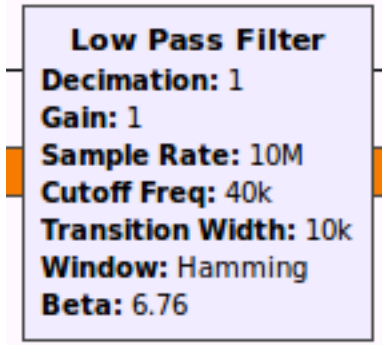


FILTERING OUR SIGNAL

Frequency Shift Keying:



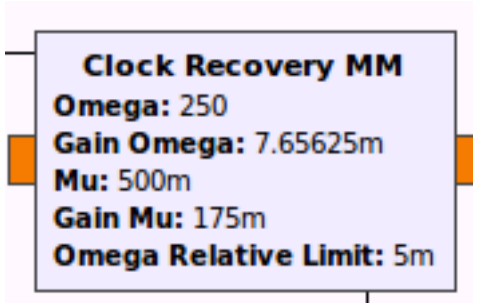
- After FIR:
- – Simple squelch
- - quadrature demodulation
- - Low pass filter



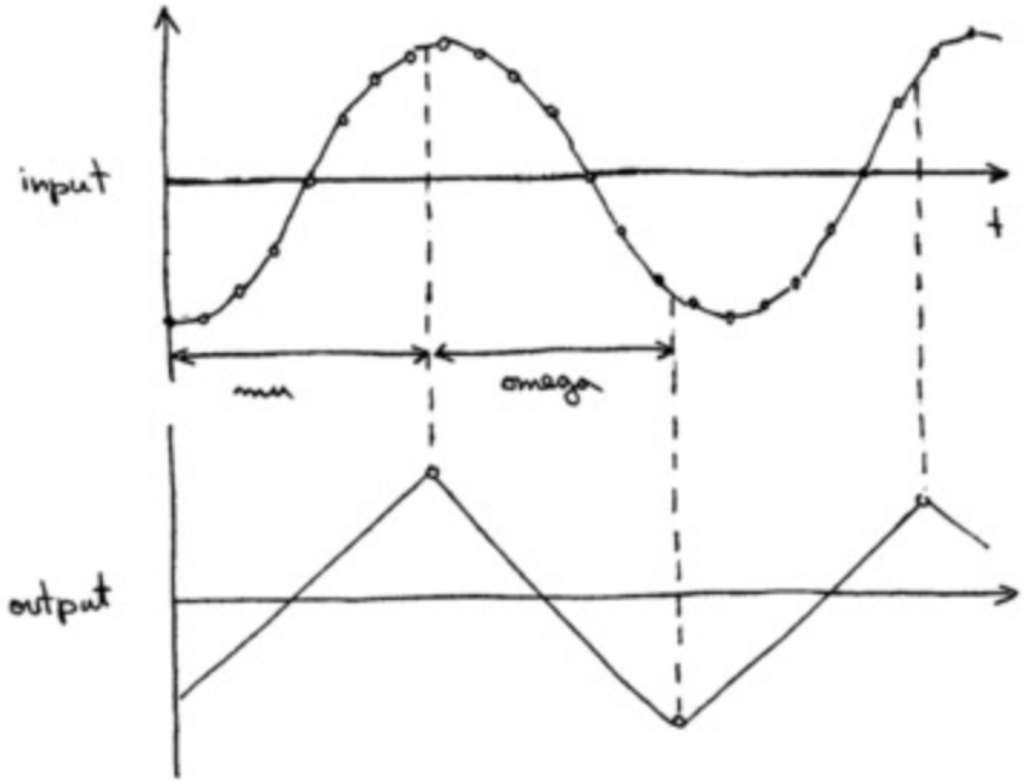
Low Pass Filter:
•Cut-off frequency
•Transitional width

•Rule of thumb:
Cut-off frequency = Baud rate Transition width = Baud rate / 2

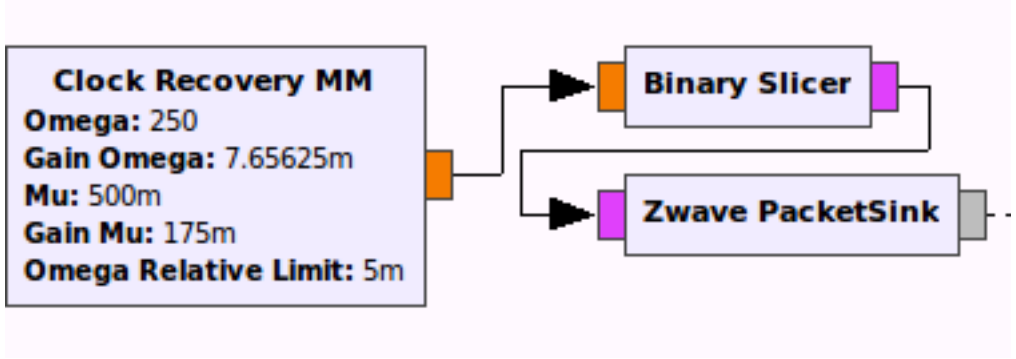
CLOCK RECOVERY



Gain Omega: 7.65625m
Mu: 500
Gain Mu: 175m
Omega Relative Limit: 5m
Omega: 250 (samples per symbol)



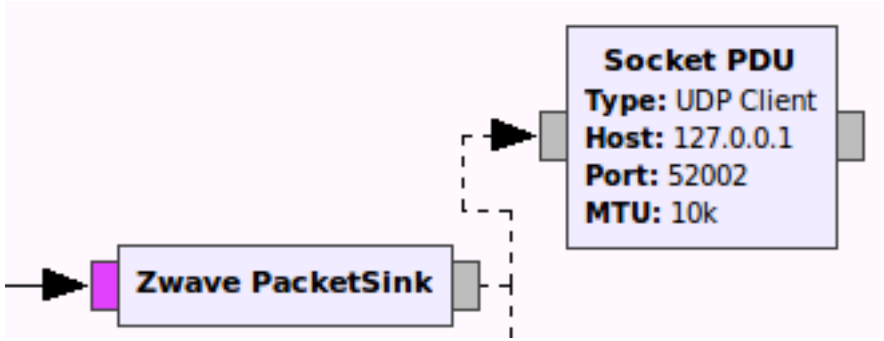
DATA RECOVERY

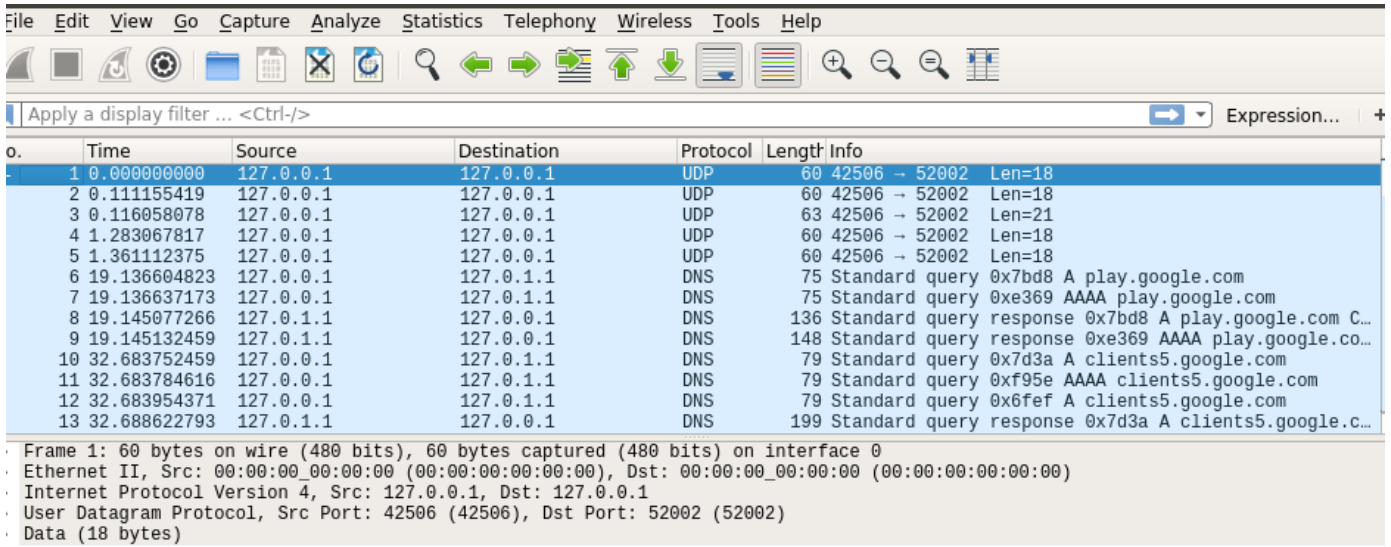


Binary Slicer:
To recover the binary bits

Zvawe PacketSink:
To recover zwave packet structure

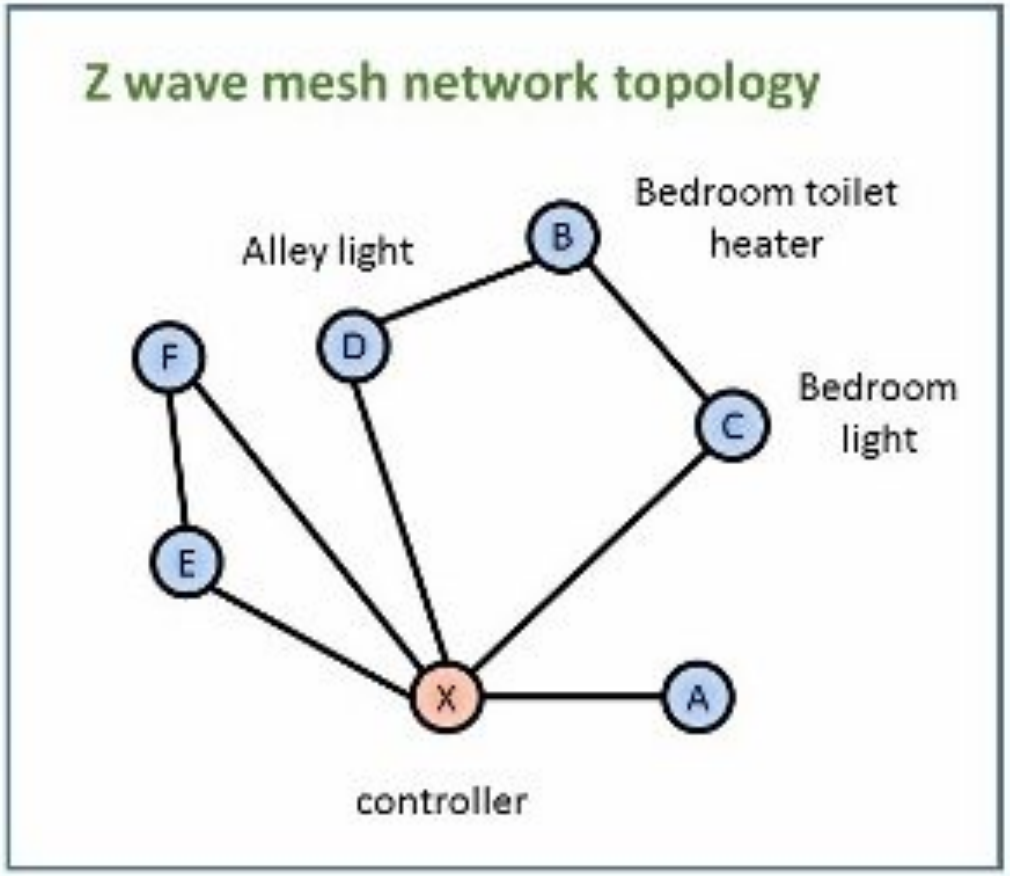
ADD DATA TO NETWORK SNIFFER



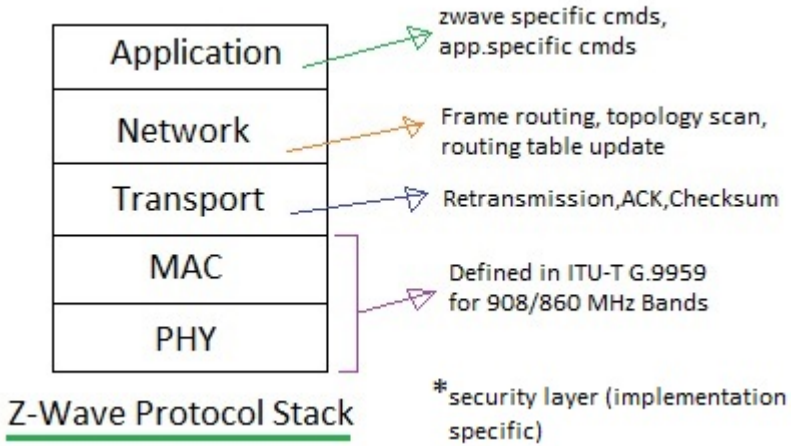


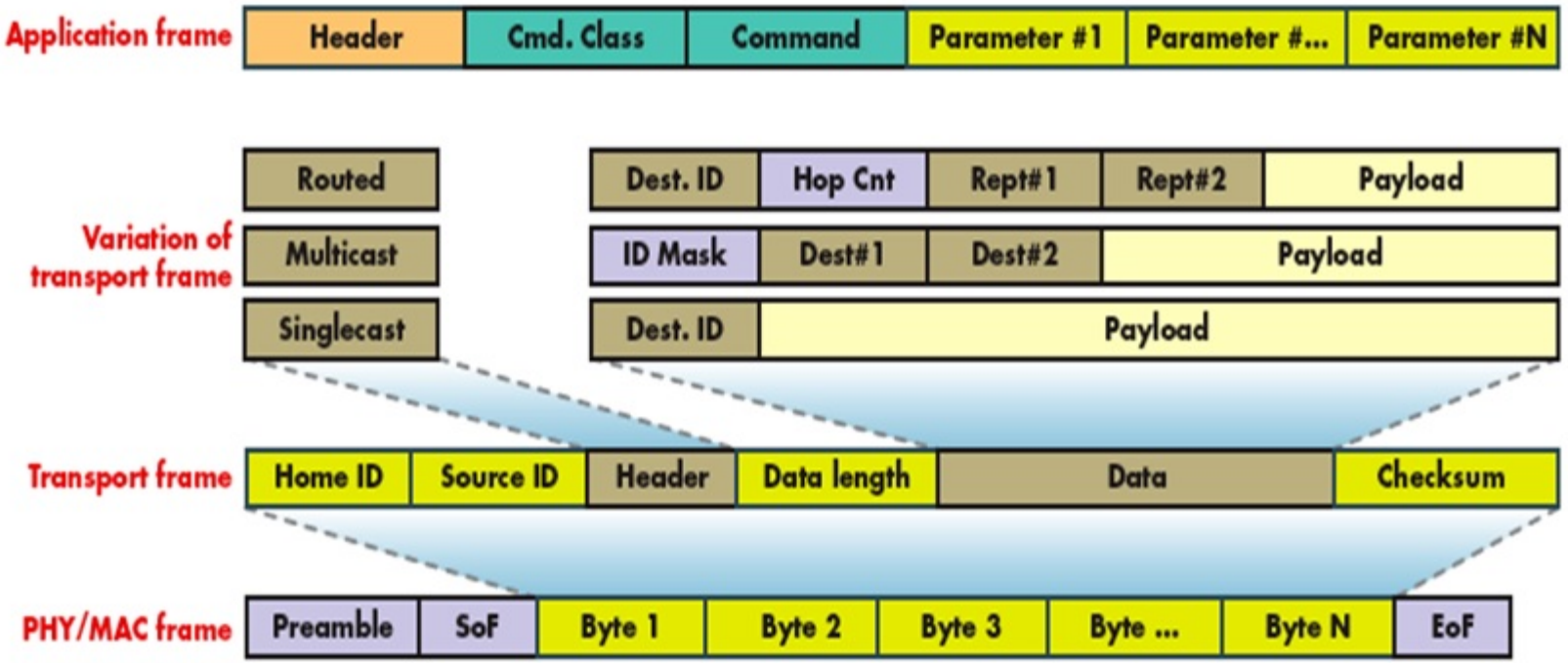
Writing data to Socket PDU:
UDP Client
Host 127.0.0.1
Port 52002
MTU 10k

Z-WAVE BASICS



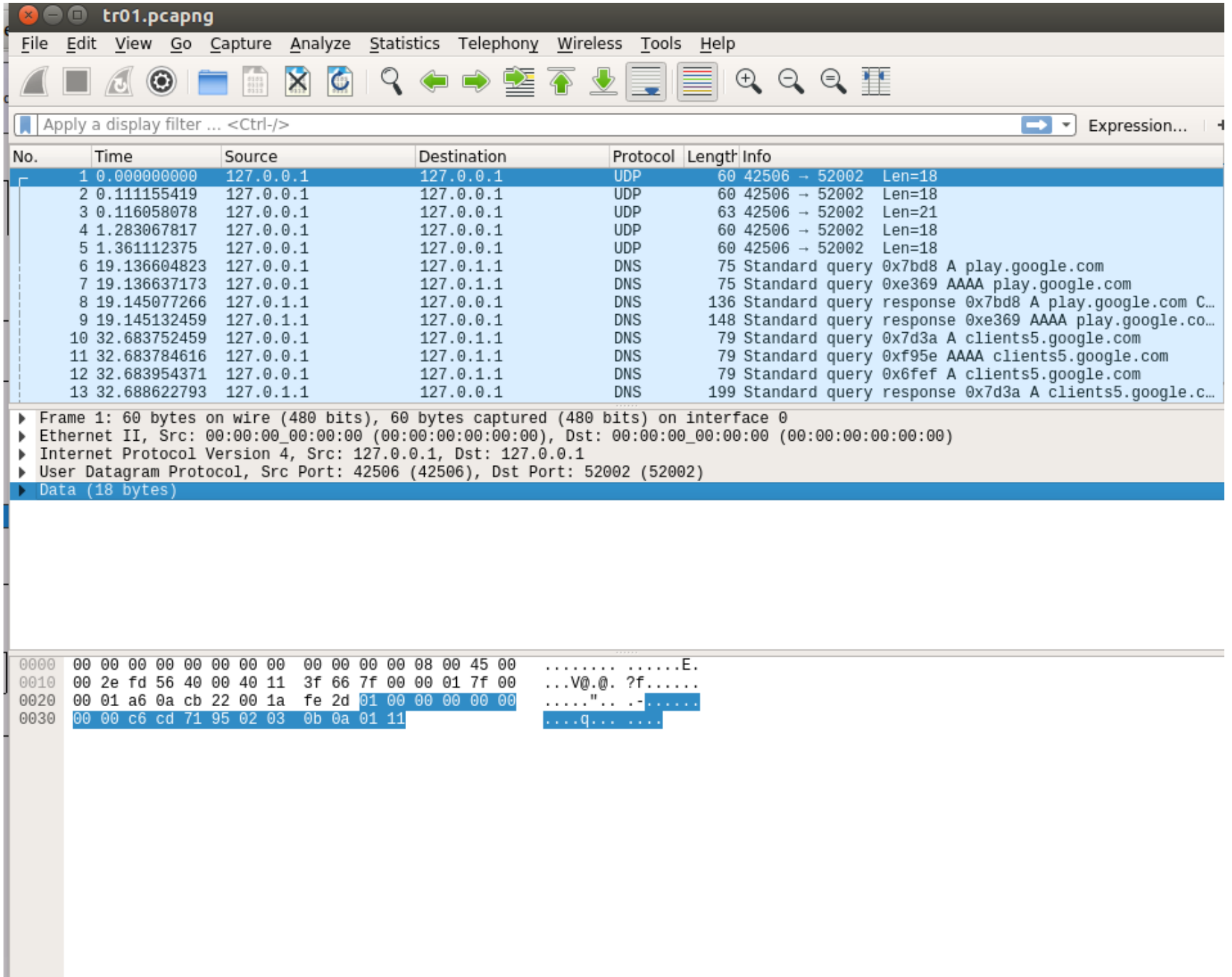
Z-WAVE PROTOCOL STACK





SNIFFING TRANSPORT FRAME

010000000000000 – preamble
c6cd7195 – HomeID
02 - Source ID
030b – header
0a – size
01 – Destination ID

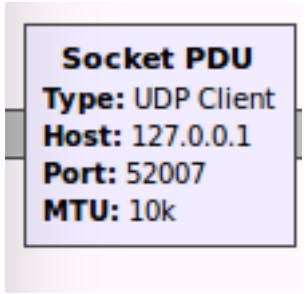


DIGITAL TRANSMITTER

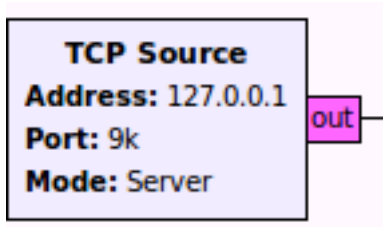
- Data source
- Modulation
- Resampling
- Adjust the signal level
- Configure the transmitter

DATA SOURCE

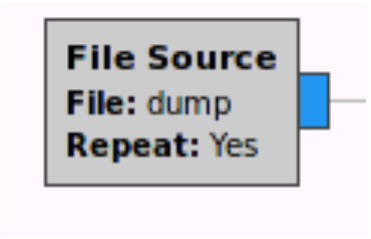
Socket PDU

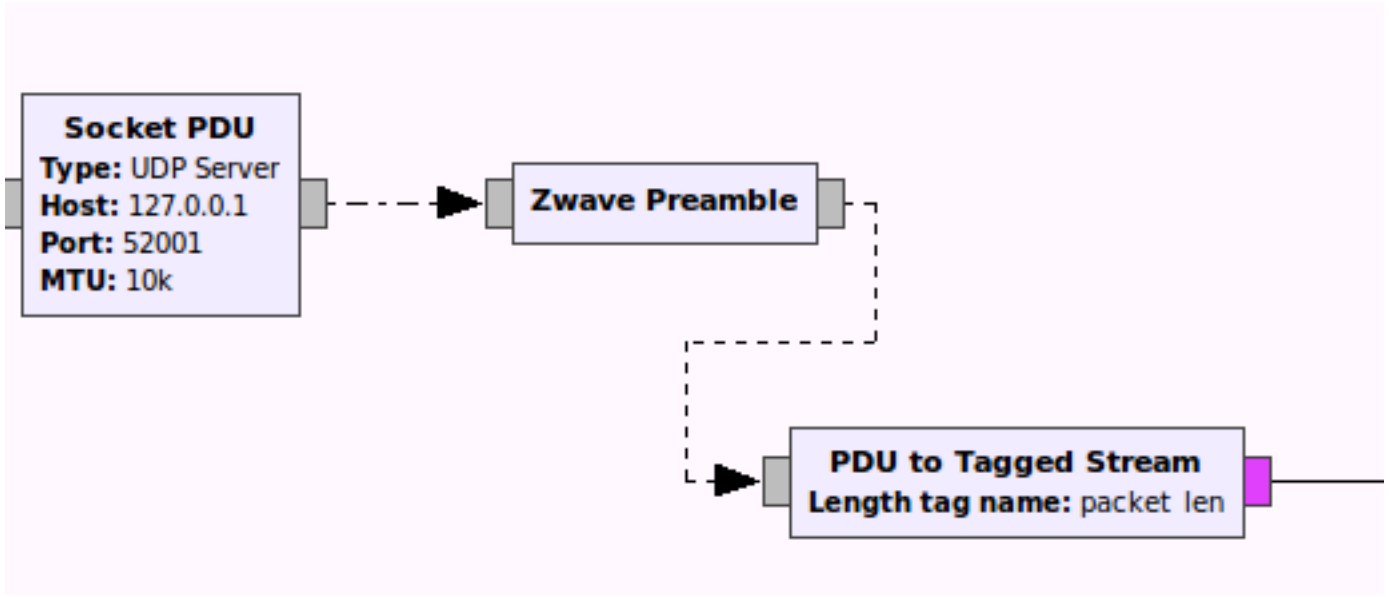


TCP Source

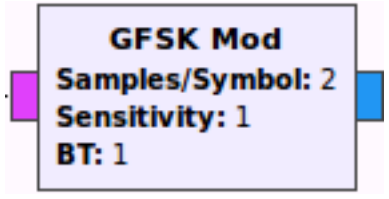


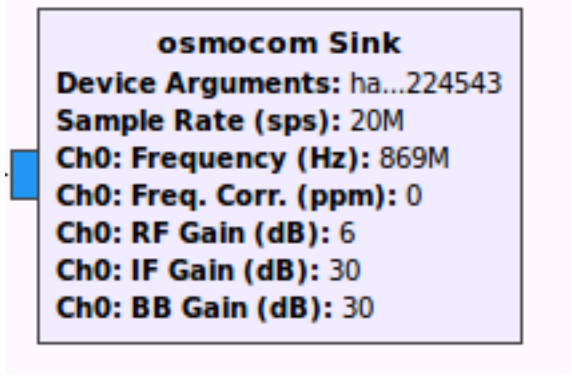
File Source (binary)





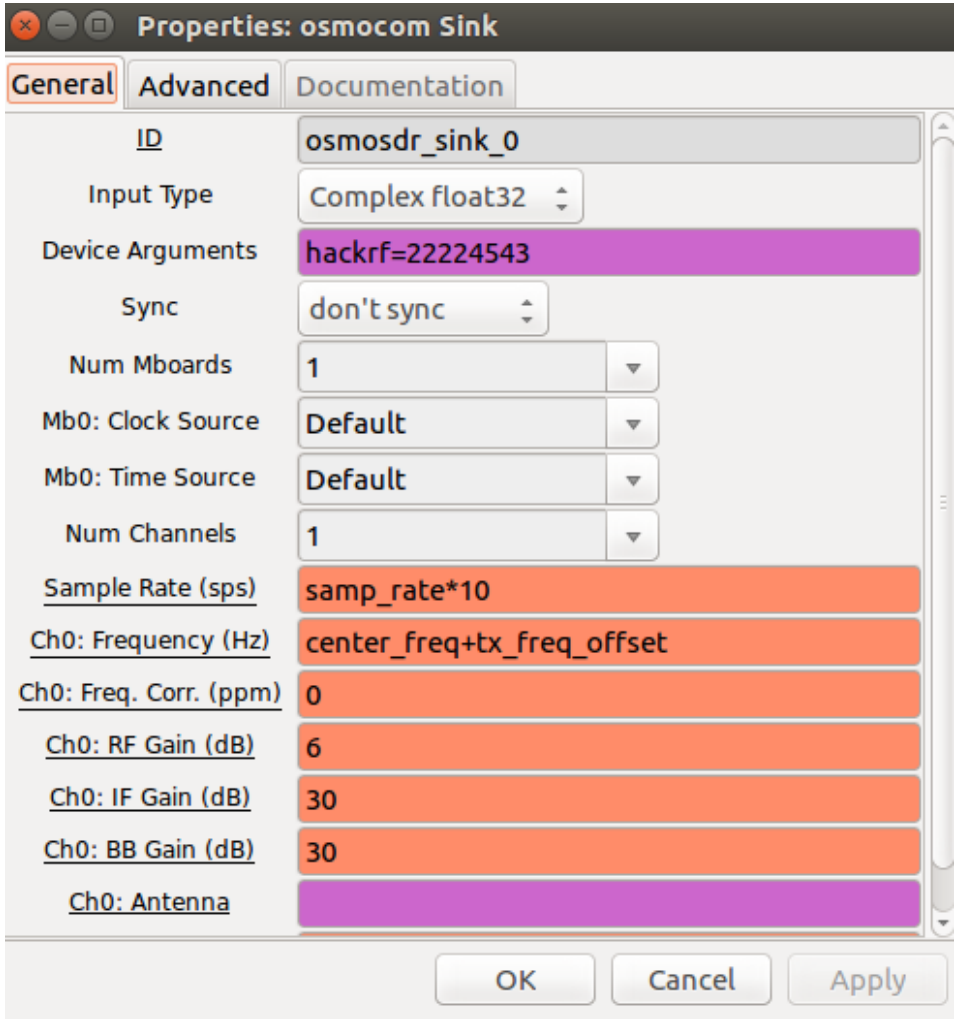
MODULATION. SINK



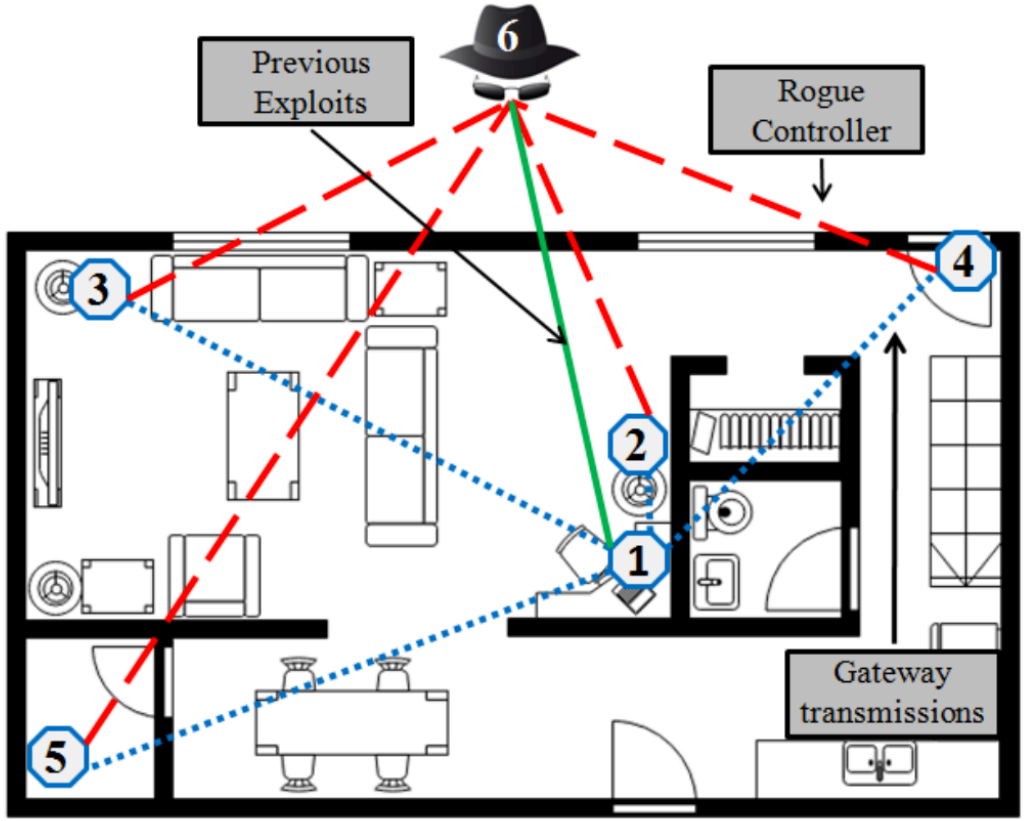


Add a GFSK Mod

Samples per symbol - 2



FAKE CONTROLLERS



Pic: http://ieeexplore.ieee.org/

Take control under your home or office

1. - Your Z-Wave controller 6. – Fake controller

HOW TO DEFENCE?

- Vendors must be interested in implementing security level
- Use crypto protocols for air transmission
- Use authentication for air transmission

THANKS FOR ATTENTION

- Elena Feldman
- Email: mila008.is@gmail.com
- Phone: +79191231966