Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms

Renato Ferreira[1] · João Gaspar[1] · Pedro Sebastião[1] · Nuno Souto[1]

Abstract

Lately, a rising number of incidents between unmanned aerial vehicles (UAVs) and airplanes have been reported in airports and airfields. In order to help cope with the problem of unauthorized UAV operations, in this paper we evaluate the use of low cost SDR platforms (software defined radio) for the implementation of a jammer able to generate an effective interfering signal aimed at the GPS navigation system. Using a programmable BladeRF x40 platform from Nuand and the GNU Radio software development toolkit, several interference techniques were studied and evaluated, considering the spectral efficiency, energy efficiency and complexity. It was shown that the tested approaches are capable of stopping the reliable reception of the radionavigation signal in real-life scenarios, neutralizing the capacity for autonomous operation of the vehicle.

Keywords GPS · Jamming · Radionavigation · SDR · Unmanned Aerial Vehicles

Renato Ferreira
renato_ferreira@iscte-iul.pt

João Gaspar
joao_filipe_gaspar@iscte-iul.pt

Pedro Sebastião
pedro.sebastiao@iscte-iul.pt

Nuno Souto
nuno.souto@iscte-iul.pt

[1] Dept. of Science and Information Technology ISCTE - University Institute of Lisbon, Portugal and Instituto de Telecomunicações, Portugal

1 Introduction

Although drone legislation exists, many pilots choose to irresponsibly fail to comply with it, generating various types of incidents and damaging the image and work of those who daily respect the rules and make the unmanned aerial vehicles (UAVs) their professional activity. Different approaches exist for dealing with the problem. For example, Dutch police trained some raptors such as eagles so that they are able to chase and hunt down UAVs whenever necessary [1]. However, there are great chances that these animals will get injured with the carbon propellers of the device, so the police are assessing the need to implement some additional protection. In Russia, a new non-destructive weapon was presented capable of solving the problem in question. Rex-1 was the solution presented as the emitter of a jammer signal to the GNSS signal. The Rex-1, in addition to blocking the connection between the device and its controller, sends signals to force the landing, also preventing the GSM (Global System for Mobile Communications) and Wi-Fi signal in the zone, so as not to allow reconnection [2]. However, the Rex 1 solution has little flexibility and does not interact with other technologies such as spoofing. To help mitigate this problem, in this paper we study effective ways to block the GPS signal [3] using low cost SDR platforms and thus prevent the autonomous flight of the Global Positioning System of the UAVs. The high degree of flexibility of SDR platforms, eases the integration of jamming functionalities with others, such as GPS signal spoofing, enabling the implementation of a low-cost neutralization system which can be effective against a wide range of UAVs [4].

Jamming makes use of intentional radio interferences to harm wireless communications by keeping communicating medium busy, causing a transmitter to back-off whenever it senses busy wireless medium, or corrupt the signal arriving at the receiver. Jamming mostly targets attacks at the physical layer but sometimes cross-layer attacks are possible too. Jammers are malicious wireless nodes that cause intentional interference in a wireless network. Depending upon the attack strategy, a jammer can either have the same or different capabilities from legitimate nodes in the network which they are attacking. The jamming effect of a jammer depends on its radio transmitter power, location and influence on the network or the targeted node. A jammer may jam a network in various ways to make the jamming as effective as possible. Basically, a jammer can be either elementary or advanced depending upon its functionality. For the elementary jammers, we can divide them into two subgroups: proactive and reactive. The advanced ones can also be classified into two sub-types: function-specific and smart-hybrid. A detailed classification of different jammers can be found in [5].

There are already a few studies regarding the generation of interference in GNSS signals using software defined radio (SDR) platforms, e.g., a system for detection and registration of GNSS jamming incidences. The system was developed on the basis of the SDR Ettus B200. The study presents also results of tests performed under real conditions [6].

The SDR chosen for all tests performed was the Bladerf x40 from Nuand[2], as it has all the specifications required for the implementation of the systems, with a cost of $420. BladeRF was designed for high performance and mobile applications. It is used by industry and academic researchers in telecommunications, RADAR, and Magnetic Resonance Imaging applications or by researchers looking for flexible, inexpensive hardware for wireless research.

The remainder of the paper is organized as follows: section 2 introduces satellite navigation systems. Section 3 describes different techniques to interfere with signals. Application of jamming techniques against the GPS signal is presented in section 4. Section 5 describes the experimental results followed by the conclusions in section 6.

[2] https://www.nuand.com/product/bladerf-x40/

2 Global Navigation Satellite Systems

Global Navigation Satellite Systems (GNSS) can provide accurate location and timing information which are required for various applications, such as in UAV autonomous operations. GPS is the most commonly used system in the vast majority of applications, especially in UAVs, although there are other systems of positioning.

Main systems that make up GNSS:

● GPS - Global Positioning System - USA, operational since 1995;
● GLONASS - GLObal'naya NAvigatsionnaya Sputnikovaya System - Russia, started in 1982 and completed in 1995;
● GALILEO - ESA EU operational in 2013.

● **Space component - GPS**
- 24 satellites (+5) of blocks II, IIA (Advanced) and IIR (Replacement) distributed over 6 orbits;
- approximately circular orbits with a radius of 26600 km, separated from each other by 60 ° in length;
- 12-hour orbital period (≈11h 58min 26s UTC), which causes the birth of the satellites to occur about 4 mins earlier each day;
- Orbital inclination near 55º, relative to the terrestrial equatorial plane.

● **Space component - Glonass**
- 24 Satellites (+3) distributed in 3 orbits;
- approximately circular orbits with a radius of 25510 km, separated from each other by 110 ° in length;
- Orbital period of 11:15 min sidereal, which causes the birth of the satellites to be given about 50 mins earlier each day;
- Orbital inclination close to 64.8º, relative to the terrestrial equatorial plane;
- Path repeats at the end of 8 sidereal days (the next satellite travels through the orbit of the previous satellite).

● **Space component - Galileu**
- 30 satellites distributed by 3 orbits;
- approximately circular orbits with a radius of 30000 km, separated from each other by 120 ° in length;
- Orbital period of 14h 21 min sidereal that causes the birth of the satellites to be given about 2h and 24 min later in each day;
- Orbital slope close to 56º, relative to the terrestrial equatorial plane [7].

GPS satellites transmit simultaneously several ranging codes and navigation data using binary phase-shift keying (BPSK). The GPS signals reach a GPS receiver from a series of satellites in terrestrial orbit allowing the positioning through trilateration. This is a method whereby the distances to three separate points, in this case satellites, are measured in order to calculate a location with an accuracy of only a few meters.
Each GPS satellite transmits two carrier waves: L1 and L2. They are generated from the fundamental frequency of 10.23 MHz, which is multiplied by 154 and 120, respectively. Thus, the frequencies (L) and the wavelengths (λ) of L1 and L2 are:

- L1 = 10,23MHz × 154 = 1575,42MHz and λ = 19 cm with a bandwidth of 15.345 MHz
- L2 = 10,23MHz × 120 = 1227,60MHz and λ = 24 cm with a bandwidth of 11 MHz

L1 is the target frequency for the proposed jammer as it is used by commercial UAVs. L1 is used for transmitting the Navigation Message, C/A and P Code. These codes are broadcasted to the receivers in the navigation message. In General, GPS satellites transmit three types of

information: almanac, ephemeris and timing information. The spectrum representation of the GPS signal is shown in Fig. 1.

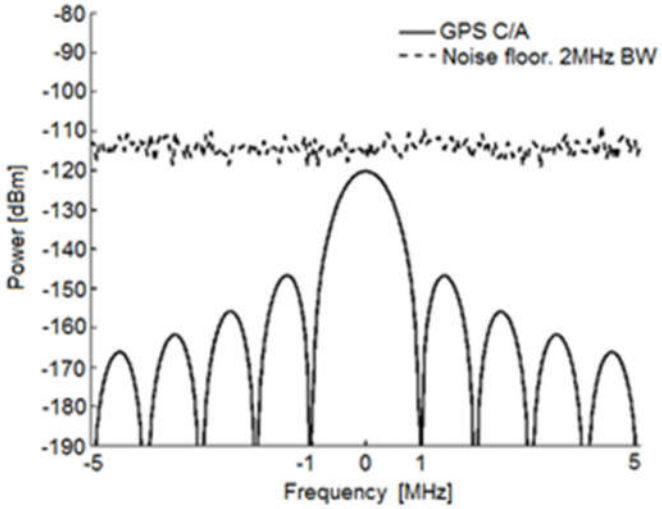

Fig. 1 Spectrum of GPS signal and thermal noise power [8]

GPS signals are very weak, about 50 W, having about the same power as the TV signals transmitted by geostationary satellites. GPS signals suffer interference when they pass through most structures. As the satellite antenna diffuses the RF signal evenly over the Earth's surface the transmitted energy is attenuated. This is mainly due to free space loss as the transmitted energy spreads spatially as it travels to the user (according to the surface of a sphere whose radius is increasing).
The minimum energy level received for users on Earth is -158.5 dBW for L / C code at L1 and -160 dBW for P code at L2 according to GPS specifications [9].

3 Radio Frequency Interference

A jammer is a device capable of interfering with the reception of signals, such as those used in GNSS systems, mobile communications systems, Wi-Fi, etc. Due to the shared nature of the wireless medium, a jammer can easily interfere with a communication channel used by RF technologies.
In order to create a jammer against GPS signals, we can apply techniques exploited in jamming for other technologies which can be categorized into five types [10]:

3.1 Barrage Jamming

It is the simplest form of interference and is generally defined as a jammer that transmits noise-like energy throughout the portion of the spectrum occupied by the target, as shown in Fig. 2 a) . It essentially increases the noise level in the receiver, making it difficult to operate the communication system.

3.2 Tone Jamming

In this technique, only a sinusoid is transmitted on the same frequency as the carrier of the GPS signal. This means that the interference is created only at the central frequency and not over the whole bandwidth. Using this technique all energy is applied at the center frequency of the carrier. The spectrum is exemplified in Fig. 2 b) .

3.3 Sweep Jamming

It is a technique that tries to replicate a behavior very similar to Barrage Jamming because it operates over the whole frequency band. The difference between these two techniques is that Sweep Jamming does not emit a static signal or a bandwidth of 15.345MHz. This technique is more efficient with respect to power spectral density since it emits a low bandwidth signal and sweeps the frequency in order to traverse the entire bandwidth of the signal to be interfered with, as shown in Fig. 2 c) . It emits a signal known as Chirp Signal [11].

3.4 Successive Pulses Jamming

This approach consists in the generation of a sequence of pulses in time with low duty cycle. By using this technique, the jamming of the carrier wave frequency can be accomplished due to the resulting spectrum of the interfering signal, which is shown in Fig. 2 d) . The signal occupies the desired band with peaks located at multiples of the frequency of the corresponding pulse sequence.

3.5 Protocol-Aware Jamming

The last interference technique presented is protocol-aware congestion. The feasibility of using protocol-aware jammers has been studied in IEEE 802.11-based wireless LAN communication systems. It was concluded that these can reach interference with very low energy requirements and low probability of protocol detection [12, 13]. Protocol-aware jammers also prevent interference with other communication systems operating on the same RF band. In this type of approach it is a common practice to use a jammer with an architecture similar to that used by the emitter of the target signal. In this way, the interfering signal mixes with the target signal using a similar spectrum in order to destroy the information thereof or otherwise make its reception virtually impossible at the receiver.
During the construction of the interference signal, the signal modulation (BPSK), the data rate (sample rate = 1.023MHz) and the channel bandwidth (15.345MHz) are considered. The resulting spectrum is illustrated in Fig. 2 e) . This technique is the one that results in a spectrum closer to the spectrum of real GPS signals.

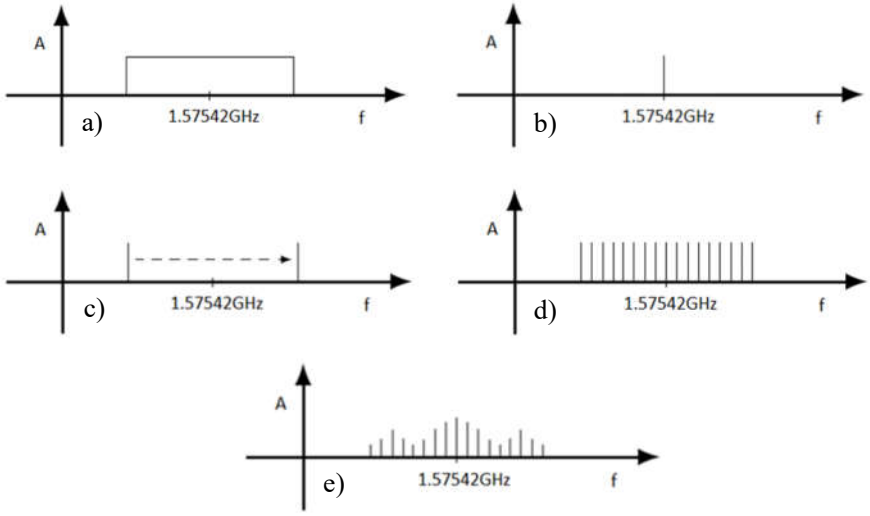

Fig. 2 a) Theoretical spectrum of Barrage Jamming; b) Theoretical spectrum of Tone Jamming; c) Theoretical spectrum of Sweep Jamming; d) Theoretical spectrum of Successive Pulses Jamming; e) Theoretical spectrum of Protocol-Aware Jamming

4 Application of Jamming Techniques in the GPS Signal

In the following, we provide the details of the implementation of the five different jamming techniques aimed at the GPS signal.

4.1 Barrage Jamming

The Barrage Jamming, using theoretical information is the best jammer that can be done in the absence of any knowledge of the target signal [14]. Blocking wireless networks can be accomplished by generating continuous noise with a power above the maximum the system supports. The negative side of this approach is the high amount of energy required which contributes to a low energy efficiency. Furthermore, it is not possible to select which signals to be affected in the RF band used. When applying this technique for GPS signal blocking, this last restriction is not an obstacle since what is intended to affect is the entire GPS frequency band.
The construction of the signal to be transmitted was programmed using the GNU Radio toolkit, where Gaussian noise is generated through the Noise Source block (Fig. 3 a)) and transmitted over the entire bandwidth of the L1 band GPS signal with a center frequency of 1.57542 GHz and a bandwidth of 14 MHz (Fig. 3 b)).
To analyze the power spectral density of the various types of jammers, the receiving antenna is connected for a spectrum analysis on the GNU Radio using the *osmocom Source* block (Fig. 3 c)), connected to the *QT GUI Frequency Sink* (Fig. 3 d)). This setting is possible because BladeRF is a transceiver. This configuration was adopted for all the techniques presented.
The BladeRF has a Variable Gain Amplifier (VGA) in the transmit module, TxVGA1 for BB (Base Band) Gain and TxVGA2 for RF (Radio Frequency) Gain. Generally, TxVGA1 should be increased before TxVGA2. Sliders for these parameters were provided in the GUI via the *QT GUI Range block* (Fig. 3 e)).

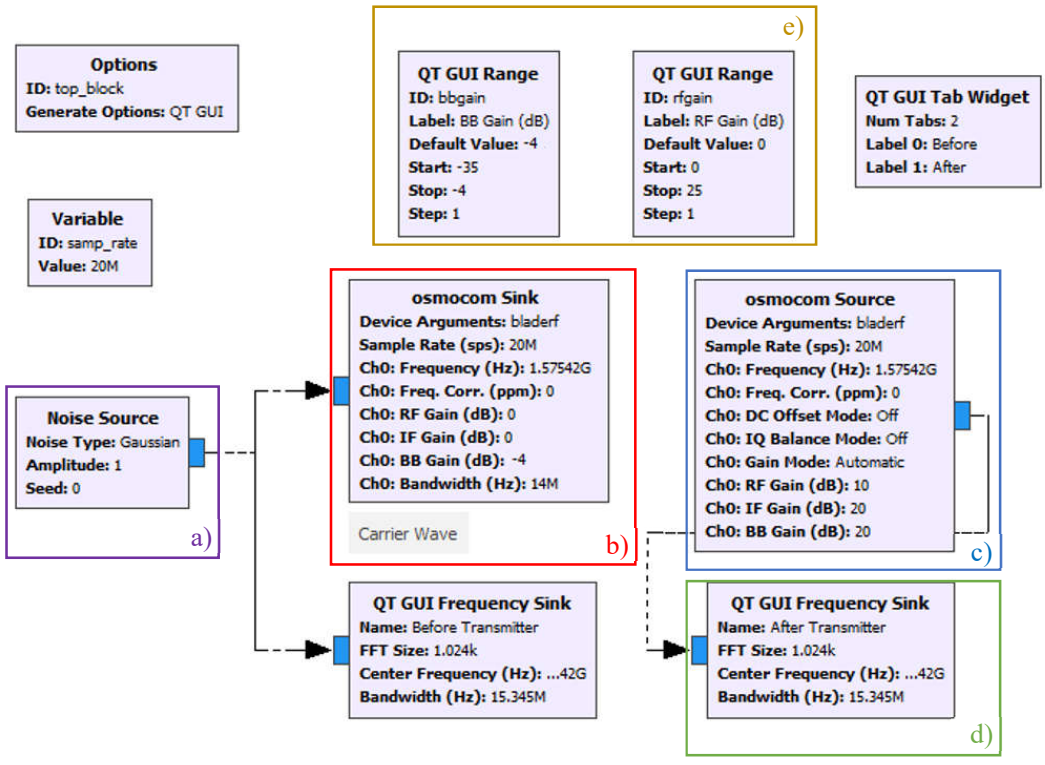

Fig. 3 Barrage Jamming programmed in GNU Radio

Using the *osmocom Source* block, the block responsible for the reception of the BladeRF, we can analyze the signal interconnecting this block to the *QT GUI Frequency Sink* to represent the transmitted signal spectrum (Fig. 4).

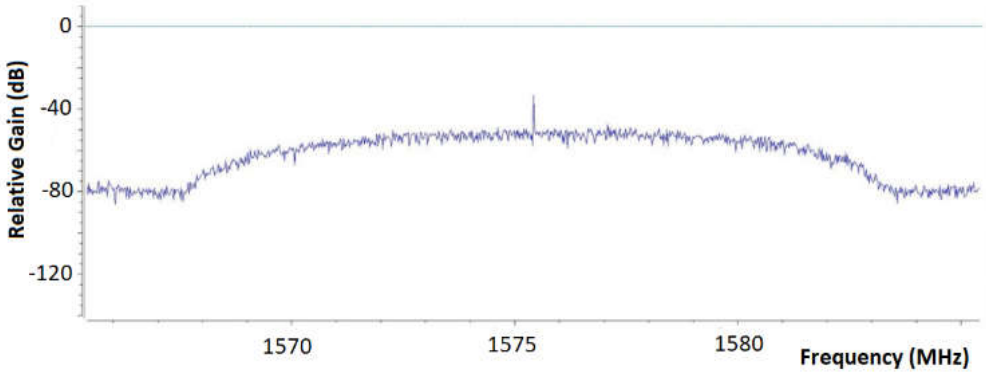

Fig. 4 Spectrum resulting from Barrage Jamming

The result in terms of spectrum of transmitted signal is the expected one according to theory, with the signal having a bandwidth of 14 MHz and an average power spectral density of -60 dBW / Hz. At the center frequency, there is a maximum peak due to the DC Offset problem. This problem lies in all the techniques presented below.

4.2 Tone Jamming

The Tone Jamming model was developed in GNU Radio, simply generating a sinusoid using *Signal Source* block with select cosine in waveform (Fig. 5 a)) which is transmitted in the central frequency of the GPS, 1.57542GHz (Fig. 5 b)).

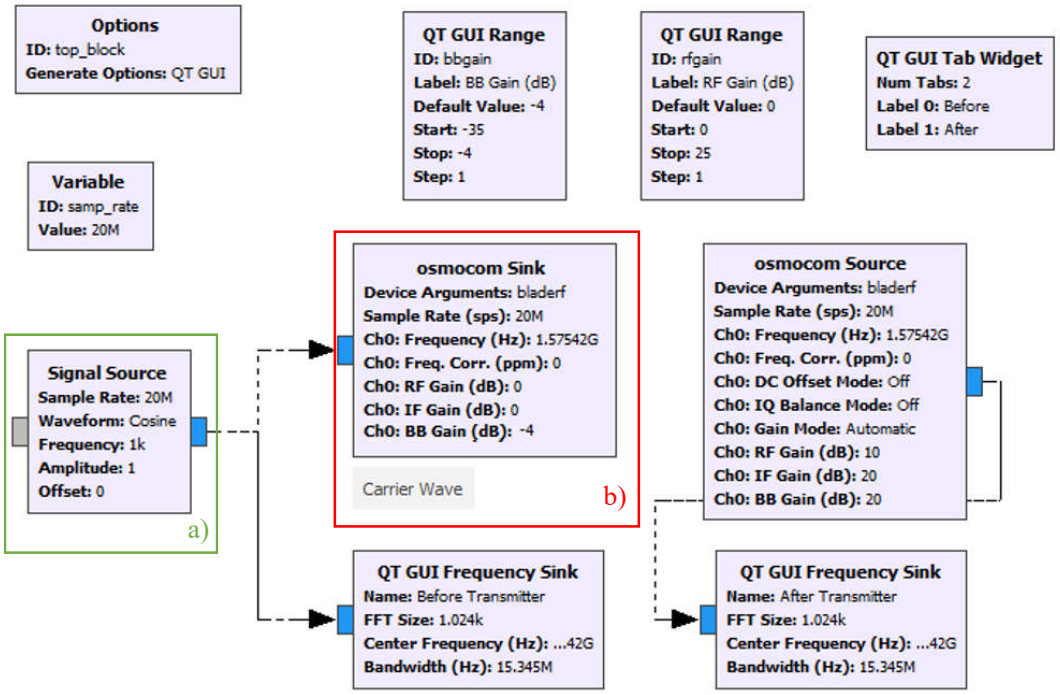

Fig. 5 Tone Jamming programmed in GNU Radio

The interference results are shown in Fig. 6. This jamming signal does not occupy the entire band of the GPS signal which is one of the possible disadvantages since the GPS signal is based on a spread spectrum approach which gives it some robustness against narrowband interference. The average power spectral density of the transmitted signal is -50 dBW/Hz.

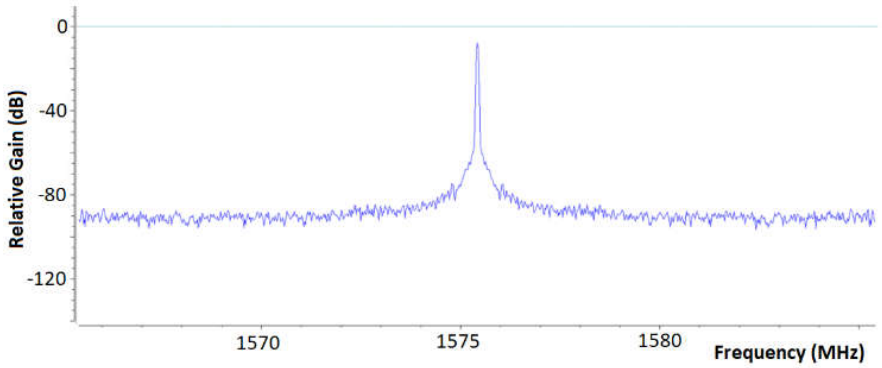

Fig. 6 Spectrum resulting from Successive Pulses Jamming

4.3 Sweep Jamming

For the Sweep Jamming technique, it is necessary to create a Chirp Signal, i.e., a signal that increases or decreases its frequency over time. The result at the spectrum level corresponds to the continuous sweep of a range of frequencies.
The base construction of the signal to be transmitted was accomplished on GNU Radio according to the flowgraph in Fig. 7. It is transmitted with the minimum bandwidth supported by the BladeRF, 1.5 MHz (Fig. 7 a)). Knowing that the bandwidth of the GPS signal is 15,345 MHz, the frequency varies between 1.5678 GHz and 1.5831 GHz, with 10 kHz jumps (Fig. 7 b)) calculated as in Eq. 1 and Eq. 2.

$$f_{min} = fc - \frac{LB}{2} = 1.57542 \times 10^9 - \frac{15.345 \times 10^6}{2} = 1.5678\ GHz \quad (1)$$

$$f_{máx} = fc + \frac{LB}{2} = 1.57542 \times 10^9 + \frac{15.345 \times 10^6}{2} = 1.5831\ GHz \quad (2)$$

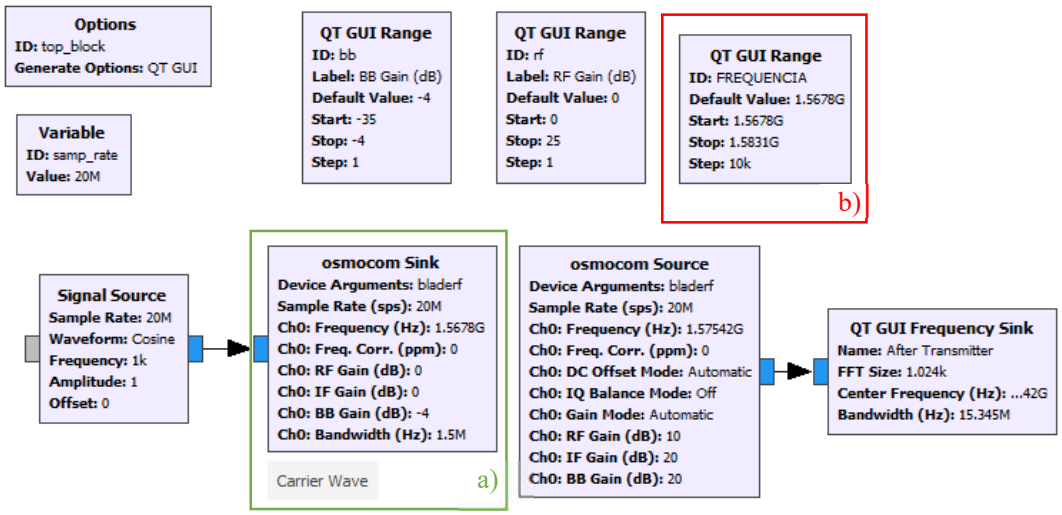

Fig. 7 Sweep Jamming programmed in GNU Radio

The result in the frequency spectrum at a certain moment is shown in Fig. 8.

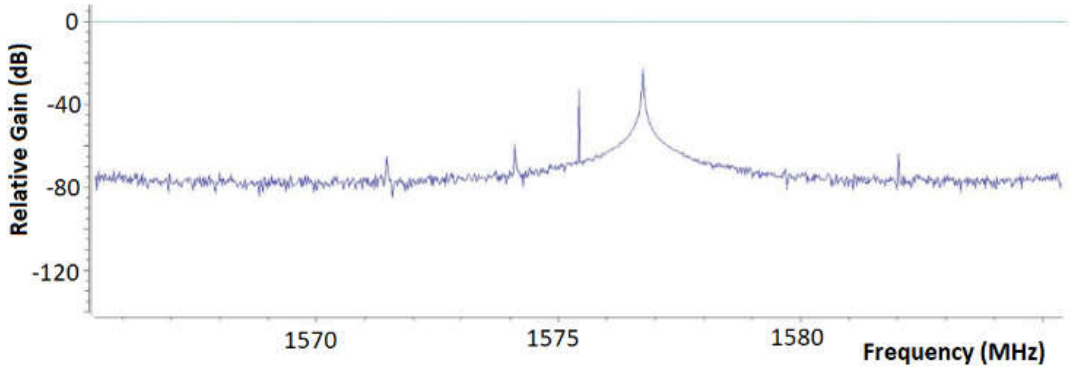

Fig. 8 Spectrum resulting from Sweep Jamming

Using this rapid sweeping approach it was observed that the transmitted signal has an average power spectral density of -50 dBW/Hz and an overall bandwidth of 15.3 MHz.

Using the waterfall spectrum from the Sharp SDR tool, Fig. 9, it can be observed that the BladeRF is constantly transmitting and there are no perceptible jumps in the frequency because of the fast sweeping applied. The analysis of this waterfall is at the carrier frequency, 1575.42 MHz. The waterfall plot shows the variation of the frequency spectrum over time. The received power signal is declared by the color. Using the scale in right side of Fig. 9 it is possible to analyze the power receive in different frequencies, being the color red the higher power and blue the lowest power.

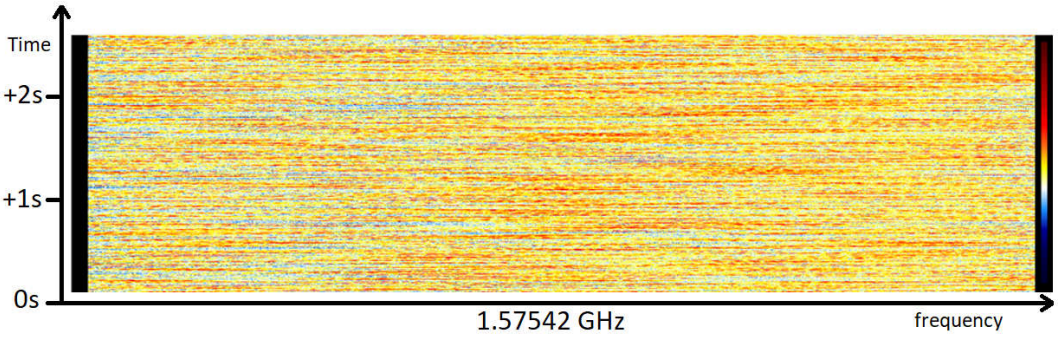

Fig. 9 Waterfall analysis of Sweep Jamming (screenshot obtained from the Sharp SDR software)

4.4 Successive Pulses Jamming

This technique consists of sending a sequence of pulses with low duty cycle, on the GPS signal frequency 1.57542 GHz, occupying all its bandwidth, 14 MHz. It was implemented using the flow graph of Fig. 10.

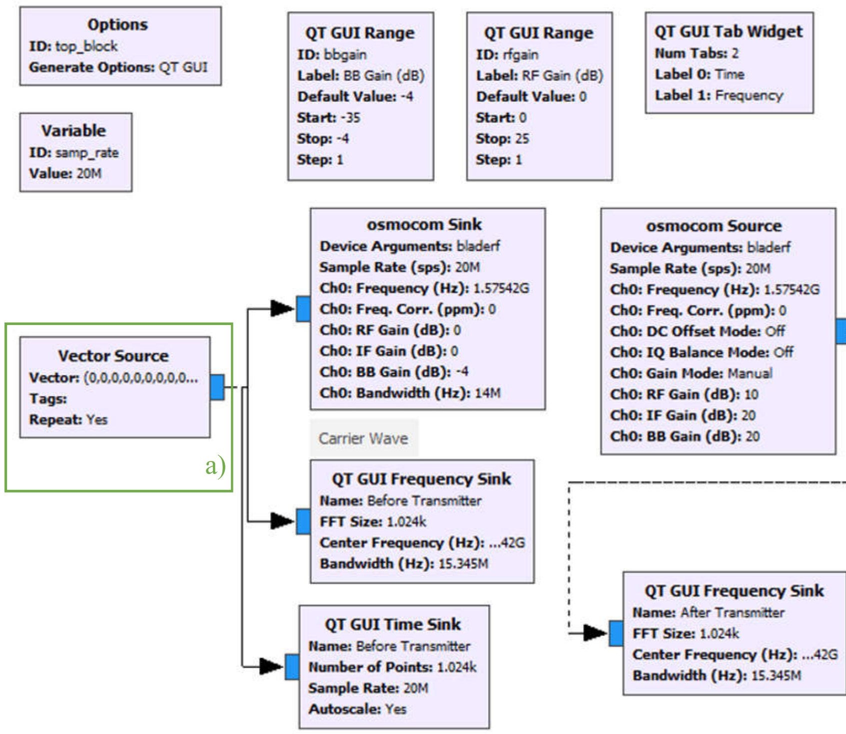

Fig. 10 Successive Pulses Jamming programmed in GNU Radio

In order to generate a low duty cycle signal in time, a vector with the following configuration is output: [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1], from the Vector Source block (Fig. 10 a)). It can be stated that the duty cycle of this signal is 2%, as we can see in Fig. 11.

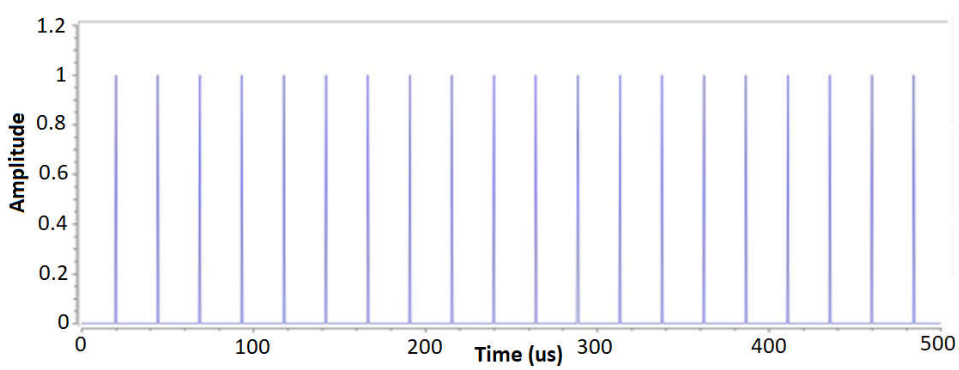

Fig. 11 Impulses in time with low duty cycle

The spectrum of the transmitted signal is shown in Fig. 12. Although the Successive Pulse Jamming technique takes up the full bandwidth of the GPS signal, it does not do it uniformly which may decrease its efficiency as a jammer. The average power spectral density of the transmitted signal is about -70 dBW/Hz, a little lower than the others.

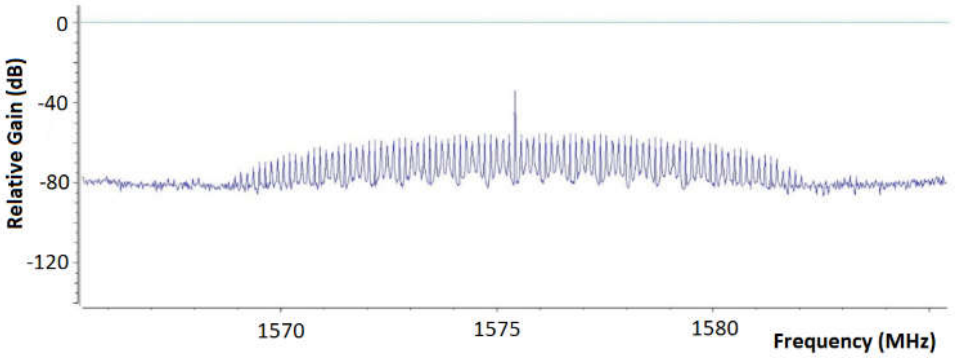

Fig. 12 Spectrum resulting from Successive Pulses Jamming

4.5 Protocol-Aware Jamming

The composition of the signal to be transmitted is represented in Fig. 13 beginning by creating a random source of bits which are converted to float by applying the block *UChart To Float* (Fig. 13 a)). In order to map the '0's and '1's to -1 and 1, respectively, there is a block that multiplies the sequence by 2 followed by an addition of -1 (Fig. 13 b)).
It is only possible to transmit the signal if it is converted to a sequence of complex valued samples (Fig. 13 c)), since the *osmocom Sink* block receives only complex values (this is the block responsible for interfacing with transmitter of the BladeRF board). The real part of the complex sequence carries the modulated signal (Fig. 13 b)) while the imaginary part is zero, the GPS signal L1 is not represented with a quadrature signal (Fig. 13 d)).

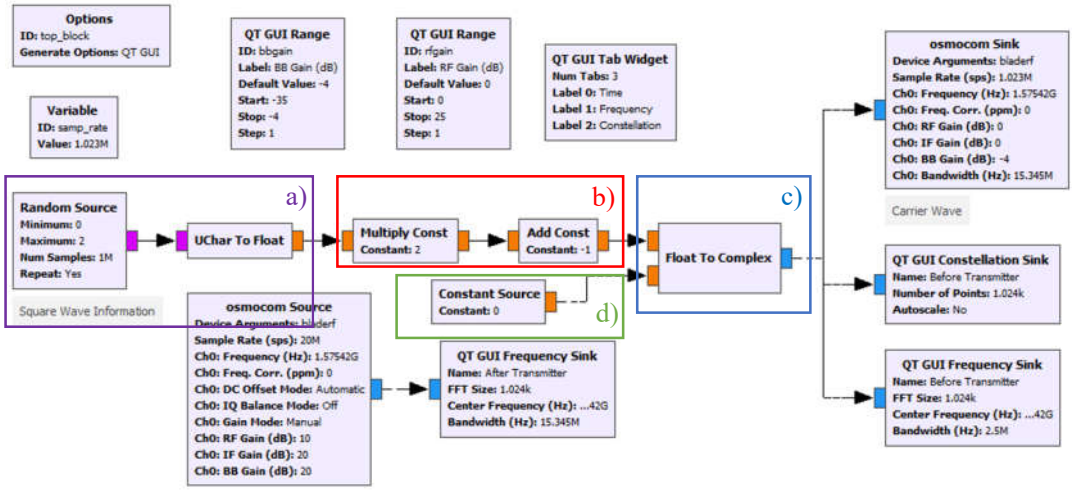

Fig. 13 Protocol-Aware Jamming programmed in GNU Radio

The result of the BPSK modulated wave at the receiver, i.e., the jammer signal received with AWGN (Additive White Gaussian Noise), is shown in Fig. 14.

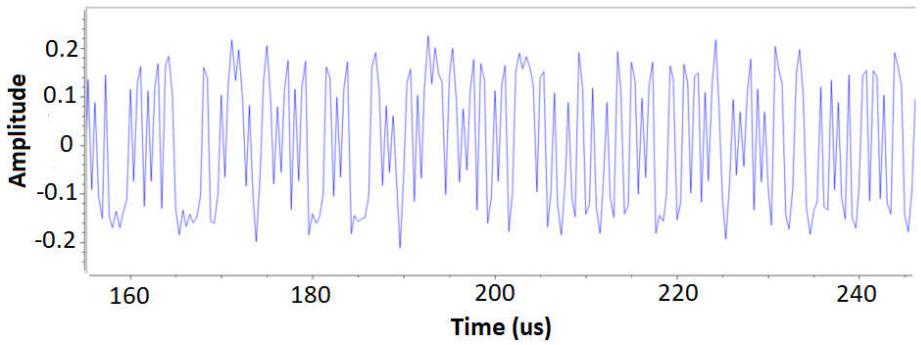

Fig. 14 Received Protocol-Aware Jamming signal in Time

The corresponding frequency spectrum is shown in Fig. 15. The average power spectral density of the transmitted signal is -60 dBW/Hz. It can be seen that it occupies the intended band with a shape similar to the GPS spectrum (i.e. stronger in the areas of the spectrum where the GPS signal is also stronger).

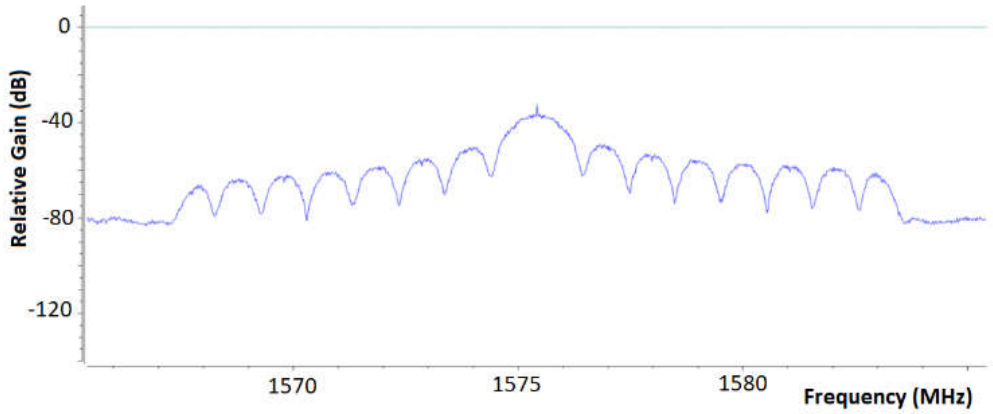

Fig. 15 Spectrum resulting from Protocol-Aware Jamming

Another solution for implementing this type of jammer is to transmit a copy of a real GPS signal. We tested this approach resorting to a GPS signal simulator and using a message with a nonexistent location. The simulator used is GPS-SDR-SIM[3] that generates GPS baseband signal data streams, which can be converted into RF using Software Defined Radio (SDR) platforms such as ADALM-Pluto, BladeRF, HackRF and USRP.

The message is created through a *.txt* file and is based on other messages created by the simulator and then adapted to the situation in question. Example of a *.txt* message line:

$GPGGA,122455.00,9845.59709719,N,18924.22292476,W,1,24,0.9,100,M,-21.3213,M,,*7C

The underlined digits are the coordinates of a point that does not exist on the planet Earth and so it is possible to shuffle the GPS receiver, translating into a GPS jammer signal.
The resulting spectrum is shown in Fig. 16, where it is visible that is resembles the one previously created (Fig. 15). The average power spectral density is slightly less than -60 dBW / Hz.

3 https://github.com/osqzss/gps-sdr-sim

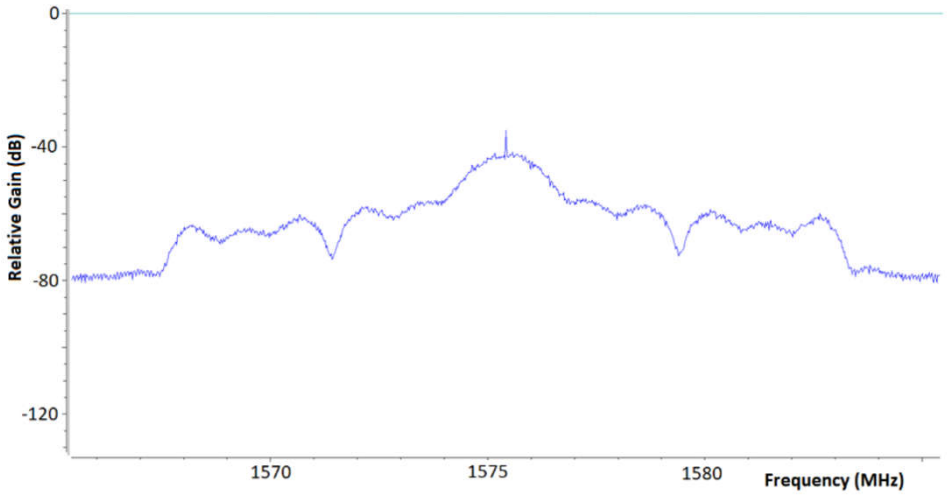

Fig. 16 Spectrum resulting from Protocol-Aware Jamming 2

5 Experimental Results

5.1 Controlled Environment Tests

In order to evaluate and compare the different GPS jammer signal generation techniques, several tests were performed using the previously discussed techniques, considering different distances between jammer and target receiver.
To analyze the power spectral density of the various types of jammers, the receiving antenna was connected to the BladeRF for a spectrum analysis on the GNU Radio. This setting is possible due to the full duplex support of the BladeRF. The distance between the receiving antenna and the transmitting antenna is almost zero (<10cm). Fig. 17 represents the hardware configuration adopted for implemented jammers.

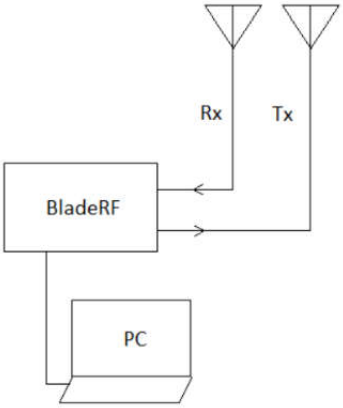

Fig. 17 Emitter block diagram (jammer)

Table 1 presents some power spectral density measurements obtained with the five techniques. The values selected for the gains TxVGA1 and TxVGA2 were -4 dBW and 25 dBW respectively. The power spectral density shown in table 1 is the maximum value.

Table 1 Spectral power density of different jammers

	Maximum Power Spectral Density	Average Power Spectral Density
Barrage Jamming	-28 dBW/Hz	-60 dBW/Hz
Sweep Jamming	-8 dBW/Hz	-50 dBW/Hz
Successive Pulses Jamming	-24 dBW/Hz	-70 dBW/Hz
Tone Jamming	2 dBW/Hz	-50 dBW/Hz
Protocol-Aware Jamming	-14 dBW/Hz	-60 dBW/Hz

The measured power output matches the expected ones, where the lowest values are those of Barrage Jamming and Successive Pulses Jamming, because they use all the GPS frequency range, 14 MHz. The fact that Successive Pulses Jamming achieves a slightly higher value than Barrage Jamming is because, even though it occupies 14 MHz, it does not do it evenly. Although Protocol-Aware Jamming also uses the 14 MHz of bandwidth it concentrates more energy in the center frequency than Barrage Jamming and Successive Pulses Jamming. For that reason it achieves higher peak on the power spectral density. Jamming Tone is the one that has a high-power density concentrated in a small area of the spectrum. Sweep Jamming in theory should get values equal to Tone Jamming, since they are the same, although Sweep Jamming sweeps the frequency. This does not happen due to the DC Offset error effect. To ensure that the conditions of the various tests are the same, it was decided to not use the actual GPS signals but to transmit a false GPS signal. This is to ensure that the intensity and reception quality is always the same, as throughout the day these two factors change using the actual GPS signals due to the orbital motion of the satellites. The GPS signals were generated.

A GPS transmitting ephemeris file specifies the constellation of GPS satellites to use. The ephemeris contains information regarding the position and the clock error of the satellites required in the positioning.

Fig. 18 shows the setup employed for the tests, where it is shown the adopted GPS receiver as well as a second BladeRF board used for the emission of the false GPS signal.

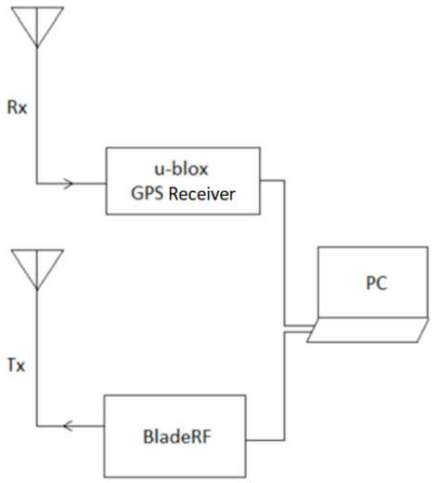

Fig. 18 Block diagram reference setup comprising a GPS receiver and false GPS transmitter (BladeRF)

The receiver used for the tests, shown in Fig. 18, is the ublox receiver shown in Fig. 19. The GPS receiver antenna is connected to the u-blox module and it is connected to the computer as shown at the top of Fig. 18. The distance between the receiving antenna and the transmitting antenna ranges from 5 to 25 meters with 5 meters' steps, as shown in Table 3.

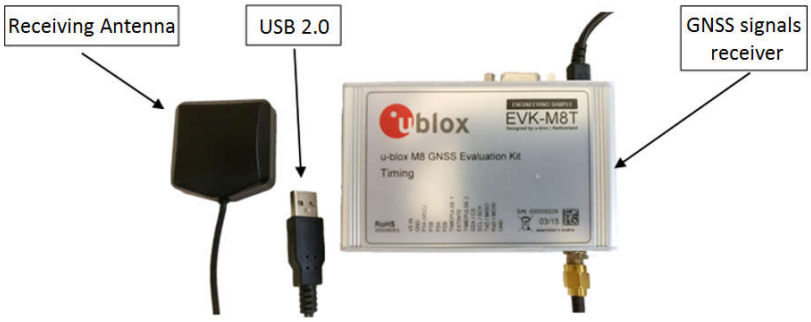

Fig. 19 Ublox receiver (EVK-M8T)

For the tests it was important to transmit the simulated GPS signal using a realistic power, considering the typical power received by an actual GPS signal. For this we used the following approach.

The process begins with the GNSS signal propagating through space until arrives at the user's GNSS receiving antenna. The power received is extremely poor, corresponding to a guaranteed signal power of -160 dBW in the case of the Global Positioning System (GPS). Considering a bandwidth of 2 MHz (the approximate null-to-null bandwidth of the GPS C/A code signal), the power of the received GPS signal is actually lower than the thermal noise power, as defined by Eq. 3 [8]. Furthermore, various terminologies used in this section are illustrated in Table 2.

$$P_{thermal\ noise} = k_B.T.\Delta f \ \ (W) \tag{3}$$

Table 2 Variables used in mathematical model

Terminology	Explanation
k_B	Boltzmann constant in joules per kelvin [J/K]
T	Absolute resistance temperature in kelvins [K]
Δf	Bandwidth in hertz over which noise is measured [Hz]
λ	Wavelength [m]
c	Speed of light [m/s]
f	Signal frequency [Hz]
d	Distance [m]

Applying the bandwidth of 2 MHz and assuming a temperature of 290 K results in

$$P_{thermal\ noise} = 1.38 \times 10^{-23} \times 290 \times 2 \times 10^{6} = 8 \times 10^{-15}\ W \tag{4}$$

which can be also expressed in dB as

$$P_{thermal\ noise} = 10\log\left(8 \times 10^{-15}\right) = -140.97 dBW \tag{5}$$

Knowing that the transmission powers of the GPS satellites lie between 20 W and 50 W, with a transmission antenna with a gain of 12 dB [15] and that the satellites are located 20200 km high (90 ° elevation), the maximum power received on the earth's surface is calculated using the free space path loss equation

(6)

$$L_{fs} = \frac{(4\pi)^2 d^2}{\lambda^2} = \frac{(4\pi)^2 d^2}{\left(\frac{c}{f}\right)^2}$$

Inserting all the specified values into Eq. 6 we obtain

$$L_{fs} = \frac{(4\pi)^2 \times (20\,200 \times 10^3)^2}{\left(\frac{3 \times 10^8}{1.57542 \times 10^9}\right)^2} = 1.78 \times 10^{18} \quad (7)$$

which can be written in dB as

$$L_{dB} = 10\log_{10}(L) = 10\log_{10}(1.78 \times 10^{18}) = 182.5\ dB \quad (8)$$

The maximum power emitted by the GPS satellite in dBW is

$$P_{TXmax}\,(dB) = 10\log_{10}(50) = 17\ dBW \quad (9)$$

Considering the power transmitted and taking into account the losses in free space previously calculated, one can easily compute the power received using

$$P_{Rx} = P_{Tx} + G_{Tx} - L_{fs} = 17 + 12 - 182.5 = -153.5\ dBW \quad (10)$$

The BladeRF with a gain $TxVGA1 = -4\ dB$ and $RxVGA1_{min} = 5\ dB$ [16] results in a false GPS signal with -122 dBW of power, measured with the BladeRF without any type of filtering. For the signal to have a power of -153.5 dBW adjustments are required.

Without the VGA1 emission and reception gains, -122 - (-4) - 5 = -123 dBW. The TxVGA1 gain adjustment can also be set to -35 dB, losing 31 dB compared to the previous case (-4-31 = -35 dB). Adding the loss of 31 dB applied through the gain adjustment TxVGA1, results in a received power of -122 -31 = -153 dBW. The GPS receiver and the false GPS transmitter must be located close to each other and with a TxVGA1 setting = -35 dB, so that the received signal power can be close to the received signal power in a real case.

In the first evaluation phase, maximum range tests were performed for each of the jammers studied in a controlled environment (Table 3).
Based on the results, a conclusion cannot yet be reached, although the best-performing jammers are Barrage Jamming, Sweep Jamming and Protocol-Aware Jamming, with a maximum range of 25 meters. Successive Pulses Jamming managed to interfere only up to 5 meters away with the receiver. The Tone Jamming achieved a maximum range of 20 meters.

Table 3 Maximum range of various jammers in a controlled environment

	5 meters	10 meters	15 meters	20 meters	25 meters
Barrage Jamming	✓	✓	✓	✓	✓
Sweep Jamming	✓	✓	✓	✓	✓
Successive Pulses Jamming	✓	×	×	×	×
Tone Jamming	✓	✓	✓	✓	×
Protocol-Aware Jamming	✓	✓	✓	✓	✓

Note: ✓ → GPS receiver without location × → GPS receiver with location

The five techniques presented have advantages and disadvantages which are presented next, before the experimental tests in a realistic environment.
Barrage Jamming has as its main advantage the capability to jam the entire GPS signal band. The major problem is the power resource, since the power distributes evenly inside the bandwidth of 15,345 MHz which can result in a low power spectral density at every frequency.
The Tone Jamming only emits a sinusoid at the center frequency, concentrating all the energy on the carrier frequency of the GPS signals but in practice this is not the case because the LimeMicro LMS6002D chip, which is responsible for the BladeRF emission, has a minimum emission bandwidth of 1.5 MHz, bandwidth than the jammer. The great advantage is to concentrate all your energy on the carrier frequency of the GPS signals.
It will be expected that the technique is not one of the most effective but has the advantage of simplicity in terms of signal generation.
The great advantage of Sweep Jamming is the ability to apply a power spectral density which, can momentarily become much higher than Barrage Jamming on a specific frequency, using a signal with a lower bandwidth. As the bandwidth of the signal is smaller, the signal power does not disperse and is more concentrated around the central frequency of the signal which can be changed over time. This technique uses a frequency sweep so that it is possible to cover the entire bandwidth of the GPS signal. The disadvantage is the need for the hardware to support frequency sweeping fast enough for this technique to succeed.
Successive Pulses Jamming can also obtain higher power spectral density values than the Barrage Jamming, because although it occupies the entire bandwidth of the GPS signal, it does not do so uniformly. The fact that jamming spacing between frequencies exists throughout the entire band of the GPS signal is a disadvantage since the receiver may be able to recover the GPS signal.
Finally, Protocol-Aware Jamming (BPSK random signal created using GNU Radio or using GPS-SDR-SIM is the same results) has a very similar behavior to Barrage Jamming, although this does not consist of noise emitting itself, but random bits modulated in BPSK. Setting the identical sample rate to GPS, makes the Protocol-Aware Jamming spectrum very similar to that of GPS.

5.2 Real Environment Tests

The aim of the second phase of the tests was to evaluate the performance of the jamming techniques with real GPS signals.
The Barrage Jamming is used as the reference technique against which the other jammers are compared. The tests consist of first evaluating the maximum distance at which the Barrage Jamming can interfere in the real environment. The maximum range obtained for the Barrage Jamming was 18 meters. This distance was defined as the reference range so that if we could place the receiver farther from the jammer, as shown in Fig. 20, we could then conclude that specific jammers had a higher range than Barrage Jamming. For these tests, the BladeRF was powered by USB 3.0, with gains of TxVGA1 = -4 dB and TxVGA2 = 25 dB.

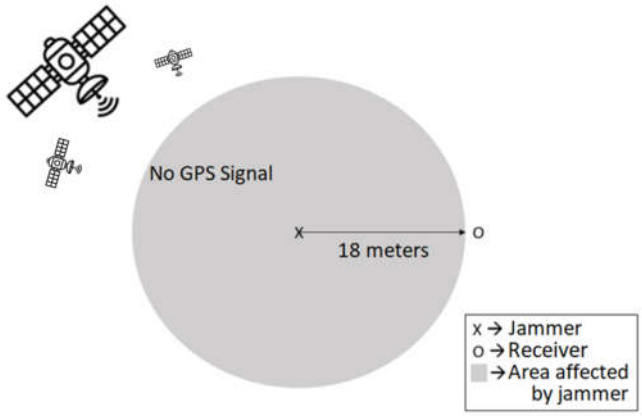

Fig. 20 Test in real environment

The Successive Pulses Jamming as expected failed to interfere with the receiver. The fact that there is not a complete coverage of all frequencies throughout the bandwidth of the GPS signal makes this technique inefficient.

The Tone Jammer can interfere with the receiver by lowering all power levels of the satellites but still, it was not able to continuously maintain the inhibition of the localization functionality of the receiver. It is important to remind that this technique does not occupy uniformly all the bandwidth of the GPS.

Sweep Jamming and Protocol-Aware Jamming (BPSK random signal created using GNU Radio or using GPS-SDR-SIM achieved the same results) were able to block the GPS signals at the receiver and were shown to be more efficient techniques compared to Barrage Jamming.

On the basis of these results, these two techniques merit a more detailed analysis. Both can cause the receiver to fail to determine the location, although the analysis of signal strengths of the GPS satellites in the receiver are different, as can be seen in Fig. 21 and Fig. 22.

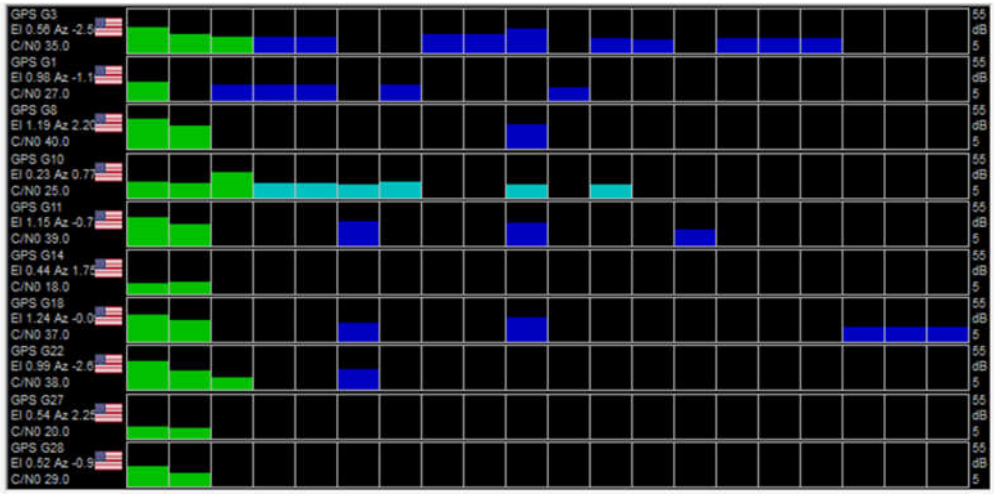

Fig. 21 Power of GPS satellite signals with Sweep Jamming (screenshot obtained from the U-Center software)

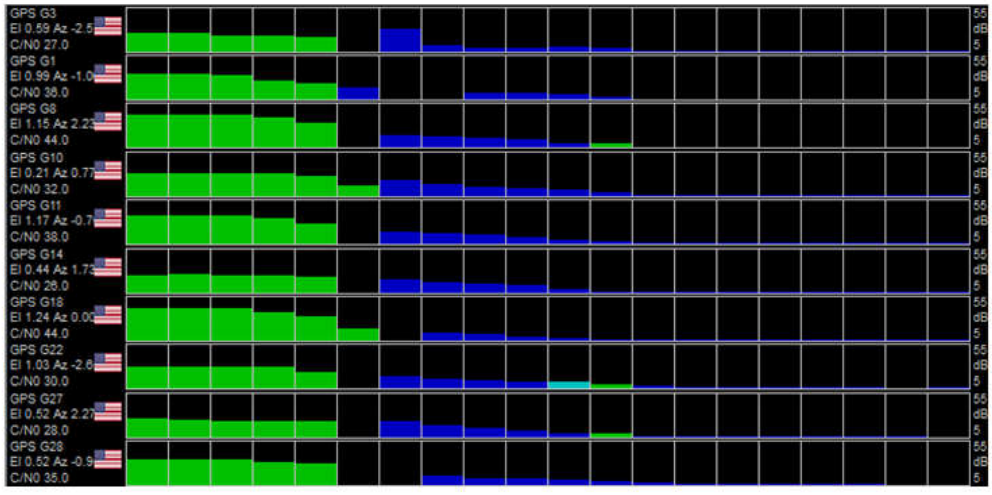

Fig. 22 Power of GPS satellite signals with Protocol-Aware Jamming (screenshot obtained from the U-Center software)

The graphs presented in both figures relate the received power level (vertical axis) and the time instants on the horizontal axis (each square corresponds to 1 second), with the oldest being represented on the left and the current on the right. The graphs of Fig. 21 and Fig. 22 were constructed using the u-center software tool. It is possible to observe that with Sweep Jamming the received power associated to each satellite never vanishes completely, whereas in Protocol-Aware Jamming as soon as the jammer is activated, the powers of the satellites gradually diminish in the following instants of time until they completely disappear for all satellites. It was concluded that Protocol-Aware Jamming was the most viable jammer in terms of its scope compared to the rest. Sweep Jamming is also a simple and effective solution, but the equipment can limit the efficiency of the technique approached. If the hardware does not allow a frequency sweep that is sufficiently fast jamming effectivity cannot be guaranteed.
Once we found the best jammer, we used it to test over a drone in flight. The drones used for the real-life tests were the DJI Spark and Parrot Bebop 2 FPV. In both cases similar behavior was observed. Selecting the auto flight mode and with the drone already in flight, whenever the jammer signal transmission was started, the drone's behavior automatically changed, stoping its flight path and gliding in the same place. It was observed that the time between starting jammer transmission and drone gliding is almost instantaneous. If the jammer is started before the drone takes off, the drone will not even perform any action. All tests were performed safely, away from air traffic and outside prohibited areas. Although it was not exploited in the paper, after the drone halts its operation due to jamming it could then be possible to emit spoofing signals so that the drone is deflected and indirectly controlled. Fig. 23 shows a prototype of an unauthorized drone protection system, which includes the proposed jamming solution.

Fig. 23 Unauthorized drone protection system

6 Conclusions

This paper compares five possible techniques capable to interfere with GPS signals resulting in the possible loss of localization and navigation capabilities of a UAV.
The different techniques were implemented and evaluated using low-cost SDR platforms and the GNU Radio software development toolkit. Several tests were performed in order to evaluate the effectivity in accomplishing the jamming of GPS signals.
The best-performing jammer was Protocol-Aware Jamming (Fig. 22) which uses an architecture similar to that used by a transmitter of GPS signals. Using this approach, the interfering signal mixes more effectively with the main signal since they exhibit identical spectral behavior, making its reception virtually impossible to perform at the receiver with lower transmitter power required. We can conclude that it is possible to block an autonomous flight of a drone by jamming its GPS receiver.

7 Acknowledgments

This work was funded by FCT/MEC through national funds and co-funded by FEDER – PT2020 partnership agreement under the project UID/EEA/50008/2019.

References

1. Thuy Ong, “Dutch police will stop using drone-hunting eagles since they weren't doing what they're told”, Dec. 2017 [Online]. Available: https://www.theverge.com/2017/12/12/16767000/police-netherlands-eagles-rogue-drones. [Accessed: 11-Jan-2018].
2. Army Recognition, “New Russian Rex-1 anti-drone rifle system ready to be tested- weapons defence industry military technology UK” , October 2017 [Online]. Available: https://www.armyrecognition.com/ weapons_defence_industry_military_technology_uk/new_russian_rex-1_anti-drone_rifle_system_ready_to_be_tested.html [Accessed: 11-Jan-2018].
3. H. Hu, N. Wei, “A study of GPS jamming and anti-jamming” Published in: 2009 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS).
4. M. Kratky, V. Minarik, “The non-destructive methods of fight against UAVs” - Published in: 2017 International Conference on Military Technologies (ICMT).
5. K. Grover, A. Lim, Q. Yang, “Jamming and anti-jamming techniques in wireless networks: a survey” - International Journal of Ad Hoc and Ubiquitous Computing, 2014 Vol.17 No.4, pp.197 – 215.
6. K. Bożek, A. Perski, A. Wieczyński, M. Baczyńska-Wilkowska, “Detection of GNSS Jamming Incidence” - Part of the Advances in Intelligent Systems and Computing book series (AISC, volume 743), 2018.
7. Faculdade de ciências da universidade de lisboa - DEGGE- hidrografia, “GNSS and Earth Observation: recent results and challenges”,2013.
8. what-when-how - In Depth Tutorials and Information, “GNSS Antennas and Front Ends (GPS and Galileo Receiver) Part 1” [Online]. Available: http://what-when-how.com/a-software-defined-gps-and-galileo-receiver/gnss-antennas-and-front-ends-gps-and-galileo-receiver-part-1/. [Accessed: 14-July-2018].
9. P. Misra and P. Enge, Global Positioning System: Signals, Measurements and Performance. Lincoln, Massachusetts: Ganga-Jamuna Press, 2010.
10. K. Pärlin, “Jamming of Spread Spectrum Communications used in UAV Remote Control Systems”, Tallinn University of Technology, School of Information Technologies, Thomas Johann Seebeck Department of Electronics 2017.
11. S. Smith, “The Scientist and Engineer's Guide to Digital Signal Processing” Chapter 11: Fourier Transform Pairs/ Chirp Signals.
12. A. Hussain, N. Saqib, U. Qamar, M. Zia, H. Mahmood, “Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks”. Journal of communications and networks, 16(4):397–406, 2014.
13. David Thuente and Mithun Acharya. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In Proc. of MILCOM, volume 6, page 100, 2006.
14. Tamer Basar. The gaussian test channel with an intelligent jammer. IEEE Transactions on Information Theory, 29(1):152–157, January 1983.
15. Global Position System Low Noise Amplifier. GPS, LNA, Sensitivity, Jamming, Cohabitation, TTFF. NXP founded by Philips. Date of release: May 2009.
16. bladeRF Power Consumption - FX3 GPIF, FPGA, and RF Active - bladeRF x40 - https://github.com/Nuand/bladeRF/wiki/bladeRF-Power-Consumption. [Accessed: 12-Mar-2018].

Conflict of Interest: The authors declare that they have no conflict of interest.