Politecnico di Torino

VULNERABILITY ANALYSIS OF THE UAV DURING GPS SPOOFING

By
Ilkhom MAMAYUNUSOV

Supervisor(s):
Prof. MARCHETTO GUIDO
RUSTAMOV AKMAL (External teaching staff)

Politecnico di Torino
2022

Abstract

As the Global Position System (GPS) based technology increasingly implemented into the civil applications UAVs, it has been driven by the mass-market that more precise and reliable GPS services are demanded. However, due to the weakness of the GPS signals, the GPS receiver performance could be easily disrupted by anthropogenic disturbances, among which the jamming and spoofing activities are extremely crucial threats. In this paper an preliminary investigation on the effects of the jamming and spoofing disturbances to the mass-market positioning and navigation units integrated in the smartphones and drones is provided. Comparative analysis will be addressed on the performance of drones under the intentional disturbances. Then we use/propose defence system and solving these challenges while running on a network of UAV devices. Because a system relying on GPS positioning to make its next step must comprehend GPS vulnerabilities and recognize threats such as jamming and spoofing, the GPS is now the most extensively used and best known example of a Global Navigation Satellite System (GNSS). Jamming and spoofing devices can be acquired for a modest price on the open market. Software Defined Radio (SDR) technology is also delivering new levels of flexibility and cost efficiency.

The following research questions will be used to investigate this technology:

- Is there a waveform, power, and amplitude combination that will cause the GPS signal to be disrupted?
- Can GPS jamming be done as easily in software as it is in hardware?
- Is GPS spoofing easier to accomplish in software?

The study consists of two tests: a GPS jamming test where focus is to realize what combination of waveform, power and amplitude is able to jam the GPS signal and a GPS spoofing test where a HackRF One is used to fool a UAV. The results from the jamming test have shown that GPS jamming is easy to accomplish using different combinations as GPS signals have low received signal power. The spoofing test proved that it is capable to spoof a UAV with a fairly inexpensive SDR setup and freely available software.

CONTENTS

CHAPTER 1 INTRODUCTION

The scope and motives that led to the production of this dissertation, as well as the goals that must be met and, finally, the structure of the dissertation, will be discussed in this first chapter.

1.1 Scope and Ambition

The Global Navigation Satellite System (GNSS) is now used by the majority of devices to navigate. The most frequently used and well-known example of GNSS is the Global Positioning System (GPS). One major problem is that many of these systems rely on the GPS, which implies that any attempt to disrupt its service could result in a simultaneous failure of these systems, which are supposed to be self-contained [1]. Missiles, ships, automobiles, planes, and drones all rely on the GPS for locating. In a world where GPS is critical, we must be aware of the GPS vulnerabilities and threats. Because GPS signals have a low received signal power, they are easily interrupted. It's also critical to recognise that the only way to detect and eliminate these risks is to develop counter-mechanisms and technologies. Two concerns stand out when it comes to exposing GPS vulnerabilities: jamming and spoofing. Because it is so simple to deny GPS positioning, jamming is a real concern. However, it pales in comparison to the impact and havoc that spoofing can wreak. Spoofing, on the other hand, is more difficult to achieve because it necessitates a complete reconstruction of the GPS signal. These dangers are no longer just a military capability, as the cost and size of jamming and spoofing equipment has decreased, and the technology can now be openly purchased online. There are various websites that describe how to build this equipment in detail and provide detailed plans for individuals with particular technical skills [2]. The rapid advancements in technology are also pushing hardware equipment to a software level, and Software Defined Radio (SDR) technology is gaining traction because it offers unprecedented flexibility and cost efficiency.

1.2 Objectives and Main Contributions

The major purpose is to investigate it on a software level after admitting and reporting the existence of numerous tests related GPS jamming and spoofing using hardware equipment. This dissertation considers SDR equipment that can be used to broadcast or receive signals, the SDR platform in GNU Radio that allows for transmission on a frequency of choosing, and test equipment that can be used to

determine if jamming and spoofing are effective. Early on, an examination of the chosen SDR equipment and its features, as well as an understanding of how it works and how it may be used in conjunction with the SDR, is carried out in order to essentially develop a jammer operated solely by software. They are two primary tests whose evaluation techniques are based on assessing test equipment behaviour in terms of signal power, amplitude, and waveform, as well as determining whether or not the equipment affected by the SDR equipment works. The first is GPS jamming, whereas the second is GPS spoofing. The major goal is to show that GPS is a weak signal that can be readily disrupted in a software environment, making it practicable for anyone with an SDR to do so. The tests will aim to find solutions to problems such as:

• Is there a waveform, power, and amplitude combination that will cause the GPS signal to be disrupted?
• Can GPS jamming be done as easily in software as it is in hardware?
• Is software-based GPS spoofing easier to achieve?

With the use of SDR equipment and platform, the goal is to contribute to the setup of radio equipment in software, particularly equipment capable of disrupting the GPS signal, using SDR technology. An article is being written that will summarise some of the work done in this dissertation and will be presented at a future conference.

1.3 Thesis Outline

The second chapter provides a literature study and overview of the GNSS, with a focus on the GPS. Jamming and spoofing are two types of radio frequency interference. On a hardware level, it reports on relevant research on GPS jamming and spoofing. Introduces GPS jamming and spoofing from a software perspective, as well as the available SDR equipment on the market and how to choose the one that will be utilised for the software tests.

Chapter 3 delves deeper into the GNSS signal model, both with and without interference, with a focus on distinct types of interference. The effect of jamming on the various GNSS receiver stages is also briefly discussed.

By presenting the HackRF One, the chosen SDR equipment, which is capable of receiving and transmitting radio signals made in software, Chapter 4 explains jamming and spoofing in a software perspective. The principles of SDR and GNU Radio are also introduced, and the device is linked to them. A case study is presented in order to gain a better understanding of how the HackRF One works.

Chapter 5 is devoted to the author's personal tests and findings. The first test is GPS jamming, which involves the HackRF One emitting various waveforms with varying amplitudes at the GPS signal in order to jam it. The second test involves using the HackRF One to send an erroneous GPS signal near a UAV in order to fool it and obtain a fix on an inaccurate location.

The major outcomes from the GPS signal jamming and GPS spoofing tests are presented in Chapter 6. There is a recognition that the shift from hardware to software makes the GPS far more vulnerable to dangers that can almost certainly be manufactured by anyone. Future work recommendations are also addressed.

Like any other similar device, a copter with Wi-Fi on board is equipped with a network adapter that has a MAC address by which it can be identified. This is how Parrot aircraft work, for example. A smartphone with an installed application serves in this case as an analogue of the control panel, from which the drone receives commands. To identify the control device, an ID Key is used - a unique label “tied” to the application installed on the smartphone (Flight control software) and the current session. The hacking principle is simple: the attacker connects to the drone network, determines a unique tag, and then sends a command to the copter that will force it to disconnect from the current control device and start receiving commands from the attacker’s smartphone that have a “copied” tag of the original device.In practice, the Aircrack-ng application was used to hack into the drone network. The program can monitor the air in search of secure Wi-Fi networks, intercept packets and export data from them for further analysis, as well as apply various network attack algorithms. Its functions are described in more detail on the manufacturer's website. It is noteworthy that the cost of programmable radio transmitters, with which you can jam or fake a GPS signal, today is relatively small and amounts to only a few hundred dollars, and you can buy everything you need on the Internet. Moreover, even for “professional” copters, overly powerful jammers are completely unnecessary: there are cases when large drones like the Phantom were “lost” near the antennas of base stations of mobile operators or high-voltage power lines. If the copter gets into the coverage area of such a jammer, it will most likely begin to drift with the wind, and due to the lack of a signal from navigation satellites, it will not be able to correctly determine its current location in order to return to the departure point.

CHAPTER 2 LITERATURE REVIEW

This chapter provides a high-level overview of GNSS systems, with an emphasis on the GPS. The effects of radio frequency interference are described, with a focus on jamming and spoofing. There is also a brief discussion of how jamming might influence the GNSS receiver stages. Relevant jamming and spoofing research is described, and lastly, the SDR technology is presented, with a decision made on which SDR equipment will be utilised for the testing.

2.1 Overview Of GNSS

The phrase "global navigation satellite system" refers to satellite navigation systems that send location and timing data from space and have worldwide coverage. There are two primary GNSSs in use today: GPS from the United States and Glonass from Russia. China is extending regional Beidou, and the European Union is working on Galileo. They all operate in a similar manner [3]. Because the focus of this dissertation is on the GPS signal, the other GNSSs will not be discussed in depth. In addition, in [4], the GNSS acquisition in the absence and presence of interference is examined in depth and reported in Appendices A and B, respectively.

As illustrated in Figure 2.1, the GPS signal is received by a GPS receiver from a series of earth orbiting satellites to establish positioning by triangulation, which is a method of measuring three independent locations to compute a location with an accuracy of only a few metres.

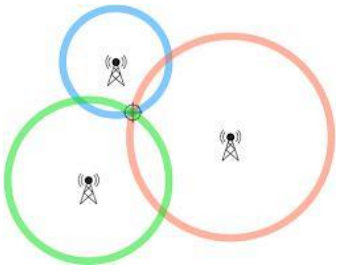


Figure 2.1: GPS Triangulation

2.1.1 GPS Ranging Codes

` The Coarse/Acquisition (C/A) and Precision (P)-codes are the two range codes used in the original GPS. The first is the Standard Positioning Service (SPS), which is used by civilians, and the second is the Precise Positioning Service, which is utilised by users approved by the US Department of Defense (PPS). To prevent unwanted users from faking the signal, the P-code was encrypted by modulating it

with a specific encryption secret sequence known as the W-code, resulting in the Y-code. The P(Y) code [5] is the name given to the encrypted signal.
The C/A code is a pseudorandom noise (PRN) code with a length of 1.023 bits that repeats every millisecond and is sent at 1.023 Mbit/s. The P(Y) code is a PRN code with a length of 6.1871 1012 bits that repeats once a week and is sent at 10.23 Mbit/s. The PRN for the C/A code is unique to each satellite, whereas the PRN for the P(Y) code is a short segment of the master P(Y) code that is roughly 2.35 1014 bits long, and each satellite broadcasts its allotted segment of the master code again.
The GPS signal utilises a Code Division Many Access (CDMA) spread-spectrum technology to allow the receiver to detect multiple satellites utilising the same frequency without mutual interference. Each satellite broadcasts a unique PRN code that does not correlate well with the PRN codes of other satellites, allowing the signal to be spread over a wide bandwidth (2 MHz for the C/A code and 20 MHz for the P(Y) code). Using various PRN sequences, many satellites can send signals at the same frequency at the same time. The varied codes used by these signals allow a receiver to discriminate between them [6]. Direct Sequence Spread Spectrum is the name of this method (DS-SS). [7] further claims that the capacity to fight radio frequency interference is a reason to employ DS-SS.

2.1.2 GPS Navigation Message

The receiver also requires specific information on the satellites' position and network, which is modulated at 50 bits per second on top of both the C/A and P(Y) codes and referred to as the Navigation message. It is made up of a 1.500-bit frame that is broken into five 300-bit subframes that each take 6 seconds to broadcast.
The navigation message is divided into three parts. The first is situated in the subframe 1 and provides the satellite's status and health, as well as GPS data and time. The second refers to subframes 2 and 3, which provide the ephemeris data that allows the receiver to compute the satellite's location. The third, known as the almanack, comprises information and status on all satellites in the constellation, as well as their locations and PRN numbers. Because subframes 4 and 5 each contain just 1/25th of the whole almanack message, the receiver must analyse 25 full frames of data to extract the entire 15000-bit almanack message, which takes 12.5 minutes from a single satellite [5].
The ephemeris information is specific and only valid for four hours, but the almanack information is more generic and good for up to 180 days. To generate a location fix using any satellite, the receiver must have an exact and full copy of that satellite's ephemeris data. After the receiver picks up that satellite's signal turn, the

ephemeris data may be retrieved immediately. The almanack helps the receiver figure out which satellites to look for.

2.1.3 PS Frequency Information

To travel from the satellite to the receiver, the GPS signal must be modulated onto a carrier frequency. The original GPS design used two frequencies: one at 1575.42 MHz (10.23 MHz 154), known as L1, and the other at 1227.60 MHz (10.23 MHz 120), known as L2. As technology progresses and new demands are placed on the existing system, the GPS system is being modernised, and more frequencies are being used to build new bands. The bands and frequencies of the most modern GPS system, as well as their use, are listed in Table 2.1. Table 2.1: GPS Frequencies

Bands	Frequency (MHz)	Phase	Usage
L1	1575.42 (10.23 × 154)	In-phase(I)	P(Y) code
		Quadrature-phase(Q)	C/A code, L1 Civilian (L1C) and Military (M) code
L2	1227.60 (10.23 × 120)	In-phase(I)	P(Y) code
		Quadrature-phase(Q)	L2 Civilian (L2C) and Military (M) code
L3	1381.05 (10.23 × 135)		Nuclear Detonation (NUDET) event detected
L4	1379.913 (10.23 × 1214/9)		Additional ionospheric correction
L5	1176.45 (10.23 × 115)	In-phase(I)	Safety-of-Life (SoL) Data signal
		Quadrature-phase(Q)	Safety-of-Life (SoL) Pilot signal

The C/A code is transmitted on the L1 band as a 1.023 MHz signal using a Bi- Phase Shift Key (BPSK) modulation technique. The P(Y) code is transmitted on both the L1 and L2 bands as a 10.23 MHz signal using the same BPSK modulation, however the P(Y) code carrier is in quadrature with the C/A carrier; meaning it is 90^{o} out of phase. The C/A code and the P(Y) code are both spread centred at the carrier frequency in Figure 2.2. The power spectral density can be lowered while the signal power remains constant.

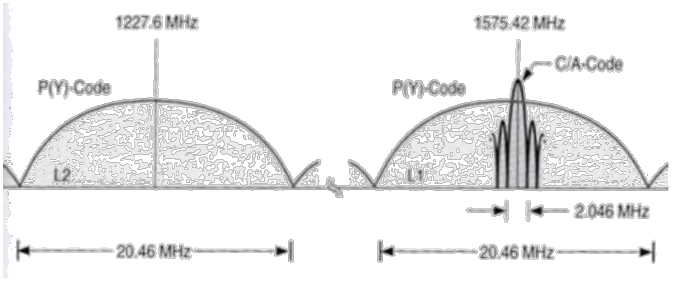


Figure 2.2: Power Spectra Of GPS Signals On L2 And L1 [7]

2.1.4 GPS Signal Power

The GPS signals are quite faint as compared to those generated on the ground. The radio frequency (RF) power of a satellite's antenna input port is around 50 W, and the transmitted power is attenuated as the satellite antenna spreads the RF signal uniformly across the earth's surface. This is mostly due to signal transmission channel loss, which occurs when the transmitted power decays with the distance squared between the orbit and the user [7].

According to GPS standards [7], the minimum received power level for users on the earth is 158.5 dBW for the C/A code on L1 and 160 dBW for the P(Y) code on L2. It's the same as 106, which is significantly below the background RF noise level perceived by a receiver's antenna. "The exceedingly low signal strength that reaches the receiver is the Achilles' heel of GPS," according to [7] and [8].

2.2 Radio Frequency Interference

Any radio frequency detected by a GNSS receiver that comes from an unwanted source is termed interference. Because of this interference, navigation accuracy may be compromised or receiver tracking may be lost entirely [6].

Unintentional and intentional interference, according to [3] and [9], exists. Interference caused by other broadcast televisions, VHF transmitters, and personal electronic devices is referred to as unintentional interference. This type of interference, as well as ionospheric effects and signal blockage, are all potential threats to GPS. SPS users that utilise a single frequency were the ones who noticed the impacts the greatest. Jamming, spoofing, and meaconing are three types of deliberate interference. Meaconing is not addressed in this dissertation.

RFI (radio frequency interference) can be intermittent or continuous. Because the pulses are shorter than the period of a GPS data bit, GPS tolerates pulsed RFI better than continuous RFI. Continuous RFI may be characterised and separated into

broadband and narrowband bandwidth, according to [10]. The bandwidth of a broadband RFI is equal to or larger than the GNSS bandwidth, which is 2 MHz for the GPS C/A code, but the bandwidth of a narrowband RFI is smaller. The simplest kind of interference is a continuous wave (CW) signal, which consists of a single tone focused in a relatively narrow band around the centre frequencies.

2.2.1 GPS Jamming

GPS jamming is defined in [10] as "the emission of sufficient strength and correct features of radio frequency radiation to prevent receivers in the target region from detecting GPS signals" Jamming signals are identified by their central frequency and power, which is expressed in decibels as the jamming-to-signal ratio (J/S). The J/S reduces as the distance between the jammer and the receiver increases.

The receivers' measured signal strength will be reduced as a result of jamming. The carrier-to-noise density ratio (C/N0), according to [3, is the essential navigation signal quality metric at the receiver, describes the signal strength. [6] defines and analyses the equation C/N0 in detail, revealing that: As the distance between the jammer and the receiver decreases, the received jammer power increases; the signal strength decreases as the jamming happens, and a greater PRN code rate, in principle, will result in a lesser fall in signal strength as the jamming occurs.

Different classes have been proposed for civilian jammers. [11] divides jammers into three categories according on the type of signal they jam: CW signals (class I); the jammer sends out a CW signal;

class II: single saw-tooth chirp transmissions, where the jammer sends out a frequency-modulated signal with a saw-tooth time-frequency (TF) evolution;

• class III: multi-saw-tooth chirp signals; the device transmits a frequency-modulated signal, but its TF evolution is more complicated, and it is determined by the combination of several saw-tooth functions;

• class IV: chirp with signal frequency bursts; the device transmits a frequency-modulated signal, but frequency bursts are used to enlarge the frequency band affected by the disturbing signal.

Experiments in [12] and [13] divided jammers into groups depending on their power source and antenna type:

• Group 1: Car cigarette lighter jammers. These jammers typically feature minimal transmitting power (less than 100 mW) and the ability to connect to an external antenna.

• Group 2: Jammers with an external antenna linked through a SMA connection and powered by a battery. Some jammers can transmit on both the L1 and L2 frequency bands, with a transmit power of up to 1 watt.
• Group 3 - Jammers that are camouflaged as innocuous technological devices, such as cell phones. These jammers usually employ saw-tooth frequency modulation and do not have an external antenna. Figure 2.3 depicts the primary civilian jammers on the market as a hybrid of both groups.

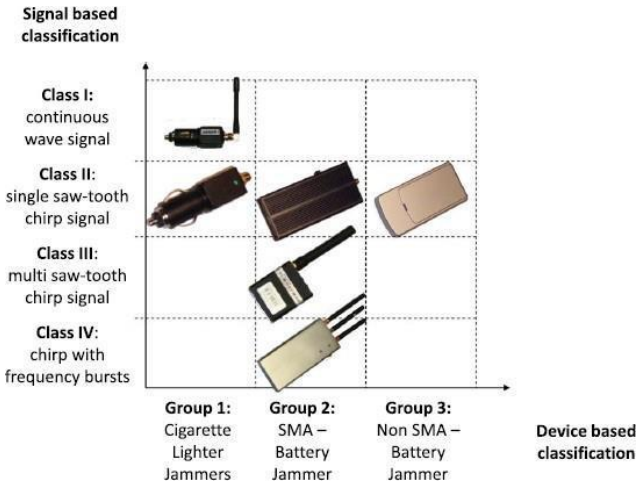


Figure 2.3: Jammers Classification [14]

Most jamming devices create broadband interference, according to a research published in [12] and [13]. More sophisticated jammers than those mentioned above are about to arrive on the market, according to [15], which also refers to [9] and [12].

2.2.2 GPS Spoofing

In [10], spoofing is described as "a method of deceiving a radar's target-ranging function that has been utilised for a long time. In the case of GPS, the goal is to get an active GPS receiver (whether or not it is currently monitoring GPS signals) to lock on to what appear to be legitimate-looking bogus signals ".. Although the P(Y) code of the GPS is encrypted and hence difficult to spoof, the C/A code's signal structure, codes, and modulation are all exposed to the public, making it easy to fake. Spoofing attacks can be classified as simple, moderate, or complex, according to [16].

The GPS simulator is used to broadcast GPS signals for the faked position to the GPS receiver under assault, thus there is no need to know the victim's original Position, Velocity, and Time (PVT). If pseudorange, C/N0, and Doppler leaps, all of which will occur, are tracked, this type of assault may be easily spotted.

In an intermediary attack, the spoofer obtains information about the target's initial PVT and attempts to recreate and broadcast the GPS signal while approaching the victim. The receiver will ultimately lock on to the greater power of the faked signal without recognising it, allowing the spoofer to return to the victim's PVT arbitrary setting. Monitoring the Doppler and pseudo range fluctuations when shifting the victim's reception antenna is one approach to identify it.

In the sophisticated assault, the same procedure occurs as before, but now numerous coordinated spoofers are employed to attempt to simulate the spatial signal domain, which requires several transmitting antennas to be successful. For a traditional single antenna receiver, this is extremely difficult to detect [17].

The majority of commercial spoofers do not assault the GNSS signal directly; instead, they introduce faked data directly at the receiver's output, which necessitates physical or software access to the victim's receiver. Spoofing RF signals is far less prevalent, and commercial GNSS RF signal generators cost at least 100.000 euros. They are not capable of an intermediate spoofing attack, but they may cause severe interference to a normal GNSS receiver. SimSAFE software, in combination with a GNSS RF-signal generator, is likely the first ready-to-buy commercial GNSS spoofer [18] that can spoof assaults on the GPS L1 and Galileo E1 bands. The current signals from the sky are tracked by a commercial GNSS receiver, which is used to create a suitable spoofing signal from the GNSS RF simulator.

2.3 Jamming Impact On GNSS Receivers

Jammers with a high power output are easy to spot. The ones that broadcast at an intermediate power level are the most harmful, since they might degrade the receiver's performance without losing lock or preventing the collection of satellite signals. Different phases of a GNSS receiver can be affected by jamming, as outlined briefly below. [14] provides a more in-depth examination of this impact, as well as examples and tests.

2.3.1 Impact On The Front-End Stage

The front-end, which has the objective of filtering the incoming signal in the required bandwidth and downconverting it to the specified IF before completing the A/D conversion, is the first receiver step that might be impacted.
Modern receivers feature an Automatic Gain Control (AGC) between the analogue section of the front-end and the ADC, and jamming affects the AGC settings and changes the sample distribution at the ADC output. As a result, some front-end components work outside of their nominal regions [14].

2.3.2 Impact On The Acquisition Stage

The acquisition block of a GNSS receiver is responsible for determining the signal existence as well as providing a preliminary approximation of the signal coding delay and Doppler frequency [6].
When there is interference, the likelihood of declaring the signal present incorrectly rises, and the acquisition block may yield incorrect Doppler and latency estimations. The effects of CWI on acquisition blocks are examined in depth in [19], while [20] has a comprehensive investigation of the impact of various types of interference on acquisition probability.

2.3.3 Impact On The Tracking Stage

The tracking block is responsible for presenting fine estimates of the signal parameters. GNSS measurements such as pseudoranges, carrier phases and Doppler shifts are generated by these estimates.
Different effects can happen depending on the power received and on the type of jamming signal. In most cases, an increased bit error rate (BER) can occur and in the worst cases, the receiver is unable to decode the navigation message [14].

2.3.4 Impact On The Position

The GNSS receiver can still produce an estimate of location if the interfered signal is processed by both acquisition and tracking stages, but this estimate will be weakened since it is based on pseudoranges influenced by the interference.
Because it is dependent on the operation position method, there is no uniform criterion for quantifying performance reduction due to positioning inaccuracy. The

jamming signal can either damage the location solution or cause total loss of GNSS signal lock depending on the J/S [14].

2.4 Research On GPS Jamming Using Hardware

The military has been aware of the possibilities of jamming GPS signals for a long time. Low-powered jammers can cause the C/A code to be interrupted across a large region. A research published in 1994 [22] shown that a simple 1 W airborne jammer could prevent a receiver from tracking a GPS signal that had previously been locked on at a distance of 10 km over a distance of 85 km. As low-power jammers have become more widely available, research on blocking civilian GPS signals has risen in recent years.

2.4.1 Receivers Ability To Determine Position

[23] did a study on the jamming susceptibility of four distinct GPS receivers to see how simple it is to jam the GPS signal. A commercial RF signal generator and passive GPS antennas are utilised to generate a frequency modulation signal on the L1 band. The signal output power ranges from 3 dBm (0.5 mW) to 17 dBm (1.5 mW) (50 mW).

An early test suggests that a jammer with a strength of 13 dBm (20 mW) may interrupt all GPS receivers up to a distance of 2 km from the jammer. Starting from that distance, the main test consists in having all receivers on the ground level, where they can establish a GPS position, and start increasing the jamming power until all receivers couldn't establish a position anymore.

Signal strength (dBm)	GPS receiver			
	Garmin 60CSx	Garmin eTrex	Trimble ProXH	Topcon GB-1000
-3	P	P	P	P
0	P	P	P	NP
1	P	P	P	NP
4	P	P	P	NP
7	P	P	P	NP
9	P	P	P	NP
10	NP	P	P	NP
12	NP	P	P	NP
13	NP	NP	P	NP
15	NP	NP	P	NP
17	NP	NP	NP	NP

P, indicates the ability to determine a position; NP, indicates that a position could not be determined.

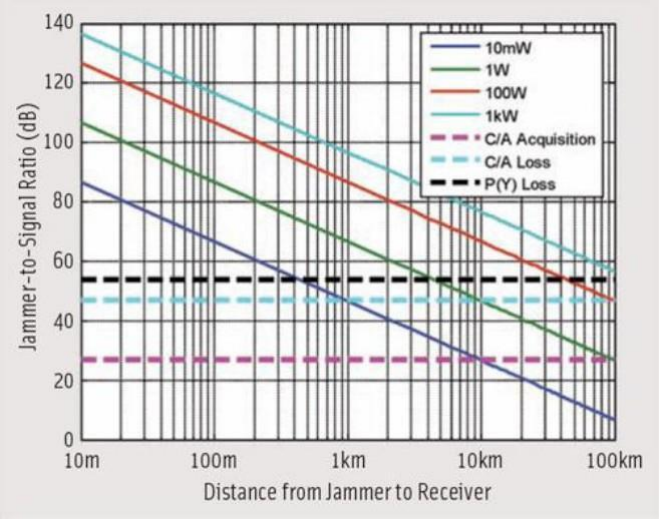
Figure 2.4: The Ability Of GPS Receivers To Resist Jamming [23]

Figure 2.4 indicates that the Trimble receiver has the best jamming resistance, while the Topcon receiver, which is the most advanced of the four, has the worst. The eTrex, the less advanced of the Garmin receivers, produces better results. The authors conclude that jamming GPS receivers is definitely simple, and that "jamming remains a severe threat to navigation integrity that requires more examination" [23].

One flaw in this study is that it does not examine the quality of the position determination throughout the range of jamming signal levels. It would be interesting to investigate the performance when the jammer intensity is close to the threshold before losing track of the satellites.

2.4.2 Jamming-to-Signal Ratio

When evaluating the J/S, studies have been undertaken to establish how susceptible a consumer-grade GPS receiver is. When the receivers are still acquiring or tracking the target signal, the maximum J/S refers to the amount of non-GNSS interference they can withstand. The horizontal dashed lines represent some common receiver thresholds, and Figure 2.5 displays theoretical values displayed in [24] for several CW broadband jammers with power ranging from 10 mW to 1 kW. Figure 2.5: The Effect Of Various Jammers On GPS Receivers [24]



According to the findings, the more effective the jammer, the greater the distance at which the C/A code may be prevented from being acquired. A 10 mW jammer will cause the receiver to lose the lock for up to 1 km, and a 1 W jammer will cause it to lose the lock for up to 10 km. These values are supported by the findings of an airborne jammer in [22].

Other investigations have been carried out to demonstrate the vulnerability of consumer GPS devices. [25] utilised a GPS L1 jammer with a 13-dBm output strength to jam six distinct receivers. At 1577 MHz, with a spectrum bandwidth of 16.3 MHz, the jammer produces a chirp signal with multisaw tooth characteristics. The test was carried out with three distinct scenarios: no jamming, maximum J/S set at 15 dB, and maximum J/S set at 25 dB.
The study suggests that receivers react differently to jamming due to their internal processes and filtering mechanisms, which supports the findings of [23]. The lowest receiver receives a position fix 16 percent of the time with a maximum error of 129 metres when the J/S is 25 dB, whereas the best receiver gets a position fix 100% of the time with a maximum error of 16 metres.

2.4.3 Carrier-to-Noise Density Ratio

The C/N0 has been the subject of several investigations since it is a quality measure at the receiver.
[26] used a multi-frequency Ipex software GNSS receiver and a 0.1 mW (40 dBW) jammer to transmit a chirp signal with a bandwidth of 11.8 MHz in the L1 band in an open-field test in Germany. The jammer is classified as broadband interference and approaches the receiver from a distance of 1200 metres away. The C/N0 values are shown against the theoretical effective C/N0 in Figure 2.6.

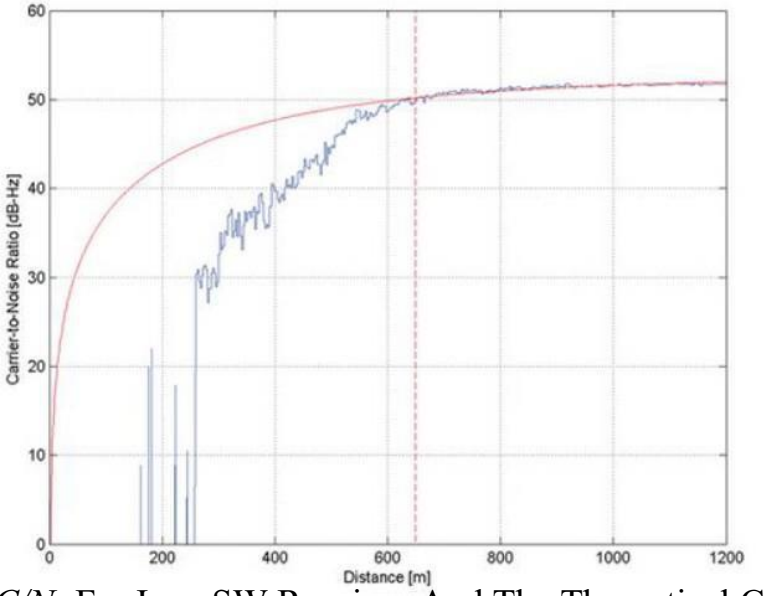


Figure 2.6: C/N_0 For Ipex SW Receiver And The Theoretical Curve [26]

Until the front end gets saturated, which happens about 650 metres, the theoretical and observed numbers coincide. Prior to saturation, the correlation process is degraded by boosting the noise level, resulting in a position inaccuracy of more than 50 metres right before the receiver loses track, as illustrated in Figure 2.7.

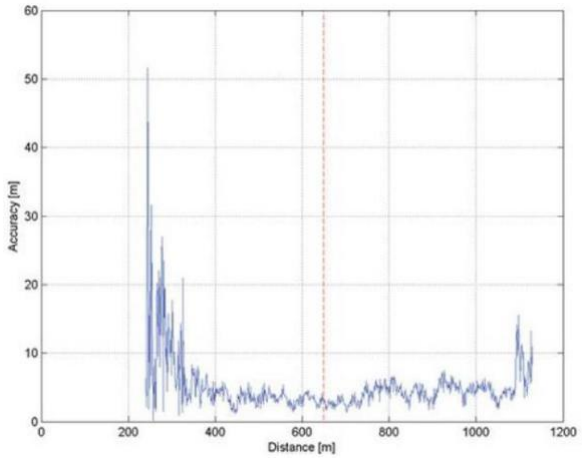


Figure 2.7: Accuracy For Ipex SW Receiver [26]

"When the front-end analogue to digital converter (ADC) is saturated, it induces significant deterioration of the signal that exceeds the pure degradation produced by increased jammer strength till signal lock loss" [26], according to the authors.
Other tests have been carried out on survey grade and mass-market receivers, and it has been discovered that when compared to the professional receiver, the professional one is interfered at a shorter distance but loses lock on the signal earlier, proving once again that the jammer's interference range is highly dependent on the receiver architecture.
Another research concentrating on the C/N0 and assessing interference outside of the L1 GPS frequency was published in [11]. The C/N0 is used to test the commercially available GPS receiver's immunity to various interference sources for the GPS L1 C/A signal. A CW signal and a broad-band Additive White Gaussian Noise (AWGN) signal (48 MHz bandwidth) both centred on the GPS L1 frequency; a Global System for UAV Communications (GSM) signal centred at 900 MHz, a Digital Enhanced Cordless Telecommunications (DECT) signal centred at 1900 MHz, and a Long Term Evolution (LTE) signal both centred at 1900 MHz, all outside the L1 frequency.

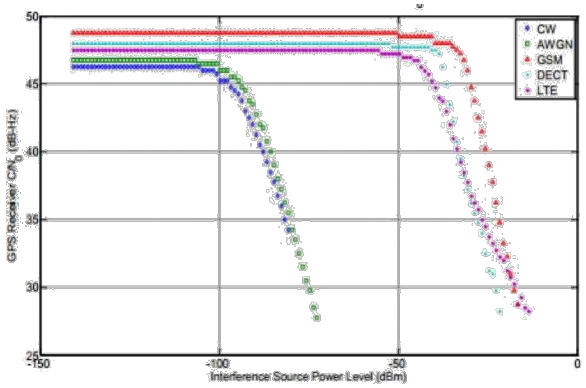


Figure 2.8: C/N_0 As Function Of Interference Power Level [11]

The C/N0 of the receiver changes with each interference source, as shown in Figure 2.8. In-band jamming sources, as predicted, produce more disturbance than out-band jamming sources. To impair the receiver's performance, the out-band sources must be much greater. The CW interference causes the receiver to lose lock first between the in-band sources, followed by the AWGN wideband noise with the same C/N0. The utilisation of numerous GNSS frequencies is considered to give jamming protection since the deliberate source that is focused at a single band will likely be less noticeable with neighbouring GNSS frequency bands.

2.4.4 Conclusions

According to the stated study on GPS jamming, it is quite simple to jam a civilian GNSS receiver across long distances. Jammers are widely accessible, and the vast majority of them cause broadband interference [12] [13].
The signal parameters of various GNSS jammers have been investigated and their influence on receivers has been assessed using GNSS simulators in several research
[25] [27]. There have also been real-world outside GPS jamming tests [23] [26]. The outcomes of these research show that GPS receivers are prone to jamming due to the combination of high sensitivity GPS devices and low signal strength from satellites. It is also determined that studying C/N0 under jamming situations makes sense because it is a critical quality indicator. When the receiver is in tracking mode, the C/N0 ratios are the focus of the investigations [11] [26]. During the acquisition phase, it would have been interesting to investigate the C/N0 ratio.

2.5 Research On GPS Spoofing Using Hardware

Spoofing is a far more elegant assault than jamming because if numerous receivers suddenly fail to lock on to the same signal, suspicions are aroused and countermeasures may be implemented before additional harm is done. Spoofing, on the other hand, can go unnoticed since the navigation system will not detect anything wrong until it is too late.

2.5.1 Spoofing A Truck

In the research conducted a simple demonstration showing GPS is prone to spoofing. A GPS Satellite Simulator, which can spoof and redirect a target cargo truck equipped with a GPS receiver, is rented for about $1,000 per week in an attempt to create a hijacking scenario in which an attack truck equipped with the GPS simulator attempts to spoof and redirect a target cargo truck equipped with a GPS receiver.

The assault is split down into three primary steps: first, the GPS receiver signal lock must be broken, which may be done with a GPS jammer or by waiting for the vehicle to pass over an impediment such as a bridge or tunnel. Second, the target truck must lock into the spoof signal, which is accomplished by approaching the truck and waiting for the truck's GPS tracking unit to latch onto the counterfeit signal. Finally, in order to retain the lock, the assault vehicle must continue to broadcast the bogus GPS signal and remain near to the target truck.

The authors believe that spoofing may occur over a wider distance with a louder signal or signal amplifiers, and that civilian GPS is subject to simple spoofing techniques that nearly anybody can use. They also recommend upgrading the clocks in GPS receivers as a low-cost countermeasure.

2.5.2 Spoofing A Drone

Another experiment was carried out in [29], this time utilising a sophisticated GPS spoofer to demonstrate a successful over-the-air spoofing assault against an unmanned aerial vehicle (UAV), as shown in Figure 2.9. The spoofer captures the drone's navigation system by transmitting synthetic GPS signals from a distance of about 620 metres. The intercepted GPS receiver is then used to deceive the UAV

with fake location and velocity solutions, which are only terminated when a safety pilot takes over manual control of the aircraft. Figure 2.9: The Hornet Mini UAV
The primary takeaways from this experiment are that a GPS spoofer may change a UAV's impression of its location from a long distance away, and that GPS receivers are unable to recognise when the PVT solution is being rewritten. Because the spoofer does not know the UAV's real-time current position and velocity, the experiment's one drawback is that long-term control of the UAV was not established.

2.5.3 Conclusions

The published research on GPS spoofing indicates that, while obtaining or building a GPS simulator to employ in a spoofing attack is an expensive and complicated procedure, once successful, most GPS receivers have no genuine defence measures in place to prevent or even detect these attacks. [28] and [29] conducted studies that created a hijacking scenario employing GPS-dependent vehicles and drones, highlighting GPS spoofing as a potential hazard.
More research and finances must be dedicated to developing and testing viable and effective countermeasures.

2.6 GPS Jamming And Spoofing On A Software View

On a hardware level, the most costly jammers on the market can only jam a single frequency that has been programmed. It is not feasible to examine or design the equipment to operate at a different frequency, limiting its usage not only by its configuration but also by its single frequency of operation. Having jamming equipment that can be examined, evaluated, and adapted to adapt to different frequencies opens up a whole new world of possibilities, allowing the GPS and all other major technologies like as GSM, UMTS, and LTE to be attacked with the same piece of equipment.
Spoofing frequently necessitates the use of a sophisticated and costly GPS simulator, which can cost thousands of dollars. The process of recreating the complete GPS signal has been a difficult one that has only been attempted by professionals and experienced users. The GPS signal may now be simulated in open source projects and generated using SDR equipment, lowering the attack's cost and making it much easier to carry out.
A SDR device is described as one that has a broad frequency range and is not tuned to a single frequency. With so many SDR items on the market in recent years, a

roundup is required to choose the finest SDR equipment for the tests to be conducted. The decision is between three HackRF One, the BladeRF, and the USRP B200/B210, which are depicted in Figure 2.10a, Figure 2.10b, and Figure 2.10c, respectively, after examining several SDRs according to cost, frequency range, ADC resolution, and capacity of broadcasting or receiving signals.

(a) HackRF One (b) BladeRF (c) USRP B200/B210

Figure 2.10: SDR Equipment

The HackRF One is the most affordable of the three, and it was one of the first low-cost SDRs to hit the market, with a price tag of roughly 250 euros. It has the ability to both receive and transmit data. It's a half-duplex transceiver, which means you'll have to switch modes manually. Its key advantages include its ability to transport data, as well as its large bandwidth and frequency range (1 MHz to 6 GHz). The only drawbacks are its low 8-bit resolution and poor RF architecture, both of which have an impact on signal-to-noise ratio (SNR) performance.

Another powerful transceiver SDR is the BladeRF. It is more costly than the HackRF, with two variants costing roughly 355 euros and 550 euros respectively, but it can work in full duplex, meaning it can receive and send data at the same time. In comparison to the HackRF, it has a narrower frequency range (300 MHz to 3.8 GHz) but a higher ADC resolution. The 12 bit ADC makes it a better receiver than HackRF, but it misses out on frequencies below 300 MHz, which may be received for an additional cost with a transverter.

The USRP B200/B210 is the most costly of the three, with two other models costing roughly 570 and 930 euros. It's regarded as a more advanced SDR geared towards the professional and research markets. It supports full duplex transmission and reception of two signals at the same time and has the same ADC resolution as the BladeRF. It has a wider frequency range (70 MHz to 6 GHz) than the BladeRF, however it misses out on frequencies below 70 MHz.

The HackRF One is the recommended SDR equipment based on cost and information accessible on the internet. It is the cheapest, gives the widest frequency range, and has superior assistance for beginners. In Chapter 3, the HackRF One is explained and studied in depth.

CHAPTER 3 HACKRF ONE AND SDR IN GNU RADIO

The HackRF One, its specs, and how it may be used as a test equipment for RF systems when combined with SDR in GNU Radio are all covered in length in this chapter. Finally, the HackRF One is demonstrated in action in a case study.

3.1 HackRF One Main Description

"Great Scott Gadgets' HackRF One is a Software Defined Radio peripheral that can transmit or receive radio signals at frequencies ranging from 1 MHz to 6 GHz. HackRF One is an open source hardware platform that may be used as a USB peripheral or configured for stand-alone operation to enable testing and development of contemporary and next generation radio technologies "[number 30]

To comprehend the HackRF One's features, which are shown in Table 3.1, and how to utilise them, a basic understanding of the device's buttons, LEDs, and ports is required. The front and rear views of the HackRF One are shown in Figures 3.1a and 3.1b, respectively.

• 1 MHz to 6 GHz operating frequency	• SMA female antenna connector
• half-duplex transceiver	• SMA female clock input and output for synchronization
• up to 20 million samples per second	• convenient buttons for programming
• 8-bit quadrature samples (8-bit I and 8-bit Q)	• internal pin headers for expansion
• compatible with GNU Radio, SDR, and more	• Hi-Speed USB 2.0
• software-configurable RX and TX gain and baseband filter	• USB-powered
• software-controlled antenna port power (50 mA at 3.3 V)	• open source hardware

Table 3.1: HackRF One Features

(a) Front View (b) Back View

Figure 3.1: HackRF One View

Three separate power supply are used by the HackRF: 3V3, 1V8, and RF LEDs. When receiving or sending a signal, they should all be turned on. If they're not all turned on, there's something wrong.

The HackRF One has been setup as a USB device by the host computer, as indicated by the USB LED.

The first three LEDs should turn on very fast once the HackRF One is connected via USB, followed by the USB LED.

The RX and TX LEDs, which stand for receive and transmit operations, respectively, are the final two LEDs on the board. If the HackRF One is receiving or emitting a radio signal, one of them should be on that.

The RESET button on the HackRF One reboots the microcontroller. It's also possible to accomplish this by disconnecting and replugging the USB power source. It's just that pressing the button is faster and easier.

The DFU button is used to enter firmware update mode, however it is seldom used because HackRF can update its own firmware without entering DFU mode. The HackRF One has a DFU mode so that it may be recovered if a firmware upgrade goes wrong and it stops operating properly. Hold down the DFU button when the HackRF One is plugged in or the RESET button is held and released to enter DFU mode.

SMA connections are used for the ANTENNA, CLKIN, and CLKOUT ports. The antenna port can also be referred to as an RF port since it can be used to connect an antenna or a cable to other RF devices.

The ANT 500, as shown in Figure 3.2, was chosen as the antenna to use with the HackRF One because it is a basic telescopic antenna that can function over a wide variety of frequencies and has a SMA male connector that allows it to connect directly to the HackRF One without any adapters.

Figure 3.2: ANT 500

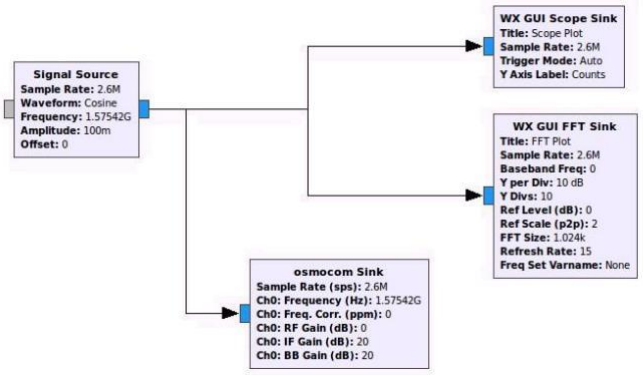
The clock in and clock out connectors are used to synchronise the clocks of several HackRF Ones or of a single HackRF One with an external clock source. A SMA cable may be connected to one HackRF One's clock out port and another HackRF One's clock in port to synchronise both clocks, or a 10 MHz square wave signal can be attached to the clock in port to have the HackRF One automatically synchronise with that external clock. The signal should range from 0 to 3.3 V.
Because just one HackRF One is utilised in the trials, these ports have not been used.

3.2 SDR In GNU Radio

SDR is a radio communication system in which components that would normally be implemented in hardware are instead implemented in software.
Digital Signal Processing (DSP) is used to process radio waveforms. An analogue signal, such as radio waves or sound waves, is a continuous variation function across time. In a horizontal axis, a digital signal is made up of discrete values at discrete places. The horizontal axis in SDR is frequently a time domain.
A software radio peripheral digitises radio waves in the same way as a sound card digitises audio waveforms in a computer. It's essentially a high-speed sound card with an antenna in place of the speaker and microphone. The HackRF One is an all-in-one SDR that fits into a compact enclosure that's about the size of a cell phone.
A sampler or an ADC in HackRF One takes an analogue waveform, samples or measures it over a discrete period of time, and then returns the value at each sample point. A digital signal is a series of numbers, each of which is a sample.
GNU Radio is a free and open-source software development toolkit that includes signal processing blocks that may be used to create software radios. It may be used to develop software-defined radios with easily accessible low-cost external RF gear, or in a simulation-like environment without hardware.
The GNU Radio programme [31] offers the foundation and tools necessary to create and execute software radio or other signal-processing applications. The

capacity to reconfigure the system, like with other SDR systems, is a major feature. Instead of requiring separate radios for different applications, a single general-purpose radio can be utilised as the radio front-end, with signal-processing software handling the application-specific processing.

GNU Radio Companion is a GNU Radio front-end graphical interface. It's a programme that generates python programmes, which are software radio programmes, automatically. The GNU Radio apps are flow graphs, which are a collection of signal processing components linked together.Figure 3.3: GNU Radio



Flow Graph

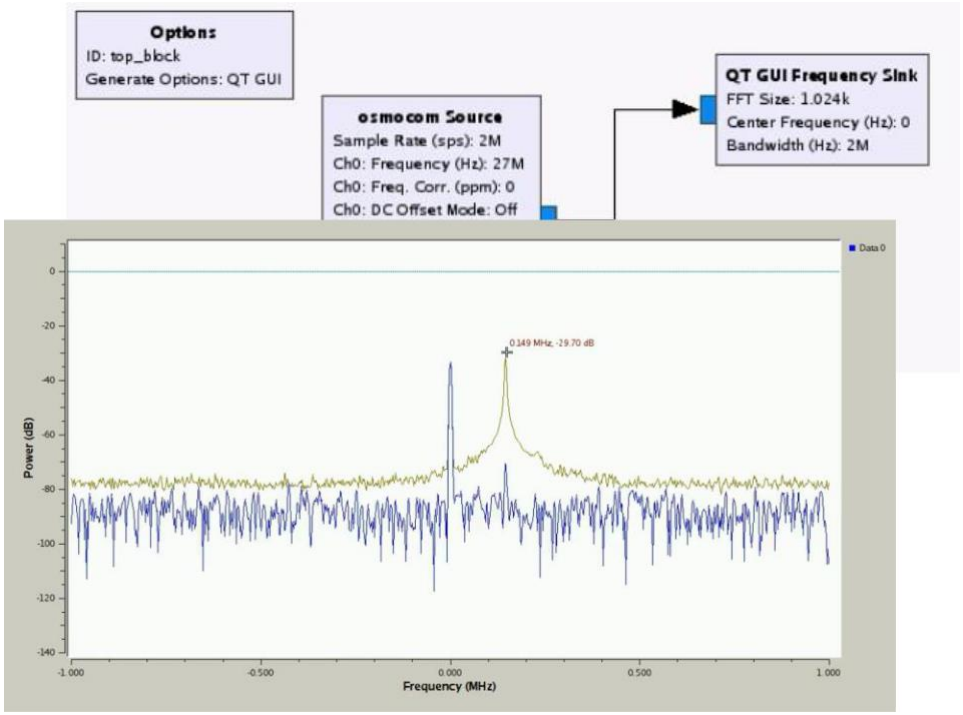
C++ or Python are two computer languages that may be used to create flow graphs. Figure 3.3 is only a visual representation of such flow graphs. Many of the user tools are written in Python, while the GNU Radio infrastructure is built fully in C++.

3.3 Case Study

This is an example of a capture and playback utilising the HackRF One with a radio-controlled vehicle as the target device. Michael Ossmann, the developer of the HackRF One [32], carried out this experiment. A signal is sent from its initial transmitter and is collected in order to repeat it and check if the automobile replies. A signal must first be collected in order to be replayed. To receive a signal from the remote control, a flow graph is established, as illustrated in Figure 3. 4 The sample rate is set to 2 million samples per second, which is the minimum suggested for use with the HackRF One.

The frequency on the osmocom source is set to 27 MHz, which corresponds to the operating frequency on the R/C car's label. The RF gain is set to 0 dB, but the IF

band and BB (baseband) gain are both set to 16 dB, which is a reasonable starting point. The rest of the parameters are left at their default settings.The QT GUI Frequency Sink displays a frequency domain view and allows you to determine the frequency of operation of a remote control.
Figure 3.4: Receiving A Signal From The Remote Control.



When the remote control is used to move the automobile, the QT GUI Frequency Sink shows a peak approximately 150 MHz above the 27 MHz when max hold is enabled, as illustrated in Figure 3.5. The frequency of operation of the radio-controlled (R/C) automobile has been determined. Figure 3.5: QT GUI Frequency Sink

A file sink is now linked to the osmocom source in order to preserve this waveform for future replay. This is a raw digital waveform; it is the information saved straight to a file from the HackRF One. The flow graph is still running, but now that the automobile is being moved using the remote control, the waveform is being stored to a file, as seen in Figure 3.6.

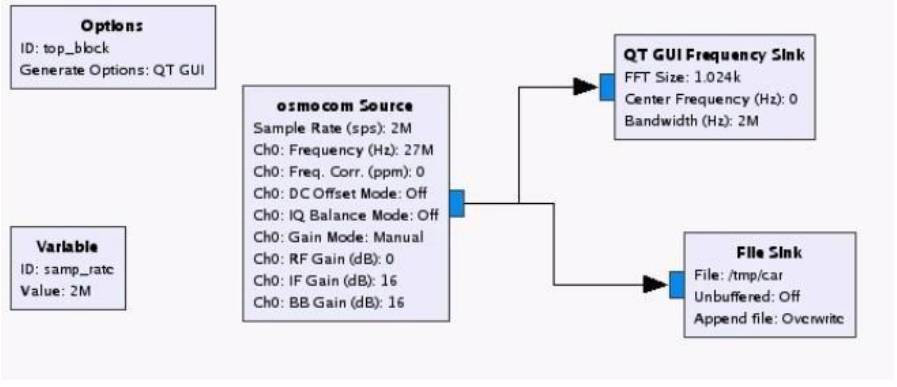


Figure 3.6: Saving The Waveform To A File

A new flow graph has to be established in order to repeat this waveform. As illustrated in Figure 3.7, instead of a file sink, a file source is now used to refer to the waveform file that was produced previously.
The flow graph's sample rate should be set to the same sample rate used for the capture, which is 2 million samples per second, for the rules to be right on the frequency and for it to perform at the same pace as real-time.

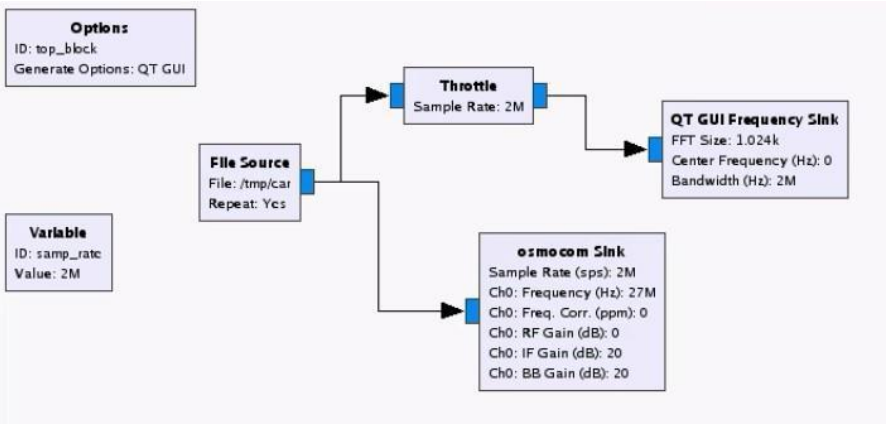
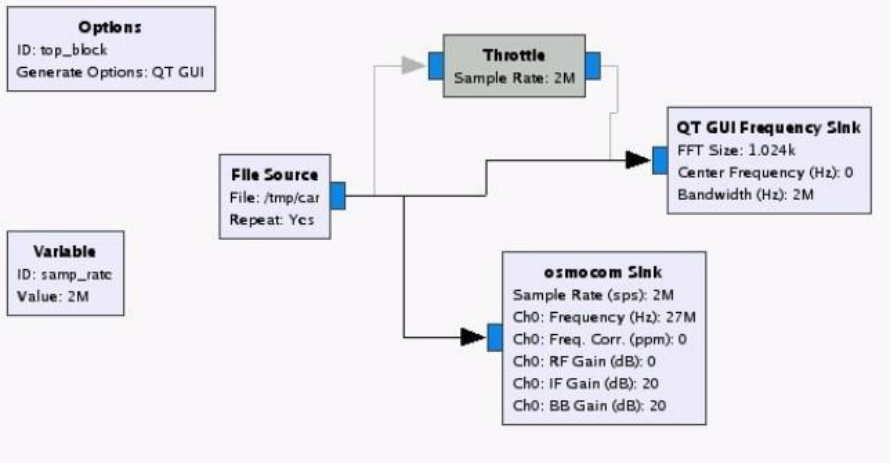


Figure 3.7: Replaying The Saved Waveform

The file source is linked to a QT GUI Frequency Sink. A throttle to the selected sample rate would be ideal. When the flow graph is not restricted by external hardware, GNU Radio will not consume entire CPU resources. The throttle block can be deactivated since an osmocom sink, which refers to the HackRF One, is required to replay this file, as illustrated in Figure 3.8. There will be a two clock



issue if there is a throttle in between.
Figure 3.8: Throttle Block Disabled

The CPU will not crash since the Frequency Sink will not be quicker than the osmocom sink because they will both be pulling data from the same file source, therefore the data will flow at the same pace to both of them.
If you run the flow graph this way, it will look exactly like Figure 3.5, except the file source will keep being repeated because it is the default value for a file source. The osmocom sink's frequency is set to 27 MHz, which is the same as the signal's capture frequency. Change the RF gain to 0 dB. When you're in transmit mode, the IF and BB gains are slightly different. Because there is no baseband amplifier on the HackRF One's broadcast line, just on the receive path, the BB gain makes no effect at all. The default IF gain of 20 dB, which is about in the middle of the gain range, can be used.
If the flow graph is performed at this point, the signal should be replayed, the R/C vehicle should be transmitted over the air, and the car should drive, however this does not happen. The first suspicion is that the signal is not being broadcast at a sufficiently high power level.

The IF gain is then increased to 47 dB, which is the highest value that may be employed and is 27 dB higher than the prior value. The same thing occurs: the automobile does not move.

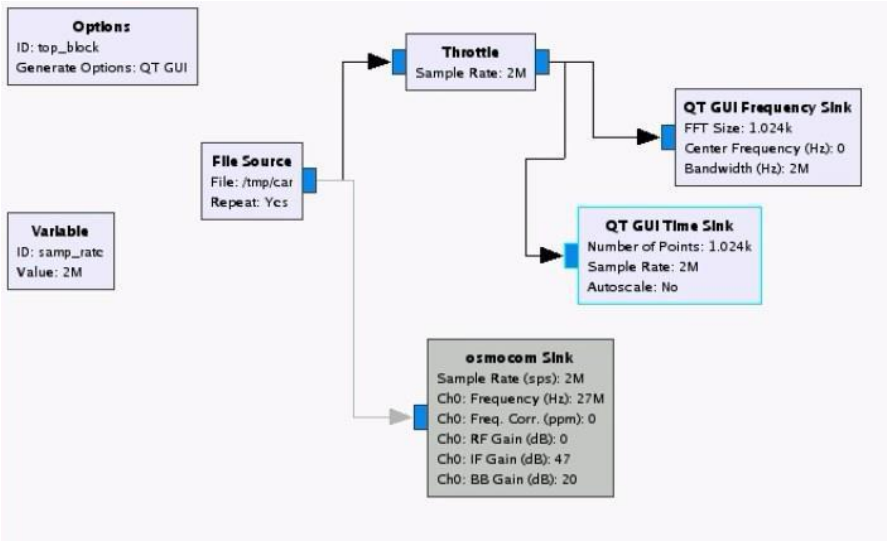


Figure 3.9: QT GUI Time Sink

One of the advantages of having a cached waveform is that we can use the same test vector every time. Every time the data is read from this file, everything should be the same. A QT GUI Time Sink, which provides a time domain view, is linked to test what could be wrong. The throttle is re-enabled, and the file source is now connected to both the frequency and time sinks. For the time being, the osmocom sink is switched off, as illustrated in Figure 3.9.

Figure 3.10 illustrates a noticeable offset from 0 to 0.1 when zooming the time view and stopping while there are no bursts of activity, which is an explanation for the 0 Hz spike in the midst of the frequency domain view. There is always a component of the signal that is a tiny bit off from 0, which is totally typical with a receiver like the HackRF One.

When stopping between bursts of activity, the visual signal is also quite faint, barely distinguishable from the background noise.

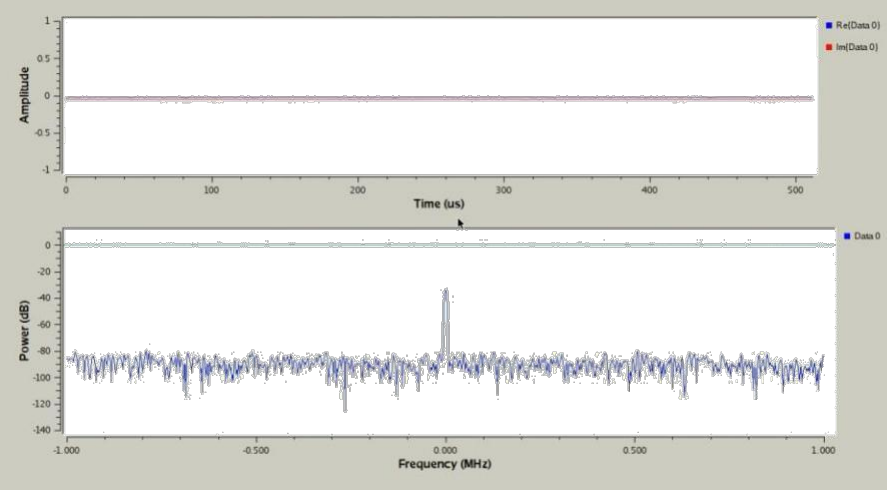


Figure 3.10: Background Noise

As demonstrated in Figure 3.11, the amplitude of this transmission only varies between around 0.1 and 0.15. The greatest amplitude is really tiny.

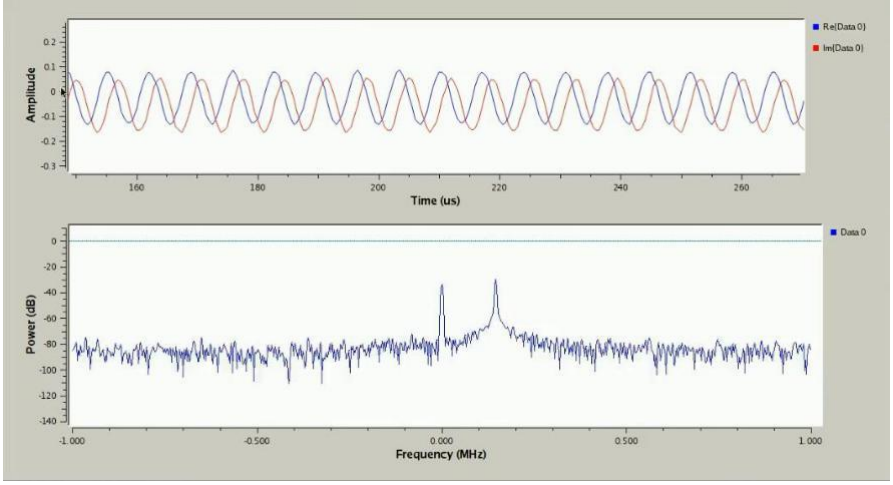


Figure 3.11: Burst Of Activity

Because when the osmocom source gets information from the HackRF One, it scales and assigns 8-bit data as floating point values between 1 and 1, the predicted scale of the amplitude is between 1 and 1. As a result, just a tiny percentage of the dynamic range is utilised.

The answer could be to enhance the signal in the digital domain before sending the waveform to the HackRF One. Multiplying samples allows them to be scaled. As illustrated in Figure 3.12, a math operator named Multiply Const is linked between the file source and the throttle block, with the value of 6.

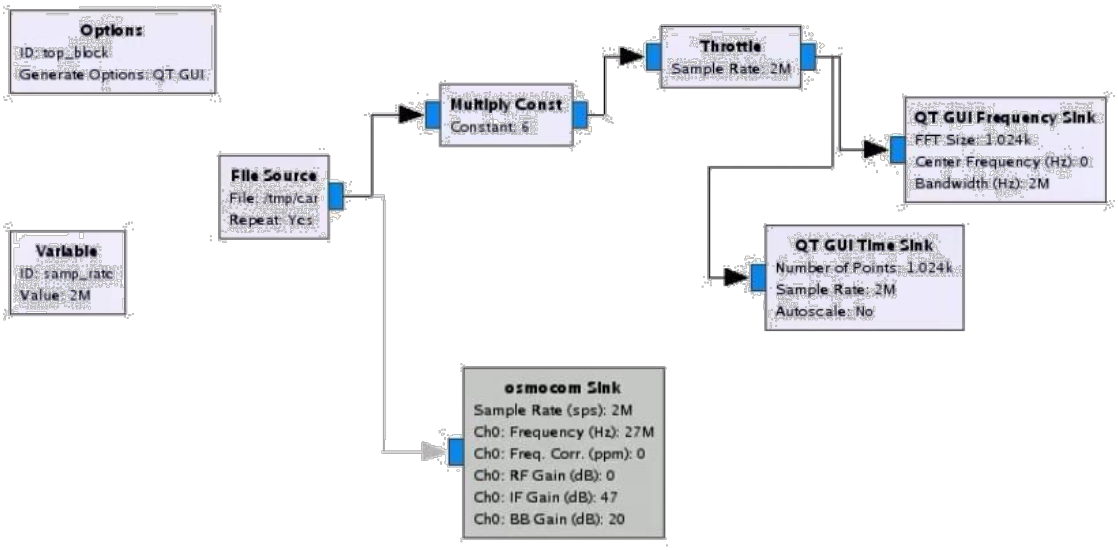


Figure 3.12: Multiply Const

The flow graph is performed again, as illustrated in Figure 3.13, and the transmission signal now differs. Its amplitude ranges between 0.5 and 1. This is a technique for amplifying a signal in the digital realm before converting it to analogue.

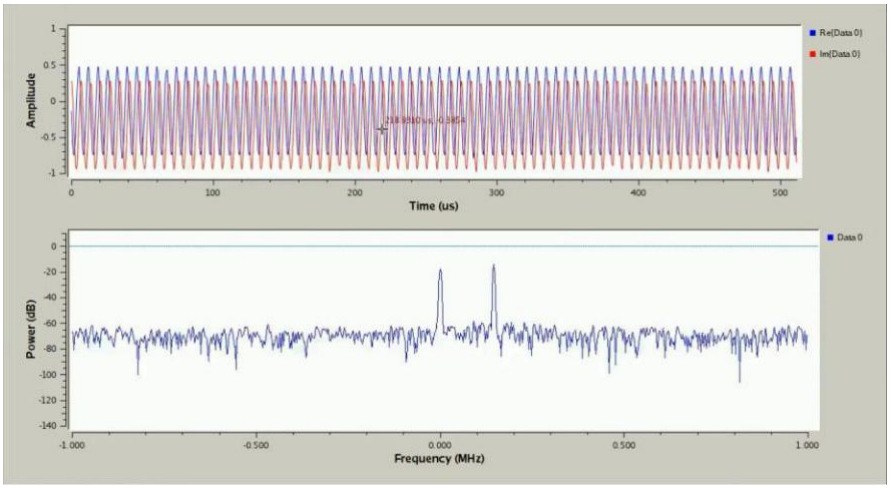


Figure 3.13: Amplified Signal

Finally, as shown in Figure 3.14, the osmocom sink is switched back on, and the waveform file is transmitted via this revised flow graph, with the Multiply Const also connected to the osmocom sink.

Now, the HackRF One imitates the remote control and R/C vehicle, moving in the exact same manner as when the file was created, and repeating the same set of actions while the flow graph is running.

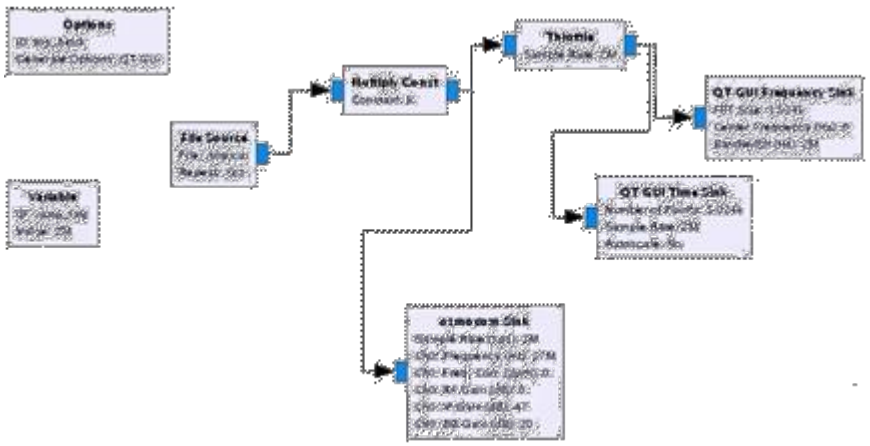


Figure 3.14: Transmitting The Amplified Signal

This case study indicates that by employing SDR equipment, in this case a HackRF One, any radio signal broadcast by a device, such as a remote control or a vehicle key, may be captured and replayed, allowing the HackRF One to masquerade as the device itself and fool the receiving equipment..

CHAPTER 4 EXPERIMENTS AND RESULTS

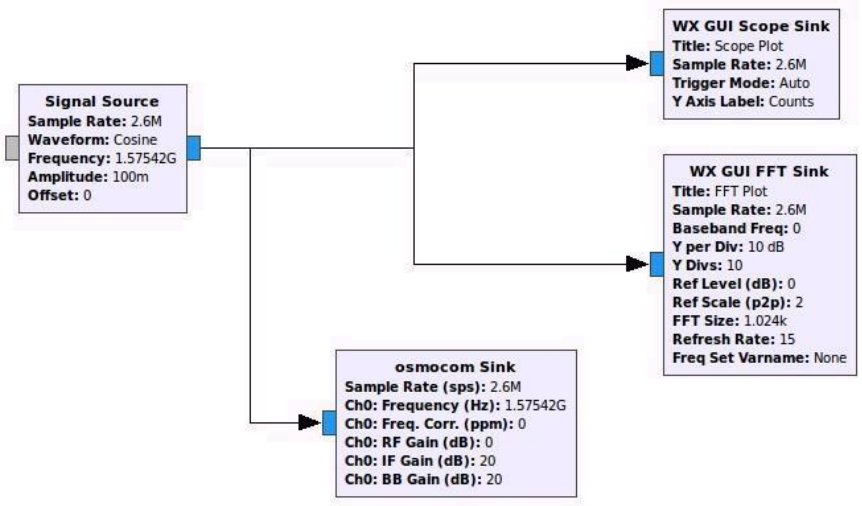
This chapter details all of the tests carried out with the HackRF One, GNU Radio's SDR, and a smartphone as a test subject with the goal of interrupting the GPS signal. It is separated into two sections, the first of which was designed to determine which signal waveform had the most impact on the GPS signal. The second component sought to do GPS spoofing, which is an effort to mislead the phone's GPS by sending false GPS signals. After then, the data was examined and a report was written.

4.1 GPS Jamming

The HackRF One was used in this experiment to send a signal developed in GNU Radio Companion in order to jam the GPS signal in a UAV. The waveforms that were put to the test were cosine, square, triangle, and saw-tooth. In addition, an additive white gaussian noise (AWGN) is investigated. The starting amplitude value for each waveform is 0.1, and it continues to be raised by 0.1, increasing the signal's power gain as well, until the GPS signal is jammed.

4.1.1 Flow Graph

Figure 4.1 shows the flow graph constructed to simulate a signal being transferred over the HackRF One.
The sampling rate, which is and should be the same throughout the flow graph, is defined by the variable block. It has a sampling rate of 2.6 million per second. When a flow graph is formed, this block is automatically produced. The signal source



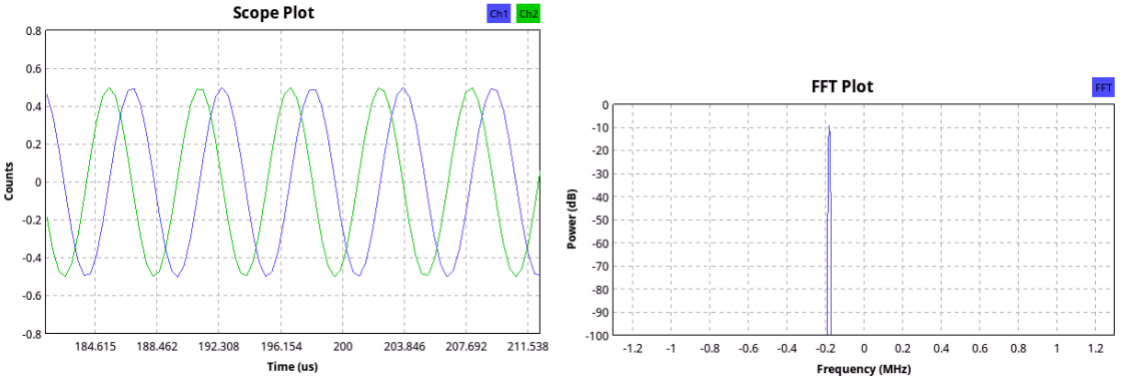
block works in the same way as a waveform generator does. As multiple waveforms are examined, the waveform parameter takes on distinct shapes. The frequency is 1.57542 GHz, which is the same as the L1 GPS frequency. During the testing, the amplitude also takes on varied levels. The offset is kept at a value of 0 by default.Figure

4.1: Signal Transmission Flow Graph

The osmocom sink allows the HackRF to communicate with the flow graph that remains. The frequency of the channel is the same as the frequency of the signal source. At 0 dB, the RF gain is set. The rest of the settings are left as they are.
The WX GUI Scope Sink and WX FFT Sink are linked, allowing you to see what's being sent. The WX GUI Scope Sink displays the signal in the time domain, whereas the WX FFT Sink displays the signal in the frequency domain. The default settings are used for all of their parameters.

4.1.2 Cosine Waveform

The output is a cosine wave with a peak amplitude specified by the amplitude parameter and an average value set by the offset parameter when the cosine waveform is selected on the signal source block.



(a) Scope Plot (b) FFT Plot

Figure 4.2: Cosine Waveform

The Scope Plot of the cosine waveform is shown in Figure 4.2a, and the FFT Plot is shown in Figure 4.2b. When the amplitude is set to 0.5, the FFT plot reveals a single spike of roughly 9 dB.

4.1.3 Square Waveform

The output is a square wave with peak-to-peak amplitude determined by the amplitude parameter and the average value set by the offset plus amplitude/2 when the square waveform is selected on the signal source block. The imaginary signal in the complex situation is essentially another square wave that has been moved by ninety degrees.

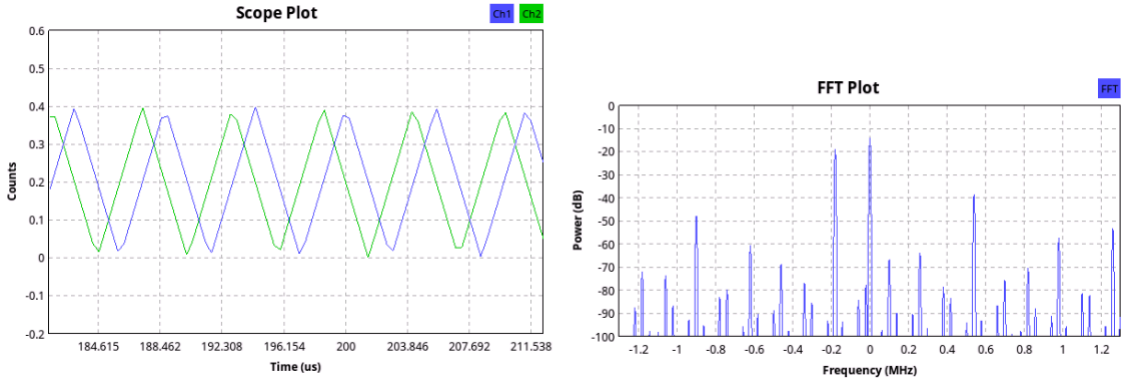
Figure 4.3a depicts the square waveform's Scope Plot, whereas Figure 4.3b depicts the FFT Plot. There are other spikes, but only two are noticeable, each with a power of over 16 dB and an amplitude of 0.3.

4.1.4 Triangle Waveform

The output of the triangle waveform on the signal source block is a triangle wave with the amplitude parameter controlling peak-to-peak amplitude and the offset plus amplitude/2 controlling the average value. The imaginary signal in the complex situation is essentially another triangle wave with a ninety-degree shift.

(a) Scope Plot (b) FFT Plot

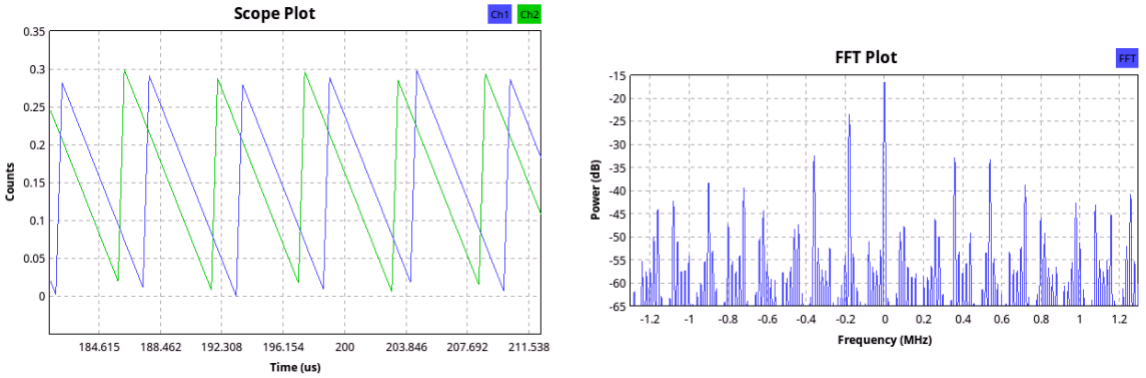
Figure 4.4: Triangle Waveform



The triangle waveform's Scope Plot is shown in Figure 4.4a, and the FFT Plot is shown in Figure 4.4b. When employing an amplitude of 0.4, the upper spike has power of about 14 dB.

4.1.5 Saw Tooth Waveform

The output is a positive-going saw tooth wave with peak-to-peak amplitude determined by the amplitude parameter and the average value set by the offset plus amplitude/2 when the saw tooth waveform is selected on the signal source block. The imaginary signal in the complex situation is essentially another saw tooth wave that has been moved by ninety degrees.



(a) Scope Plot (b) FFT Plot

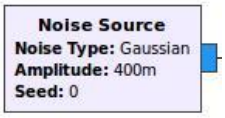
Figure 4.5: Saw Tooth Waveform

The saw tooth waveform's Scope Plot is shown in Figure 4.5a, and the FFT Plot is shown in Figure 4.5b. When an amplitude of 0.3 is used, one spike highlights with a power of 16 dB.

4.1.6 Additive White Gaussian Noise

As illustrated in Figure 4.6, the signal source block is replaced with a noise source block with the noise type set to gaussian, resulting in a gaussian distribution.

Figure 4.6: Noise Source Block



The AWGN's Scope Plot and FFT Plot are depicted in Figures 4.7a and 4.7b, respectively. When employing an amplitude of 0.3, the average power gain is roughly 45 dB.

4.1.7 Results

The waveforms with various amplitudes that were examined are shown in Table 4.1. The check indicates that the GPS signal was jammed, but the cross shows that it was not. When the frequency spans from 10 MHz to 2150 MHz, the HackRF One has a maximum transmit power of 15 dBm. The gain determined by the signal source or AWGN is added to the total transmitted power.

Only until the power increase of the cosine waveform reaches 9 dB is it able to jam the UAV's GPS. With a power gain of 16 dB, the square and saw tooth waveforms can jam it, whereas the triangle waveform can only jam it with a power gain of 14 dB. With a power increase of 45 dB, the AWGN can jam the GPS on a UAV, making it the one that requires the least amount of power gain to achieve the desired result. Table 4.1: Different Waveforms And Amplitudes

Amplitude	Cosine		Square		Triangle		Saw Tooth		White Gaussian Noise	
0.1	-23 dB	✗	-26 dB	✗	-26 dB	✗	-26 dB	✗	-55 dB	✗
0.2	-18 dB	✗	-20 dB	✗	-20 dB	✗	-20 dB	✗	-50 dB	✗
0.3	-14 dB	✗	-16 dB	✓	-16 dB	✗	-16 dB	✓	-45 dB	✓
0.4	-11 dB	✗			-14 dB	✓				
0.5	-9 dB	✓								

Table 4.1 displays the sum of the HackRF One transmit power and the power gain, as well as the conversion of the total transmitted power from dBm to watts for each signal source and the AWGN. Equation 4.1 is used to convert power from dBm to watts.

$$P\,(W) = 1W \times 10^{(P(dBm)/10)}/1000 \quad (4.1)$$

The cosine waveform requires the most power to jam the GPS signal in the UAV, whilst the AWGN requires the least.

Waveforms	HackRF One TX Power (dBm)	Waveform Power Gain (dB)	Total TX Power (dBm)	Total TX Power (mW)
Cosine	15	-9	6	3.98
Square		-16	-1	0.794
Triangle		-14	1	1.26
Saw Tooth		-16	-1	0.794
AWGN		-45	-30	0.001

Table 4.2: Total Transmitted Power

CHAPTER 5 CONCLUSIONS AND FUTURE WORK

5.1 Conclusions

The HackRF One, or any other SDR capable of sending and receiving signals, may be used to capture and replay a radio signal, according to this research. This technology allows malevolent individuals to take advantage of the numerous RF applications available. Because the SDR equipment can replicate the identical radio signal that is being carried across the air to the receiving equipment, assaults like unlocking a car or disabling an alarm system become simple to carry out. To eliminate these hazards, countermeasures must be put in place.Software Defined Radio has emerged as a means of bridging the gap between so-called hackers and ordinary users with harmful intent. What used to be a subject of complicated radio comprehension and hardware expertise is now a question of a relatively simple research process, a grasp of DSP, and SDR software frameworks. This research also indicated that when SDR is used, GPS becomes a much more sensitive signal, answering all of the problems posed in Chapter 1. GPS jamming has always been a very simple assault to carry out, and now, thanks to the usage of SDR, it has been proved that it is just as simple and, significantly, less expensive. The white gaussian noise is the ideal waveform for jamming the GPS signal, according to the reported GPS jamming experiment, since it requires the least amount of power and amplitude. The antenna's characteristics hampered the attack's efficiency because the range between the HackRF One and the UAV had to be kept small. Without SDR, GPS spoofing is impossible due to the numerous hurdles involved in producing a GPS stream that will transmit a signal to a GPS receiver. It's also costly since it necessitates high-precision equipment. The GPS spoofing experiment demonstrated that it can be done simply with a relatively affordable SDR equipment and freely accessible software. The use of a single HackRF One with the GPS-SDR- SIM programme enables for GPS signal spoofing without the use of expensive gear. Because neither of these methods has been met with resistance from UAV devices, it is critical that detection and mitigation technologies be created and deployed in order to avoid or at least make these attacks more difficult.

The transmission of information between the aircraft and the ground station controller usually uses a Wi-Fi network that complies with the IEEE 802.11 standard. The specified network is vulnerable to security breaches. In particular, the lack of

encryption on the on-board chips of drones or the execution of a “man-in-the-middle” attack by an attacker makes it possible to seize control of an aircraft at a considerable distance. The unencrypted Wi-Fi used with the drone also leads to the drone being hacked. There are many solutions (such as Sky using node.js and the node-ar-drone client) that are designed to autonomously search, hack and wirelessly take full control of any other drones within wireless network or range and then create an army of zombies. drones under the control of an attacker. This threat can be prevented, for example, by using the Wi-Fi Protected Access software solution, which provides password authentication for the drone, which makes it difficult for an attacker to gain access to the drone. Let's take a look at the most typical attacks carried out against a swarm of drones that generate an open Wi-Fi connection to which multiple hosts can connect. By connecting to the drone, you can find the IP address associated with it and conduct further reconnaissance. You can use the Nmap scanning tool, which is used for network discovery and security auditing, to determine which ports are open on the drone. In the problem under consideration, a free open source utility designed to investigate and check the security of network objects will allow you to get a list of open ports on the target object. To implement a deauthentication attack, you can use Aircrack-ng, which is a set of various tools used to assess the security of a Wi-Fi network. First, a passive scan is performed to find a wireless network. Once a network is found using the airodump-ng module (included with Aircrackng), packets from only that particular wireless network can be filtered and stored. The list of clients associated with the network is then made available and a deauthentication attack can be performed. For example, using the Aireplay-ng module, which allows frame disconnect injections to connected clients with the drone's MAC address and the client's specific MAC address (if a targeted attack is performed) to disconnect them from the access point. The tool will send 128 packets for each specified deauthentication, where 64 packets will be sent to the drone and 64 to the client. It is expected that the connection between the controller and the drone will be successfully deauthenticated when aircrack-ng is run. The behavior of drones after deauthentication is more difficult to predict - some drones land, others just crash. Considering that control over the American RQ-170 was intercepted over the western border areas of Afghanistan and Eastern Iran, there is another version of what happened, associated with favorable terrain. Eastern Iran is replete with many mountain ranges with peaks from 2800 to 4000 meters, and the deployment of GPS spoofers in this area increases by several tens of times the likelihood of successful suppression of the GPS satellite channel by a false channel emitted directly by a spoofer with a powerful

amplifier, since the antenna of the intercepting complex is located on several kilometers closer to the enemy drone. Such an interception could be most favorable if the flight of the RQ-170 Sentinel UAV took place at an altitude of 2.5-3 km. In this case, it was enough for Iranian spoofers to be located on any mountainous hill in the eastern part of the country in order to get into the viewing area of the RQ-170 GPS antennas, after which it was possible to launch a “spoofing” attack.

To conduct an impeccable "spoofing" attack, constantly updated information with the exact coordinates of the GPS module carrier unit is required, which can be obtained thanks to modern electronic intelligence equipment, which are in service with the Islamic Republic of Iran Air Force. The simplest and most accurate of them can be considered the Kasta-2E2 radar. The station operates in the decimeter range, and is capable of detecting and tracking small air targets, including UAVs, with an accuracy of up to 100 m. This is quite enough to reliably identify such a large drone as the RQ-170 Sentinel. When the radar sets up the target’s track, and “packets” of data with a changing real location of the target enter the operator’s room of the “spoofing” complex with short breaks, the first stage of the attack begins - exposure of the drone to a slightly more powerful spoofer GPS signal with the correct “packet” of coordinates targets received by the radar. Then, the electronic warfare operators, using a software “spoofing” algorithm, gradually reject the flight path of the enemy’s unmanned vehicle set by the satellite, turning it from an autonomous into a guided air “tool”, with which you can do almost everything, up to turning into a kamikaze drone, but only only within the scope of the “spoofing” complex (Iran does not yet have its own satellite navigation constellation).

It is also worth noting here that the Russian 1L222 Avtobaza electronic intelligence systems purchased for the needs of the Iranian Air Force, from a technical point of view, cannot be used to suppress and “hack” the RQ-170 Sentinel GPS channel, since Avtobaza is passive means of RTR. Moreover, 1L222 cannot be used as a tool for analyzing "packets" of data from the GPS satellite constellation, since its receiver covers only the centimeter frequency range from 8 to 17.544 GHz. The Avtobaza complex is designed for direction finding of X-/J- and Ka-band airborne tactical aviation radars, radio altimeters of the Tomahawk TFR and other high-precision missile weapons flying in the terrain envelope mode, as well as active radar seeker of air-to-ship missiles / ground "and air combat missiles of medium and long range. More logically, information

regarding the use of experienced Belarusian electronic warfare systems Naves-U, designed to jam GPS channels, may look more logical.

Other sources also weave complete nonsense, claiming that a failure in the operation of the INS and the entire avionics of the RQ-170 drone could have been created by the SNP-4 powerful noise interference stations supplied by Belarus. Pseudo-specialists have completely forgotten about the true purpose of the SNP-4 complex. Firstly, the station is designed for passive electronic reconnaissance of enemy radio-emitting multifunctional airborne radars operating in the centimeter range, as well as their further suppression at a distance of no more than 60 km. The SNP-4 station is not a heavy-duty ground-based electronic countermeasures capable of completely disrupting the stable operation of the autopilot systems of the RQ-170 Sentinel type UAV, as the Ranets-E microwave complex is capable of doing. Secondly, most of the element base of modern avionics equipment, including all loops, wiring and other components, is shielded, and is often covered with specialized radio absorbing materials to get rid of the negative impact of electronic countermeasures. And the maximum power of the SNP-4 noise interference station does not exceed 2.5 kW, which, by the standards of modern radio engineering concepts, is a “drop in the ocean”. The bottom line is this: a “spoofing” attack is the most realistic option for intercepting control over the American RQ-170 Sentinel UAV.

5.2 Future Work

Because this study only looked at GPS technology on a UAV, more research should be done to see if Software Defined Radio may be utilised to uncover the weaknesses of other technologies and equipment. On the other hand, SDR-based research for the development of detection and mitigation systems is beginning to emerge. The distance the attacking equipment can disturb the receiver would have increased if a more powerful antenna or additional amplifiers had been utilised in these studies, boosting the efficacy of the GPS jamming and spoofing. It's possible to take control of the impacted equipment, such as drones or self-driving cars, via navigational control. If additional study is done, there will be a public safety issue since mid-air collisions with other aerial vehicles or buildings, as well as driving accidents, might occur. Also, because everything is being interconnected through the internet in a process known as the Internet of Things, these security dangers are the most important factor to consider. Everything becomes a potential target for a hostile assault, from homes to

phones. It is critical to perform further study in order to better understand how to detect and combat these threats. In this work, the synthesis and analysis of the scheme for organizing the transmission of UAV information with the fulfillment of the requirements was carried out. The analysis performed showed the presence of channels of influence on the UAV control system. Various avenues of influence were considered, the purpose of which is the interception of control over UAVs, various advantages and disadvantages of each of them are revealed. It can be seen from the synthesized scheme that when developing schemes of influences on the specific implementation of the control system must take into account the susceptibility of the communication line to external attacks. An important factor in the implementation of impacts is the mutual influence of the various components of the system on each other. When organizing the impact on a specific implementation of the control system, an important factor is the availability of access to documentation. It is also necessary to take into account the presence of software vulnerabilities that can provide the possibility of organizing an undocumented control channel. When analyzing UAV security threats, it was revealed that the most vulnerable element of the UAV control system is the impact on the spatial positioning system. This is due to the large number of combinations of various actions on external UAV sensors and the fact that initially, when developing such systems, the issue of counteracting targeted malicious influence was not so acute. Based on the foregoing, it was decided to direct further research to assess the vulnerability of the spatial positioning system. В данном исследовании рассмотрены наиболее часто используемые злоумышленниками различные уязвимости, с помощью которых может быть перехвачено управление роемдронов: отказ в обслуживании, деаутентификация, человек-посередине, несанкционированный доступ с полномочиями суперпользователя и подмена пакетов. Кроме того, в статье описана возможность реализации блокировщика (БПЛА) дронов на основе контроллера Raspberry Pi, который запускает скрипты bash.

Bibliography

[1] M. Thomas, J. Norton, A. Jones, A. Hopper, N. Ward, P. Cannon, N. Ack- royd, P. Cruddace, and M. Unwin, *Global Navigation Space Systems : reliance and vulnerabilities*, 2011.
[2] S. Yarwood, "Jamming & radio interference: understanding the impact," vol. IET Sector Insights, pp. 1–6, 2012.
[3] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle, *GNSS - global nav- igation satellite systems: GPS, Glonass and more*, 1st ed. Springer-Verlag Wien, 2008.
[4] D. Borio, "A Statistical Theory for GNSS Signal Acquisition," *Dipartimento di Elettronica*, vol. Doctoral T, p. 293, 2008.
[5] R. Bingley, *Handouts Satellite Based Positioning (H24VST)*. University Nottingham, 2013.
[6] E. Kaplan and C. Hegarty, *Understanding GPS. Principles and applications.* Norwood, Massachusetts: Artech House, 2006

[7] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements and Performance*. Lincoln, Massachusetts: Ganga-Jamuna Press, 2010.
[8] D. Last, *GNSS: The Present Imperfect*. InsideGNSS, 2010.
[9] S. Pullen and G. X. Gao, *GNSS Jamming in the Name of Privacy*. InsideG- NSS, 2012.
[10] J. Volpe, *Vulnerability assessment of the transportation infrastructure relying on the global positioning system*. National Transportation Systems Center, 2001.
[11] P. Craven, R. Wong, N. Fedora, and P. Crampton, *Studying the Effects of Interference on GNSS Signals*. San Diego, California: International Technical Meeting of The Institute of Navigation, 2013.
[12] R. Mitch, R. Dougherty, M. Psiaki, S. Powell, B. O'Hanlon, J. Bhatti, and T. Humphreys, *Signal characteristics of Civil GPS Jammers*. ION GNSS 2011, 2011.
[13] T. Kraus, R. Bauernfeind, and B. Eisfeller, *Survey of In-Car Jammers – Analysis and Modelling of the RF Signals and IF Samples*. ION GNSS 2010, 2011.
[14] D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti, "Impact and Detec- tion of GNSS Jammers on Consumer Grade Satellite Navigation Receivers," *Proceedings of the IEEE*, vol. 104, pp. 1233–1245, 2016.
[15] E. Axell, F. Eklöf, M. Alexandersson, and P. Johansson, *Jamming detection in GNSS receivers: Performance evaluation of field trials*. Nashville, Tennessee: ION GNSS 2013, 2013.
[16] T. Humphreys, B. Ledvina, M. Piaski, B. O'Hanlon, and P. Kintner, *Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer*. ION GNSS 2008, 2008.
[17] M. Psiaki, S. Powell, and B. O'Hanlon, *GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data*. ION GNSS 2013, 2013.
[18] K. von Hunerbein and W. Lange, *A New Solution of Generation of Spoofing Signals for GNSS Receivers*. In Proceedings of International Symposium on Certification of Gnss Systems and Services (CERGAL), 2014.
[19]. Lolita C. Baldor. Flashy drone strikes raise status of remote pilots. The Boston Globe.
2012. URL: http://www.bostonglobe.com/news/nation/2012/08/11/air-force-works-fillneed-for-drone-pilots/ScoF70NqiiOnv3bD3smSXI/story.html
20. CNN Wire Staff. Obama says U.S. has asked Iran to return drone aircraft. 2011 URL:

http://edition.cnn.com/2011/12/12/world/meast/iran-us-drone
21 Noah Shachtman Exclusive: Virus Hits U.S. Drone Fleet. URL:
http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet
22. STANAG 4586 (NATO Standardization Agreement 4586) is a NATO Standard Interface
of the Unmanned Control System (UCS) Unmanned Aerial Vehicle (UAV). URL:
https://defense-update.com/products/s/stanag_4586.htm
23. Podins K., Stinissen J., Maybaum M., (Eds.). The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment // 5th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, 2013.
24. Borodin V.V., Petrakov A.M., Shevtsov V.A. Transfer efficiency analysis
data in the communication network of a group of unmanned aerial vehicles // Proceedings
MAI. 2015. No. 81. URL: http://www.mai.ru/science/trudy/published.php?ID=57894
25. Kornilin D.V., Kudryavtsev I.A. The study of the characteristics of navigation signals of GPS, GALILEO, GLONASS systems. - Samara: Samara Publishing House State Aerospace University, 2011. - 27 p.