Targeted GPS spoofing

July 8, 2018

Bart Hermans
Security and Network Engineering
University of Amsterdam
bart.hermans@os3.nl

Luc Gommans
Security and Network Engineering
University of Amsterdam
os3-gps@lucgommans.nl

***Abstract*—This work investigates whether it is possible to directionally spoof one GPS receiver over a distance. Spoofing GPS signals is known to work, but other GPS receivers that are in range are also affected. If the impact to other receivers can be limited, GPS spoofing could be used in a variety of applications, such as moving a drone that is blocking the landing of an air ambulance. By transmitting parts of the GPS signal from multiple geographically dispersed directional antennas, one could potentially limit the impact of the GPS spoofing attack to a single GPS receiver that would be present at the intersection of the signals. Only at the intersection of the directional signals, a GPS receiver would be able to see enough of the spoofed satellites to compute the spoofed location.**

The researchers performed a number of experiments to investigate whether this technique could be used in practice. The directional antenna used did not direct the signal sufficiently and leaked a large amount of signal on the side. Transmitting part of the signal from different antennas worked; however, due to synchronization issues, the receiver would have an error in its position of between 250 meters and 18 kilometers. A more directional antenna and more precise time synchronization are required for successful use in practice.

I. Introduction

The Global Positioning System (GPS) is a satellite-based system that provides location and time synchronization services to civilians and military. GPS-based location is used heavily in navigation equipment. Time synchronization based on GPS is a useful functionality for computer networks and the telecommunications industry[1].

Currently GPS is owned by the government of the United States of America. Operating GPS infrastructure (including the satellites) is delegated to the United States Air Force. While GPS knows a long development cycle with its first satellite being launched in 1978. GPS itself only became fully operational in 1993[2].

Almost 10 years after GPS became fully operational, spoofing GPS signals was described in academic literature. Before the spoofing vulnerability, it was already known that GPS was susceptible to jamming and blocking[3, 4].

Recently, the first maritime (unconfirmed) incident has been reported where a ship in the Black Sea was sent in another direction due to GPS spoofing[5]. Additionally, it is known that unmanned aerial vehicles (UAVs) are vulnerable to GPS spoofing[6, 7]. UAVs are aircrafts which are guided using a remote control, autonomously, or both[8]. An example that supports the claim that UAVs are susceptible to GPS spoofing, happened in 2011. Iran captured a RQ-170 UAV by allegedly jamming the frequency which was used to control the UAV[9]. This resulted in the UAV switching over to autopilot. In this mode, the UAV flies based on its GPS location. Iran then spoofed GPS signals such that the UAV would land on its own at a location controlled by Iran. Although it is not officially confirmed by the United States that the UAV was brought down, the lack of proper anti GPS spoofing functionality of the UAV should make this scenario possible [9, 10]. Note that UAVs usually only use GPS in the autonomous mode. Therefore, one can still avoid being impacted by GPS spoofing by switching from autonomous to remote control mode. Not all drones have support of completely disabling GPS [11, 12, 13].

Over the years, research has been done on detecting GPS spoofing attacks[4, 14, 15, 16]. Although these countermeasures are valid in some situations, they can be evaded or produce a large amount of false positives. Especially the countermeasures that try to detect GPS spoofing based on the properties of the signal itself, or the locking of GPS, are found easy to evade. Furthermore, the most effective GPS spoofing countermeasures are typically quite well researched but far from being implemented in commercial off-the-shelf GPS receivers[1, 17, 18, 19]. We therefore argue that in 2018, GPS spoofing in commercial GPS receivers is still an issue without modification of the GPS receiver's software.

In this paper, the possibility of spoofing GPS in a very specific area is investigated by using directionality and multiple transmitters. If found possible, this would enable one to guide an UAV out of airspace[20] at a busy airport, guide it away from a crowd, or force it to land when an air ambulance needs the airspace. Traditionally, one could jam the GPS signal to make it land automatically, but that is not always an option (above crowds) or would affect a lot of other users (planes near an airport)[21]. Another goal of this research is to make research on GPS spoofing more practical using off-the-shelf hardware such as software defined radios (SDRs).

II. GPS

GPS is a technology that is part of Global Navigation Satellite System (GNSS). GNSS is term that describes all geospatial positioning systems that have global coverage and

provide location services in an autonomous way. Examples of other GNSS technologies are GLONASS, Galileo and BeiDou[22].

As of this writing (2018-06-14) there are 31 satellites that actively provide the GPS signal[23]. A minimum of three additional satellites only provide the GPS signal in the situation where one (or more) of the 31 active satellites fail or become inaccessible[24]. One of the services that the GPS signal provides to receivers on the earth, is location detection with an accuracy of about 5 meters[25]. For the GPS receivers to be able to detect a 2D location (latitude and longitude), the signals of a minimum of three satellites should be received. If a minimum of four satellites are available to the GPS receiver, a 3D (latitude, longitude and altitude) location can be established[26]. To synchronize the receiver's clock with the atomic clock in a satellite, one also needs a minimum of four satellites because the location is required to determine the time signal's travel time[27].

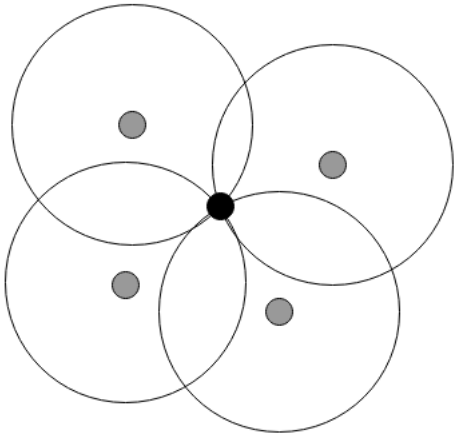

Fig. 1. Trilateration example with four satellites

The receivers calculate a location using a technique called trilateration. Compared to triangulation, trilateration measures the distance instead of the angle towards a point of measurement (in the case of GPS, this is a satellite). By comparing the distance of the received GPS signal and the distance between the satellites from where the signals were received, a location can be determined at the point where an intersection happens[28]. Figure 1 shows an example of trilateration with four satellites. The gray circles resemble the satellites and the four big circles their distance to the receiver. The black circle visualizes the GPS receiver.

So-called master stations on the earth are used to control and monitor the satellites. Examples of monitoring responsibilities of the master stations are to compare the time of the four atomic clocks that are present in the satellite against atomic clocks on earth and determining the position of the satellite in the orbit around the earth. If in these examples, an error is detected (such as time difference or position error) the master stations can readjust these errors. Note that almost all errors detected by master stations are readjusted and not corrected[29].

A. Location calculation

Equation 1 is used by the GPS receiver to determine its location[30]:

$$\begin{aligned} \mathrm{d}_n &= c(t_{t,n} - t_{r,n} + t_c) \\ &= \sqrt{(x_n - x)^2 + (y_n - y)^2 + (z_n - z)^2} \end{aligned} \tag{1}$$

Where $distance_n$ equals the distance to one of the satellites. The speed of light is identified in the equation by c. In this equation, the speed of light is in meters per second (m/s). $t_{t,n}$ specifies the time at which satellite n transmitted their signals. When the signal from the satellites is received by the GPS receiver, the internal (less accurate) clock is used to determine the time at which the signal was received ($t_{r,n}$, the time at which the specific signal was received). Because the receiver's clock is off, t_c is used adjust errors in the inaccuracy. x_n, y_n, z_n represent the coordinates of the satellites. Both $t_{t,n}$ and x_n, y_n, z_n are part of the GPS signal transmitted by the satellite.

Equation 1 is solved simultaneously for the four satellites to determine x, y, z, t_c.

B. Time synchronization

As stated at the beginning of Section II, all satellites have four atomic clocks aboard. Subsection II-A describes how a location can be determined using signals transmitted by GPS satellites that are in line of sight of the receiver. The location determination relies heavily on time. As a result, GPS receivers can use the time broadcast by satellites to synchronize their time[31]. This is accomplished by subtracting or adding the offset adjustment (t_c) to the time contained within the signal broadcast by a GPS satellite[32]. The offset is defined as follows: $t_c = sat_{time} - receiver_{time}$. This is the same offset used in the calculation of the location of a GPS receiver.

The sat_{time} is the UTC time at which the signal was generated by the satellite. Receivers also have their own internally generated C/A code to compare the time difference. $receiver_{time}$ identifies the moment at which the GPS receiver generated its internal C/A code.

Note that the location and time are calculated simultaneously as a solution to the equation by the GPS receiver. Therefore, the location cannot be calculated before the time and vice versa[33].

C. Frequency and modulation

Each GPS satellite transmits carrier signals on two frequencies: L1 and L2. The former is 1575.42 MHz and the latter 1227.60 MHz. GPS uses different bandwidths in these frequency bands: 15.345 MHz for the L1 band and 11 MHz for the L2 band[34]. The GPS L1 band is used the most for navigational purposes for civilian signals. Three different signals are transmitted on this frequency: C/A, P(Y), and M-code[35].

C/A code stands for coarse acquisition, which is a pseudo random number (PRN) code. This PRN-code with a length of 1023 chips is uniquely defined for each of the satellites and is transmitted at a frequency of 1.023 MHz. Note that chip means the same as bit in the sense that it is described by ones and zeroes. However, they differ on the fact that a chip does not carry any information. The PRN-code is repeated every millisecond, resulting in 1023000 chips per second. Because of the length of the PRN code, there are a lot of possibilities. Unfortunately, only 37 PRN codes allow for auto and cross correlation to measure the signal propagation time. These 37 possible PRN codes are called the Gold codes and, because of their weak correlation, direct identification of a satellite is possible. The precise (P) code is for military use, transmits 10230000 chips per second, and can be encrypted with the 'Y-code' if required. Another signal that is aimed at military use is the M-code. The L2 frequency is also used to transmits three frequencies: modernized civil code, P(Y) ,and M-code[36, 35].

The civilian GPS signals are phase modulated using binary phase-shift keying (BPSK)[35]. BPSK changes the phase by 180 degrees to respectively modulate a binary 1 or 0. Because all active GPS satellites use the same frequency, the PRN-code of the satellite is used for Code Division Multiple Access (CDMA). Otherwise, signals from different satellites would interfere with each other[37]. Figure 2 visualizes how the GPS satellites create the L1 and L2 modulated signal. In the example, only the modulation of the civilian and military signal on the L1 frequency band and military signal on the L2 frequency band is shown.

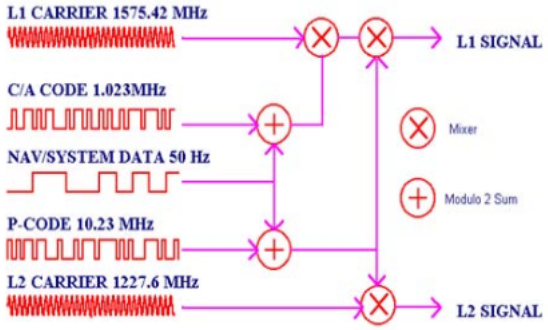

Fig. 2. Modulation of the L1 and L2 GPS signal[32]

The "Modulo 2 Sum" components create a sum of, for example, the C/A code and NAV/SYSTEM data chips. Because a chip can only be a zero or a one, the modulo operator is used to prevent the result from being greater than one. Mixers are used to create the modulated signal by multiplying the result of the "Modulo 2 Sum" operation by the L1/L2 carrier. The L1/L2 carrier in Figure 2 are so-called local oscillators.

D. The Navigation Message

As described at the beginning of Section II, GPS satellites receive information from master stations on earth. This information allows the satellites to construct the so-called Navigation Message. This message is sent to GPS receivers, which in turn use this message to compute their location and synchronize the time[38].

The oldest Navigation Message that exists for GPS is the L1 C/A Navigation Message. Additionally, there exist four other Navigation Messages: l2-CNAV, CNAV-2, l5-CNAV and MNAV. While each message type has its own format, timing, and use, only the L1 C/A Navigation Message is described here, as this one applies to our research[38].

The L1 C/A Navigation Message consists of 25 frames and will be transmitted by a satellite over the course of 12.5 minutes. Each frame in this message has a length of 30 seconds. Each frame is split up into 5 sub-frames of each 6 seconds. The sub-frames in turn consists of 10 words (30 bits per word), each with a length of 0.6 seconds. Figure 3 visualizes the structure of the aforementioned Navigation Message[38].

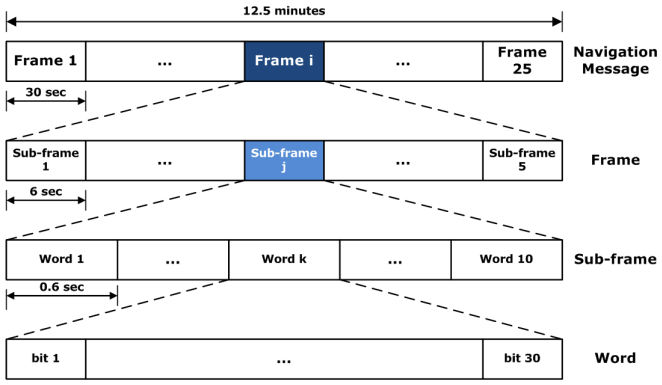

Fig. 3. L1 C/A Navigation Message format[38]

For each frame, the first sub-frame is required by the GPS receiver to apply its clock correction. The second and third sub-frame contain the satellite ephemeris and is used in Equation 1. Sub-frame 4 provide ionospheric model parameters and are used as adjustment for refraction caused by the ionosphere. The last sub-frame contains the information for the GPS receiver to determine from which satellite the signals originated[38].

E. Spoofing

When looking at academic as well as non-academic literature, it is unclear which steps are actually taken in the process of spoofing GPS signals in practice[1, 39, 40]. To understand GPS spoofing in practice, we studied the source code of GPS-SDR-SIM[1], commit `1ada56c`. The goal of this is to determine how software that uses SDRs accomplishes GPS spoofing.

The Crustal Dynamics Data Information System (CDDIS), which is part of the National Aeronautics and Space Administration (NASA), creates and publishes so-called broadcast ephemeris files. These ephemeris files contain predicted or extrapolated satellite orbit information transmitted from GPS

[1] https://github.com/osqzss/gps-sdr-sim

satellites to receivers on earth. Predicted ephemeris files only have information for a few hours into the future. Ephemeris files for GPS are generated either hourly or daily. The hourly ephemeris files are merged at the end of the day to a daily ephemeris file[41].

When spoofing a static location (using coordinates), GPS-SDR-SIM uses the CDDIS ephemeris file to determine which of the satellites should be visible at that location at a specific UTC time. Furthermore, it determines the location in the orbit around the earth of each of the visible satellites. Based on the orbit information of the subset of satellites, GPS signals are generated that solve the equation from Subsection II-A for the GPS receiver to be located at the specific location. Afterwards, the pseudo GPS signals are modulated, resulting in I/Q data, the signal representation of the actual data.

Finally, an SDR can be used transmit the I/Q sample data by specifying 1575.42 MHz as frequency and a sample rate of 2.6 MHz.

F. Calculating Effective Radiated Power

Effective Radiated Power (ERP) is used to determine the amount of electromagnetic power that is radiated out into space. Just like the Equivalent Isotropically Radiated Power (EIRP), the ERP is measured in front of a transmitting antenna. Regulators like the European Telecommunications Standards Institute (ETSI) use the ERP to identify how much power may be transmitted into space at a specific frequency[42]. The ERP can be specified either in milliwatts (mW) or Decibel-Milliwatts (dBm). In Dutch regulations, the ERP is defined in mW[43].

To calculate the ERP in dBm, Equation 2 can be used[44, 45].

$$\text{ERP}_{dBm} = (P_t - L_c + G_a) - 2.15 \tag{2}$$

The result of Equation can be converted to milliwatts using the formula in Equation 3[46].

$$\text{ERP}_{mW} = 10^{ERP_{dBm}/10} \tag{3}$$

Output power of the transmitter is defined by P_t in dBm. The output power of a device can be found in the data sheet of the transmitter. L_c defines the sum of the cable and connector loss in dB. The antenna gain is specified in dBi by G_a. As with the output power of the transmitter, the gain of an antenna is also specified on its data sheet.

Loss of signal caused by the connector belongs to the category of insertion loss. Insertion loss is loss of signal caused by the difference in transmission medium. Equation 4 specifies how insertion loss can be calculated for the SMA converter[47].

$$\text{Insertion loss} = \text{c}_l \cdot \sqrt{f_s} \tag{4}$$

The connector loss factor is identified by c_l and is different for each type of connector[47, 48]. The frequency on which the transmitter is active is specified by f_s. Note that, as stated at the beginning of this section, insertion loss should be taken into account at each point where a connector is used in the transmission line between the antenna and transmitter or receiver.

Although there exist formulas to calculate the loss caused by a cable, these rely on theoretical properties of the cable. Among these theoretical values, the cable loss is also specified with a higher precision. If a (coaxial) cable is used between the antenna and the radio, it is therefore recommended to rely on the theoretical cable loss specified by the manufacturer. Note that cable loss values are specified at 100 meters. Therefore, one should always convert that value to the actual length of the cable[49, 50].

III. Research Questions

Our main research question is defined as follows:
Is it possible to limit GPS spoofing to a single receiver?

To answer this main research question, the following supporting sub research questions are defined:

1) *Can a spoofed GPS signal be contained within a radius of 10 meters without the use of a Faraday cage?*
2) *Is it possible to direct spoofed GPS signals using a directional antenna?*
3) *Does the GPS receiver still compute an accurate position when dividing the spoofed GPS signal over two transmitters?*

A. Research scope

Altering the properties of the transmitting radio is considered within this research's scope. Specifically, the effect of applying a different gain setting on the spoofed GPS signal is investigated. We additionally modify the software that makes GPS spoofing within our research possible.

In the Netherlands, spoofing and jamming of GPS signals is illegal[51]. Without having access to a large (and tested) Faraday cage, one must take other measures to make sure that the experiments are performed in a legal and ethical way. This is because GPS signals have a negative Signal-to-Noise-Ratio (SNR), which means that the signal has less power than the noise floor. Specifically, it is 26dB below the noise floor[52]. To work around this limitation, we conduct our experiments on frequency bands that do not require a license. The closest unlicensed frequency bands to the GPS L1 band are the 868 MHz and 1.8775 GHz frequency bands. Both frequency bands are not usable for conducting experiments with GPS signals because their channel bandwidth is lower than the bandwidth required for GPS L1 signals (Subsection II-C)[53, 43].

However, as described in Section V-A, we are able to operate the spoofing software (GPS-SDR-SIM) with a bandwidth of 2.5 MHz. The 868 MHz frequency band is still a challenge to use because regulatory requirements on duty cycle state that the category of devices where our experimental setup would fall under is only allowed to transmit 36 seconds per hour (0.1% duty cycle)[53]. On the other hand, the 1.8775 GHz frequency band has a bandwidth of maximum 4.5 MHz, does

not specify regulations around duty cycle, and is closer to the frequency where the valid GPS signals are sent on[43].

Because the 1.8775 GHz frequency band only allows for a maximum Effective Radiated power (ERP) of 50 mW, we do not investigate the effect of signal above 50 mW ERP[43]. Research of GPS spoofing on frequencies other than 1.8775 GHz is also considered out of scope.

Furthermore, the investigation is primarily focused on researching directionality of GPS signals. To accomplish this, we focus ourselves on the software implementation of GPS spoofing. Research on components that can be used in combination with the antennas is also considered out of scope. Because we only focus on the GPS signal, GNSS signals other than GPS are out of this research's scope.

Designing custom antennas that are resonant at 1.57542 or 1.8775 GHz, is considered out of scope. GPS consists of multiple frequency bands. In our research we focus only on civilian signals in the L1 frequency band. GPS frequency bands other than the L1 band are therefore considered out of scope. On the L1 band, two classes of GPS signals are transmitted: civilian and military signal. Because we focus on the civilian signal only, the military signal is also considered out of scope.

Investigating the signal properties (other than frequency) on the receiving side is also considered out of the scope of this research. The reason for this is that, typically, one does not have access to or is not able to modify the properties of the receiver. Furthermore, we want to stay as close to an off-the-shelf GPS receiver as possible.

Although we describe example use cases of our research in Section I, those specific uses are not the goal of this research. This includes advantages and disadvantages of example use cases we present in this paper.

B. Report structure

This paper begins with the motivation and problem statement of our research. These statements are accompanied by introductions to the subject of UAVs and GPS, and can be read in Section I. The result of studied literature on the subjects of GPS, GPS spoofing and antenna ERP can be found in Section II. The content of this section is important as theoretical groundwork for the remainder of our paper.

The research question along with the scope is found in Section III. Research that has been conducted in the past that either has overlap or is used as starting point for our research is described in Section IV. In the section that follows (Section V), we present the approach we employ throughout our research in order to answer the main research question. Note that, apart from the approach itself, we also present the experimental setup including the considerations for each of the experiments in this section.

Based on the approach from Section V, we present the results in Section VI. Any criticism on or shortcomings of our research are discussed in Section VII. We present a conclusion of the entire research in Section VIII. Based on the shortcomings presented in the Discussion and Conclusion sections, we also describe research proposals for which our research could be used as input in Section IX.

Supporting information which does not fit in the regular sections can be found in the Appendices (Section).

IV. Related Work

Since the inception of GPS, it has been a given that GPS signals can be spoofed[54]. To mitigate this, a separate code is built in which is unpredictable and therefore much harder to spoof. This code should only be known by the satellites and authorized receivers, making it impossible for attackers to transmit a fake signal with the correct time. Still, affordable or even publicly available radio equipment was not ubiquitous until recently. Up until 1991, the standard GPS receiver weighed about 16kg[55]. Therefore, a GPS transmitter to spoof the signal would not have been able to be constructed using commodity hardware. We have not been able to find references to any software prior to 2000 which can actually perform such an attack[56]. We are also unaware of any software fit for this purpose and publicly available prior to 2015[2]. Later in 2015, software became available which generates the spoofed GPS signals in signals in real-time, rather than having to precompute and transmit them in separate stages[3].

One of the tools we use in our experimental setup is an open-source GPS receiver called GNSS-SDR. This GPS receiver is the result of a research conducted by Fernandez-Prades et al.[57]. Wen et al. conducted a research in 2005 where they researched countermeasures for detecting spoofed GPS signals. During this research, they also identified the minimum RF signal power of GPS in the L1 frequency when the GPS signal hit the earth[58]. We base our experimental setup on this research. In particular, we make sure to not to amplify the spoofed GPS signal too much in order to mimic the behavior of valid GPS signal.

In 2011, Tippenhauer et al. looked into the properties of the RF signal sent by a GPS spoofer. One of their goals was to determine the optimal GPS spoofing configuration (including relative signal power) to prevent a loss of lock on the GPS receiver. In their research, they acknowledge that spoofing a specific target GPS receiver requires one to be within proximity of the target to prevent affecting any other GPS receivers with the spoofed signal. The research also describes the possibility to make use of a directional antenna to spoof a specific victim. However, in their research this claim is not supported by any experiments[1]. We use this research as starting point for our experimental setup. In particular, we use their results to determine the transmission power of our GPS spoofer. Furthermore, we build on their research by verifying the claim whether using a highly directional antenna removes the requirement of having close proximity to the target to avoid affecting other GPS receivers.

[2] https://github.com/osqzss/gps-sdr-sim/blob/ad465dbc29ac53cecab3a64008d58600ef7234a0/gpssim.c

[3] https://github.com/osqzss/bladeGPS/commit/b3b75ae7ca9cc835f04c3eee1343d34ad7e2494c

In 2014, Kerns et al. researched hijacking an unmanned aircraft using GPS spoofing. In particular, their research consisted of theoretical, modeled spoofing attacks to hijack an unmanned aircraft and verified these models. However, their research uses omnidirectional antennas with a short range to target a single GPS receiver instead of directional antennas[20]. We extend on this research by using their results as inputs of our experiments. An example of inputs are the rudimentary GPS spoofing detection techniques (such as J/N monitoring) identified in the paper and how to avoid triggering these detection.

V. Methodology

At the start of this research a literature study is conducted on the subject of GPS and GPS spoofing in order to determine the scope of our research. Based on this, we construct a main research question. In order to answer this main research question to the full extent, several sub research questions are defined as well. We use the result of our literature study as input for the construction of our experimental setup. This experimental setup is primarily used to execute experiments on and to verify additional claims that we encounter during our literature study. Another place in our research where we use our literature study as input, is at the point where we define our experiments. We also use the verified claims as input for defining our experiments. After obtaining the results, we conclude our research by discussing the results and drawing a conclusion. Additionally, we define several research ideas to extend our research upon in a future research.

Although the 1.8775 GHz frequency is an unlicensed frequency within the regulatory requirements, we still aim to limit (and potentially prevent) impact to others that use this frequency. Therefore, we first listen on the spectrum for any usage before transmitting. Furthermore, during the experiments, we listen every three minutes. If we detect any usage, we try to contact the person using the spectrum to ask for him or her to stop using the frequency if possible. If this is not possible, we wait until the spectrum becomes free again.

A. Experimental setup

The two main components we use during our research are a GPS receiver and transmitter. As the receiver we use the GPS software GNSS-SDR, version 0.0.9, together with a HackRF One SDR. The git commit hash that belongs to this software version is 31311ae[4]. Note that, for GNSS-SDR to determine its location, sub-frames 1, 2 and 3 of at least four satellites need to be received[57].

Where the setup of the GPS receiver is used to receive GPS signals, we use the GPS transmitter for sending spoofed GPS signals. GPS-SDR-SIM is used as GPS spoofing software. The git commit hash that belongs to the version we use in our research is 1ada56c[5]. Both GNSS-SDR and GPS-SDR-SIM are open source software and allow their frequencies to be altered by design. This is the main reason we choose to use these software programs for transmitting and receiving GPS signals in our experimental setup.

In order to determine directionality, we use two additional software packages: osmocom_siggen and osmocom_spectrum_sense. Osmocom_siggen is provided by gr-osmosdr version 0.1.4. We use this tool to send out a sinusoidal wave pattern from the directional antenna. The received power level of this wave pattern that is received by the (GPS) receiving equipment is measured in dB by osmocom_spectrum_sense. Osmocom_spectrum_sense is also provided by gr-osmosdr version 0.1.4.

As spectrum analyzer to determine usage of the spectrum we use GQRX version 2.9[6].

The SDRs we use for transmitting GPS signals are two BladeRF x40[7]. Note that we only use both BladeRFs in the experiment where we determine the possibility of transmitting spoofed GPS signal over multiple transmitters. For receiving (GPS) signals we use the HackRF One as SDR. When comparing these SDRs, the main difference is that the BladeRF has an internal Voltage Controlled Temperature Compensated Crystal Oscillator (VCTCXO) with an accuracy of 1 parts per million (ppm). 1 ppm is the lowest accuracy allowed for transmitting GPS signal[59, 60].

To comply with regulatory requirements on the unlicensed spectrum we use, we tune the bandwidth of the signals that GPS-SDR-SIM transmits to 2.5 MHz. Section III-A also describes that we are only allowed to transmit a maximum ERP of 50 mW. Therefore, we use the equations from Section II-F to determine the ERP before transmitting. The first parameter of the ERP formula from Equation 2 is the output power. For the transmitting SDR this is defined at 6 dBm (without additional gain)[61].

For the experiments, we use both omnidirectional and directional antennas. The omnidirectional antenna is used in the first experiment on both the transmitter and receiver. Experiments 2 and 3 use a directional antenna on the transmitter and an omnidirectional antenna on the receiver. The reason we do not use a directional antenna for the receiver, is because we aim to mimic an off-the-shelf GPS receiver as much as possible. GPS receivers have omnidirectional antennas in order to receive satellite signals from multiple directions.

As for the omnidirectional antennas, we use a 5 dBi monopole antenna that is delivered with an Alfa AWUS051NH[8]. The antenna has a length of 16.9 cm and is visible in Figure 4.

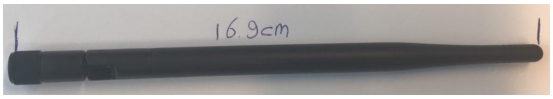

Fig. 4. Omnidirectional antenna

[4] https://github.com/gnss-sdr/gnss-sdr
[5] https://github.com/osqzss/gps-sdr-sim
[6] http://gqrx.dk/
[7] https://www.nuand.com/blog/product/bladerf-x40/
[8] https://tweakers.net/pricewatch/276586/alfa-network-awus051nh.html

Because the connector of the antenna is RP-SMA male and the connection to both the SDRs are SMA female, we use a RP-SMA female to SMA male connector between the SDR and antenna. Figure 5 show the SMA converters we use in our research. The connector loss factor of an SMA connector equals 0.06 dB per side[47].

Fig. 5. SMA converters

The SMA converter is placed between the antenna and SDR. Therefore, the insertion loss of current flowing from the SDR to the converter and from the converter to the antenna (and vice versa) needs to be taken into account.

As directional antenna we use a 13 element 13 dBi Yagi antenna. Figure 6 shows the directional antenna. The RG58 coaxial transmission line of the antenna has a length of 29.5 $\pm$ 2.5 centimeter. At 100 meter on 1.8775 GHz, the coaxial cable has a loss of 70.9 dB[50]. Therefore, the loss introduced by the transmission line equals 0.2092 $\pm$ 0.0178 dB.

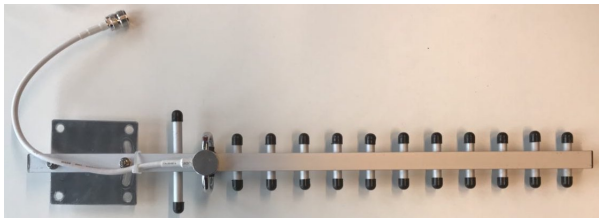

Fig. 6. Directional antenna

At the end of the transmission line, a N-Type female connector is located. Therefore, we also need a converter that has a N-Type male connector on one side and a male SMA connector on the other side. Figure 7 shows the converter we use to connect the Yagi antenna to the SDR. Note that the N-Type connector side of the converter has a connector loss factor of 0.05 dB, which is 0.01 dB less than the SMA side of the converter.

Fig. 7. N-Type to SMA converter

Note that all antennas, connectors and coaxial transmission lines that we use have an impedance of 50 Ω. We want to minimize the diffraction, refraction, reflection and scattering of radio waves when coming into contact with artificial and non artificial properties. Therefore, we conduct all experiments outside in a field of grass. The GPS coordinates that belong to this location are: 51.4304 degrees latitude, 5.47901 longitude and an altitude of 62 meters. The only impact radio waves can experience at this location is absorption. However, when comparing absorption to the aforementioned effects, absorption does not alter the direction of radio waves traveling in free space.

For measuring distances and lengths during our experiments, we use a measurement tape. Due to the level of detail the measurement tape provides and inaccuracy of the environment of our experimental setup, we include a measurement error of 5 centimeter in all of our measurements.

The location that we spoof during our experiments has a latitude and longitude of respectively 51.337000 and 4.1337000 °. The altitude equals 1337 meters. The specific satellite C/A codes that we use in our spoofed signal only include: 02, 03, 04, 06, 09, 17, 22, 23 and 26.

B. Experiment 1: Limiting Impact Area

In experiment 1 we measure the possibility of limiting signal to a specific area. We conduct this experiment in order to determine whether any future research on GPS spoofing can be conducted on a remote location without access to a Faraday cage. During this experiment we use GPS-SDR-SIM to spoof GPS signal. We measure the GPS signals received by GNSS-SDR on a 100 centimeter distance from the transmitting antenna. When measurements are taken, we increase the distance with 100 centimeters and take measurements again. These steps are repeated until we are not able to receive any subframes.

After 10 meters, we increase the steps from 100 centimeters (1 meter) to 5 meters. The reason for this is because up until 10 meters, we want to determine whether the possibility of acquiring a location from the spoofed signal can be contained. After 10 meters, we want to determine whether it is possible to contain subframes that (if the amount is sufficient) make it possible to acquire a location.

Figure 8 visualizes the aforementioned approach of experiment 1. Note that the (black) dot in the center of the circles is the GPS receiver. The smaller (gray) dots placed on each circle are the measurement points that are taken at a specific distance using the GPS transmitter. We do not measure at multiple locations on a specific distance because the antennas we use for this experiment have the omnidirectional property.

At each measurement point, we measure the following properties:

- The number of identified satellite C/A codes which are also being transmitted from GPS-SDR-SIM.
- The number of satellite subframes being received of the first frame.
- Whether a GPS location can be determined.
- How long it takes for the location to be determined.

For the first bullet point, if at a specific distance we cannot receive any subframes, we conduct the measurement again

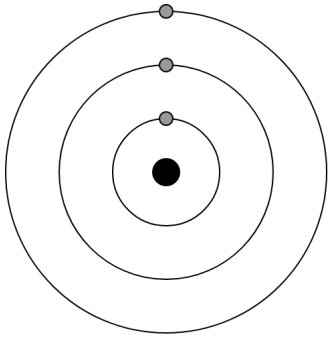

Fig. 8. Schematic visualization of the first experiment

without the GPS transmitter being active. Afterwards we compare the two measurements in order to determine if satellite C/A codes are being received from the GPS transmitter, or if these are so-called false positives (detected from noise).

In Section II-D we mention that each frame that contains sub-frames required by the GPS receiver for determining its location has a duration of 30 seconds. As mentioned in Section V-A, the GPS receiver software in our experimental setup requires the first three (out of five) sub-frames of at least four satellites before a location can be determined. Therefore, it takes at least 18 seconds for the GPS receiver to receive the required sub-frames if both the GPS transmitter and receiver are started at the same time, excluding computational overhead and excluding time it takes for the receiver to lock onto a satellite's signal. In practice, a fix can be obtained in 26 seconds. The difference is mainly due to the time needed to lock onto the satellites' signals. To be sure that the GPS receiver has enough time at a measurement point to determine its location, we wait 180 seconds before moving over to the next measurements point.

To determine the impact of halving the ERP to the maximum distance, we conduct experiment 1 twice. The first time with an ERP that is close to 50% of the regulatory limit. The reason we do not transmit at regulatory requirement is that we want to prevent the possibility of the signal having a very long range. When we conduct the experiment a second time, we make sure to transmit at least 25% lower than the previously used ERP value. Table V-B shows the ERP values in milliwatt that we use during experiment 1. Note that P_t is the CW output power of the BladeRF including additional gain.

P_t	L_c	G_a	ERP_{mW}
10 dBm	0.1644 dB	5 dBi	18.5658 mW
8 dBm	0.1644 dB	5 dBi	11.7142 mW

TABLE I
MONOPOLE ANTENNA ERP IN MILLIWATTS WITHIN REGULATORY SPECIFICATIONS

C. Experiment 2: Directionality of GPS signal

In experiment 2, we determine the directionality of spoofed GPS signals when using a Yagi antenna. This experiment builds on the results of experiment 1 by using the determined maximum distances as starting point for our measurements. This reduces the risk of our results being impacted because of the side and back lobes of the Yagi antenna. Before conducting this experiment with GPS signals, we first send a sinusoidal wave out of the Yagi antenna. On the GPS receiver we then measure the received signal power in dB. The goal of this is to determine whether the Yagi antenna is directional enough at the 1.8775 GHz frequency.

If the signal is found to be directional, we determine the directionality of the Yagi antenna when transmitting GPS signals. Table V-C specifies the ERP in milliwatts of GPS transmitter during experiment 2. Note that this ERP remains the same when measuring the directionality using sinusoidal waves as well as with the GPS signal.

P_t	L_c	G_a	ERP_{mW}
6 dBm	0.2092 $\pm$ 0.0178 dB	13 dBi	46.1577 $\pm$ 0.1884 mW

TABLE II
YAGI ANTENNA ERP IN MILLIWATTS WITHIN REGULATORY SPECIFICATIONS

Because the Yagi antenna is different from the monopole antenna in experiment 1, the Yagi antenna might have a different range. In this case, we increase or decrease the range by 100 centimeter at a time until only position can be acquired in front of the antenna at two consecutive measurements. We rotate the antenna in steps of 90°. At each step we take two measurements. During each measurement we collect the following information:

- The number of satellite subframes being received of the first frame.
- Whether a GPS location can be determined.
- How long it takes for the location to be determined.

As described in experiment 1, we also measure the number of subframes being received from the first frame in experiment 2. The reason we measure this in both experiments is to determine reliability of the received GPS signal. With reliability we mean how much of the signal (measured in subframes) is received at the start.

Figure 9 visualizes the measurement points we take using the GPS transmitter during this experiment, identified by the smallest (gray) dots. The black dot in the center identifies the GPS receiver.

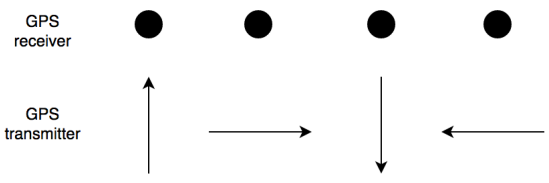

Fig. 9. Schematic visualization of experiment 2

D. Experiment 3: Multiple GPS signal transmitters

Experiment 3 builds on the results of experiment 2. This experiment determines whether it is possible to split spoofed GPS signal over two sources in order to only spoof GPS receivers which are located at the intersection of the two spoofed GPS signals.

Initially, we attempted to split the signal by modifying GPS-SDR-SIM to modulate only six satellites in total, three into each signal file. These signal files would then be simultaneously transmitted using a bladeRF-cli script. The start of these transmissions would be synchronized by using a FIFO pipe, as shown in Appendix A.

Next, we attempted to split the signal by modifying the source code of the real-time version of the GPS-SDR-SIM[9] spoofing software. This version of the software allows us to more precisely control when signals are starting to be transmitted. For synchronization, we use the POSIX `clock_gettime` in a busy wait loop: looping until the time reaches a certain value. As obtaining the current time also takes a certain amount of time, this method is not extremely precise. The results of measuring the precision of our method can be found in appendix B. Further synchronization would have to be done using methods such as inserting a certain number of NOP instructions, real time scheduling, CPU pinning, etc.

Each antenna only transmits the signal of three satellites. As discussed Section II, a complete GPS location fix can only be made using the broadcasted GPS signals of four or more satellites. We define a complete location fix as a fix on latitude, longitude and altitude. The complete GPS location fix should also include a synchronization of the UTC time between the spoofed satellites and the GPS receiver.

This experiment focuses on determining whether the receiver can still compute an accurate position when the spoofed GPS signal is split over two transmitters. For completeness, however, both omnidirectional and directional antennas are tested. In the setup with directional antennas, the receiver is moved around to see whether the position fix is indeed lost when it is outside the reach of one of the directional antennas. Only at the intersection a location fix should be possible.

See Figure 10 for a visualization of the directional setup. We purposefully did not oppose the two directional antennas as this may cause unintended effects. This is also not a realistic scenario in the case of an airborne UAV.

VI. Results

In this section we present the results of the three experiments we conducted in our research. Note that we present the results in numerical order, starting with the results of experiment 1.

A. Limiting the area where a location can be acquired

The results that we publish in this section are the acquired using the approach outlined in Section V-B. Figures 11 and 12 show how long it takes for the GPS receiver to acquire a GPS location. In both measurements, the GPS receiver is able to determine a location at 5 meter. After this measurement point, the possibility of acquiring a location becomes less reliable. Although, we use different transmit powers which result in a different ERP, the GPS receiver is not able to acquire a location at a distance of 7 meters. At 8 meters the GPS receiver is in both cases able to determine a location using GPS again. This is also the maximum distance where it is possible to acquire a location.

[9] https://github.com/osqzss/bladeGPS/commit/80c75a20b1415b8b954d802d5cb4ef3176ef6b19

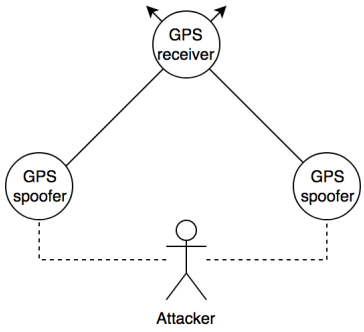

Fig. 10. Schematic visualization of experiment 3

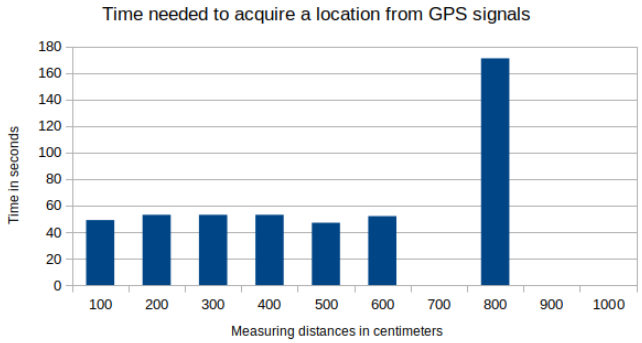

Fig. 11. Time required to acquire a GPS location with a transmission power of 8 dBm.

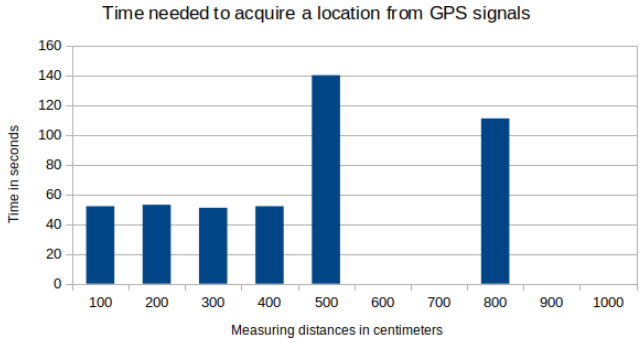

Fig. 12. Time required to acquire a GPS location with a transmission power of 10 dBm.

At the same measurement distances used in the aforementioned results of this Section we also measured the number of subframes from one frame we received from each satellite C/A code transmitted by the GPS transmitter. Figures 13 and 14 visualize the results from executing this measurement with different transmission powers.

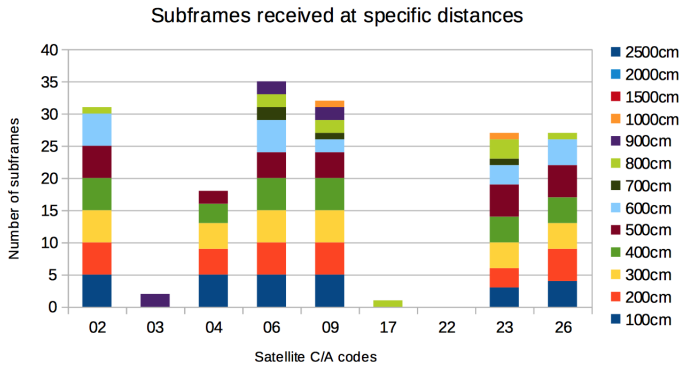

Fig. 13. Subframes acquired from one frame at a transmission power of 8 dBm.

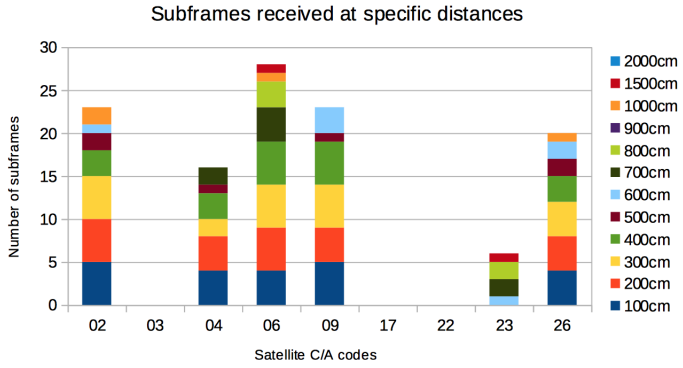

Fig. 14. Subframes acquired from one frame at a transmission power of 10 dBm.

When comparing the results in Figure 13 with Figure 14, the subframes of a greater number of satellites are received with a lower transmission power at short distances. Although, we transmitted subframes from satellite C/A code 22, we were not able to receive any subframes from that satellite in both measurements using the GPS receiver. Note that in Figure 12, we are able to acquire a GPS location after 111 seconds at a distance of 8 meters. However, in Figure 14 we only have subframes received by satellite C/A code 06 and 23 at that distance. This is caused due to the fact that within the first frames, the GPS receiver is not able to collect enough frames to calculate a GPS location. The result of this is that the GPS location is acquired only after 111 seconds at 8 meter.

With a transmission power of 10 dBm we are not able to receive subframes from any satellite at a distance of 20 meters. When using a transmission power of 8 dBm, the distance where we are not able to receive subframes is 25 meters. Although Figure 13 shows we also did not receive any subframes at a distance of 20 meters, we still measure at 25 meters. This is because, from a later frame, we still received one subframe at the distance of 20 meters, which was still within the 180 seconds.

Based on the results from Figures 13 and 14, we determine the distance at which no satellite subframes are received is 25 meters at a transmission power of 8 dBm and 20 meters at a transmission power of 10 dBm. In Figures 15 and 16, we visualize the amount of detected satellite C/A codes with and without spoofing GPS signals.

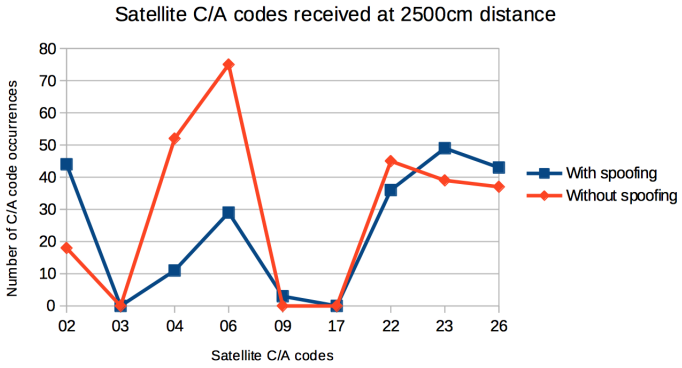

Fig. 15. Detected C/A codes at a transmission power of 8 dBm.

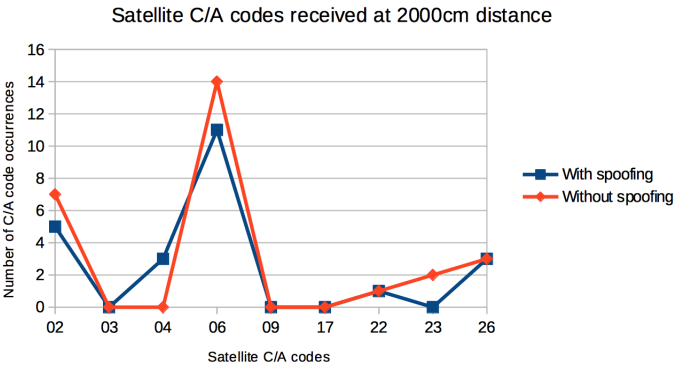

Fig. 16. Detected C/A codes at a transmission power of 10 dBm.

In both situations, the number of occurrences of C/A code 06 is higher when not transmitting than when we are transmitting GPS signals. Furthermore, it is also visible that the amount of detected C/A codes is higher when a lower transmission power is used. In both cases, we did not detect C/A codes 03 and 17, even though the GPS spoofing software transmitted these.

B. *Directionality of the antenna*

As described in Section V-C, we first generated a sinusoidal wave to measure signal strength at different angles from the directional antenna. The relative power level was recorded over the period of one minute, measuring twice per second, for each orientation of the transmitting antenna. The results are shown in a Tukey box plot in Figure 17. On the X-axis, there

is a label called ”Control”. This label identifies the recorded relative power level when the transmitter was turned off.

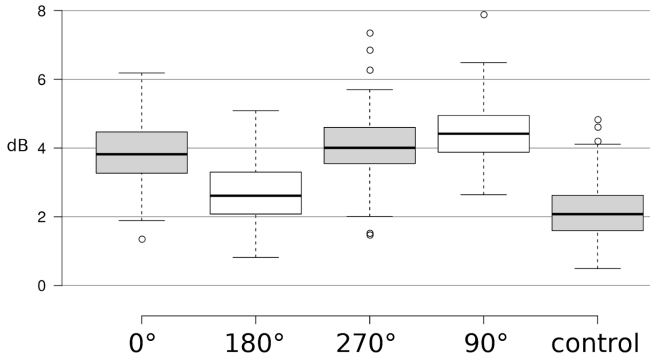

Fig. 17. Tukey box plot of power level per orientation in dB

We see that the power is measured most strongly when the transmitter is either aimed at the receiver, or is aimed at 90 or 270°. The difference between those orientations is not very significant, all share measurement values within the interquartile range. Based on some initial testing, all tests with the directional antenna are conducted with a distance between the receiving and transmitting antenna of 200 centimeter. This was the maximum distance at which we were able to acquire a location from spoofed GPS signals. Based on the results from Figure 17, directionality is only exhibited when the receiving antenna is positioned behind the transmitting antenna.

C. Directionality of GPS signals

Based on the results of Section VI-B we tested whether we could observe the same behavior with the GPS signals. As the receiver is made to pick up very weak signals from between the noise, we want to test what effect a directional antenna has. The time in seconds before a GPS location is acquired is shown in table III. As described in Section V-C, we ran all tests twice.

Orientation	0°	90°	180°	270°
Test run 1	56s	-	-	175s
Test run 2	71s	86s	-	56s

TABLE III
TIME TO FIRST POSITION FIX

Similarly to the sinusoidal test, where the signal is worse at 180°, we see that the software can obtain no fix at that angle. During a control test at 30 centimeter, we get a position fix in under 50 seconds, like in experiment 1. It seems that finding the position is slightly more difficult with the directional antenna, and much more difficult at 180°.

Because in both test runs we were not able to acquire a location from the transmitted GPS signals at an angle of 180 ° does not mean no GPS subframes are received. In Figure 18 and 19 we show the amount of subframes received at different angles from each satellite that we spoof the signals of. At an angle of 270 and 90 ° we determined that just (not) enough subframes are received from enough satellites to satisfy the requirement of the GPS receiver software of receiving subframes of at least four satellites in both runs.

At an angle of 0 ° we exhibit subframes from 5 satellites in both test runs. As with the results in Section VI-B, the signal is very weak to even receive subframes that can identified by the receiver's GPS software. Only in the first run we were able to identify subframes from two satellites.

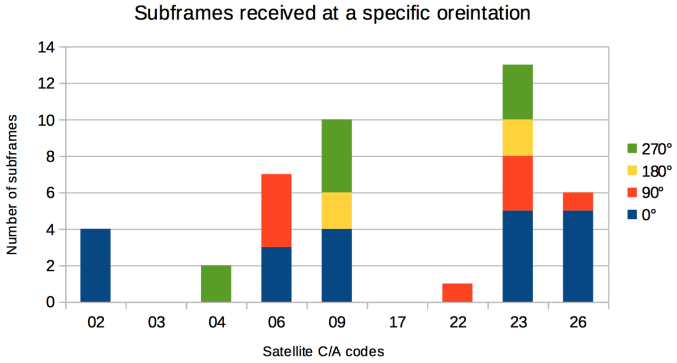

Fig. 18. First test of Subframes acquired from one frame at specific orientations

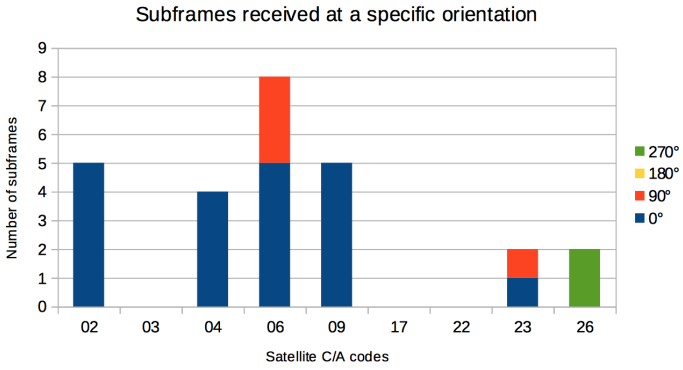

Fig. 19. Second test of Subframes acquired from one frame at specific orientations

D. Spoofing the signal over two transmitters

After modifying the software as described in Section VI-D and starting the transmitters using omnidirectional antennas, we are able to calculate a position on the receiver. The setup is identical to the setup with the directional antennas as depicted in the experimental setup in Figure 10, except that the antennas are omnidirectional. The accuracy of the position varied widely. See Table IV for the results.

When using the directional antennas, it is much harder to obtain a position fix. The reason for this is unclear. The results of the test runs in which we obtained a position fix are also included in Table IV. The column ‘Initial 3D error’ shows how far the calculated position is off at its initial fix.

Antenna	In sync	Run	Satellites	Initial 3D error
Monopole	Yes	#1	4	18 451 m
Monopole	Yes	#2	6	250 m
Monopole	Yes	#3	6	7 751 m
Monopole	Yes	#4	6	4 440 m
Monopole	Yes	#5	6	5 195 m
Monopole	Yes	#6	6	9 552 m
Monopole	No	#1	5	482 106 m
Yagi-Uda	Yes	#1	4	86 903 m
Yagi-Uda	Yes	#2	4	108 642 m

TABLE IV
POSITION ACCURACY OF EXPERIMENT 3

In all cases, the time taken to obtain a first position fix was between 40 and 50 seconds. In one test, the one marked as not in sync, the signal transmitted by one antenna was purposefully delayed by 5 microseconds. This has a large impact on the accuracy, as it is by far the most incorrect position obtained. The directional Yagi antennas have a large impact on the signal quality, as it would often fail to obtain enough satellites at all. Where it had enough satellites, it would only have the required minimum of four, and hence the calculated position is quite inaccurate.

After the initial 3D fix, i.e. a position fix in the three dimensions, the error in the position calculation showed interesting patterns over time. For example in the run with only 250 meters error, the pattern shown in Figure 20 emerged over the course of about an hour.

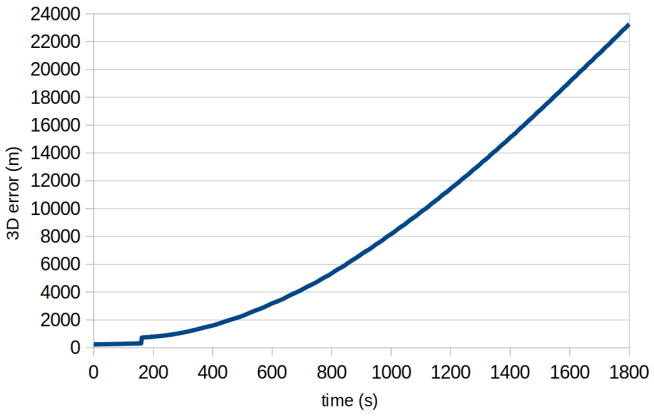

Fig. 20. Longitude, latitude and altitude error (3D) vs. time of run 2 with the monopole antenna

When visualizing the error as increase over time rather than absolute error, as in Figure 21, the spike around 162 seconds becomes even more visible. When investigating this spike, it turns out that the receiver lost one of the satellites. After this spike from the loss, the increase in error is fairly constant again, though slowly gaining.

In other test runs with omnidirectional antennas, similar patterns are visible: the rate of change is fairly stable unless a satellite is lost. The rate of change, however, is different for each run, similar to how the initial error is different each run.

Directional antennas appear to behave similarly in this regard. Since there is more error due to fewer satellites, the main difference appears to be that all values are heightened. However, there are too few data points to draw reliable conclusions.

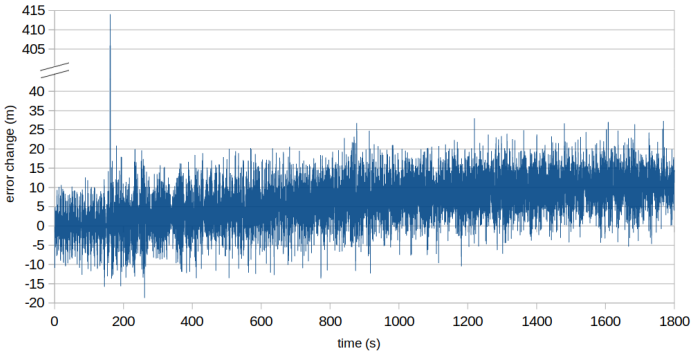

Fig. 21. Changes in the 3D error over time of run 2 with the monopole antenna

A variable amount of error does not occur when transmitting the GPS signal from a single source. There, too, the loss of a satellite results in a correction in position, but because the amount of absolute error is much lower, it does not have as big an impact. Position error is in the order of 5-15 meter.

Section VI-C shows that directionality of the Yagi antenna is only noticeable when the receiver is positioned behind the transmitting antenna. In the setup as shown in Figure 10, moving the receiver therefore would have little effect: even if the receiver is outside the main lobe of either transmitter, it would still receive sufficient signal to complete a location fix. Additionally, the bad signal made it impossible to reliably test this with the current setup.

VII. DISCUSSION

All of our experiments are conducted on the 1.8775 GHz frequency, which is different from the frequency on which genuine GPS signals are transmitted: 1.57542 GHz. However, as described in Section III-A, we made sure to select an unlicensed frequency which was close to the GPS frequency. Both frequencies are microwave frequencies, apart by only 0.30208 GHz. When conducting tests in a small Faraday cage in the form of a bag, there was no observable difference between the frequencies.

Another point of criticism could be that we use antennas which are resonant at the 2.4 GHz frequency. We argue that the aim of this research was to use off-the-shelf hardware. The scope also specified that we excluded antenna design out of our research. Therefore, we had to focus ourselves on hardware that was readily available to us. Both omnidirectional as well as directional antennas are widely available for 2.4 GHz. Another possibility was to use antennas which are resonant at the 1.57542 GHz frequency. Although, omnidirectional antennas are widely available, directional antennas are not. Those that are available, are not usable in terms of reproducibility of our research. The reason for this is because they lack proper documentation.

Some GPS receivers use low noise amplifiers to amplify only signals on the GPS frequency without impacting the level of noise too much. We were not able to find a low noise amplifier that could be delivered within two weeks for our research. Therefore, we were not able to verify our results for GPS receivers that have this hardware component installed. Constructing a low noise amplifier ourselves was considered out of scope. We propose a research into validating our results with a (self constructed) low noise amplifier as future work.

In the first experiment, we measure the number of detected satellite C/A codes when spoofing GPS signals against the detected C/A codes when we are not transmitting GPS signals. It might seem odd that more satellite C/A codes are detected when the GPS signal is not transmitted. We assume that the detected satellite C/A codes are the result of random noise on the frequency. After all, the GPS receiver software is designed to detect GPS signal between the noise.

In Section VI-D we describe that we use a different version of GPS-SDR-SIM for experiment 3. The reason that we did not use this same version for experiment 1 and 2 is because the real-time version allows for more precise time synchronization. In experiments 1 and 2, this requirement does not exist. The real-time version remarks that it is a 'very crude implementation', made to work specifically with a BladeRF. We initially assumed the generic version is therefore more mature and use that where possible. However, after having studied portions of the source code of both and having used both, it appears to us that both versions work equally well.

Because it is unclear why the directional antennas worked much less well than the omnidirectional antennas, we assume the reproducibility of this part of the research is low. Testing the antennas at the resonant frequency of 2.4 GHz, was impossible due to the high amount of noise on that channel. It is possible that the antenna itself was bad, that one of the connectors had a bad connection, or that we miscalculated the power loss of some part. This resulted in a low amount of measurements, and we were unable to test whether the targeting system works as intended when using directional antennas in combination with multiple transmitters.

Finally, is it not certain why the position in experiment 3 is off by multiple kilometers, or why the error drifts over time. We assume that the former issue is caused by a mediocre initial synchronization and the latter is caused by clock drift in either the BladeRF or in the software generating the signal. In this research, this could not be proven. Similarly, because the receiver software (GNSS-SDR) only shows the time in seconds, it was not possible to determine the accuracy of the time synchronization. In all cases it appeared to be spot on, but only with a resolution of one second. As shown in Section VI-D, even five microseconds can give extreme error values.

A. Pitfalls

In this section, we briefly describe a few pitfalls that we encountered during our research and our solutions. This is to give further insight into our methods, aiding reproducibility, as well as to help future researchers avoid those pitfalls.

At the start of our research we proposed conducting our experiments on the same frequency as GPS. However, the ethical committee did not allow for such research to be conducted on this frequency without a change in the proposed countermeasures. Therefore, we moved our scope away from the GPS frequency to an alternative frequency. First we tried spoofing GPS on the 2.4 GHz ISM frequency band. However, were not able to create a reproducible setup with reliable measurements due to the fact that this frequency was too crowded. Even in the woods where the GQRX spectrum analyzer did not identify any usage of the spectrum, we were unable to gather reliable results. Therefore, we had to move over to a different frequency. The challenge here was that no specific frequency provided the same characteristics in term of bandwidth, antenna ERP and duty cycle. Therefore, the only usable frequency closest to GPS we were able to identify was the 1.8775 GHz frequency band. The only adjustment we had to make to the transmitted GPS signal was to reduce the bandwidth to 2.5 MHz.

During our research we identified that in some situations, the spoofed GPS signal was not receivable by the GPS receiver. We experienced this behavior even when the distance between the receiving and transmitting antenna was 1 centimeter. Troubleshooting the problem showed that this behavior only occurred when the USB cable of the transmitting SDR touched the USB cable of the SDR that was receiving the signals. Therefore, we made sure that in each of the experiments, the USB cables of the SDRs were as far apart as possible from each other.

VIII. Conclusion

Based on sub research question 1 we researched the possibility of limiting transmitted GPS signals to a physical location. We determined that it is possible to limit the GPS signal in a way that no decodable subframes can be received with a GPS receiver that is not equipped with a low noise amplifier. When looking at the different amplification levels we used, the GPS signal is decodable at a greater distance when the amplification is reduced. The GPS receiver software also reports seeing satellites based on noise. Therefore, we were unable to determine whether the transmitted GPS signal was completely isolated.

The second sub research question focused on researching the possibility of aiming GPS signals towards a specific direction using a directional antenna. By transmitting a sinusoidal wave, we determined the directionality of our Yagi-Uda antenna. The result of this was that, compared to the side lobes, the back lobe was smaller. We confirmed the same directionality when using the Yagi-Uda antenna to transmit GPS signals. We also confirmed that the reliability of acquiring a GPS location is lower when the Yagi-Uda antenna is positioned at an angle of 90° or 270° towards the GPS receiver. From the back lobe of the Yagi-Uda antenna, we still received subframes. Therefore, the back lobe is still too big in order to completely suppress usable GPS signal.

Determining the effect on the accuracy of the location when splitting the spoofed GPS signal over two transmitters was researched in sub research question 3. When dividing the GPS signal over two transmitters, we identified that time synchronization of the spoofing software is a challenge. By increasing the time difference between the two transmitters, we confirmed that this lowered the precision of the acquired position considerably and vice versa. When comparing the setup of two transmitters with two monopole antennas against two Yagi-Uda antennas, it proved difficult to acquire a position with the Yagi-Uda antennas. When a position could be acquired, the accuracy was a lot lower compared to the monopole antennas.

IX. Future Work

Because we did not have access to a Faraday cage that has the size of at least 30 by 30 meters to, for example, determine directionality. We propose a research into verifying our results on the GPS frequency when one has access to a sizable Faraday cage that allows for this.

Another research where our results could be verified in a different setup is a research that constructs low noise amplifiers and antennas that are resonant at the 1.8775 GHz frequency. The goal of this would be to determine the effect of our approach on GPS receivers that are equipped with a low noise amplifier. Furthermore, when constructing resonant antennas, one could also look into increasing the directionality compared to the directionality of a 13 dBi gain Yagi antenna.

In experiment 3 we spoof the GPS signal over multiple sources. One could conduct a future research into determining the effect of this approach on the existence of (valid) GPS signal in terms of jamming.

Appendix A
FIFO pipe based synchronizer

A simple way of synchronizing the start of commands is by using a named FIFO pipe on a standard GNU/Linux system such as Debian Linux. When the to be synchronized commands try to read from the same pipe, they will both block until something was written to the pipe.

The pipe is first created using a command such as `mkfifo`. After prefixing the commands to be synchronized with a command to read from the pipe, the commands are executed. They are now attempting to read from the pipe, but no data is being written to it. Finally, we write to the pipe and thereby unblock the readers.

See Figure 22 for a demonstration in a graphical environment. Note that the commands in the bottom two terminals are executed before the `>/tmp/fifo` command.

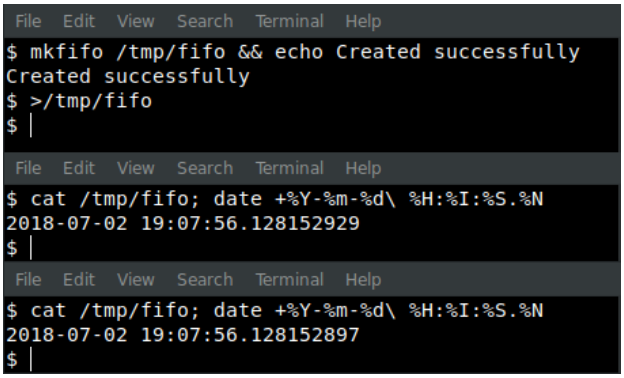

Fig. 22. Demonstration of synchronization based on a named pipe

Note that the time difference between both `date` commands is 32 nanoseconds. When testing this more extensively, it was found that this method is not very reliable: while 25% of 100 runs are below 100 nanoseconds, the median is 1.3 microseconds and the mean is 8.6 microseconds with a standard deviation of 10 microseconds.

Appendix B
Clock based synchronizer

To verify our time synchronization accuracy when using the clock interface as defined by POSIX, two processes were run in parallel with the following code:

```
int target = atoi(argv[1]);
do {
clock_gettime(CLOCK_MONOTONIC, rtime1);
} while (rtime1.tv_sec < target);
printf("%d.%09d", rtime1.tv_sec,
rtime1.tv_nsec);
```

The monotonic clock represents the time since some unknown starting point and is not affected by discontinuous jumps in the system time.

When both processes reach their target time, they stop and print the current time. Comparing the two outputs reveals how long much difference there is between the time at which they exited the busy wait loop. Because both processes ask the same source, namely the kernel, for the current time, it is assumed that the time is accurate between two processes.

Running the experiment 100 times, the difference between the exit times is on average 8 nanoseconds, with a standard deviation of 6 nanoseconds and a median of 6 nanoseconds. This seems sufficient for time synchronization between two transmitters.

References

[1] Nils Ole Tippenhauer et al. “On the requirements for successful GPS spoofing attacks”. In: *Proceedings of the 18th ACM conference on Computer and communications security*. ACM. 2011, pp. 75–86.

[2] Thuy Mai. *Global Positioning System History*. https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html.

[3] James V Carroll. "Vulnerability assessment of the US transportation infrastructure that relies on the global positioning system". In: *The Journal of Navigation* 56.2 (2003), pp. 185–193.

[4] Jon S Warner and Roger G Johnston. "GPS spoofing countermeasures". In: *Homeland Security Journal* 25.2 (2003), pp. 19–27.

[5] Maritime Administration. *2017-005A-GPS Interference-Black Sea*. https://www.marad.dot.gov/msci/alert/2017/2017-005a-gps-interference-black-sea/.

[6] Jie Su et al. "A stealthy gps spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle". In: *IFAC-PapersOnLine* 49.22 (2016), pp. 291–296.

[7] YUAN Jian. *GPS SPOOFING OF UAV*. https://www.syscan.org/slides/2015_EN_GPSSpoofingofUav_YuanJian.pdf.

[8] John F. Guilmartin. *Unmanned aerial vehicle*. https://www.britannica.com/technology/unmanned-aerial-vehicle.

[9] Steve Ragan. *Reports Say U.S. Drone was Hijacked by Iran Through GPS Spoofing*. https://www.securityweek.com/reports-say-us-drone-was-hijacked-iran-through-gps-spoofing.

[10] CNN Wire Staff. *Obama says U.S. has asked Iran to return drone aircraft*. https://edition.cnn.com/2011/12/12/world/meast/iran-us-drone/index.html.

[11] Jonathan Feist. *Does your drone need GPS?* https://www.dronerush.com/drone-gps-10778/.

[12] DroneOmega.com. *How GPS Drone Navigation Works*. http://www.droneomega.com/gps-drone-navigation-works/.

[13] Ben Sullivan. *Drone Pilots Are Buying Russian Software to Hack Their Way Past DJI's No Fly Zones*. https://motherboard.vice.com/en_us/article/8x9jv4/drone-pilots-are-buying-russian-software-to-hack-their-way-past-djis-no-fly-zones.

[14] Ali Broumandan et al. "GNSS spoofing detection in handheld receivers based on signal spatial correlation". In: *Position Location and Navigation Symposium (PLANS), 2012 IEEE/ION*. IEEE. 2012, pp. 479–487.

[15] Kyle Wesson, Mark Rothlisberger, and Todd Humphreys. "Practical cryptographic civil GPS signal authentication". In: *Navigation* 59.3 (2012), pp. 177–193.

[16] Panagiotis Papadimitratos and Aleksandar Jovanovic. "GNSS-based positioning: Attacks and countermeasures". In: *Military Communications Conference, 2008. MILCOM 2008. IEEE*. IEEE. 2008, pp. 1–7.

[17] Ali Jafarnia-Jahromi et al. "GPS vulnerability to spoofing threats and a review of antispoofing techniques". In: *International Journal of Navigation and Observation* 2012 (2012).

[18] Kai Jansen et al. "Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks". In: (2018).

[19] Daojing He et al. "Flight Security and Safety of Drones in Airborne Fog Computing Systems". In: *IEEE Communications Magazine* 56.5 (2018), pp. 66–71.

[20] Andrew J Kerns et al. "Unmanned aircraft capture and control via GPS spoofing". In: *Journal of Field Robotics* 31.4 (2014), pp. 617–636.

[21] Omroep Zeeland. *Vrouw na spoedbevalling in bakkerij Hulst overleden*. https://www.omroepzeeland.nl/nieuws/105624/Vrouw-na-spoedbevalling-in-bakkerij-Hulst-overleden.

[22] Michael Venezia. *What is the Difference Between GNSS and GPS?* https://www.semiconductorstore.com/blog/2015/What-is-the-Difference-Between-GNSS-and-GPS/1550/.

[23] U.S. Coast Guard Navigation Center. *GPS CONSTELLATION STATUS FOR 06/14/2018*. https://www.navcen.uscg.gov/?Do=constellationStatus.

[24] Aarthi Ravikumar. *History of GPS Satellites and Commercial GPS Tracking*. https://www.geotab.com/blog/gps-satellites/.

[25] a1ronzo. *GPS Basics*. https://learn.sparkfun.com/tutorials/gps-basics.

[26] Philip Barker. *What is GPS and how does it work?* https://360.here.com/2015/02/04/gps-work/.

[27] Yuheng He and Attila Bilgic. "Iterative least squares method for global positioning system". In: *Advances in Radio Science: ARS* 9 (2011), p. 203.

[28] GISGeography.com. *Trilateration vs Triangulation - How GPS Receivers Work - GIS Geography*. https://gisgeography.com/trilateration-triangulation-gps/.

[29] Henk Key and Dr Mathias Lemmens. *GPS: Position, Time and Distance*. https://www.gim-international.com/content/article/gps-position-time-and-distance.

[30] Dr. Robert G. Melton. *Details of the GPS position calculation*. https://www.courses.psu.edu/aersp/aersp055_r81/satellites/gps_details.html.

[31] Roger Wattenhofer. *Clock Synchronization*. https://disco.ethz.ch/courses/hs14/distsys/lecture/chapter%2005%20clock%20sync-4up.pdf.

[32] Maryam Sadeghi and Majid Gholami. "Time synchronizing signal by GPS satellites". In: *WSEAS Transactions on Communications* 7.5 (2008), pp. 521–530.

[33] BowlOfRed. *How does GPS receiver synchronize time with GPS satellites?* https://space.stackexchange.com/questions/5423/how-does-gps-receiver-synchronize-time-with-gps-satellites.

[34] Raghav Kapur. *GPS Frequency Bands*. https://www.everythingrf.com/community/gps-frequency-bands.

[35] University FAF Munich. *GPS Signal Plan*. http://www.navipedia.net/index.php/GPS_Signal_Plan.

[36] Kowoma.de. *Transmitted GPS Signals*. https://archive.is/20120804185510/http://www.kowoma.de/en/gps/signals.htm.

[37] Arun Saha. *Spread Spectrum, CDMA and GPS*. http://alumni.cs.ucr.edu/~saha/stuff/cdma_gps.htm.

[38] J. Sanz Subirana, JM. Juan Zornoza and M. Hernandez-Pajares, University of Catalunia, Spain. *GPS Navigation Message*. http://www.navipedia.net/index.php/GPS_Navigation_Message.

[39] Dan Gerrity. *How does GPS spoofing work?* https://www.quora.com/How-does-GPS-spoofing-work.

[40] Guy Buesnel. *DEFCON25: GPS time spoofing now "simple party trick" - researcher*. https://www.spirent.com/Blogs/Positioning/2017/September/DEFCON-25.

[41] NASA. *Broadcast ephemeris data*. https://cddis.nasa.gov / Data_and_Derived_Products / GNSS / broadcast_ephemeris_data.html.

[42] RF Venue. *What is ERP?* https://www.rfvenue.com/blog/2014/12/15/what-is-erp.

[43] De Minister van Economische Zaken. *Regeling gebruik van frequentieruimte zonder vergunning en zonder meldingsplicht 2015*. wetten . overheid . nl / BWBR0036378/2016-12-28.

[44] Impinj. *EIRP and ERP*. https://support.impinj.com/hc/en-us/articles/202756628-EIRP-and-ERP.

[45] everythingRF. *EIRP Calculator*. https : / / www . everythingrf.com/rf-calculators/eirp-effective-isotropic-radiated-power.

[46] RapidTables. *dBm to mW Conversion*. https://www.rapidtables.com/convert/power/dBm_to_mW.html.

[47] Amphenol RF. *What is Insertion Loss and how is it specified?* https://www.amphenolrf.com/faq/technical/what-is-insertion-loss-and-how-is-it-specified.html.

[48] Pasternack Enterprises. *N Male to N Male Low Loss Cable 200 cm Length*. https://www.pasternack.com/images/ProductPDF/PE3C0231-200CM.pdf.

[49] Joseph Crowley. *RF Cable Line Loss Calculations*. https://productsupport.globalstar.com/2017/06/27/rf-cable-line-loss-calculations/.

[50] Times Microwave Systems. *Coaxial Cable - Attenuation and Power Handling Calculator*. http://www.timesmicrowave.com/calculator/.

[51] Agentschap Telecom. *Jammers — Agentschap Telecom*. https : / / www . agentschaptelecom . nl / onderwerpen / jammers.

[52] Brandie Chenoweth. *Why Can't I See the GPS Signal with My Spectrum Analyzer?* http://www.gps-inside.com/?p=88.

[53] EU-publications. *UITVOERINGSBESLUIT (EU) 2017/1483 VAN DE COMMISSIE*. https://publications.europa.eu/nl/publication-detail/-/publication/ed3648d1-83e0-11e7-b5c6-01aa75ed71a1/language-nl.

[54] TA Stansell. "The WM 102 P code channel beats a full house of squared channels". In: *Position Location and Navigation Symposium, 1990. Record. The 1990's-A Decade of Excellence in the Navigation Sciences. IEEE PLANS'90., IEEE*. IEEE. 1990, pp. 557–566.

[55] Catherine Alexandrow. "The story of GPS". In: *50 Years of Bridging the Gap*. DARPA. 2015, pp. 54–55.

[56] Alison Brown, Neil Gerein, and Keith Taylor. "Modeling and simulation of GPS using software signal generation and digital signal reconstruction". In: *Proceedings of ION Technical Meeting*. 2000.

[57] Carles Fernandez-Prades et al. "GNSS-SDR: an open source tool for researchers and developers". In: *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*. 2001, pp. 780–0.

[58] Hengqing Wen et al. "Countermeasures for GPS signal spoofing". In: *ION GNSS*. Vol. 5. 2005, pp. 13–16.

[59] Stefan Kiese. *Gotta Catch 'Em All! – WORLDWIDE! (or how to spoof GPS to cheat at Pokémon GO)*. https://insinuator.net/2016/07/gotta-catch-em-all-worldwide-or-how-to-spoof-gps-to-cheat-at-pokemon-go/.

[60] NotPike. *GPS Simulator*. https://forums.hak5.org/topic/38290-gps-simulator/.

[61] Nuand. *bladeRF Product Brief - Nuand*. https://www.nuand.com/bladeRF-brief.pdf.