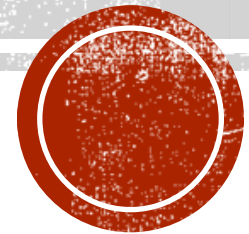


HOW TO HACK WIRELESS SCADA

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

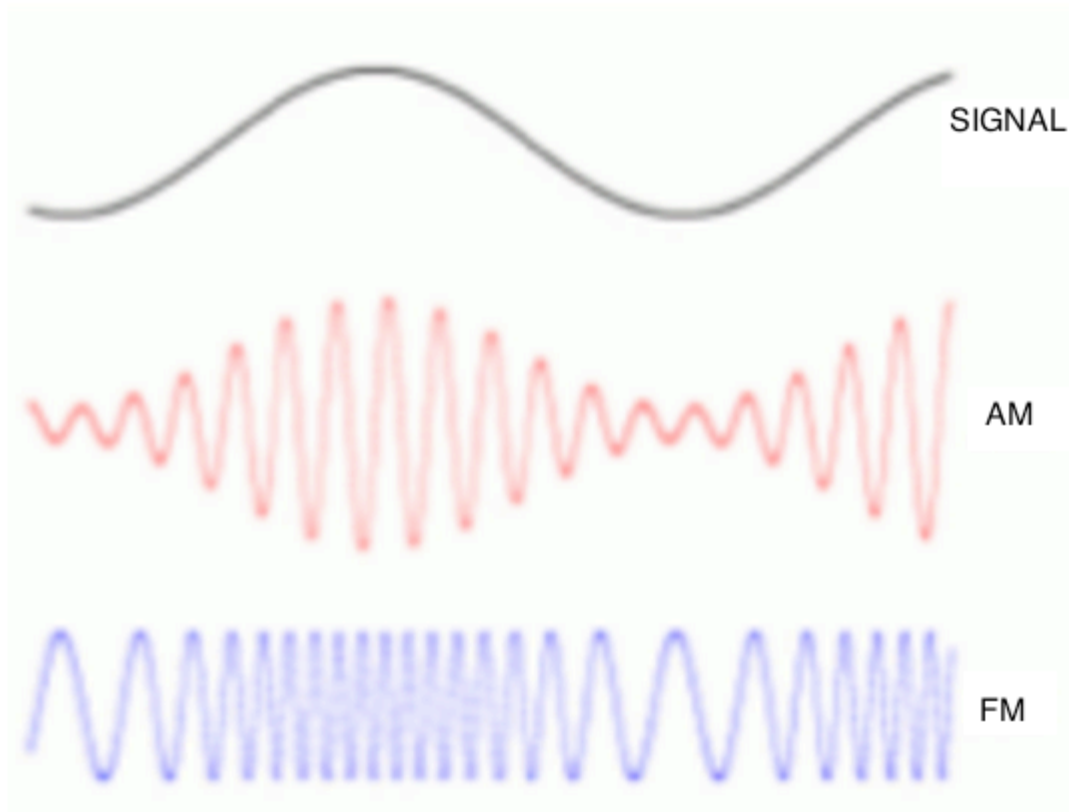


AGENDA

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

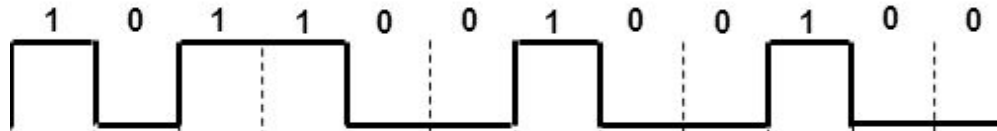


SIGNAL AND MODULATION



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

osmocom Source

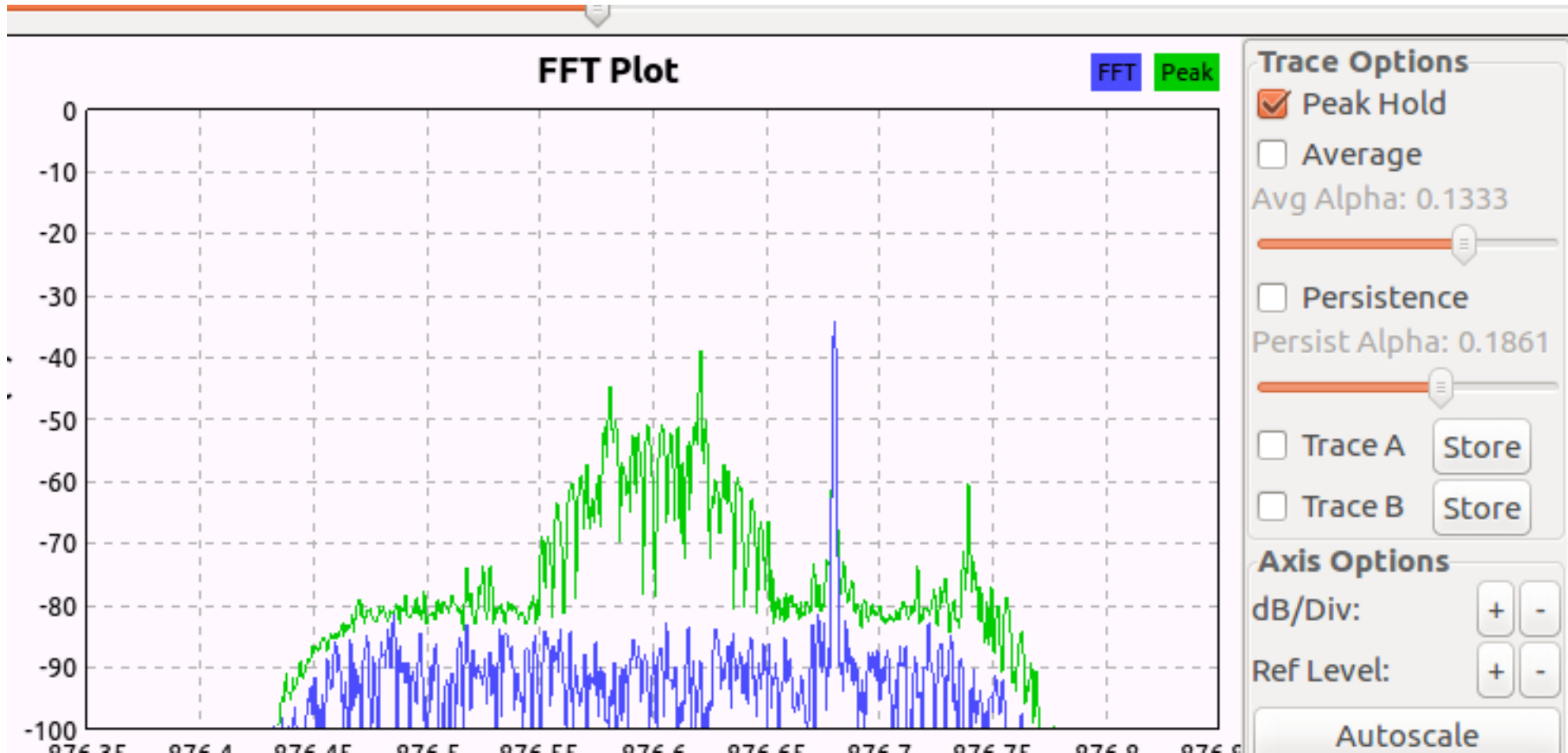
Device Arguments: hackrf=0
Sample Rate (sps): 10M
Ch0: Frequency (Hz): 869.075M
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Automatic
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 14
Ch0: IF Gain (dB): 24
Ch0: BB Gain (dB): 24

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

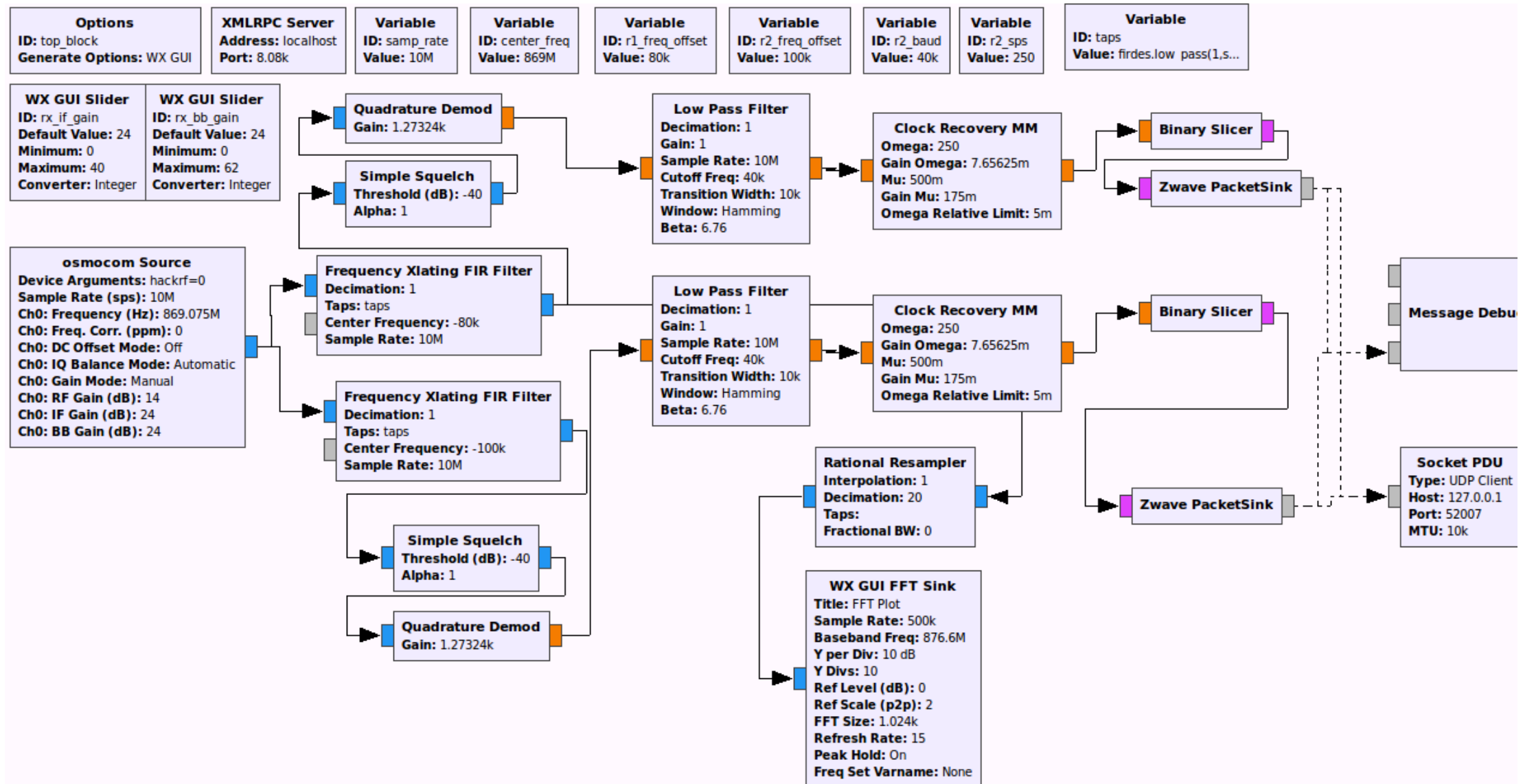


DEBUG?

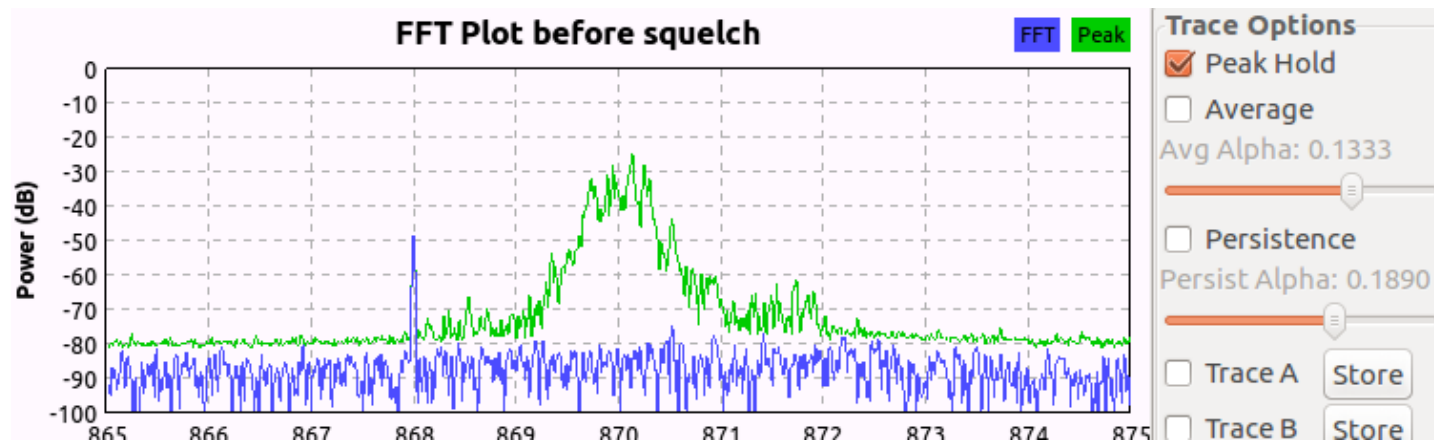
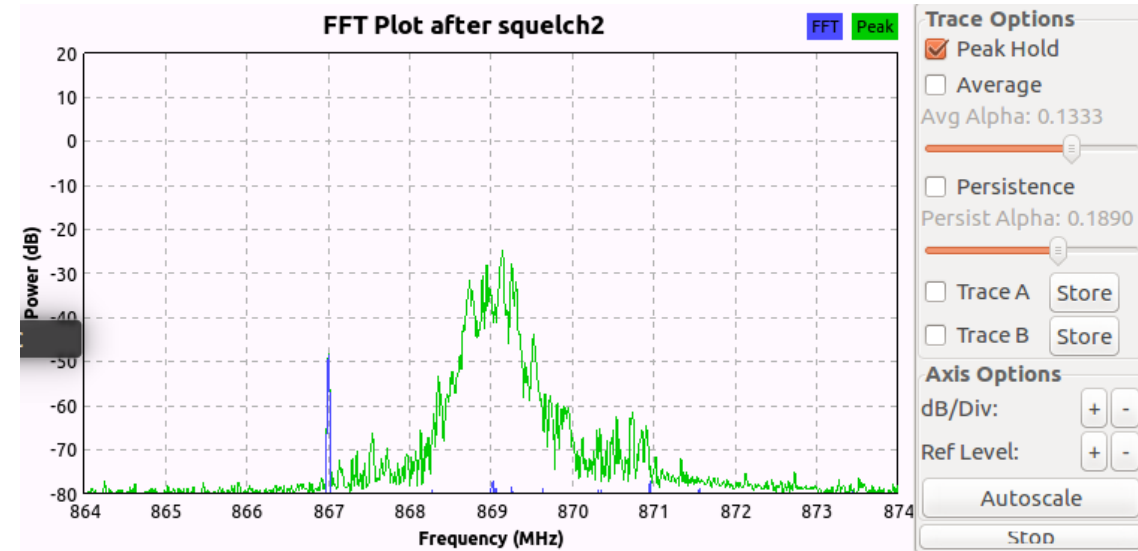
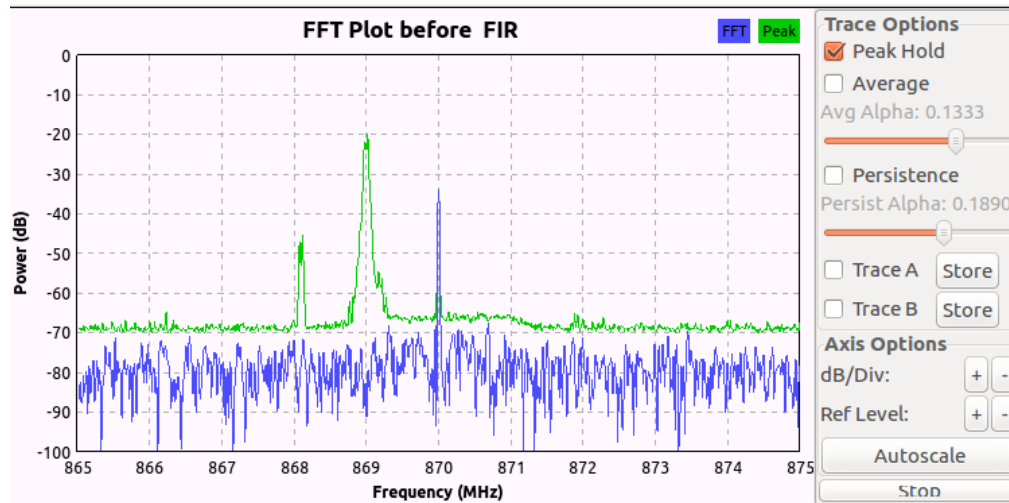
- First – watch signal



DEBUG: SEE SIGNAL GRAPH



DEBUG: ADD PLOTS BEFORE AND AFTER



CENTERING SIGNAL — XLATING FIR FILTER

Frequency Xlating FIR Filter

Decimation: 1

Taps: taps

Center Frequency: -80k

Sample Rate: 10M

Variable

ID: taps

Value: firdes.low_pass(1,s...

Properties: Frequency Xlating FIR Filter

General Advanced Documentation

ID	freq_xlating_fir_filter_xxx_0
Type	Complex->Complex (Complex Taps)
Decimation	1
Taps	taps
Center Frequency	-1*r1_freq_offset
Sample Rate	samp_rate

OK Cancel Apply

Properties: Variable

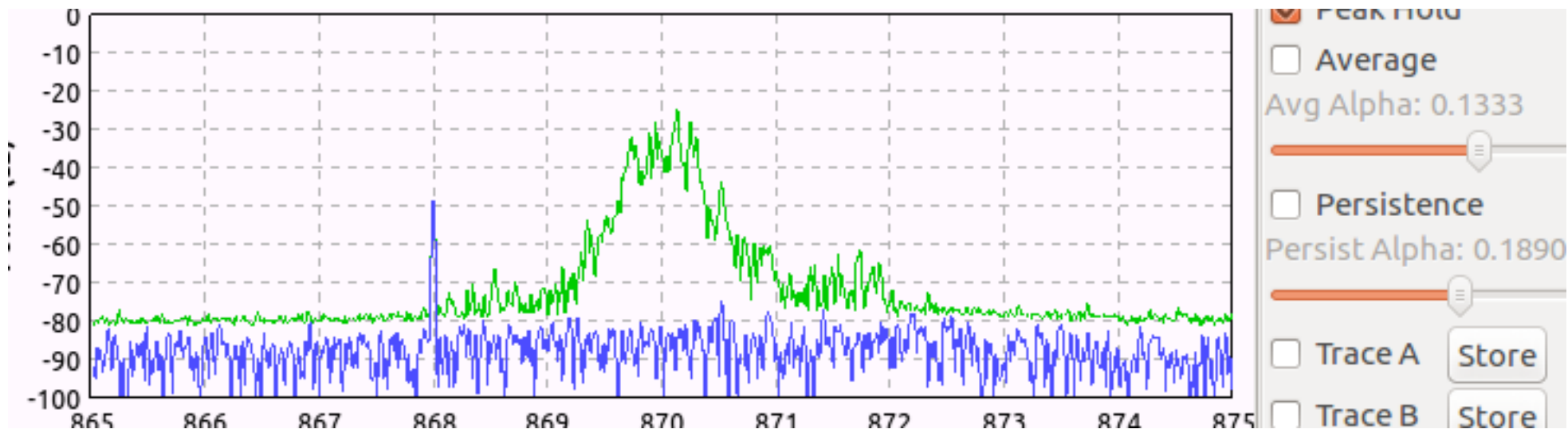
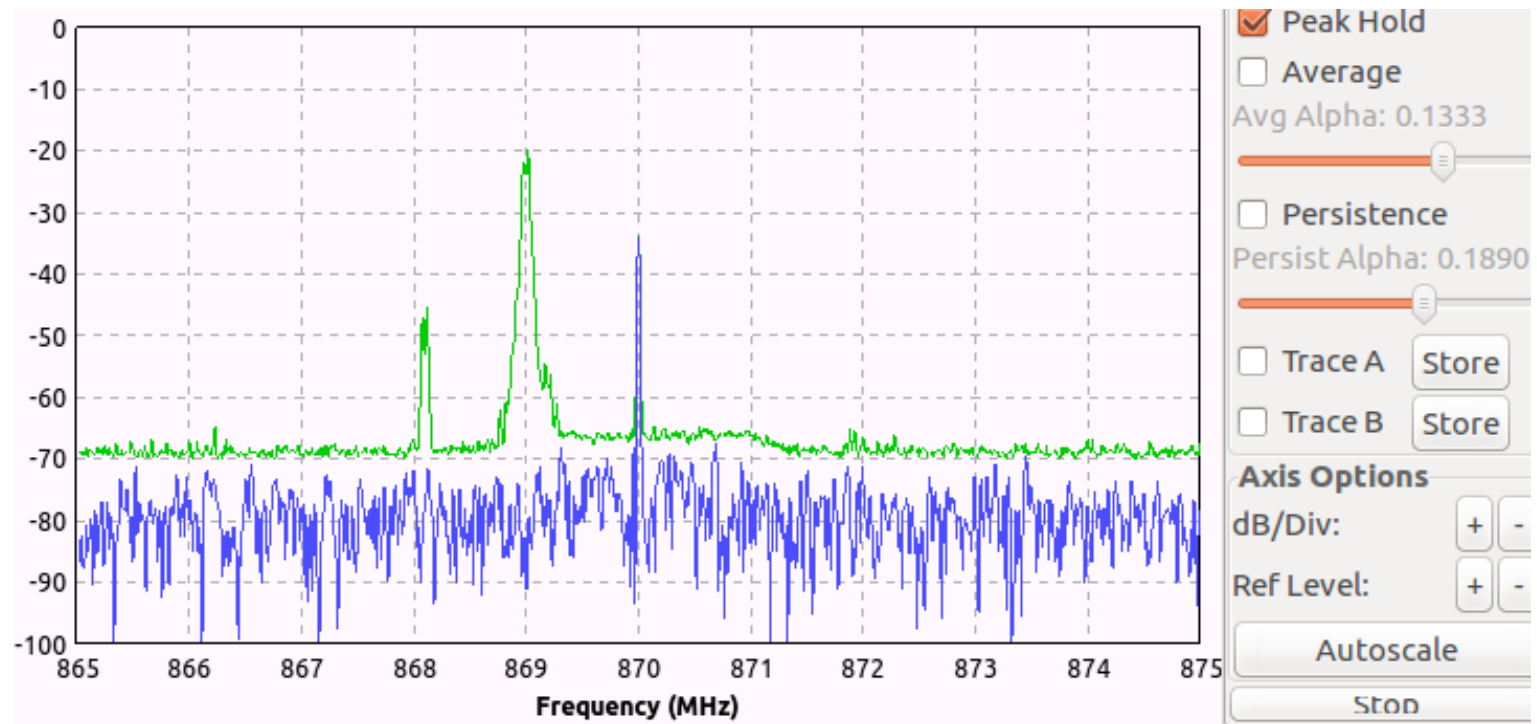
General Advanced Documentation

ID	taps
Value	firdes.low_pass(1,samp_rate,150e3,50e3,firdes.V

OK Cancel Apply

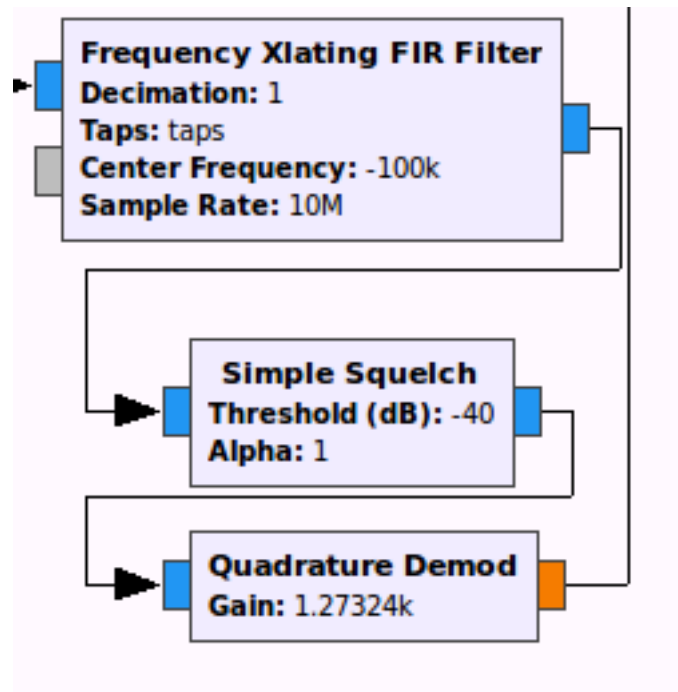


XLATING FIR FILTER

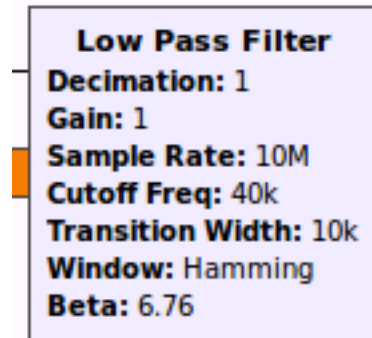


FILTERING OUR SIGNAL

Frequency Shift Keying:



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



Low Pass Filter:

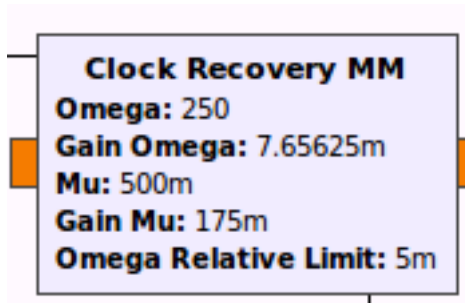
- Cut-off frequency
- Transitional width

•Rule of thumb:

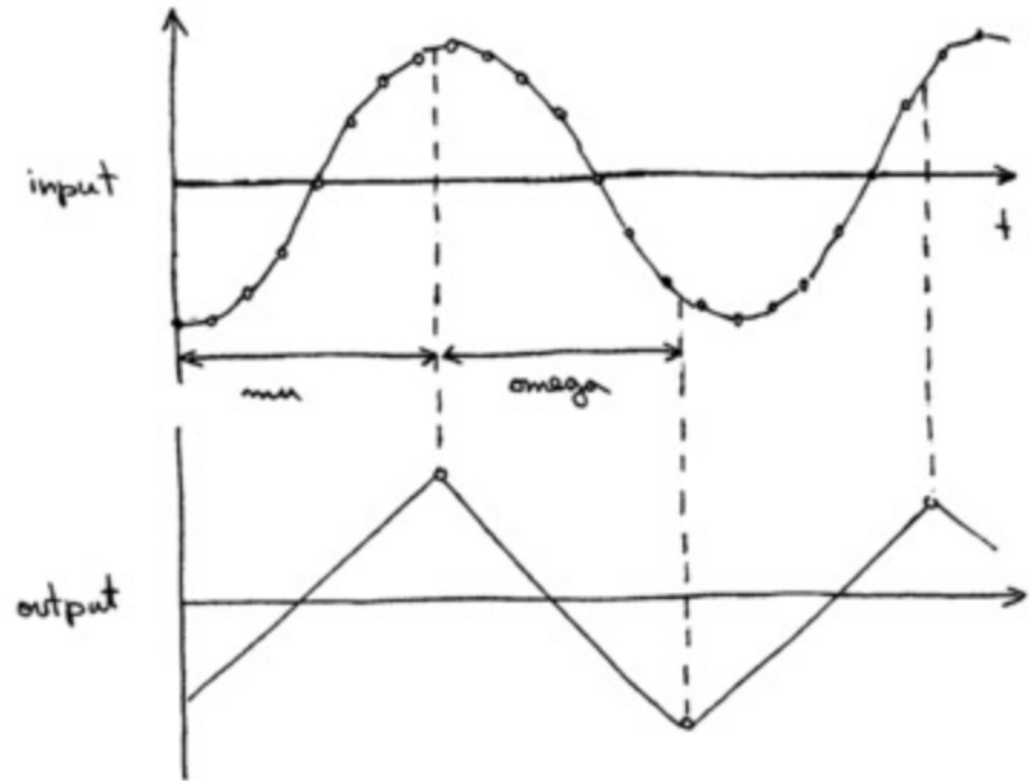
Cut-off frequency = Baud rate / 2
Transition width = Baud rate / 2



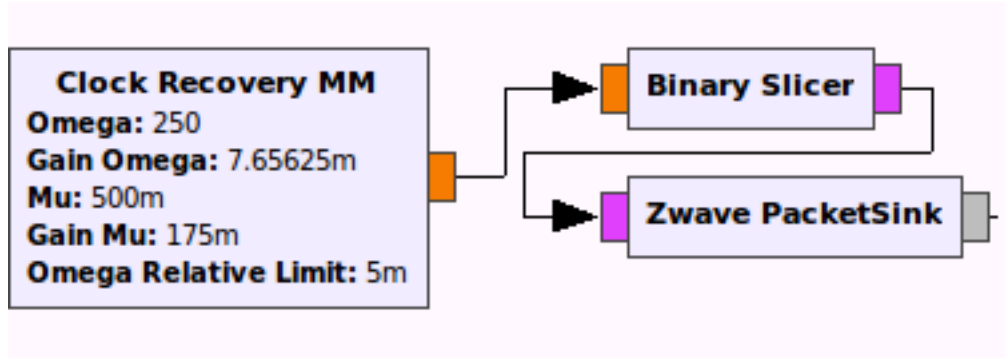
CLOCK RECOVERY



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



DATA RECOVERY

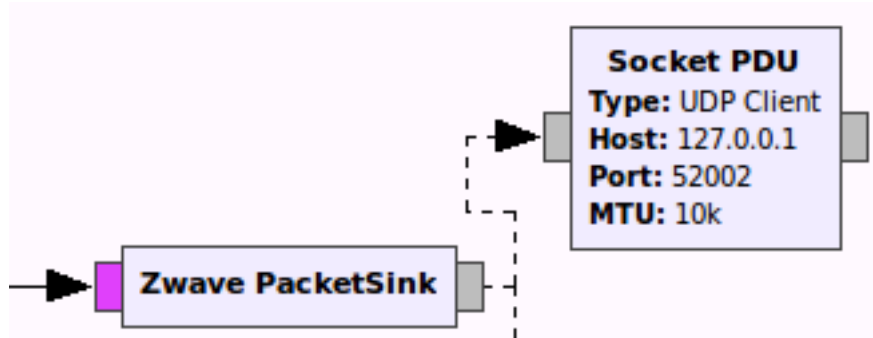


Binary Slicer:
To recover the binary bits

Zvawe PacketSink:
To recover zwave packet structure



ADD DATA TO NETWORK SNIFFER



The screenshot shows a network sniffer interface with a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. Below the toolbar is a display filter input field with the text "Apply a display filter ... <Ctrl-/>". The main area displays a list of captured packets with columns for Time, Source, Destination, Protocol, Length, and Info. The first packet is highlighted in blue.

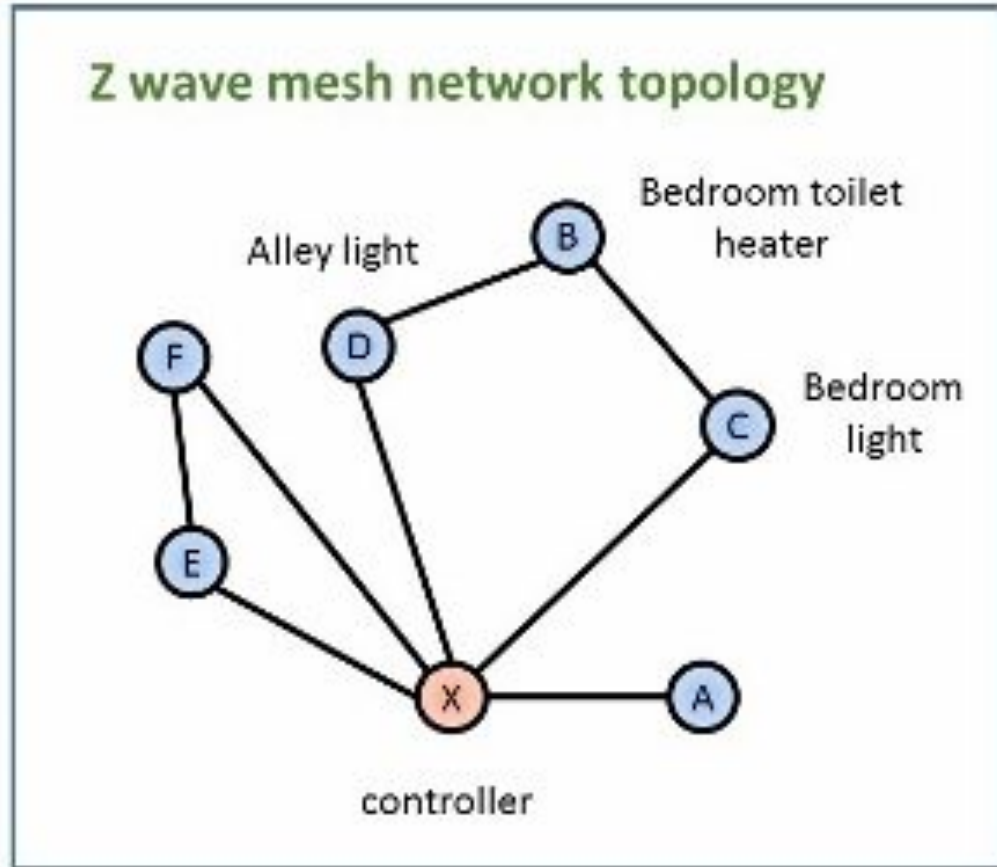
Time	Source	Destination	Protocol	Length	Info
0.000000000	127.0.0.1	127.0.0.1	UDP	60	42506 → 52002 Len=18
0.111155419	127.0.0.1	127.0.0.1	UDP	60	42506 → 52002 Len=18
0.116058078	127.0.0.1	127.0.0.1	UDP	63	42506 → 52002 Len=21
1.283067817	127.0.0.1	127.0.0.1	UDP	60	42506 → 52002 Len=18
1.361112375	127.0.0.1	127.0.0.1	UDP	60	42506 → 52002 Len=18
19.136604823	127.0.0.1	127.0.1.1	DNS	75	Standard query 0x7bd8 A play.google.com
19.136637173	127.0.0.1	127.0.1.1	DNS	75	Standard query 0xe369 AAAA play.google.com
19.145077266	127.0.1.1	127.0.0.1	DNS	136	Standard query response 0x7bd8 A play.google.com C...
19.145132459	127.0.1.1	127.0.0.1	DNS	148	Standard query response 0xe369 AAAA play.google.co...
32.683752459	127.0.0.1	127.0.1.1	DNS	79	Standard query 0x7d3a A clients5.google.com
32.683784616	127.0.0.1	127.0.1.1	DNS	79	Standard query 0xf95e AAAA clients5.google.com
32.683954371	127.0.0.1	127.0.1.1	DNS	79	Standard query 0x6fef A clients5.google.com
32.688622793	127.0.1.1	127.0.0.1	DNS	199	Standard query response 0x7d3a A clients5.google.c...

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
User Datagram Protocol, Src Port: 42506 (42506), Dst Port: 52002 (52002)
Data (18 bytes)

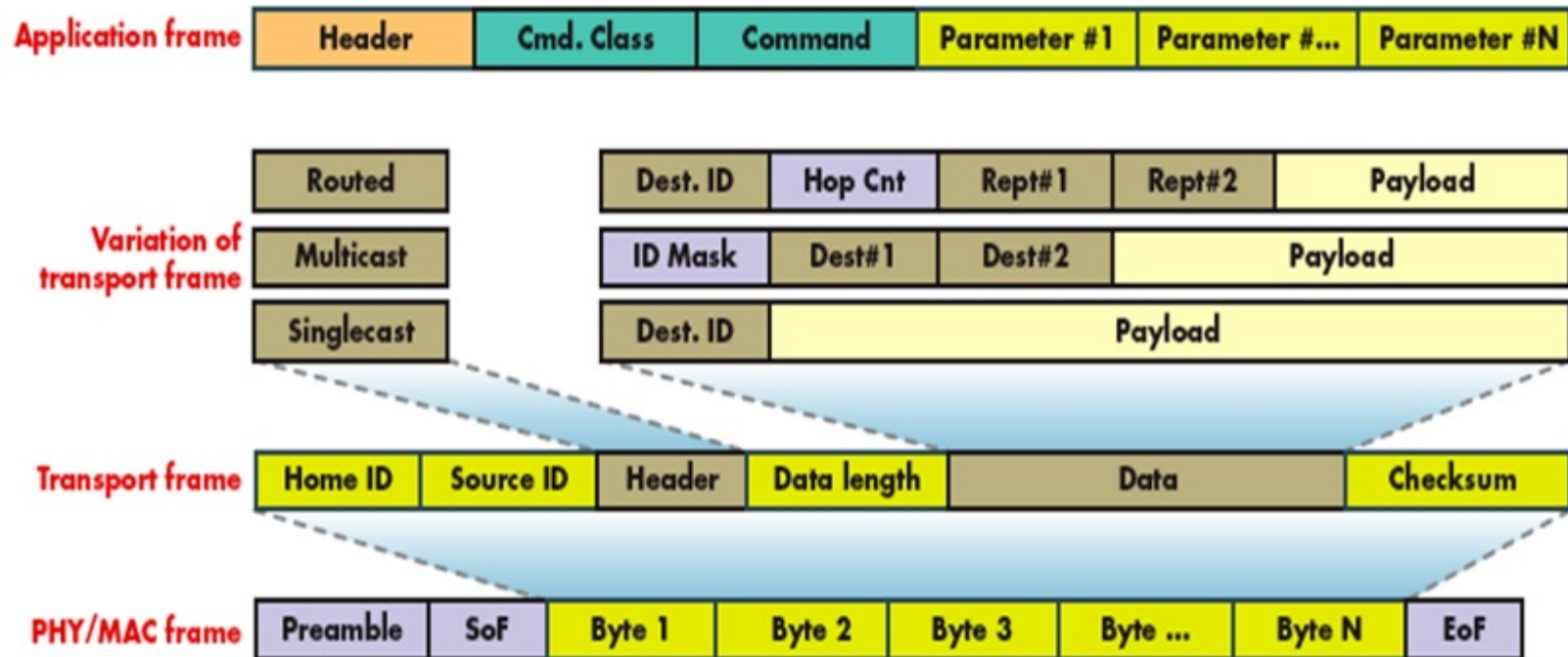
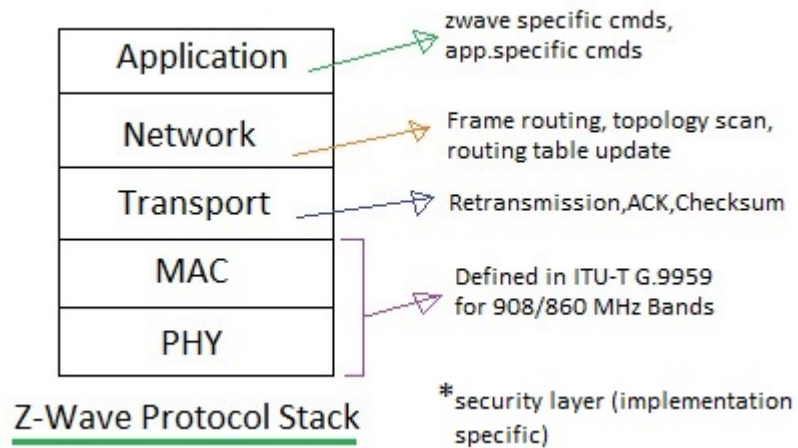
Writing data to Socket PDU:
UDP Client
Host 127.0.0.1
Port 52002
MTU 10k



Z-WAVE BASICS



Z-WAVE PROTOCOL STACK



SNIFFING TRANSPORT FRAME

010000000000000000 – preamble
c6cd7195 – HomeID
02 - Source ID
030b – header
0a – size
01 – Destination ID

tr01.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	UDP	60	42506 → 52002 Len=18
2	0.111155419	127.0.0.1	127.0.0.1	UDP	60	42506 → 52002 Len=18
3	0.116058078	127.0.0.1	127.0.0.1	UDP	63	42506 → 52002 Len=21
4	1.283067817	127.0.0.1	127.0.0.1	UDP	60	42506 → 52002 Len=18
5	1.361112375	127.0.0.1	127.0.0.1	UDP	60	42506 → 52002 Len=18
6	19.136604823	127.0.0.1	127.0.1.1	DNS	75	Standard query 0x7bd8 A play.google.com
7	19.136637173	127.0.0.1	127.0.1.1	DNS	75	Standard query 0xe369 AAAA play.google.com
8	19.145077266	127.0.1.1	127.0.0.1	DNS	136	Standard query response 0x7bd8 A play.google.com C...
9	19.145132459	127.0.1.1	127.0.0.1	DNS	148	Standard query response 0xe369 AAAA play.google.co...
10	32.683752459	127.0.0.1	127.0.1.1	DNS	79	Standard query 0x7d3a A clients5.google.com
11	32.683784616	127.0.0.1	127.0.1.1	DNS	79	Standard query 0xf95e AAAA clients5.google.com
12	32.683954371	127.0.0.1	127.0.1.1	DNS	79	Standard query 0x6fef A clients5.google.com
13	32.688622793	127.0.1.1	127.0.0.1	DNS	199	Standard query response 0x7d3a A clients5.google.c...

▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▶ User Datagram Protocol, Src Port: 42506 (42506), Dst Port: 52002 (52002)
▶ Data (18 bytes)

0000	00 00 00 00 00 00 00 00	00 00 00 00 08 00 45 00E.
0010	00 2e fd 56 40 00 40 11	3f 66 7f 00 00 01 7f 00	...V@.@. ?f.....
0020	00 01 a6 0a cb 22 00 1a	fe 2d 01 00 00 00 00 00".....
0030	00 00 c6 cd 71 95 02 03	0b 0a 01 11q.....

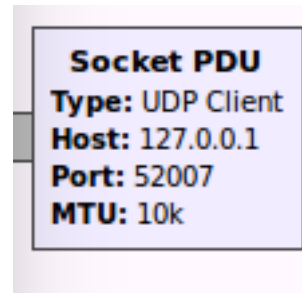
DIGITAL TRANSMITTER

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

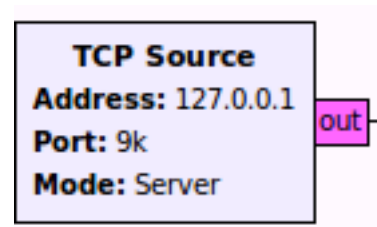


DATA SOURCE

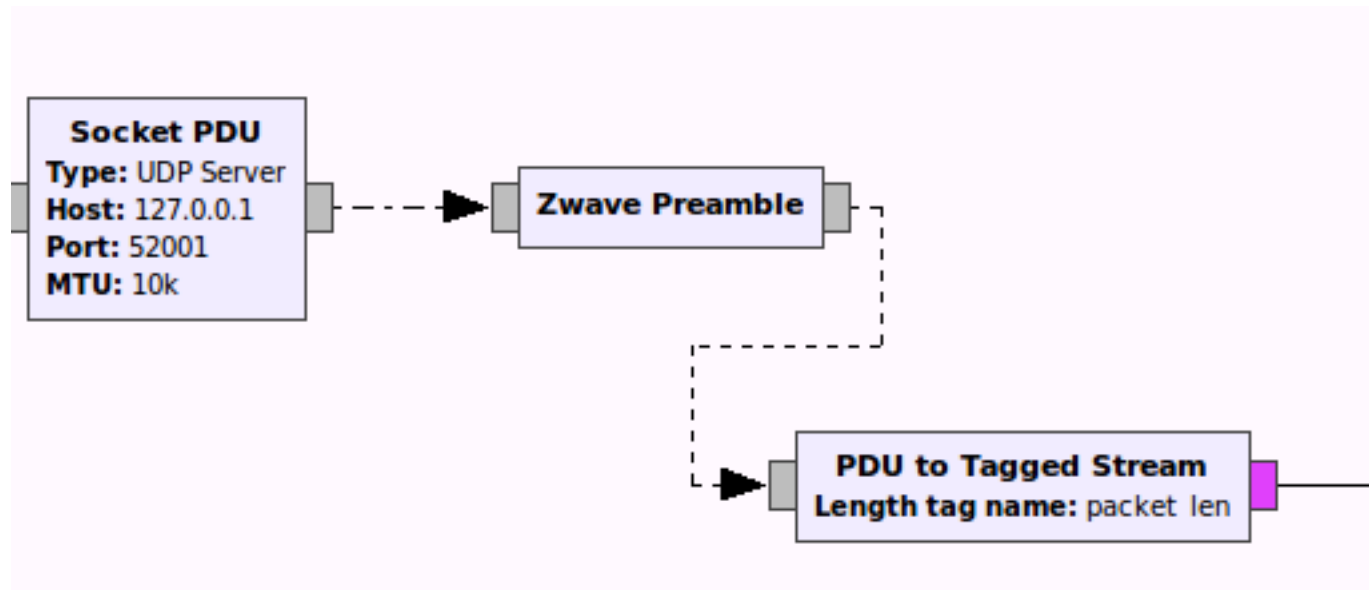
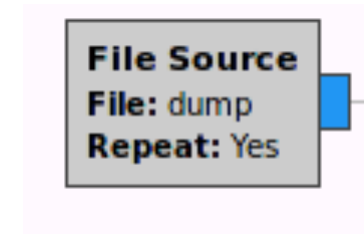
Socket PDU



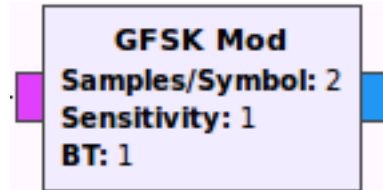
TCP Source



File Source (binary)

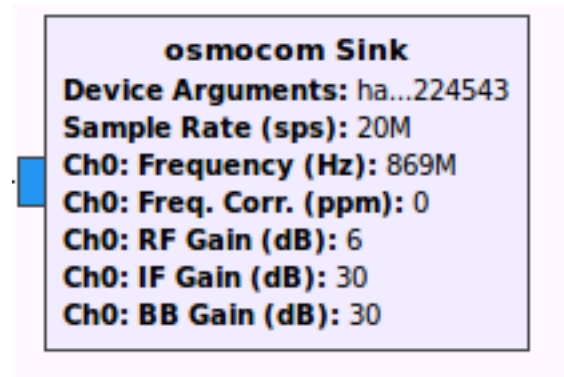


MODULATION. SINK



Add a GFSK Mod

Samples per symbol - 2

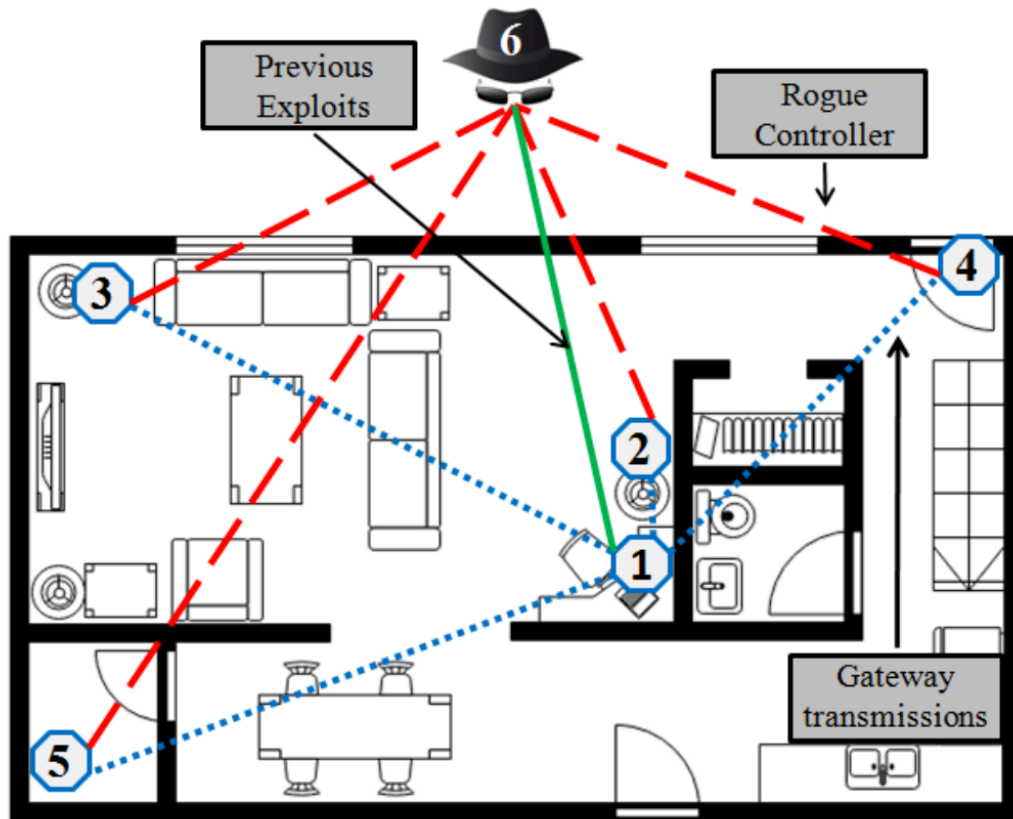


A screenshot of the 'Properties: osmocom Sink' dialog box. The 'General' tab is selected. The dialog box contains the following fields and values:

Field	Value
ID	osmosdr_sink_0
Input Type	Complex float32
Device Arguments	hackrf=22224543
Sync	don't sync
Num Mboards	1
Mb0: Clock Source	Default
Mb0: Time Source	Default
Num Channels	1
Sample Rate (sps)	samp_rate*10
Ch0: Frequency (Hz)	center_freq+tx_freq_offset
Ch0: Freq. Corr. (ppm)	0
Ch0: RF Gain (dB)	6
Ch0: IF Gain (dB)	30
Ch0: BB Gain (dB)	30
Ch0: Antenna	

Buttons at the bottom: OK, Cancel, Apply.

FAKE CONTROLLERS



Take control under your home or office

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

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



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

