https://doi.org/10.1590/jatm.v17.1393 ORIGINAL PAPER

Electronic Global Positioning System Jammer Using Software Defined Radios

Marcelo Bender Perotoni[1,*], Ricardo Gaspar[1], Alessandro Campos[1]

1.Universidade Federal do ABC – Centro de Engenharia, Modelagem e Ciências Sociais Aplicada – Santo André/SP – Brazil.

***Correspondence author:** marcelo.perotoni@ufabc.edu.br

ABSTRACT

This article describes the use of a commercial software-defined radio (SDR) to generate an intentional interfering signal for protection against drones. The system aims to counter unauthorized and offensive drone actions. The particular case of the geo-location system is analyzed, where the sensitivity limit to block its operation is measured in two different receivers: an external Stoton module and a Samsung mobile phone, serving as a drone surrogate. The USRP B-210 software-defined radio, controlled by GNU Radio, was employed to generate the jamming signal. The final experiments took place in an outdoor environment, with two different antennas and in two different sites. Results were compared with literature reports as well as a first-order approximation based on the free-space formula (Friis) free-space propagation formula (Friis). A radius of protection of approximately 29 meters was observed by using the radio with a simple omnidirectional monopole antenna, designed and constructed for this test.

Keywords: Electronic warfare; Global positioning system; Jammers; Software defined radio.

INTRODUCTION

Drones or unmanned aerial vehicles (UAVs) have found applications across various sectors, extending beyond entertainment to include logistics, autonomous goods delivery (Rejeb *et al.* 2023), military surveillance (Kaag and Kreps 2014), and agricultural practices (Kim *et al.* 2019). However, their deployment on the battlefield has transformed traditional combat methods, enabling long-range surveillance and participation in offensive operations, such as dropping explosives while being remotely controlled. Particularly during the Russian invasion of Ukraine, the role of drones has significantly altered the expectations of traditional security experts, as lightweight UAVs equipped with low-tech weapons systems have dramatically changed battlefield dynamics (Kunertova 2023). Their strategic use has effectively addressed gaps left by the absence of precision-guided munitions. On the battlefield, small UAVs can deliver ordnance and return to base or engage in kamikaze-like attacks where they are not expected to return. Their low cost and high-quality imaging capabilities make them a viable alternative to traditional artillery systems.

Given their small dimensions and the use of lightweight, non-metallic materials, drones backscatter low levels of electromagnetic energy, making them more difficult to detect by radar. Visual detection is also challenging due to their compact size and low-altitude flights. Consequently, mass-produced consumer-grade drones with dual-use capabilities on the battlefield pose a significant threat to high-cost, sophisticated weapons systems and established combat doctrines. In short, their use also enables new forms of asymmetric warfare. Furthermore, drones equipped with lethal explosives can target authorities or civilians in terrorist attacks, presenting a substantial risk due to their widespread availability and ease of use.

Two solutions exist for countering UAVs: hard kill and soft kill (Ding *et al.* 2024). The term "hard kill" refers to traditional anti-aircraft kinetic methods, such as lasers and missiles. While this approach is a mature and conventional defense strategy against

Received: Jan. 28, 2025 | **Accepted:** Jun. 06, 2025
Peer Review History: Single Blind Peer Review.
Section editor: Lifan Sun

manned aircraft, the small size, low radar cross sections (RCS), and low altitudes of UAVs can complicate or increase the costs associated with its implementation. In contrast, "soft kill" neutralizes the drone threat through electronic means, disrupting or rendering ineffective the communication or guidance links that drones rely on for operation.

A jammer is one example of the soft-kill weapons used against drones. It can be defined as a system that transmits an electromagnetic signal designed to block legitimate communications by overpowering them. Consequently, the jammer creates a virtual zone around itself where the communication systems that guide and control the drones become ineffective.

Saturating drone receivers at a certain distance requires relatively large field amplitudes to be transmitted by the jammer. This necessity implies that jammers must be supplied with large direct currents (DC) and are equipped with thermal radiators to dissipate heat generated during operation. Additionally, UAV communication channels are varied, typically utilizing the industrial, scientific, and medical (ISM) frequency range, as presented in Table 1. Since ISM devices operate without the need for licenses, they are restricted in their effective isotropic radiated power (EIRP). In the United States, the Federal Communications Commission (FCC) regulates this EIRP to -1.23 dBm, for the ranges of 902 to 928 MHz and 2,400 to 2,500 MHz. Operation above these limits is prohibited; however, off-the-shelf amplifiers can be readily employed to boost EIRP levels, therefore extending the range of the virtual protection zone. The use of directional antennas can also enhance this range, particularly for frequencies above the 2,400 MHz range, as high-gain antennas are typically moderate in size. Nonetheless, directional antennas are not practically applicable unless the drone's direction is known in advance, which is often not the case.

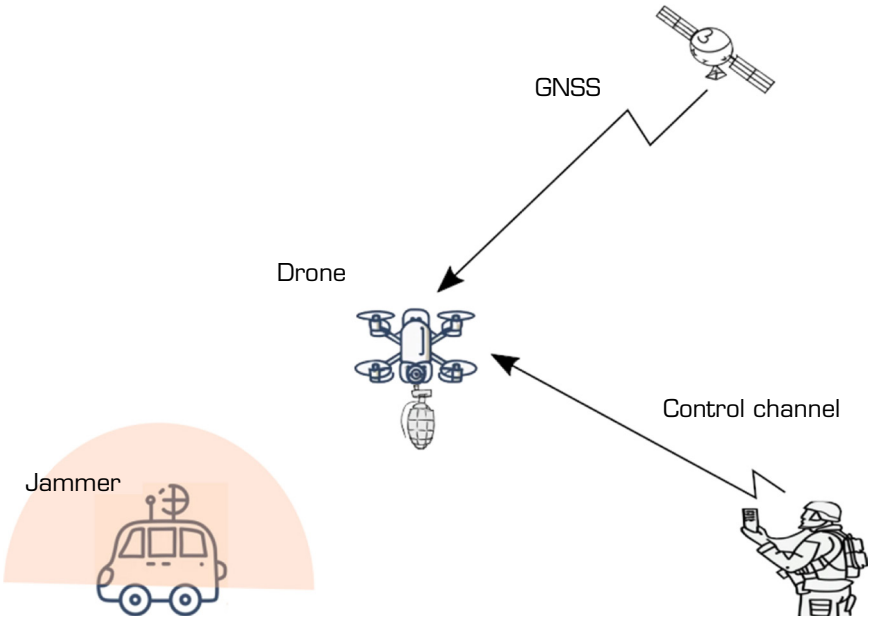
Table 1. Frequency ranges commonly found in drones' wireless channels.

Frequency range (MHz)	Usual application	Drone usage
433.05-434.79	Telemetry, which involves communication with devices at low data rates.	Drone telemetry, but not video transmission.
902-928	RF identification (RFID), internet of things (IoT)	Drone telemetry, but not video transmission; first-person view (FPV).
1,575	GPS	Localization of the drone using satellite networks.
2,400-2,500	Wireless network (Wi-Fi) and bluetooth	Drone link with video.
5,725-5,875	Wireless network (Wi-Fi)	Drone link with video.

Source: Elaborated by the authors.

Given their unlicensed nature, a large number of ISM devices and modules are mass-produced at low cost, particularly for the 2,400-2,500 MHz range. This frequency range provides reasonable video transmission quality while achieving moderate distances; however, it is susceptible to nearby interferences. In contrast, the next range, around 5,800 MHz, offers a less crowded spectrum, enabling higher data rates suitable for transmitting video signals. Figure 1 illustrates the operation of the jammer and its main components, demonstrating how it creates a protection zone around a vehicle. Drones are typically controlled at a distance using one of the ISM frequencies and can have their position determined with the assistance of the Global Navigation Satellite System (GNSS). Currently, lower-cost drones lack GNSS receivers because they do not fly far enough due to their limited battery life; they rely solely on ISM channels operating in 2,400 MHz and/or 5,800 MHz.

Typically, the control channel operates at moderate distances, depending on the ISM frequency and antenna gains (approximately 4 km), while satellites providing geo-location are situated about 20,000 km from the Earth's surface. The jammer creates a protection volume around itself, with dimensions and geometrical shape primarily determined by the transmitted power and antenna power pattern. Proximity to obstacles and terrain profile are also relevant; however, these factors are not easily controlled in real-world applications. Since the UAV's position is not known *a priori*, the coverage is ideally omnidirectional. That omnidirectional coverage is achieved in common off-the-shelf jammers using monopole antennas, which, in addition to their omnidirectional patterns, are simple, rugged, and capable of withstanding large power levels.



Source: Elaborated by the authors.

Figure 1. Scheme of the jammer operation. The jammer creates a protection volume around its radiant system.

In contrast to the control channel implemented with ISM frequency radios, the GNSS system has global coverage through a network of satellites. Currently, various GNSS systems are available for civilian use, and their respective receivers are mass-produced and low-cost, with the presence in nearly every mobile phone. Some of these GNSS systems are listed in Table 2.

Table 2. Frequency ranges commonly found in drones' wireless channels.

System	Country	Number of active satellites	Frequencies (MHz)		Start	Altitude (km)
GPS	United States	24	L1	1,575.42	1995	26,600
			L2	1,227.69		
			L3	1,381.05		
			L5	1,176.45		
Glonass	Russia	24	Same as GPS		1995	25,510
Galileo	European Union	30	E1	1,575.42	2013	30,000
			E5a	1,176.45		
			E5b	1,207.14		
			E6	1,278.75		
Beidou	China	27	B1	1,561.098	2000	21,150
			B2	1,207.14		
			B3	1,268.52		

Source: Adapted from Ferreira *et al.* (2020) and Saleem (2020).

The Global Positioning System (GPS) operates on two primary bands, L1 and L2, both of which are Binary Phase Shift Keying (BPSK) modulated. Civilian applications utilize only the L1 band, while military operations can access both bands (Jones 2011), providing military users with higher accuracy and added encryption to prevent unauthorized access. Additional bands include the Quadrature Phase Shift Keying (QPSK)-modulated L5, designed for safety-of-life applications, and L3, which is used for detecting nuclear explosions. The GPS channel employs right-hand-circular propagation (RHCP), benefiting from atmospheric

absorption. If linearly polarized waves were transmitted from the satellites, they would undergo polarization changes while traversing the atmosphere due to the natural magnetic field. This polarization change aids the receiver in better discriminating signals originating from the satellite and those from reflections; reflected signals change their polarization and are not absorbed by a properly designed RHCP antenna (Rao *et al*. 2013).

This article describes the use of software-defined radios (SDR) to perform jamming operations. The sensitivity for the jammer, defined as the radio frequency (RF) level that disrupts satellite reception for two GPS receivers – one independent module and one mobile phone – is evaluated. This threshold level enables a first-order estimate of the protection radius in relation to the output power of the jammer. Following this evaluation, two real-world experiments are conducted using an off-the-shelf SDR: one employing a directional antenna and the other utilizing an omnidirectional monopole antenna. The main contribution of this article is the description of a jammer operation using a commercial SDR, with all the versatility that the software part of the SDR provides in terms of jamming type and frequency, allied to the simple deployment. Another contribution point is the sensitivity measurement of two commercial GPS receivers, which can be taken as parameters for other similar studies. Finally, five different types of jamming are presented, implemented in GNU Radio, and one of them is tested in an experimental environment.

The article is organized as follows: the next section details the SDR, their characteristics and applications to intentional jamming systems, followed by another section detailing the software, with examples of jamming deployments using GNU Radio. The used methodology alongside analytical expressions used for estimating the jamming range and comparison to actual measurements is described next, followed by outdoor results.

Software-defined radios

Software-defined radios have found wide application across various fields due to their versatility in modifying parameters such as frequency, modulation, and bandwidth through software, eliminating the need for hardware modifications. Several commercially available SDR options exhibit different characteristics; some function solely as receivers, while others also serve as transmitters. Table 3 presents three different SDRs with transmitting capabilities that are well-suited to operate as core components in jammers and are frequently referenced in the literature to generate intentional interference.

Table 3. Characteristics of three different SDRs for use as jammers.

Name	Number of transmitter (TX) channels	Number of receiver (RX) channels	Maximum instantaneous bandwidth (MHz)	Number of analog-to-digital converter (ADC) bits	Frequency range (MHz)	Average price (USD)
HackRF One	1	1	20	8	10-6,000	350
USRP B210	2	2	56	12	70-6,000	1,300
Blade RF	1	1	122	12	300-3,800	450

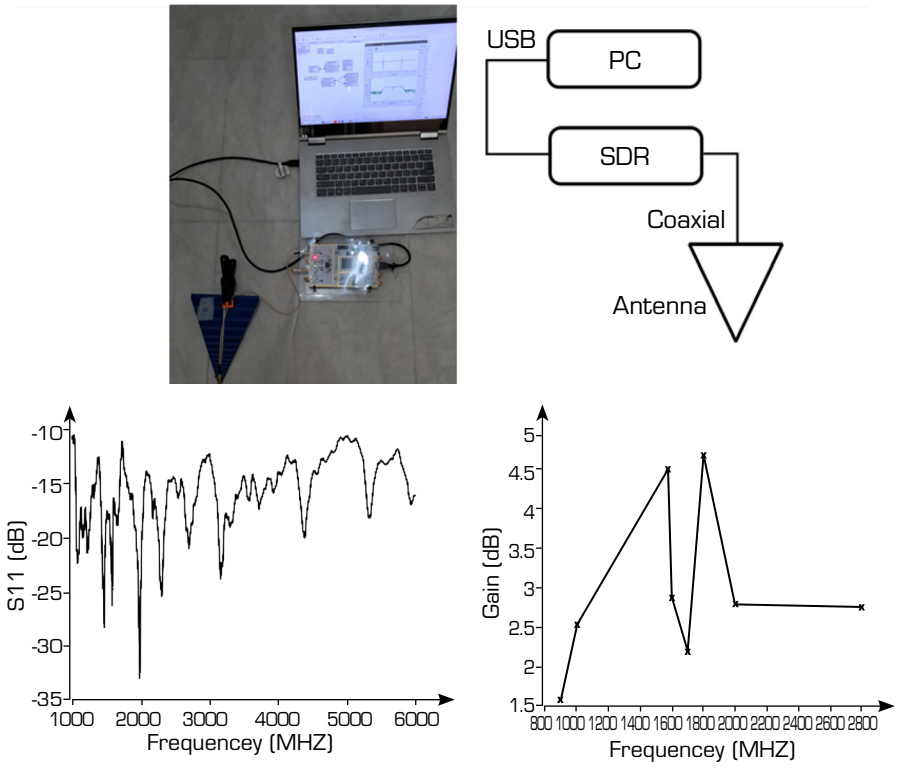
Source: Elaborated by the authors.

Their prices vary, as clone versions are also available that follow the same electrical schematics as the originals but utilize different boards and components. For instance, HackRF One has an open-source design, allowing it to be freely reproduced. In terms of RF ports, HackRF One features a single port, enabling operation as either a receiver or transmitter in half-duplex mode. In contrast, the USRP B210 supports 2 × 2 multiple-input multiple-output (MIMO) operation, which is advantageous when phase locking between different ports is necessary, as all ports are synchronized to the same oscillator. The Blade RF has two ports that can operate in full-duplex mode, with one port designated as a transmitter and the other as a receiver. The maximum instantaneous bandwidth parameter affects the effective width on the frequency domain that one intends to jam. For example, GPS requires 24 MHz of protected bandwidth, while Wi-Fi has a significantly larger bandwidth of 70 MHz for the 2,400 MHz and 500 MHz for the 5,800 MHz bands. Therefore, an SDR with a smaller bandwidth (also referred to as sample rate) may not be capable of jamming the entire channel simultaneously.

In the literature, a B210 unit was programmed using LabVIEW to generate a jammer that interfered with a digital signal, which was also received by the same SDR (Bhojan and Josh 2016). That operation requires phase locking among its different

ports, justifying the use of the B210. Using the Blade RF, the communication channels of two commercial drone manufacturers were successfully jammed after customizing the emitted energy to their proprietary Frequency Shift Keying (FSK) protocols, Futaba Advanced Spread Spectrum Technology (FASST) and Advanced Continuous Channel Shifting Technology (ACSST), both operating in the 2.4 GHz ISM band (Paerlin *et al*. 2018). Tailoring the jamming signal to a specific waveform allows for more effective jamming with less transmitted power than other methods (Ferreira *et al.* 2020). The same Blade RF was integrated into an anti-drone electromagnetic rifle, disrupting the 2,400-MHz communication link (Ferreira *et al*. 2022). The more affordable HackRF One was utilized to jam the GPS link of a commercial DJI Phantom 4 Pro drone, aided by a directional antenna and a power amplifier, both with unspecified gains (Rahman *et al*. 2021). Additionally, the HackRF One was employed to disrupt the 2,400 MHz 802.11 a/b/g Wi-Fi channel, with the impact of the intentional interference measured by the channel data speed (Sarbu and Neagoie 2020). Fang *et al*. (2018) also employed the HackRF One to spoof the GPS and communication link of unauthorized drones, employing power amplifiers and voltage-controlled oscillators (VCOs) to effectively block the GPS and ISM links. A Blade RF SDR integrated with power dividers operated as a 3-GHz cross-eye retrodirective array, automatically directing a jamming signal toward the source (Pieterse and du Plessis 2021). The capability to locate unauthorized flights and direct jammer energy to that point in space was also investigated using a Blade RF SDR, which identifies signal spikes in the electromagnetic spectrum and triangulates their position based on receivers placed at different positions. Tests were conducted in the frequency range between 746 MHz and 757 MHz, with low transmitter power of the SDR increased through power amplifiers and directional antennas (Alamleh and Estremera 2024). Spoofing of Beidou GNSS signals was carried out using a YunSDR-Y550 SDR (Ding *et al*. 2024), successfully tested against a real-world UAV (undisclosed brand) at a distance of 600 meters.

In the tests performed for this work, two HackRF One units were tested (named A and B), as well as a USRP B210, to measure their effective output power. A log-periodic antenna (LPDA) unit was employed to be the radiant system. Figure 2 shows the components used in the test as well as the block diagram, with the measured insertion loss and gain of the LPDA antenna.



Source: Elaborated by the authors.

Figure 2. Components of the experimental setup and the block diagram. At the bottom, the antenna return loss (S11) is shown on the left, and its broadside gain (in dB) on the right.

Table 4 presents the maximum output power measured with a spectrum analyzer at the GPS L1 frequency of 1,575 MHz. The HackRF One A is a more expensive model than the B unit, although both share the same circuit design. For the transmission block, the HackRF One offers the option to switch an RF amplifier on and off, providing a nominal gain of 14 dB, along with an additional baseband amplifier known as a variable gain amplifier (VGA). In contrast, the USRP allows for linear or decibel-based adjustment of the power output.

It can be seen that the USRP has a much larger output power than the lower-cost HackRF One, so it makes a big difference in terms of distance reach when jamming. Therefore, the real-world tests were carried out with the B210 as the active element.

Table 4. Maximum output power for two different SDR at the frequency 1,575 MHz.

Name	Maximum output power (dBm)	Settings
HackRF One unit A	-19.3	RF amplifier ON and VGA gain = 40 dB
HackRF One unit B	-20	
HackRF One unit A	-22	RF amplifier OFF and VGA gain = 40 dB
HackRF One unit B	-21.5	
USRP B210	14.4	Pot = 1 (linear)
USRP B210	0.66	Pot = 0.8 (linear)
USRP B210	-25.5	Pot = 0.5 (linear)

Source: Elaborated by the authors.

Software

SDR data can be manipulated, interfaced, and visualized with various applications, among which GNU Radio stands out as an open-source tool. GNU Radio Companion offers a block-oriented programming language that allows it to interface with SDR commands and controls, as well as perform visualization and signal processing functions. This software can run on different operating systems and generate a standalone Python code, in addition to being executed directly from the GNU Radio Companion interface.

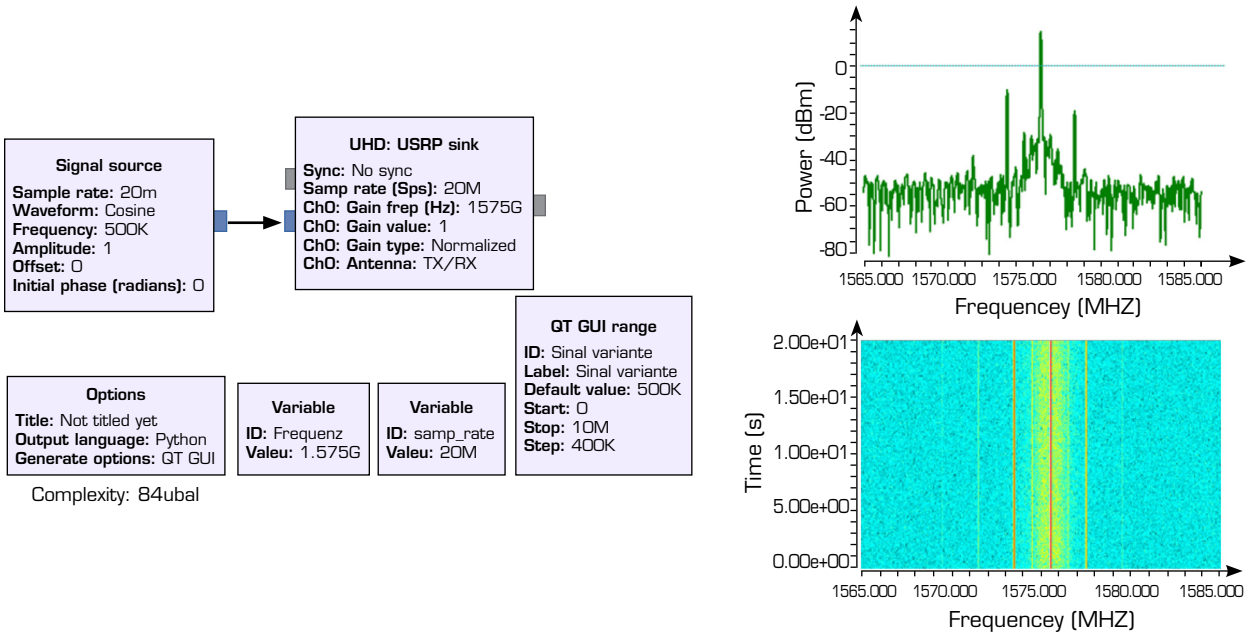
In terms of jamming schemes, five different methods are mentioned (Rahman *et al*. 2021):

- Tone: as the name implies, this method broadcasts a single frequency. It is efficient for blocking narrowband services, such as GPS.
- Barrage: this technique distributes jamming energy in a band-limited fashion across the frequency domain. While it is less effective because the total energy is spread across the entire band, it is necessary when the service to be interfered with employs frequency hopping or has a large bandwidth.
- Sweep: similar to the tone jamming, this method involves sweeping the tone across discrete positions within a defined bandwidth. It offers advantages over the barrage case, as the energy is concentrated on a single carrier rather than being distributed across the entire bandwidth.
- Pulse: This technique can transmit either barrage or tone jamming at specific intervals, depending on the system it aims to interfere with. It is energy-efficient but allows for a recovery time for the attacked system when no jamming energy is being transmitted.
- Protocol-aware: This method customizes the jamming waveform or frequency spectrum to match the target system. It offers improved efficiency and a lower probability of detection, although it comes at the cost of increased complexity (Ferreira *et al*. 2020).

More complex jamming formats, such as sweep and protocol-aware jamming, benefit significantly from the use of SDRs. In the case of sweep jamming, the software can be programmed to perform frequency hopping in a random manner, with specified dwell times for each frequency. For protocol-aware jamming, SDRs facilitate the deployment of complex digital modulation schemes through the built-in blocks available in GNU Radio, enhancing the efficiency and effectiveness of the jamming process.

Tone jamming

For tone-based jamming, Fig. 3 illustrates the GNU Radio Companion program that interfaces with the SDR. It is a very lean program, since its task is only exciting the SDR (operating at the GPS civilian L1 frequency, 1,575 MHz) with a tone in the kHz



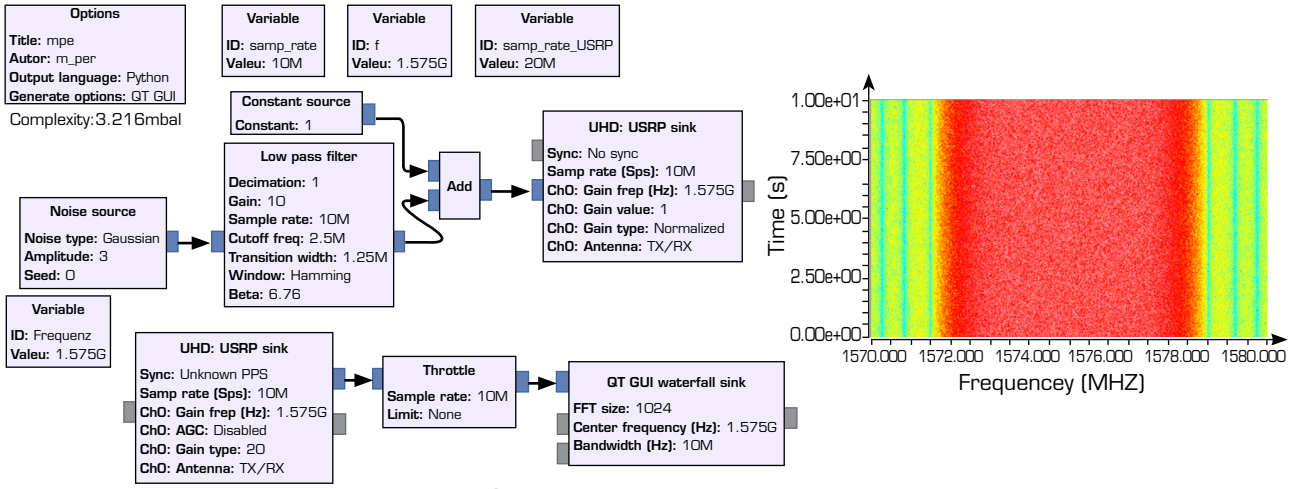
Source: Elaborated by the authors.

Figure 3. Gnu Radio Companion program to set the USRP B210 as a transmitter, operating in the tone-based jamming, along with the power spectrum and its waterfall plot.

range. The kHz signal could have been replaced by a constant value, since it is very close to the actual GPS frequency. The sample rate is set to 20 MHz, allowing for an effective transmitted bandwidth of 20 MHz centered around 1,575 MHz. The gain parameter in the USRP sink block is set to 1, enabling it to operate at its maximum nominal output power, as noted in Table 4. Other available ports on the SDR could be configured to monitor the transmitted power to verify whether transmission is occurring. However, utilizing additional RF ports affects the USB connection to the computer, risking sample loss during transmission. This condition triggers a warning in GNU Radio, indicating that the USB port has been overloaded. When jamming a large bandwidth service, such as Wi-Fi, that extra port usage might impact the overall performance.

Barrage jamming

Barrage jamming can be implemented as shown in Fig. 4, with a broadband noise source, whose time samples undergo later



Source: Elaborated by the authors.

Figure 4. GNU Radio Companion program using the USRP B210, operating in the barrage-based jamming, along with the waterfall plot.

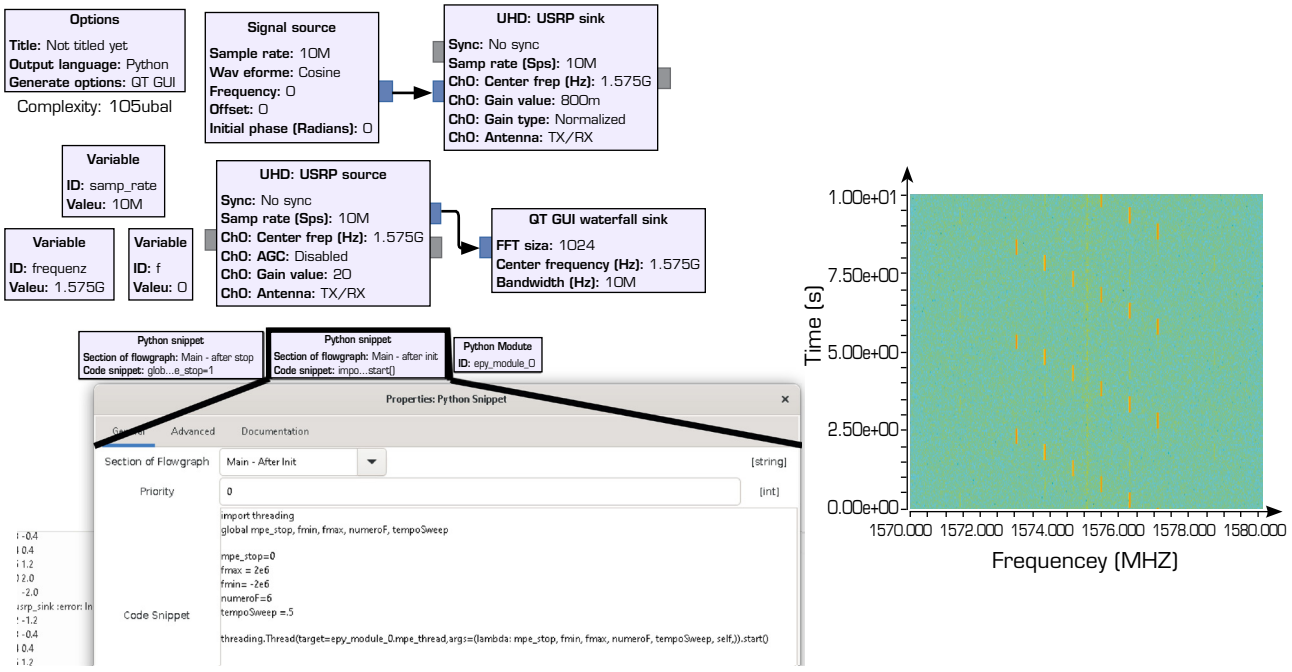
a low-pass filtering, which in turn formats the incoming energy into the desired frequency bandwidth. If $n(t)$ is the noise series in the time domain, the modulated RF fed into the antenna can be described as:

$$m(t) = Re\left[\{1 + n(t)\}e^{j2\pi f_c t}\right] \quad (1)$$

where $f_c(t)$ is the central frequency, in the program set by the frequency variable to 1,575 MHz.

Sweep jamming

An example of a program implementing the sweep type using the GNU Radio is shown in Fig. 5. A Python snippet block sweeps the central frequency variable *f* between *fmin* and *fmax*, in numeroF discrete steps (shown in detail in Fig. 5). Another variable, tempoSweep, sets the dwell time, i.e., the time the SDR actively transmits each tone.



Source: Elaborated by the authors.

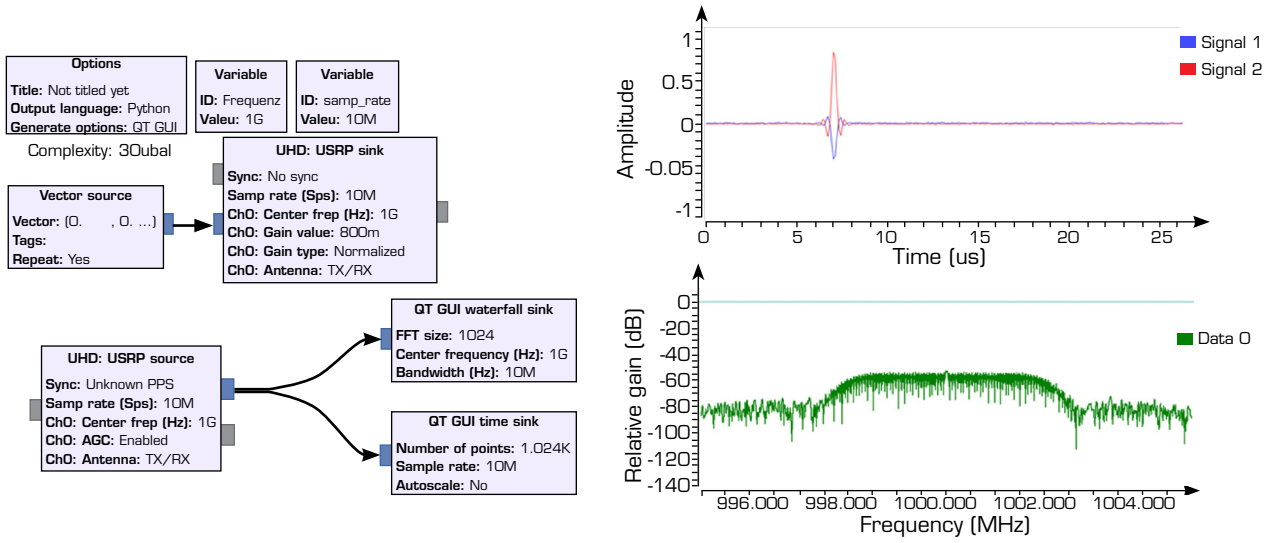
Figure 5. GNU Radio Companion program operating in the sweep-mode jamming, along the waterfall plot. In detail, the Python snippet sets the main sweep parameters.

Pulse jamming

In pulse jamming, the approach follows Merakeb *et al.* (2020), where a predetermined frequency response covering a bandwidth *B* is computed by forming a time-domain pulse whose expression can be written as:

$$m(t) = sinc(2\pi f_c t).h\left(\frac{Bt}{5}\right).\sin(2\pi f_c t) \quad (2)$$

where *B* is the desired pulse bandwidth and *h* represents a window function, in this case, Hanning. The GNU Radio program that implements this method is shown in Fig. 6. The complex pulse is synthesized with an external Python code and imported into GNU Radio as a vector block.

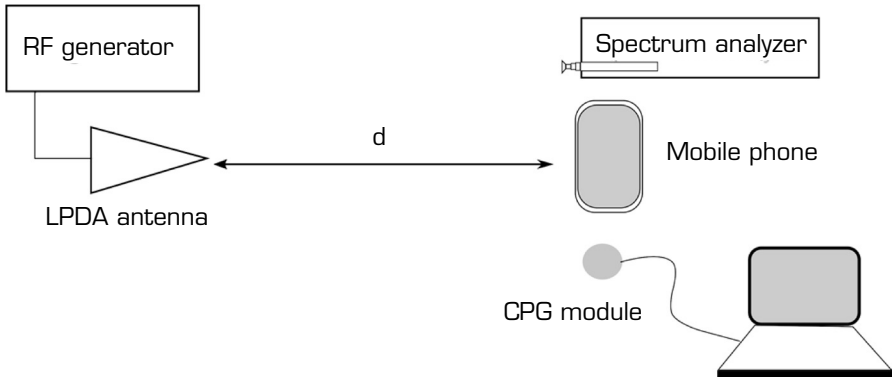


Source: Elaborated by the authors.

Figure 6. GNU Radio Companion program that implements the pulse mode, with the time-domain waveform and respective power spectrum.

METHODOLOGY

Unfortunately, GPS is highly vulnerable to jamming (Faria *et al.* 2016), due to its low power at the Earth's surface. Jamming can occur by overpowering of the legitimate signal or through the more sophisticated technique of spoofing (also known as a logical attack), where a fake signal is fed to the system under attack, misleading it into believing, for instance, that a drone is flying at a different location (Arteaga *et al.* 2019). It is crucial to emphasize that, in addition to the risks posed by low-cost UAVs as vectors for attacks, their electronic and communication systems typically lack security and encryption, making their video and location data susceptible to compromise by third-party eavesdroppers along the transmission channel. A well-known malware example is Maldrone, designed to hack drones controlled via the internet by exploiting a transmission control protocol (TCP) backlink to gain total control of the device (Gandhi *et al.* 2024). Commonly used ports include 21 and 23, which correspond to file transfer protocol (FTP) and Telnet. Regarding GPS spoofing, military-grade drones are generally protected against this vulnerability due to their use of encrypted GNSS signals (Arteaga *et al.* 2019). The nominal power received by a GPS receiver at the Earth's surface is approximately -160 dBm, which is below the noise floor of the receiver (Jones 2011), typically about 25 dB lower (Rao *et al.* 2013). To determine the actual power level that renders the reception inoperative, an experiment was conducted as illustrated in Fig. 7.



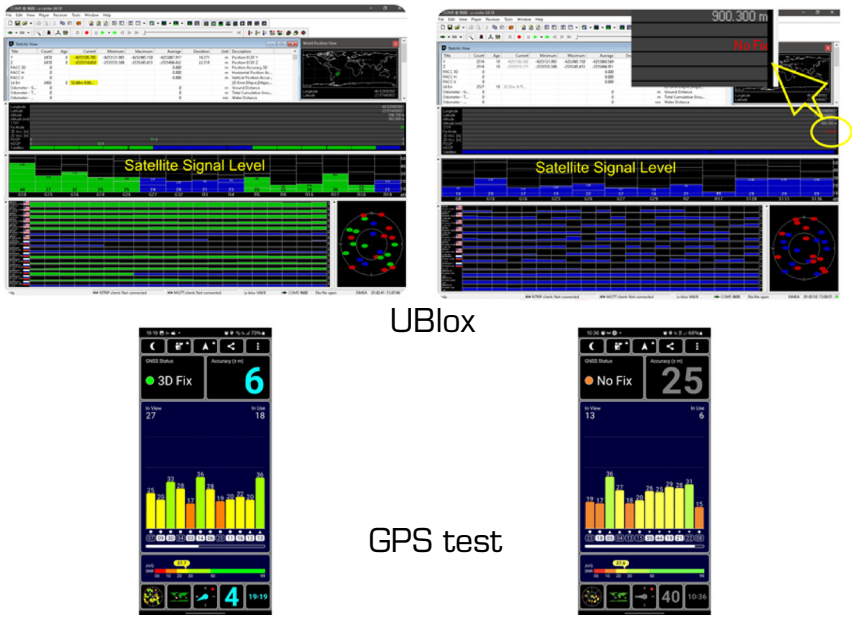
Source: Elaborated by the authors.

Figure 7. Measurement setup to define the threshold GPS receiving level.

An Android mobile phone (Samsung M34) was used to monitor the GNSS signal by an application (GPS Test), and was placed near a Rhode & Schwartz FS315 Spectrum Analyzer equipped with an 18-cm long telescopic antenna. Additionally, a Stoton GPS Module was used as a receiver, operating autonomously connected to a USB port. On the transmitter side, an RF generator was connected to an LPDA element, which had a measured gain of 3.8 dB at the frequency of 1,575 MHz. The separation distance *d* between the transmitter and the receivers was set to 2 meters. It was observed that the GPS failed to acquire signals from satellites when the power level was approximately -70 dBm for the mobile phone and -66 dBm, for the Stoton module. The results align closely with findings from Faria *et al.* (2016), which indicated that when the power at the GPS receiver reached -65.9 dBm, it lost its coordinates.

These measured values are approximate due to several factors: (1) the antenna gains of both the mobile phone and Stoton module are unknown, making it is unlikely that the power observed on the spectrum analyzer reflects what is received by the GPS units; (2) both the transmitter and spectrum analyzer antennas are linearly polarized, while the receiver antennas operate in RHCP; (3) the conditions for locking and unlocking GPS signals on the receivers are not instantaneous, it takes about 1 minute to achieve a complete stabilization, introducing measurement imprecision. Additionally, hysteresis was observed in the operation; for instance, transitioning from ON to OFF might result in a different power cut-off level than transitioning from OFF to ON.

Figure 8 depicts the interface of the UBlox program running on a computer, which controls the external Stoton module, alongside the GPS Test application operating on the mobile phone. The interface displays a wealth of available data, including satellite signal levels and GPS coordinates. In detail, the message "No Fix" is displayed to warn the user that the connection has been lost when the jamming level becomes excessive.



Source: Elaborated by the authors.

Figure 8. UBlox and GPS Test interfaces, for the case of normal operation (left) and when the jamming overpowers the proper reception (right), showing in detail the "No Fix" status.

Analyzing the GPS Test interfaces, it can be observed that, from the perspective of pure signal-to-noise ratio (SNR), both scenarios do not differ significantly, with values of 27.7 and 27.6 dB for the normal and jammed cases, respectively. No additional information or parameters are available in these two applications to indicate that jamming is occurring, apart from a gradual decrease in the number of visible satellites and the estimated distance precision.

To establish a quantitative estimate of the effective distance at which the jammer can overpower the GPS receiver, the Friis free-space propagation formula is utilized:

$$P_R = \frac{P_T G_T G_R}{\left(\frac{4\pi df}{c}\right)^2} \tag{3}$$

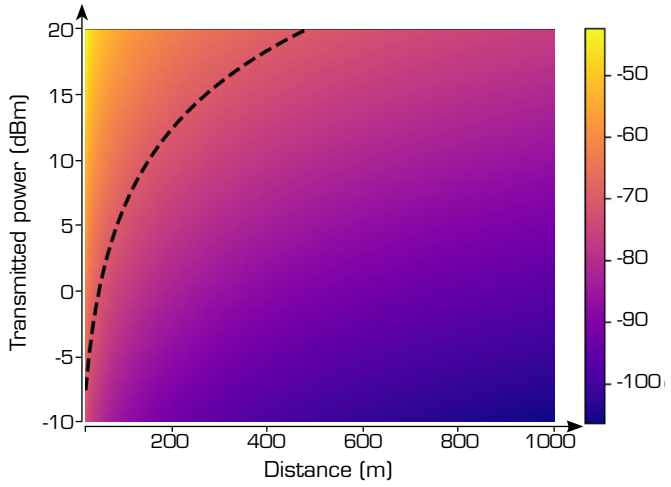
where P_R and P_T are, respectively, the received and transmitted power, G_R and G_T represent the receiver and transmitter antenna gains, d is the distance between the transmitter and receiver, f is the frequency, and c is the speed of light, all units in International System of Units (SI). The free-space loss (*FSL*), in dB, can be defined as:

$$FSL = 20log_{10}\left(\frac{4\pi df}{c}\right) \tag{4}$$

Therefore, the received power, in dBm, can be expressed as:

$$P_{RdBm} = P_{TdBm} + G_{TdBm} + G_{RdBm} - FSL \tag{5}$$

Assuming antenna gains to be 0 dB (i.e., isotropic), for simplicity, Fig. 9 illustrates the computed received power in dBm. The dashed line depicts the loci where the measured threshold of -70 dBm is found. This shows that with a transmitted power of 10 dBm, a distance of approximately 150 meters can be achieved, assuming both antennas are omnidirectional. Faria *et al.* (2016) considered a more conservative threshold figure of -30 dBm to disrupt the GNSS signal at the receiver, based on real-world measurements conducted with various commercial GPS systems, including an Android Samsung Galaxy S3 running the same GPS Test app and an automotive Folston receiver. Additionally, another threshold value, theoretically computed from the GPS regulations, yielded a value of 1.38E-12 W, or approximately -88 dBm (Rao *et al.* 2013).



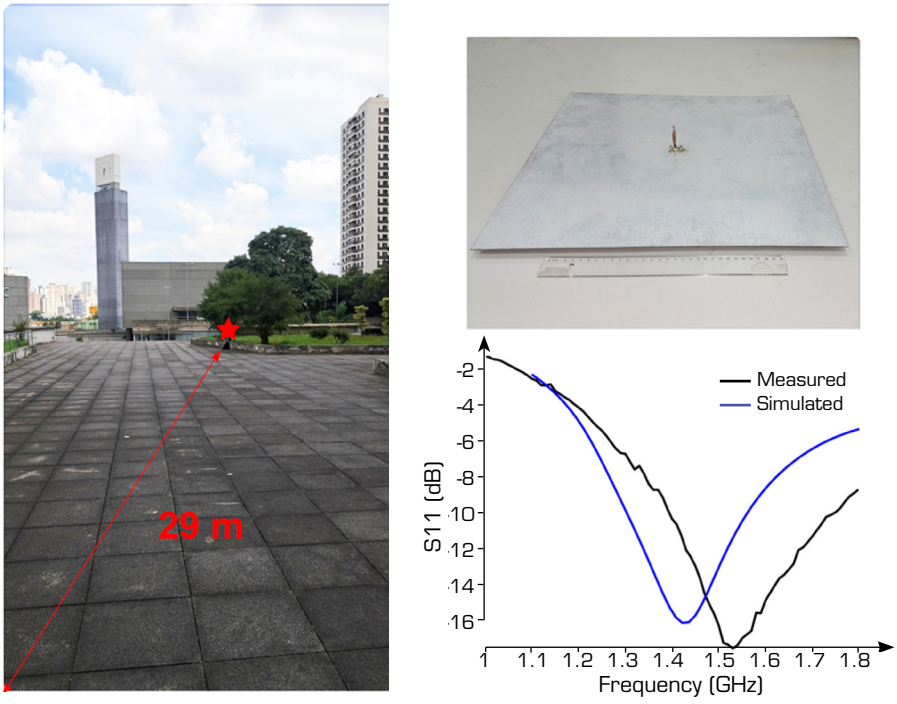
Source: Elaborated by the authors.

Figure 9. Received power in dBm, varied according to the distance and transmitted power, computed after the Friis equation. The interrupted line represents the reception power equal to the threshold of -70 dBm.

Outdoor test results

A test was conducted using the SDR USRP B210 operating at 1,575 MHz with its maximum power output of 14.4 dBm, as shown in Fig. 10, using the tone jamming technique. The test was performed in an outdoor area, where a radius of approximately 29 meters was observed, effectively disrupting GPS reception on a Samsung M34 mobile phone. A monopole antenna was employed to generate an omnidirectional power pattern, featuring an element length of 4.96 cm and wire radius of 1.3 mm. The metallic

ground plane used was a square measuring 49 cm on each side. Simulations to optimize the antenna design were carried out using FEKO, utilizing the method of moments, and are illustrated in Fig. 10. The antenna's computed gain was approximately 3 dB. This antenna design is justified due to previous tests with simple wire antennas connected to the SDR, which yielded mediocre results (with a radius of only 4 meters). It was determined that these antennas had low gain at the GPS frequency, measuring -4 and -12 dB for two different models tested. An even more efficient antenna would ideally have a semi-spherical radiation pattern, particularly when operating with right-hand circular polarization; for instance, patch antennas (Nascimento and Lacava 2009) could be used, although they typically suffer from low bandwidth.



Source: Elaborated by the authors.

Figure 10. Outdoor test with the SDR using an omnidirectional wire antenna, and in detail, the used antenna and its return loss, computed and measured.

Another test, this time with the printed log periodic antenna (shown in Fig. 2), is presented in Fig. 11. The antenna was positioned on the window ledge of a seventh-floor building, directed toward street level, while transmitting with the same 14.4 dBm output power and tone transmitted from the SDR. It was observed that the GPS signal, as monitored on the mobile phone, was lost after 70 linear meters from the building, which is equivalent to 78 meters from the antenna.

These results, obtained with both the monopole and with the LPDA, fall short of the expected 400 meters, even when considering the output power in conjunction with the antenna gains (4 dB LPDA and 3 dB for the monopole). The observed issues were primarily related to antenna alignment, obstruction from the metallic window frame (as shown in Fig. 11), and other practical implementation details. The free-space model assumes a non-obstructed scenario, which contrasts with the actual outdoor environment, with a strong multipath content. Besides that, there is also the reflection from the ground and antenna-related factors, such as polarization mismatches and losses, and cables. These items account for the 121-meter difference in the first-order prediction. This indicates that a more conservative threshold should be used to ensure that the GNSS signal is effectively lost at the receiver site, such as the -30 dBm suggested by Faria *et al.* (2016). Furthermore, it was noted that prior to the "No Fix" warning being displayed on the receiver, the error in distance increased, reaching tens of meters, which demonstrates the degradation of the computed reading.

Source: Elaborated by the authors.

Figure 11. Outdoor test with the SDR using the directional LPDA, in detail, the antenna on the window ledge.

DISCUSSION

Five different jamming techniques were presented, using the same SDR platform operating with GNU Radio. The actual tests were performed with the tone technique, since the GPS occupies a narrow frequency band. Other larger bandwidth protocols, such as Wi-Fi, for instance, would benefit from the other techniques, to better spread the noise across the bandwidth.

The results demonstrated that the implementation of a jammer using SDR is feasible. Tests conducted with the specific GPS service confirmed that satellite signal acquisition on both a mobile phone and an external module was indeed disrupted. A range approximation was derived based on the free-space formula (Friis), which proved to be overly optimistic compared to the results obtained from the tests. In the literature, Fang *et al.* (2018) reported a jamming effect extending up to 120 meters with an output power of 20 dBm. Considering Eq. 3 and using the same threshold of -70 dBm (not informed in the original article), one would expect a maximum range close to 480 meters, which is also longer than what was observed in the experiment.

In addition to the observed differences with the free-space attenuation formula, there was a strong dependency on the actual antenna installation and performance. Unreliable connections, low-gain antennas, and interference from nearby objects played significant roles, highlighting the importance of thorough antenna design. A brute-force approach, which involves delivering higher output powers using power amplifiers, is sometimes employed by rugged commercial jammers that utilize simple thick monopoles as radiating systems. When there is a need to cover multiple frequency bands, more than one monopole is employed. These systems are designed to circumvent non-ideal installation conditions, such as being mounted on top of vehicles or encased in soldiers' backpacks, while still delivering substantial power.

In terms of regulation, the FCC, with its Communications Act of 1934, already prohibited the disruption of radio communications, whereas its Section 333 prohibits deliberate interference with authorized radio services. It also prohibits the advertisement and sale of jammers, and only allows their use by federal law agencies under specific circumstances.

CONFLICT OF INTEREST

Nothing to declare.

AUTHORS' CONTRIBUTION

Conceptualization: Perotoni MB; **Methodology:** Perotoni MB; **Software:** Perotoni MB; **Validation:** Perotoni MB; **Formal analysis:** Perotoni MB; **Investigation:** Perotoni MB; **Resources:** Perotoni MB; **Data curation:** Perotoni MB; **Writing – Original Draft:** Perotoni MB; **Writing – Review & Editing:** Perotoni MB, Gaspar R, and Campos A; **Visualization:** Perotoni MB; **Supervision:** Perotoni MB; **Final approval:** Perotoni MB.

DATA AVAILABILITY STATEMENT

The data will be available upon request.

FUNDING

Not applicable.

ACKNOWLEDGMENTS

Not applicable.

REFERENCES

Alamleh H, Estremera L (2024) System for detecting and jamming unauthorized communications using RF-SDR. Paper presented 2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference. IEEE; New York, USA. http://doi.org/10.1109/UEMCON62879.2024.10754753

Arteaga SP, Hernandez LAM, Perez GS, Orozco ALS, Villalba LJG (2019) Analysis of the GPS spoofing vulnerability in the drone 3DR solo. IEEE Access 7:51782-51789. https://doi.org/10.1109/ACCESS.2019.2911526

Bhojan R, Joshi R (2016) An integrated approach for jammer detection using software defined radio. Procedia Comput Sci 79:809-816. https://doi.org/10.1016/j.procs.2016.03.113

Ding J, Tang C, Zhang L, Yue Z, Liu Y, Dan Z (2024) UAV communication and navigation signals jamming methods. Paper presented 14th IEEE International Conference on Signal Processing, Communications and Computing. IEEE; Bali, Indonesia. https://doi.org/10.1109/ICSPCC62635.2024.10770465

Fang L, Wang XH, Zhou HL, Zhang K (2018) Design of portable jammer for UAV based on SDR. Paper presented 2018 International Conference on Microwave and Millimeter Wave Technology. Chengdu, China. IEEE; https://doi.org/10.1109/ICMMT.2018.8563735

Faria LA, Silvestre CAM, Correia MAF (2016) GPS-dependent systems: vulnerabilities to electromagnetic attacks. J Aerosp Technol Manag 8(4):423-430. https://doi.org/10.5028/jatm.v8i4.632

Ferreira R, Gaspar J, Sebastião P, Souto N (2020) Effective GPS jamming techniques for UAVs using lowcost SDR platforms. **Wirel Pers Commun** 115(4). https://doi.org/10.1007/s11277-020-07212-6

Ferreira R, Gaspar J, Sebastião P, Souto NA (2022) Software defined radio based anti-UAV Mobile system with jamming and spoofing capabilities. Sensors 22(4):1-17. https://doi.org/10.3390/s22041487

Gandhi NR, Kumar D, Arunkumar E, Parameshwari S, Sadim M, Al-Fatlawi RR (2024) A detailed review analysis of GPS used in drone technology and its challenges. Paper presented 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering. IEEE; Greater Noida, India. https://doi.org/10.1109/ICACITE60783.2024.10616508

Jones M (2011) The civilian battlefield: protecting GNSS receivers from interference and jamming. Inside GNSS 6(2):40-49.

Kaag J, Kreps S (2014) Drone warfare. Cambridge: Polity Press.

Kim J, Kim S, Ju C, Son H (2019) Unmanned aerial vehicles in agriculture: a review of perspective of platform, control, and applications. IEEE Access 7:105100-105115. https://doi.org/10.1109/ACCESS.2019.2932119

Kunertova D (2023) Drones have boots: learning from Russia war's in Ukraine. Contemp Secur Policy 44(4):576-591 https://doi.org/10.1080/13523260.2023.2262792

Merakeb Y, Ezzedine H, Huillery J, Bréard A, Touhami R, Duroc Y (2020) Experimental platform for waveform optimization in passive UHF RFID systems. Int J RF Microw Comput-Aided Eng 1-15. https://doi.org/10.1002/mmce.22376

Nascimento DC, Lacava JCS (2009) Circularly-polarized microstrip antenna radiation efficiency simulation based on the wheeler cap method. Paper presented 2009 IEEE Antennas and Propagation Society International Symposium. IEEE; North Charleston, USA. https://doi.org/10.1109/APS.2009.5171900

Paerlin K, Alam MM, Le Moullec Y (2018) Jamming of UAV remote control systems using software defined radio. Paper presented 2018 International Conference on Military Communications and Information Systems. IEEE; Warsaw, Poland. https://doi.org/10.1109/ICMCIS.2018.8398711

Pieterse F, du Plessis WP (2021) Retrodirective cross-eye jammer implementation using software-defined radio (SDR). Paper presented 2021 IEEE Radar Conference. IEEE; Atlanta, USA. https://doi.org/10.1109/RadarConf2147009.2021.9455215

Rahman ADBA, Ghani KA, Khamis NHH, Sidek ARM (2021) Unmanned aerial vehicle (UAV) GPS jamming test by using software defined radio (SDR) platform. J Phys: Conf Ser 1793(012060):1:8 http://doi.org/10.1088/1742-6596/1793/1/012060

Rao BR, Kunysz W, Fante R, McDonald K (2013) GPS/GNSS antennas. Boston: Artech House.

Rejeb A, Rejeb K, Simske SJ, Treiblmaier H (2023) Drones for supply chain management and logistics: a review and research agenda. Int J Logist Res Appl 26(6):708-731. https://doi.org/10.1080/13675567.2021.1981273

Saleem M (2020) Jamming techniques for Global Positioning System (GPS L1) signal using RTL-SDR (master's thesis). Islamabad: Institute of Space Technology. https://doi.org/10.13140/RG.2.2.14800.79368

Sarbu A, Neagoie D (2020) WiFi jamming using software defined radio. Int Conf Knowl-Based Organ 26(3):162-166. https://doi.org/10.2478/kbo-2020-0132