Laboratory 4: Jamming Resistant Communication

Vasileios Dimitrakis and Niclas Scheuing

December 3, 2015

1 Introduction

Communication jamming is a technique that entirely prevents or reduces the ability of communicating parties to pass information by the deliberate use of electromagnetic signals. We distinguish the jamming from interference. Devices that simply cause interference are regulated under different regulations. The jamming is categorized in the intentional and unintentional jamming. The first one occurs when a device transmits in a busy medium without first checking if it is already in use. The second case aims at radio signals, in order to interrupt the communication and prevent availability. Jamming attack is effective, when the attacker has enough power to transmit, so that the receiver will not be able to receive the message or the jamming signal has certain characteristics that prevent the processor from extracting the original message.

2 Materials and Methods

Throughout the lab exercise 4 we used different materials and methods, that are presented below:

- *SDR - Software Defined Radio*: Is a hardware device that is capable of synthesizing arbitary radio signals.
- *hostapd*: Is a user space deamon for Access point and authentication servers.
- *GNU Radio*: Is a free software development toolkit that provides signal processing blocks to implement software-defined radios and signal processing systems.

3 Terminology and Topology

In the current lab exercise we examine the following topology and we use the appropriate terminology:

- *Access Point (AP)*: One machine serves as an Access Point and is used for the communication with the client.
- *Client (C)*: One PC of the group serves as the client, which sends the ICMP messages through the ping command to AP.
- *Attacking device*: The attacking machine uses the USRP device to transmit the jamming signal, in order to interrupt the communication.
- *Monitoring device*: The monitoring device uses the other USRP device to constantly monitor the wireless channel.

4 Setup

4.0.1 Attacking Team

In the attacker's configuration, we set a low-pass filter, because this kind of filter removes the noise that is produced by the Noise source outside the band that we observe. Moreover, the low-pass filter determines the bandwidth that the jamming signal will have. See Figure 1 for the *GNURadio* configuration.

4.0.2 Monitoring Team

The other USRP is used to observe the signals. Its *GNURadio* configuration does nothing but monitoring and can be seen in Figure 2

4.1 Channel selection

The center frequencies of channels 1, 6 and 11 are $2.412GHz$, $2.437GHz$ and $2.462GHz$, respectively. Every 802.11 Wi-Fi channel has bandwidth equal to $22MHz$. In this lab exercise, we used for communication the Wi-Fi channels 1, 6 and 11, because they are the only non-overlapping channels and we avoid interference between the experiments of the lab teams.

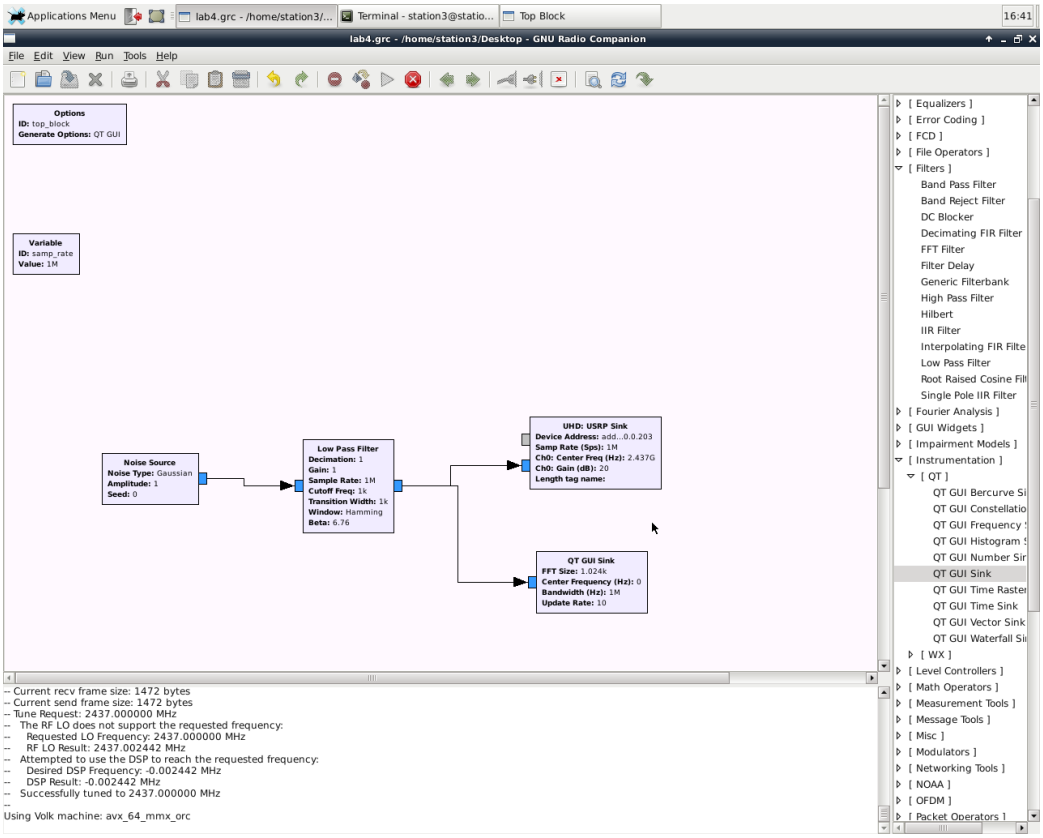

Figure 1: *GNURadio* configuration of the jammer.

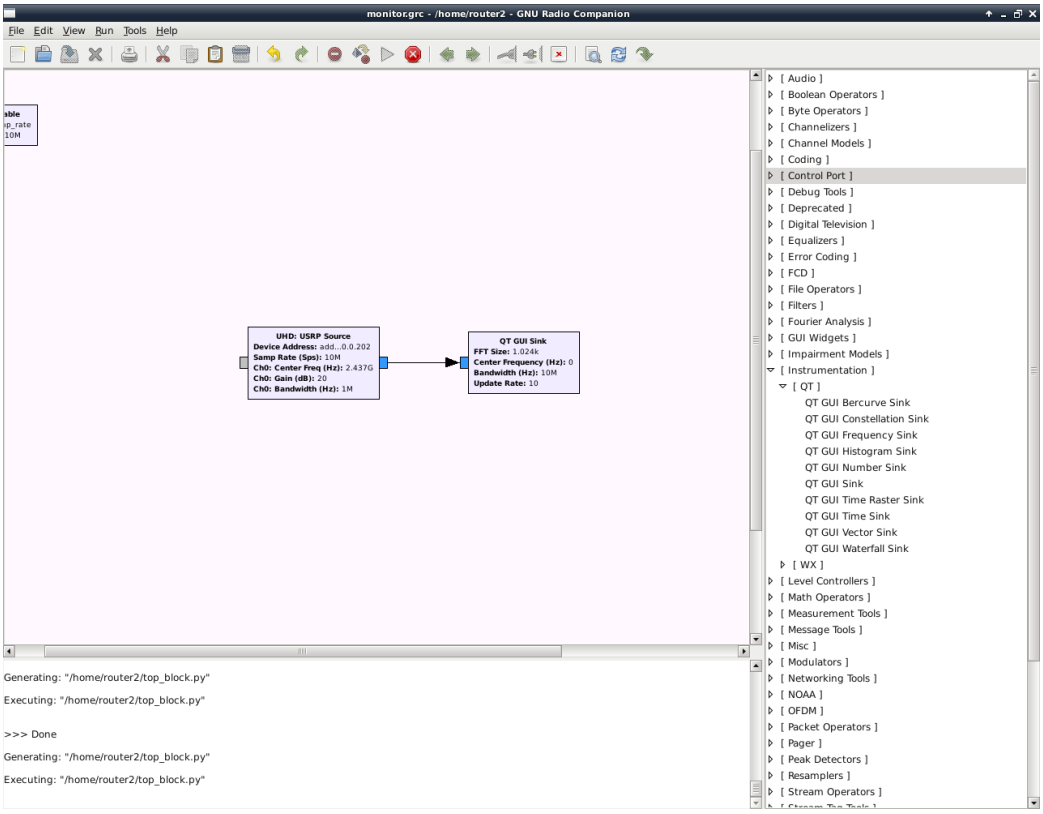

Figure 2: *GNURadio* configuration of the monitor.

5 Experiment

The Attacking team aims at the interruption of the communication between the client and the Access Point. The characteristics of the jamming signal are configured by the GNU radio software tool and it is transmitted through the USRD2 Software Defined Radio.

5.1 Jamming with 1kHz bandwidth

The first attempt to jamming the channel was using a Gaussian-random-noise signal with a bandwidth of 1kHz and a gain of 20dB.

Hypothesis 1 *The bandwidth of the jamming signal in this case is* $1kHz$*, which is a very narrow signal. Therefore, we expect that this jamming attack will not significantly affect the transmitting signal and it will not interrupt the communication between the client and the Access Point, which communicate through the ping messages.*

After starting the jamming signal, we can observe that its bandwidth is equal to $1kHz$. Refer to Figure 3

Moreover, the ICMP messages of the ping command are not interrupted and we can deduce that the certain jamming attack was not effective.

The bandwidth of the Jamming signal is $1kHz$ and it is much lower than the one of the channel. The ratio between both signal bandwidths is $\frac{JammingSignalBandwidth}{ChannelBandwidth} = \frac{1}{22000} = 0.00005$. This major difference in bandwidth makes this jamming attack ineffective. Refer to Figure 4.

5.2 Jamming with 100kHz bandwidth

After finishing the first jamming attempt, the attacking team changed the cut-off frequency of low pass filter to $100kHz$ increasing in this way the bandwidth of the jamming signal.

Hypothesis 2 *In this second attempt, we can hypothesize that the jamming attack will be effective , as we increased the bandwidth.*

After starting the jamming signal (Figure 6), we observe that the ping command is interrupted, as the client receives messages: "Host unreachable". One interesting point in this case is that with very limited jamming bandwidth (100 kHz), we managed to interrupt the communication in a Wi-Fi channel, that has 22 MHz bandwidth. See Figure 6.

This outcome is due to the fact that the 802.11 b standard uses very short, 11bit, pseudorandom code length for the DSSS modulation. This means the

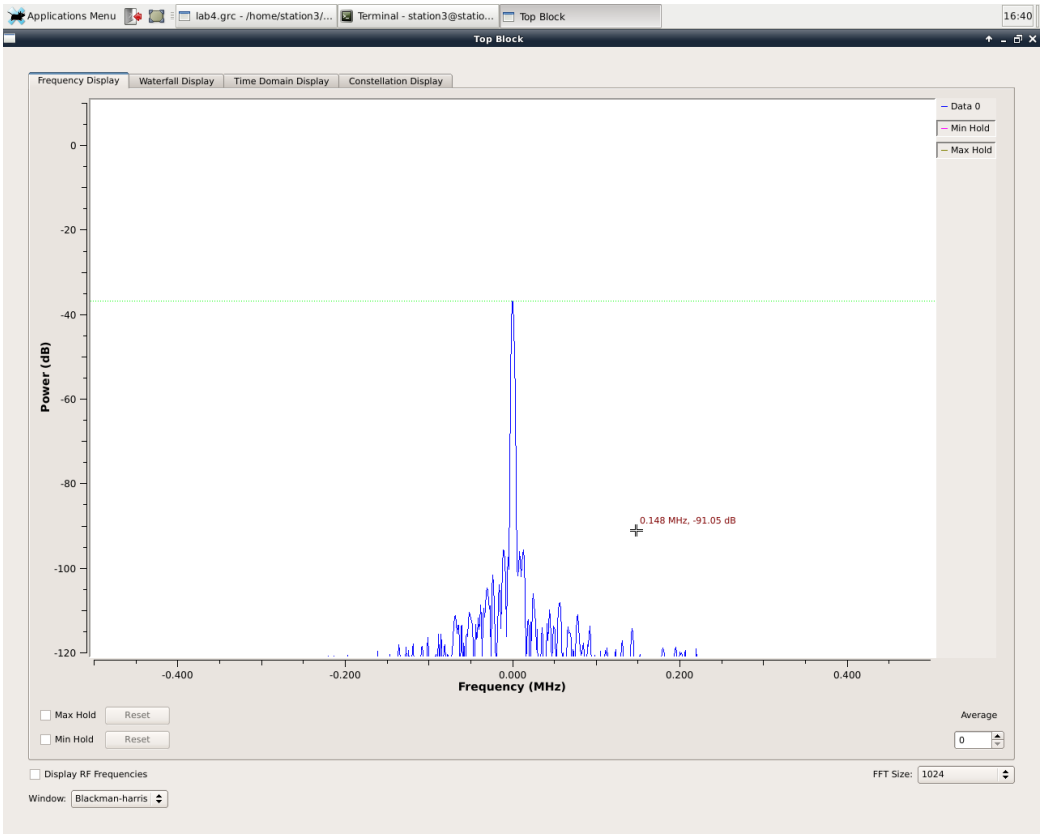

Figure 3: Jamming signal with 1kHz bandwidth from the *Attacking device*.

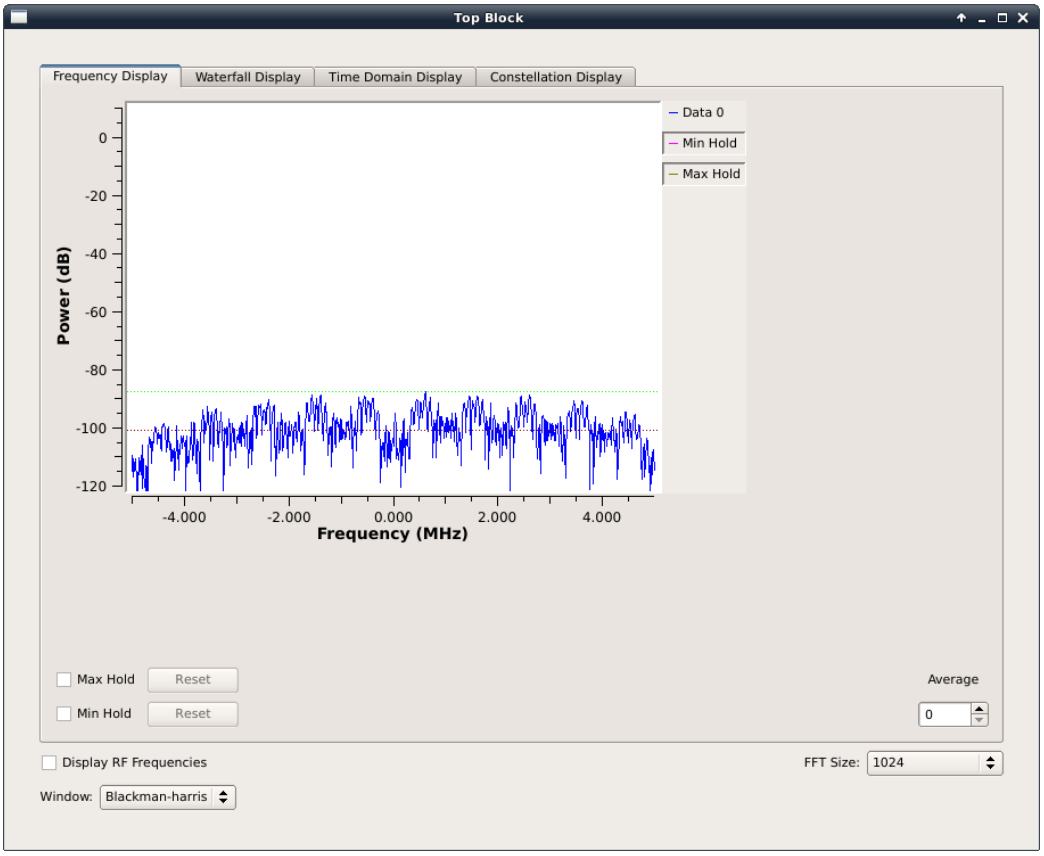

Figure 4: Ping signal and jamming signal with 1kHz bandwidth. The jamming signal is hardly visible.

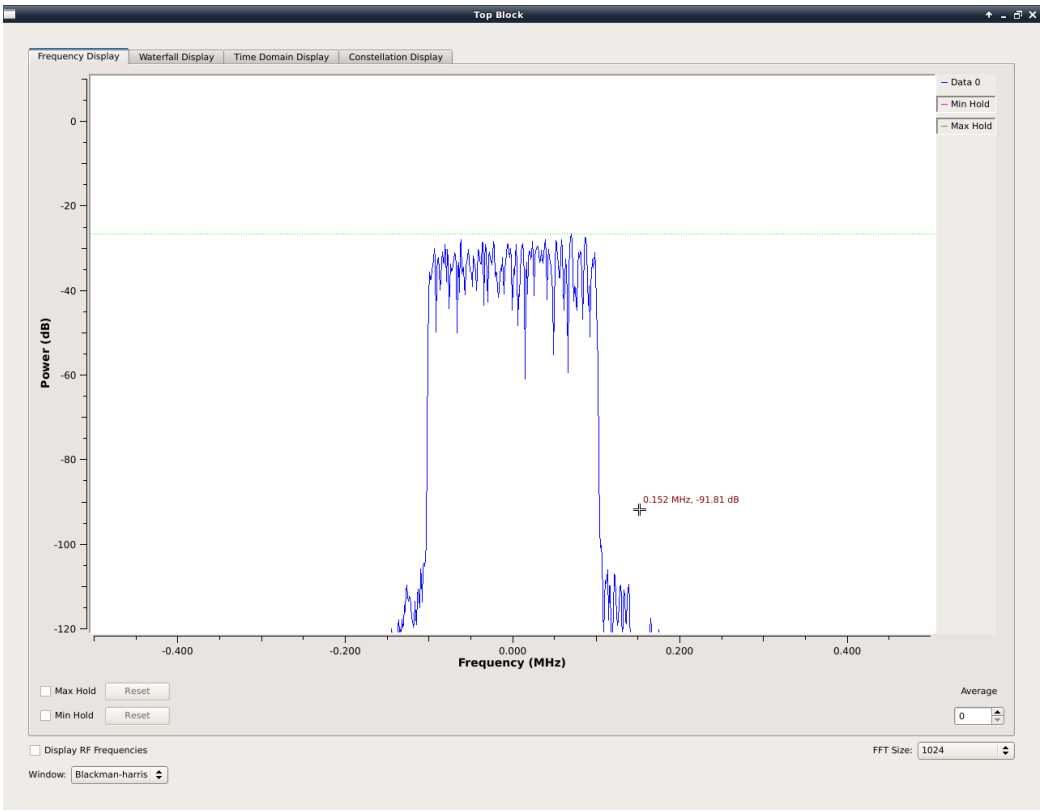

Figure 5: Jamming signal with 100kHz bandwidth observed on the *Attacking device*

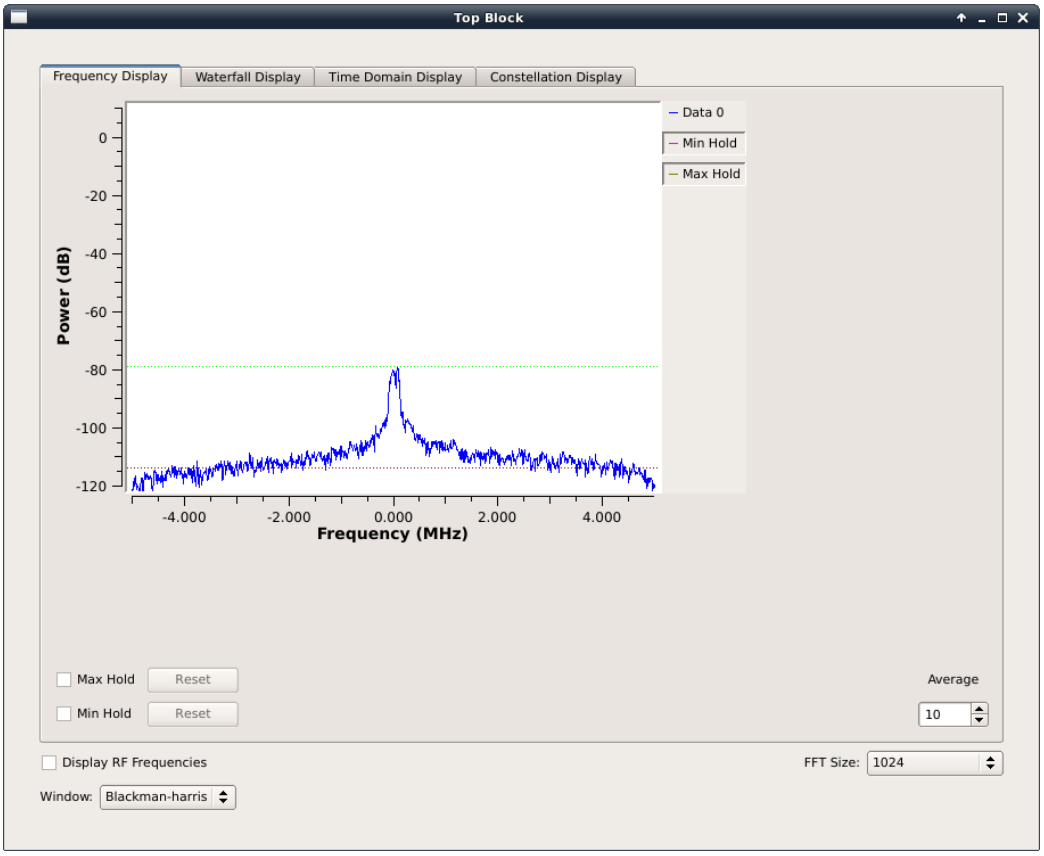

Figure 6: Ping and jamming signal with 100kHz bandwidth observed on the *Monitoring device*. The peak in the center is the jamming signal.

signal is only spread a little, resulting in a narrow bandwidth and thus being more prone to jamming. Using longer codes could solve this.

5.3 Jamming with infinite bandwidth

In third approach we removed the low-pass filter from the jammer.

Hypothesis 3 *Jamming on all frequencies will stop all ping transmissions, not only our group's, but the other groups' as well.*

This turned out to be partly true. Our transmission was in fact stopped, but not the other's. We assume this due to the distance to the other's receivers. Notice that the peak power of the jammer was still set to the same value and that the power of the signal should not have gotten spread over more frequencies, if the radio could have provided enough power. But apparently this was not the case and we assume that the devices maximum power got spread over a large frequency range. See Figure 7.

6 Analysis

After completing the lab exercise about Jamming Resistant Communication, we can summarize the following statements:

- Without jamming we could observe a pattern similar to a `sinc` function in the frequency domain.
- We observed that a jamming signal of narrow bandwidth is able to interrupt a DSSS modulated communication if short chip-codes are used.
- The Jamming attack can be sometimes ineffective and this is due to its narrow bandwidth, its weak transmission power, or its long distance from its target.

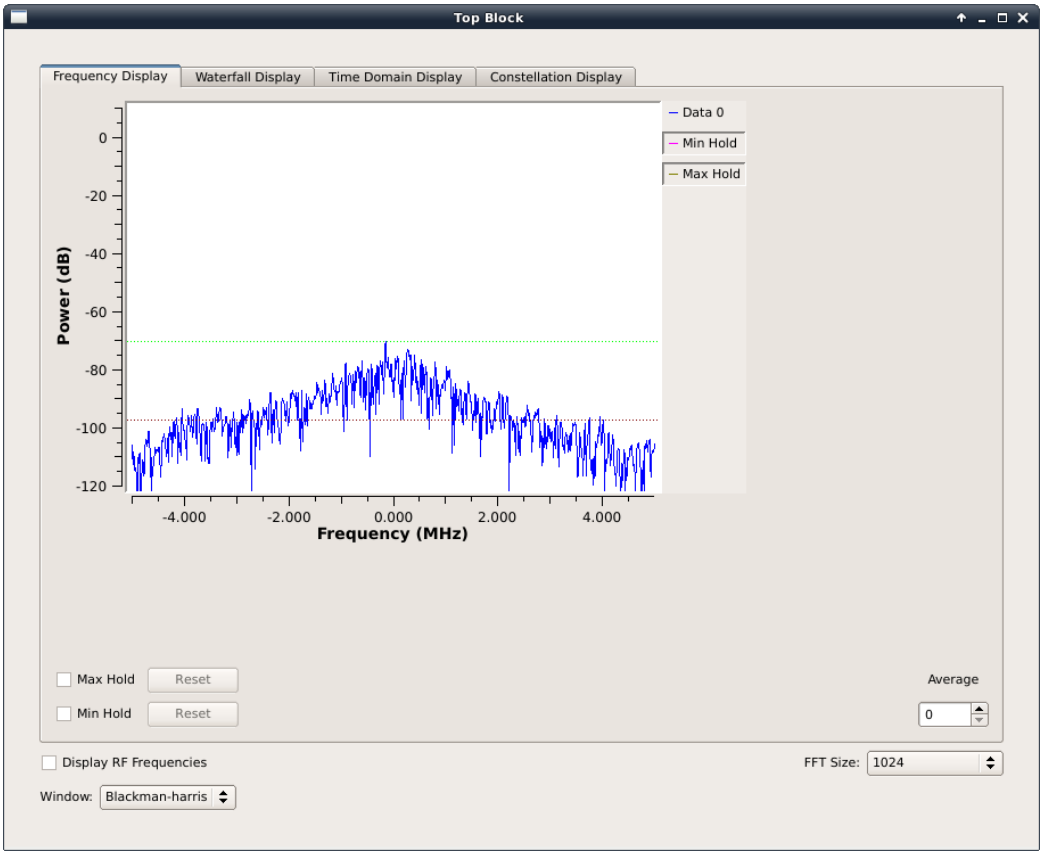

Figure 7: Jamming and ping signal when no filter is applied to the jamming signal.