Wrocław University of Science and Technology

Faculty of Information and Communication Technology

Field of Study: **Algorithmic Computer Science**

Specialization: **Cryptography and Computer Security**

Master Engineer Diploma Thesis

Functionality structure and Security in Global Positioning Systems

Grzegrzółka Mikołaj

Thesis supervisor

Dr inż. Przemysław Błaśkiewicz

Keywords: Global Navigation Satellite Systems, GNSS, Spoofing, Jamming, GNSS Security

Wrocław 2022

Table of content:

Abstract

Nowadays, global positioning systems play a key and irreplaceable role in any segment of operation. This applies to every utility sphere, from obtaining a precise location in everyday life, through an extensive communication network and air / sea / land traffic, to guidance systems for modern weapon systems and drones. Continuous system innovation, introduction of new satellites into orbit and coordination of various satellite systems together with completely new operational signals accelerate the continuous process of complete GNSS integration in each utility segment. Due to such a large use of the system, it is easy to imagine the importance of its uninterrupted availability and reliability of the operation. Moreover, given how vulnerable are Global Positioning Systems for different types of attacks. Especially the general availability and lack of major security methods for the civil sector GNSS are major contributing factors to the vulnerability to various types of attacks. Starting from standard jamming consisting in covering the actual signal in order to prevent receiving any information, to more sophisticated methods, such as spoofing, in which the attacker is able to imitate the operation of satellite and trick the logical possibility of the system to present the actual location. To make things worse, such types of attacks are nowadays relatively easy to implement, due to the access to a large number of devices and ready-to-use tools.

The aim of the thesis is to present the vulnerability of Global Positioning Systems, both in terms of use and in more specialized applications. Listing and discussing the types of attacks carried out in order to disrupt and cheat systems, also presenting practical solutions for real protection of systems. Additionally, more experimental solutions and individual ideas for GNSS security will be discussed. The practical aspect of this work is to investigate the possibility of GPS spoofing based on SDR in practice.

1. Global navigation satellite systems (GNSS)

By default, the system developed for the needs of the military in the field of reconnaissance and secure communication called NAVSTAR was created in 1974. On its basis, the now well-known GPS was created, which achieved full functionality with 24 satellites in 1993. At the same time, other systems of other countries were created, including GLONASS, BeiDou, Galileo and regional and augmentation support systems. While the essence of the operation is similar, these systems differ significantly in the context of the operating technology used, band frequencies, ranging codes etc.

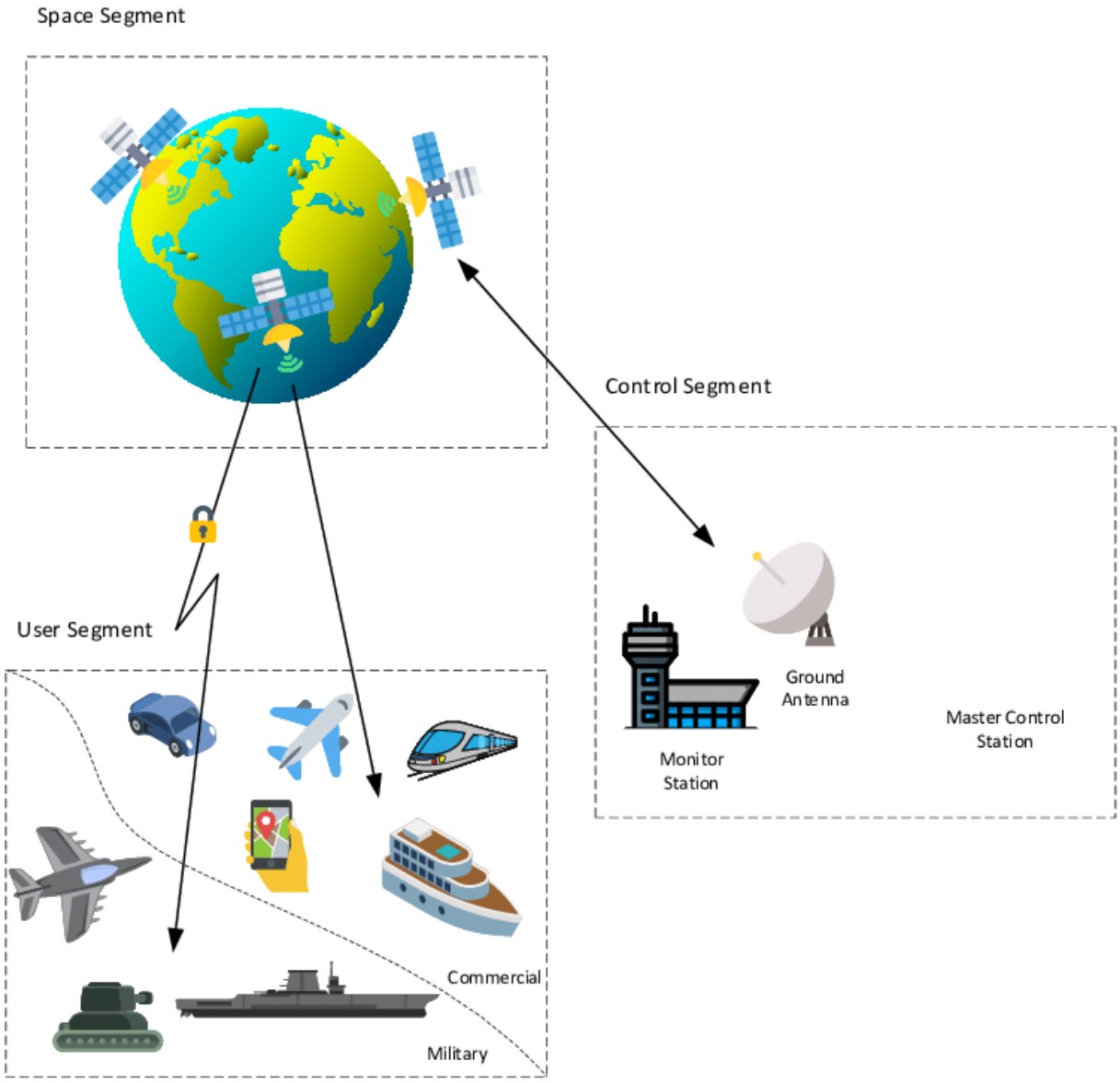

Fig. 1.1 Visualization of GNSS segments

In simple terms, the very operation of the system consists in providing the user with positioning, navigation and appropriate timing (PNT) data based on the most accurate clocks. The operating segments themselves are divided into three. The satellite segment, the control segment including all ground stations providing additional control and monitoring of the satellites, adjustment of their position and clocks, and are also responsible for general access to the information obtained from the satellites. The last segment is users, i.e. the entirety of recipients of the transmitted signal. Basically, the satellite transmits their orbital parameters and timing signal to the receivers, so they can acquire time synchronization and obtain location data.

1.1 Usage and applications of GNSS based systems

Global positioning systems are now used in virtually every consumer segment in the world. Most of the GNSS applications constituting the basic foundation of the operation in the field of modern navigation, any transport services, construction, agriculture and overall survey. Moreover, most of the engineering fields are based on the functioning of GNSS, its activity is also very important in everyday use. In addition, it is also a basic utility element for military positioning systems and for all military applications. Regardless of whether it is about transport capabilities and logistic activities or the guidance structures of modern ground-class missiles, unmanned aerial vehicles, etc. Basically, GNSS is indispensable and ubiquitous in world applications as the basic segment to allow underlying services and systems to function.

One of the most critical and vulnerable GNSS applications is general aviation and maritime utility navigation. Overall, more than 70% of all flights are GNSS assisted [35], including route planning, landing considerations and general aircraft handling, also in severe weather conditions In this case, the question of dependence lies in the use of the ADS-B (Automatic Dependent Surveillance-Broadcast) protocol used in the broadcasting status data of the aircraft and the interpretation of data obtained by the aircraft in navigation with ground stations, of which GNSS is an integral component. Moreover, many current aviation systems, in addition to standard radio communication methods, use additional support for position information from GNSS. For example TCAS (Traffic Alert and Collision Avoidance System), i.e. a system responsible for reducing the possibility of aircraft collisions, or other systems like those responsible for identification and tracking. All GNSS signals used in the aerospace segment are civilian, not encrypted and completely susceptible to various attempts to disrupt or mislead them.

The satellite positioning system itself was created for military purposes and is used there on a huge scale. In basic individual receivers and systems used to support the navigation of own troops, and at the same time to track the movements of the enemy troops. In addition, a significant part of the guidance and tracking systems in the applications of modern precision-guided weapons, cruise missiles and ballistic missiles are based on GNSS satellite guidance. Moreover, all types of military aircraft and unmanned aerial vehicles use GNSS. The very issue of the application of satellite navigation systems is, of course, an element of electronic warfare, so all of the above-mentioned military GNSS applications are at risk of attack.

1.2 GNSS positioning method

The standard positioning method used in GNSS is multilateration, where the positioning guidelines and time synchronization are determined based on a Time of Arrival (ToA) calculation (time needed to reach the receiver from the satellite). The minimum number of satellites needed to determine a position is four. Simplifying a bit, the whole process comes down to the concept of calculating the pseudorange for each of the used satellites and then calculating the Time Difference of Arrival (TDoA) in order to make comparisons for each individual satellite ToA‘s. The general formula for calculating the pseudoranges *P* for each one of four satellites will be given as:

$$P_1 = \sqrt{(x_1 - x_R)^2 + (y_1 - y_R)^2 + (z_1 - z_R)^2} + c * \Delta_E + \varepsilon \tag{1.1}$$

$$P_2 = \sqrt{(x_2 - x_R)^2 + (y_2 - y_R)^2 + (z_2 - z_R)^2} + c * \Delta_E + \varepsilon \tag{1.2}$$

$$P_3 = \sqrt{(x_3 - x_R)^2 + (y_3 - y_R)^2 + (z_3 - z_R)^2} + c * \Delta_E + \varepsilon \tag{1.3}$$

$$P_4 = \sqrt{(x_4 - x_R)^2 + (y_4 - y_R)^2 + (z_4 - z_R)^2} + c * \Delta_E + \varepsilon \tag{1.4}$$

Let (x_i, y_i, z_i), i={1, 2, 3, 4} be the coordinates of the i-th satellite and $x_R, y_{R,} z_R$ represents cordinates of GNSS receiver. We also define the difference between the time of a given GNSS and the internal time of the receiver as Δ_E. Parameter c is the speed of light, and we should also include ε to account for other potential errors. Therefore, in order to calculate our unknowns, i.e. the data on the receiver's position and its local clock offset, the equation for several satellites must be solved. Essentially, each signal emitted by the satellites in the system includes an identifier for its landmark made up of the coordinates of its position and the time of broadcasting the signal. It should also be taken into account that, unlike satellites equipped with atomic clocks, the receivers are only equipped with an accurate chronometer that receives signals at certain times and offsets.

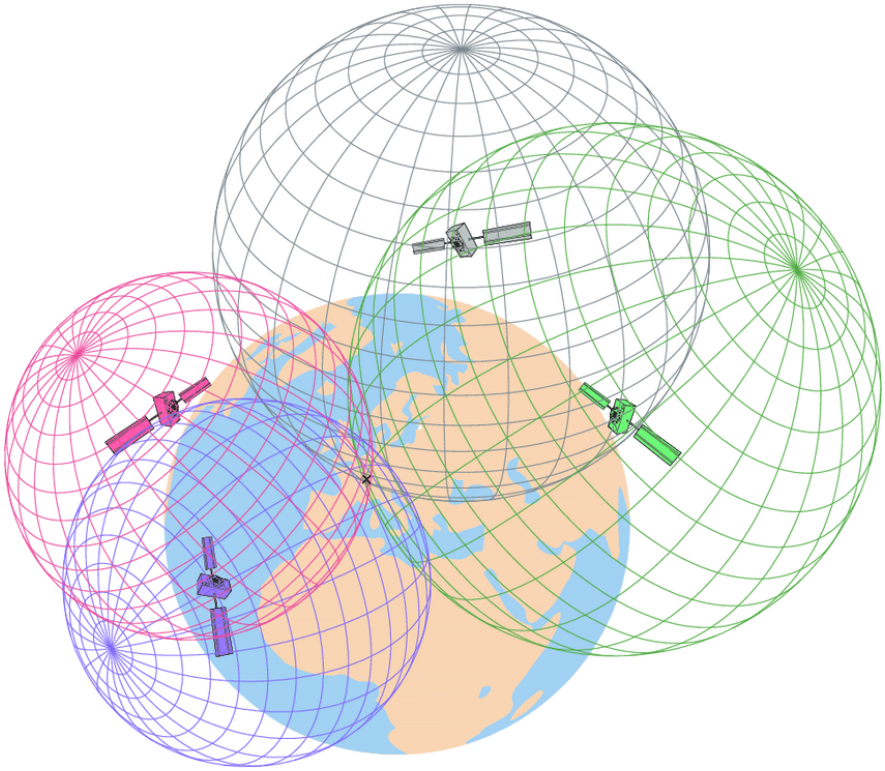

Fig. 1.2 Visualization of GNSS multilateration

An important thing to mention is also the ongoing tracking process that allows civil GNSS to accurately confirm the start of the used navigation message. Based on the satellite ephemeris data, the overall frame start time, together with the calculated receiver time, the standard time needed for signal transmission from the satellite transmitter to the receiver is calculated. In general process used by GNSS to obtain pseudorange, the time obtained from the satellite transmitter is compared to the receiver in relation to the speed of light. The pseudorange itself is simply the distance it takes for the signal to travel from the transmitter to the tracking satellite,

taking into account possible errors in the measurement by the clocks. In order to calculate the receiver position and synchronization with the calculations of the global time used by the GNSS system, we compare the pseudorange obtained from different satellites.

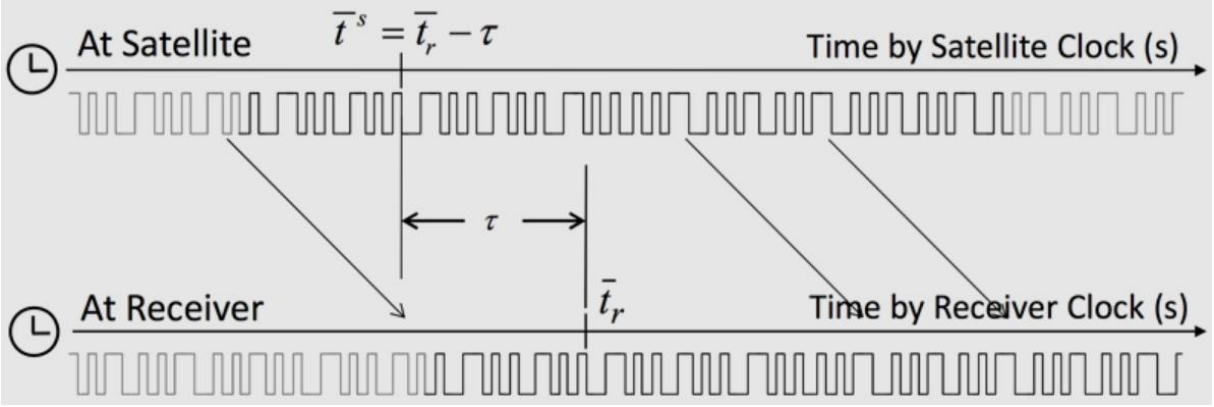

Fig. 1.3 Visualization of pseudorange measurments [50]

1.3 GNSS signals characteristics and processing

Most GNSS systems transmit two types of signal, a standard signal for civilian receivers, access to which is completely unprotected and generally available, and a special signal for military operators secured using at least secret spreading codes (usually resisted to cryptoanalisis). Time is crucial for the correct operation of the system. Each satellite is equipped with an atomic clock, thanks to which its signal is precisely synchronized with the entire system. At the same time, the satellites together with several terrestrial transmitters form a specific time correction network.

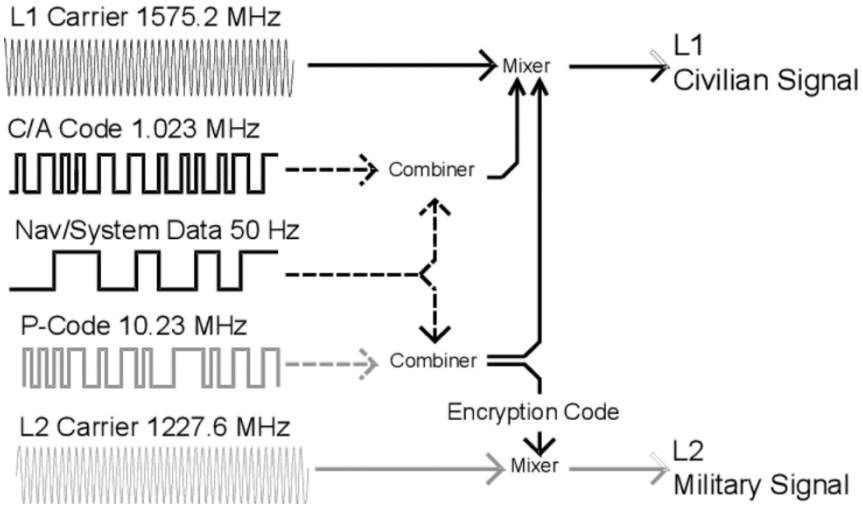

Fig. 1.4 GPS satellite signals L1 and L2

All GNSS systems have their own specific signal characteristics in their own usage segment. Nevertheless, there are many GNSS and signals that they are using, so it is necessary to counteract the possibility of attenuation and interference of signals between GNSS. The systems do use similar frequencies, however they use different ranging codes to prevent interference. The identification is done using a Pseudorandom Noise Number (PRN) in order to apply Code Divison Multiple Access (CDMA). These codes are referred to as C/A, or Coarse and Acquisition. Standard civilian signals also have an additional low bit rate navigation message. This is used to provide information on the calibration of satellite clocks, position data, ionospheric model data for correcting potential errors, and overall mapping of the remaining satellites in the constellation.

For signal processing in GNSS, we have a receiver responsible for receiving and reconstructing the signal using a signal processor. Then the reconstructed signal is compared with the reference signal of the receiver. The received signal is Doppler shifted to account for the constant movement of the satellite. The code range checking process is carried out by correlating the generated and received code. The signals are sent on a time basis to obtain the best possible correlation.

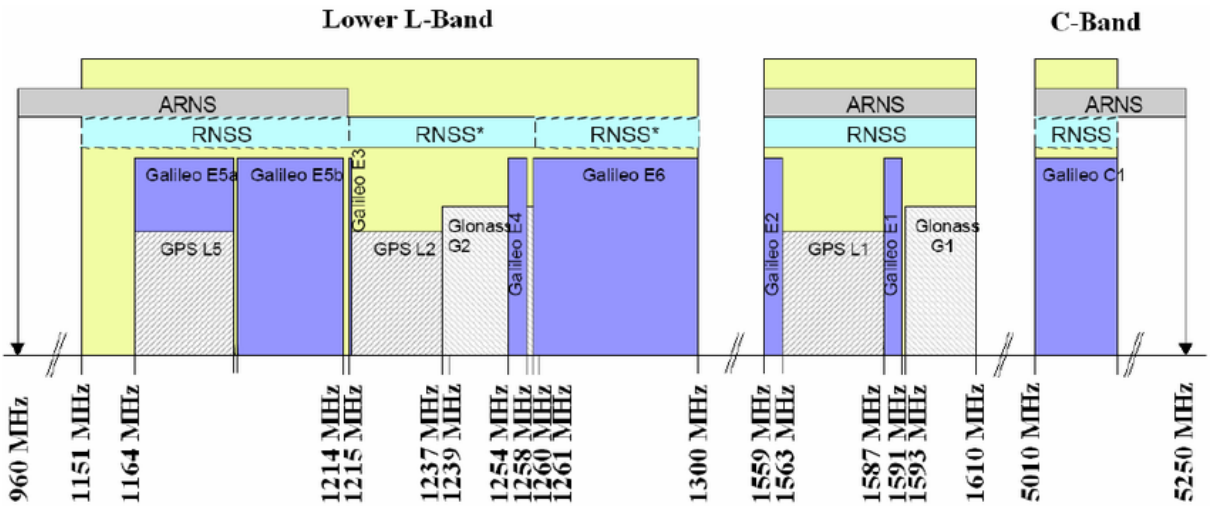

Fig. 1.5 Radio-Navigation Satellite Systems defined for GNSS

Taking GPS as an example, [17] signal reaches the user on two carrier frequencies L1 = 1575.42 MHz (wavelength 19.029 cm) and L2 = 1227.6 MHz (wavelength 24.421 cm). The comparison of the phase difference of both signals allows for the precise determination of the propagation time, which varies slightly as a result of the variable influence of the ionosphere, but not to a degree that makes it impossible to determine coordinates. The identification of the

satellites is based on the split method. All satellites transmit on the same frequencies, but the signals are modulated with different codes. Signals from different satellites are separated after demodulation using uniqe binary sequence know also as Gold code [51].

		GPS	GLONASS
Satellites	Available satellites	32	24
	Orbital planes	6	3
	Orbital inclination	55°	64.8°
	Orbital altitude	20.180 km	19.140 km
	Period of revolution	11h 58m	11h 15m
Signals	Separation technique	CDMA	FDMA
	Fundamental Frequency	10.24 MHz	5.0 MHz
	Carrier frequency L1/G1	1575.42 MHz	1598.0625 - 1609.3125 MHz
	Carrier frequency L2/G2	1227.60 MHz	1242.9375 - 1251.6875 MHz
	Code clock rate C/A	1.023 MHz	0.511 MHz
	Code clock rate P	10.23 MHz	5.11 MHz
	Code length C/A	1023 Chip	511 Chip
	Code length P	6.187104 * 10^12 Chip	5.11 * 10^6 Chip

Tab. 1.1 GPS and GLONASS comparison

If we compare it with GLONASS, [17] satellites of this system transmits two types of signal: the standard signal ST - Standartnaya Tochnost and the high precision signal VT - Visokaya Tochnost. The signals use similar DSSS (Direct Sequence Spread Spectrum) coding and PSK (Phase Shift Keying) binary modulation as GPS. All GLONASS satellites transmit the same code as their ST signal, however each transmits on a different frequency using the FDMA (Frequency-Division Multiple Access) technique. It covers each side of the transmission from 1602.0 MHz, known as the G1 band. The standard center frequency is 1602 MHz + n * 0.5625 MHz, where n is the satellite frequency channel number (n = -7, -6, -5,…, 0,…, 6, previously 0,…, 13). The signals are transmitted using right-hand circular polarization and an EIRP of between 25 to 27 dBW, or approximately 316 to 500 watts. The G2 band signals use exactly the same FDMA as the G1 band signals, but different transmission technique at 1246 MHz, and their center frequency is given by the following equation: 1246 MHz + n * 0.4375 MHz, where n covers the same range of frequency numbers satellite channel like G1. Since 2008, a new type of CDMA (Code Division Multiple Access) signals have been used in GLONASS systems, part of the exact specification remains classified, but according to the information provided by Roskosmos, there will be three open and two restricted CDMA signals. The specification for the L3 band will have the center frequency given by the formula 1202

MHz + n * 0.4375 MHz, so the separation between the carriers will be the same as for the G2 band.

What is relevant here is that the GPS L1 band is more accurate due to doubled value of ranging code chipping rate (the overall number of pulses per second of transmitted or received code) compared to GLONASS (1023 Chip vs 511 Chip).

Of course, both systems also have a secured P-code (L2/G2 band) available only to authorized military personnel. The P-code provides very accurate location information up to 2 meters. In the case of GPS, we also have an autonomous M-code containing a PRN code with a different length transmitted at a frequency of 5.115 MHz, in this case the user's position is calculated only on the basis of the M-Code signal. On the next page also the comparison with other systems.

	GPS	GLONASS	Galileo	BDS
First Launch	1978-02-22	1982-10-12	2005-12-28	2017-11-05
FOC	1995-07-17	1996-01-18	/	/
Service type	Military/civil	Military/civil	Commercial/open	Military/civil
No. of designed satellites	24	24	30	30
No. of orbital planes	6	3	3	3 (MEO)
Orbital inclination	55°	64.8°	56°	55° (MEO)
Orbital altitude	20,200	19,100	23,222	21,528 (MEO)
Orbital period	11 h 58 m	11 h 15 m	14 h 04 m	12 h 53 m (MEO)
Coordinate system	WGS84	PZ-90	GTRF	BDCS
Time system	GPST	UTC(SU)	GST	BDT
Modulation mode	CDMA	FDMA	CDMA	CDMA
Frequencies	L1:1575.42 L2:1227.60 L5:1176.45	G1:1602.00 G2:1246.00 G3:TBD	E1:1575.42 E5a:1176.45 E5b:1207.14 E6:1278.75	B1:1575.42 B2:1176.45 B3:1268.52

Tab. 1.2 Main GNSS signals characteristics comparison

1.4 GNSS operation and errour sources

In the case of the GNSS operation principle, the navigation signals are transmitted by satellites using the parts of L-band and optimized depending on the system and signal application, although their structure is quite similar. The standard broadcast satellite signal can be represented as:

$$s_s(t) = \sqrt{2P_s} * c_s(t) * m_s(t) * \cos(2\pi f_{RF} t) \tag{1.5}$$

s is a given satellite, P_s determines the transmit power, $c_s(t)$ is the chipping sequence (pseudo-random code), $m_s(t)$ is the navigation message, and f_{RF} is the standard value of the carrier frequency. The operational dependence on time is defined as t. In transmitting the beacon message, symbol rate per seconds in the range 20 to 100 is used, and these symbols are encoded in the signal as +1 or -1. Depending on the signal type, chipping sequence also uses encoding as +1 or -1 at a higher rate in the range from 0.5 to 10 MHz for encoded signals, for civilian use the chipping sequence value is periodic.

As far as the received signal is concerned, the issue of signal propagation delays is important, as it causes further differences in clocks between satellites and receivers, the basic form of the received signal will be as follows:

$$r_s(t) = \sum_{s=1}^{S} \sqrt{2 * \frac{S}{N_o}} * c_s\big(t - \Delta_E(t)\big) * m_s\big(t - \Delta_E(t)\big) * \cos\Big(2\pi f_{RF}\big(t - \Delta_E(t)\big)\Big) + W(t) + \varepsilon(t) \tag{1.6}$$

Received signal $r_s(t)$ in the case when S determines the number of satellites. By default, the minimum number of satellites for determining the position is four, additionally, we take into account the value of Signal to Noise ratio defined as $\frac{S}{N_o}$. W stands for white noise value. The rest of the markings remain the same as in formulas 1.1-1.4. The signal strength of considered satellites remains the same for all of them. The received signal strength is under standard conditions at the level of -130 dBm. The signal amplitude value is less than the noise amplitude value. This is possible as long as the reference is the same as the underlying signal and as long as the averaging process produces an effective bandwidth small enough to drop the noise power,

the signal can thus be "dug out of noise". To calculate the Doppler shift $f_{D,S}$ value for a considered satellite, the following formula should be used:

$$f_{D,S} = -\frac{f_{RF}}{c} * \frac{d\Delta_S(t)}{dt} \tag{1.7}$$

It should also be noted that the received signal $r_s(t)$ while being digital processed is filtered by the front-end of the receiver. During digital processing, the receiver synthesizes a replica of the transmitted signal with predicted delay values and Doppler shift, and through the matched approach filter it takes the values $\hat{\Delta}_S$, $\hat{f}_{Dopp,S}$. Which can be described as:

$$\hat{\Delta}_S, \hat{f}_{D,S} = arg \max_{\Delta_S, f_{D,S}} \left| V_{C,S}(\Delta_S, f_{D,S}) \right| \tag{1.8}$$

where $V_{C,S}(\Delta_S, f_{D,S})$ is correlator value.

An important issue is also the analysis and understanding of the possibility of potential errors, the basic assumption regarding the accuracy of positioning requires the knowledge of possible error thresholds. Basically, GNSS signals have a very low power, and during the overall signal transmission, they are thus susceptible to many possible signal disturbances and errors of the infrastructure itself, and also therefore, due to the multitude of error sources, we call the measured range a pseudorange.

The most crucial thing for GNSS is time, all the results generated by receivers come from time measurements. In this case, only the satellite segment is endowed with incredibly precise atomic clocks which, despite their excellent accuracy, do actually drift a small amount. An example satellite clock error of one nanosecond will correspond to a value of 30 cm of the error pseudorange (the actual error will most likely be more). Unlike the clocks used in the satellite segment, the receivers (and potentially the SDR-simulated transmitters) are equipped with inexpensive crystal clocks. So the real error of the receiver is much greater than the error of the satellite's atomic clock. Usually, in addition to the possibility of using much better clocks, a comparison between satellites is used for correction purposes, or possibly error estimation as an additional unknown parameter during position calculations.

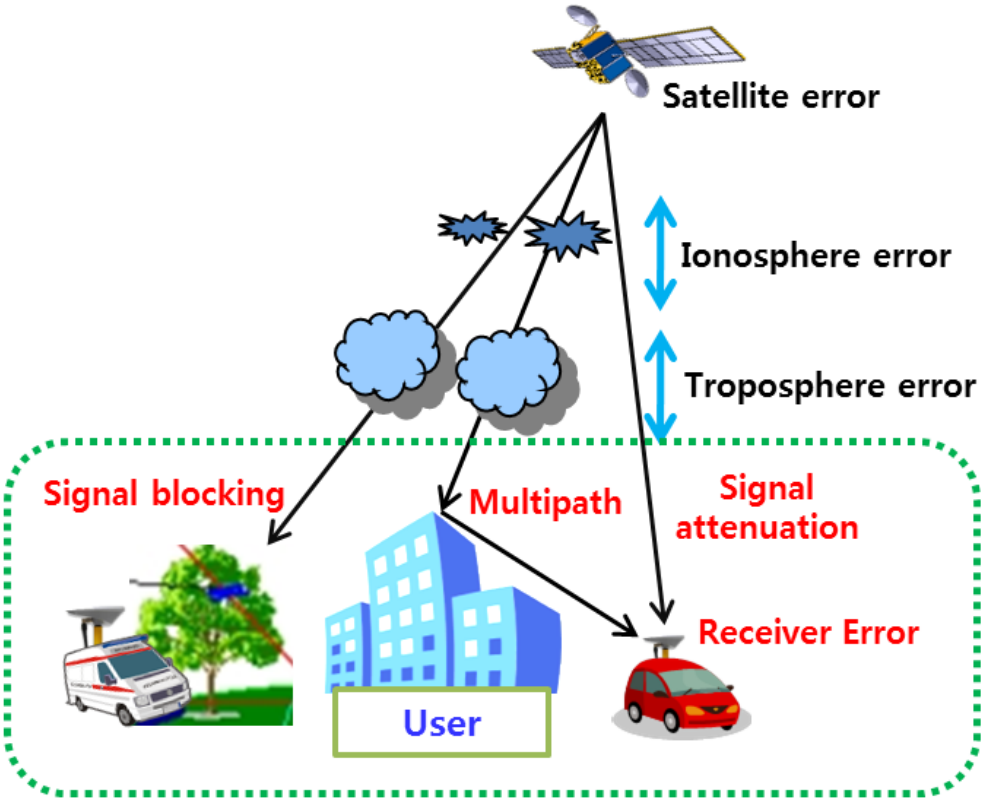

Fig. 1.6 Possible GNSS error sources

In addition to time errors, there are also errors related to signal propagation due to environmental influences. In the case of tropospheric delay, they occur depending on the signal propagation path and the interaction resulting from changes in humidity, temperature and atmospheric pressure. In addition to tropospheric delays, there are also ionospheric delays resulting from total solar activity, specific season, time, and location. In addition, GNSS signals are vulnerable to multipath interferences due to the possibility of reflecting the signal from natural objects or buildings. In this case, the reflected signal travels a little further to reach the antenna, so the reflected signal is received by the receiver with a delay.

Additionally to the sources described, there are also intentional system disruptions that are of most interest to us. Like signal jamming consisting in broadcasting malicious radio frequencies in order to prevent GNSS receivers from receiving the appropriate signals. However, most important type of attack in our case is GNSS signal spoofing, also much more difficult to detect. Spoofing is based on generation of a signal similar to the actual GNSS signal. Attacks of this type also have an impact on the possibility of errors in GNSS signal propagation, but they will be described in detail later in the Section 2 of this work.

2. Global satellite systems vulnurabilities

Although the world nowadays is unable to do without the use of GNSS, and the technology itself is effective, it also has a number of vulnerabilities. Starting with the environmental disadvantages, the main problem in urbanized areas is the lack of direct line-of-sight in the case of GNSS satellite signals, which does not allow to obtain a permanent possibility of precise positioning. Moreover, the very design of the signals based on radio frequencies results in an increased susceptibility to ionospheric delays or a series of radio wave interferences. The construction issue of such systems, which may cause additional errors due to errors resulting from the types of signal modulation, additional convergences in the functioning of integrated GNSS and the entirety of errors related to clocks. Also important are weather conditions in space and this conclude most of the unintentional vulnerabilities.

Another form of GNSS vulnarabilities are those that can be deliberately used by someone to disrupt or maliciously modify the operation of the system, those kind of vulnerabitilies will be a major part of this thesis. The main problem enabling the implementation of attacks on GNSS is the extreme weakness of the transimated signals (it depends on the type of the satellite). Measurments of $\left(\frac{S_c}{N_0}\right)_{eff}$ comes from method presented by authors in [53].

System	Satellite Type	Transmit Power [W]	$\left(\frac{S_c}{N_0}\right)_{eff}$ [dB-Hz]
GPS	IIA	50	45
	IIR	60	38
	IIR-M	145	42
GLONASS	IIF	240	43
	M (standard)	25-85	43
	M+	100	43
	K1	105 or 135	43
Galileo	IOV	95-105	44
	FOCe	265	45
	FOC	265	45

Tab. 2.1 Transmit power and effective Carrier to Noise ratio of different Satellite Types

This leads to the increase of possibility for in-band interference. In the case of jamming, i.e. deliberate transmission of electromagnetic signals in the GNSS frequency band, we try to overpower weak GNSS signals in general, which results in the impossibility of further reception

of the signal. Although this practice is illegal, possession of small jamming devices is not regulated everywhere around the world with the same strictness. In addition, jamming is one of the basic elements of electronic warfare, related to preventing the opponent from general use of systems based on the electromagnetic spectrum, mainly in the field of logistics, communication and radar. In this case, there is also the potential for unintentional interference, due to the fact that some GNSS frequencies are also used by certain radar systems and the general fact that signals are sensitive to external interference, such as air navigation systems, amateur radio usage, TV harmonics or a damaged electronic radio equipment.

The second form of attack is spoofing which, unlike jamming, consists in generating a copy of the actual GNSS signal using changed parameters to confuse the system and cause a false positioning solution. Compared to jamming, which is closer to brute-froce attacks, spoofing is a more sophisticated method that requires much more technological intensity and knowledge. In addition, spoofing is usually undetectable (a copy of the correct signal) and even if it is not possible to force a different solution of the positioning coordinates, the signal itself may lead to jamming as an additional effect of the attack.

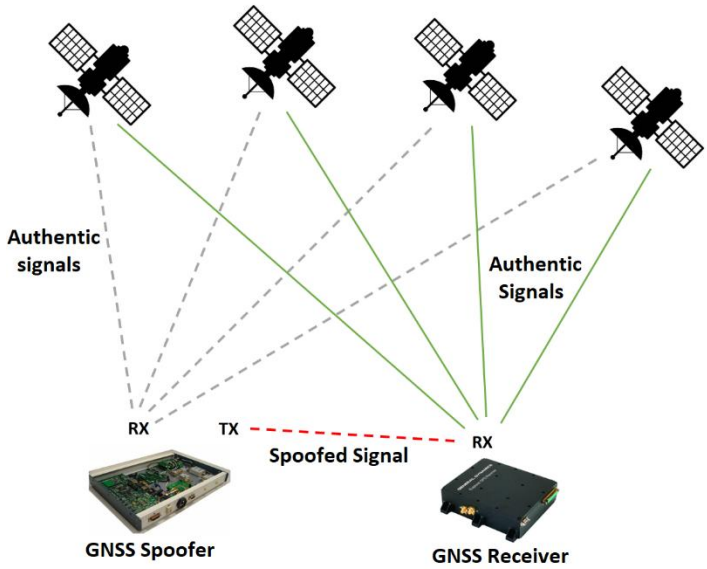

Fig. 2.1 Spoofing attack visualization

A slightly simplified form of spoofing is the so-called meaconing, i.e. reception and retransmission of the captured GNSS signal. In this case, the effect of such an action is also a bad positioning result transmitted by the GNSS receivers, it is due to the fact that in the case of re-transmission or reception of the signal, the actual delay value in the GNSS signal is changed. As the system uses such a delay calculation and compares it with the actual GNSS signals delay, consequently the positioning result is incorrect.

2.1 GNSS Jamming

The vulnerability of GNSS to the form of various attacks based on system disruptions with the use of publicly available devices is now well known, and there have been many studies describing the possibility of their implementation. Based on the weakness of GNSS signals, it has been proven how simple it is to disrupt the functioning of GNSS with various types of widely used receivers.

The simplest forms of attack are the usual form of continous electromagnetic wave emission with constant amplitude and frequency values, or a slightly more advanced form, i.e. chirp signal. In this case unlike continuous wave, there is a constant shift of the frequency center to cover the larger bandwidth. These types of jammers mainly rely on the ability to overpower the GNSS signal and the overall occupation of the signal spectrum.

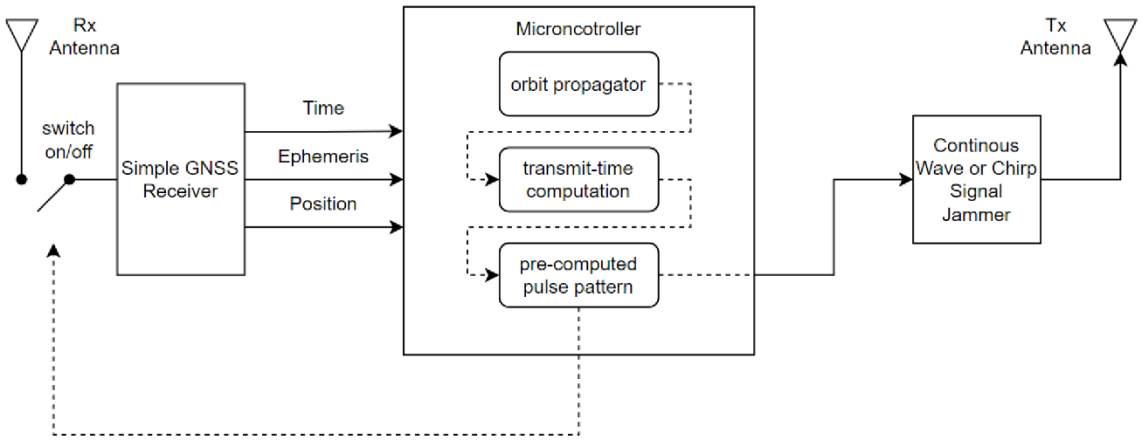

Fig. 2.2 Construction of typical Continous Wave or Chirp Signal Jammer

These types of devices, also refered as PPDs (Personal Privacy Devices), can be very small and relatively cheap to buy. There are various PPD models and their applications, usually used in

the civilian segment, such as hiding your position by drivers, interfering with anti-theft systems (GNSS based), or simply to hide your position for safety. In the case of these devices, the effective jamming range ranges from several meters to several kilometers. Often, the range declared by the manufacturer is in fact much greater. In addition, some of these cheaper devices are able to cover the military GNSS bands.

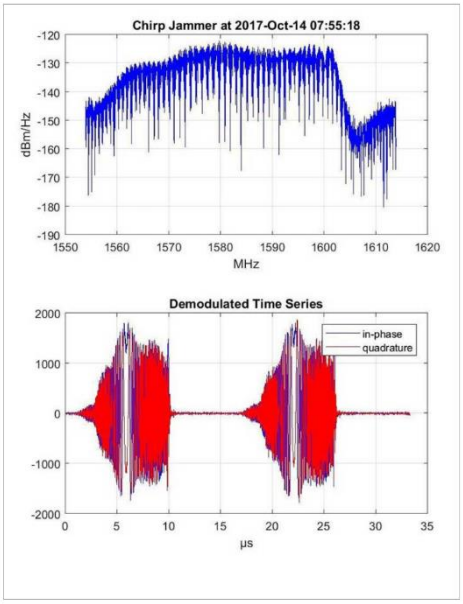

Fig. 2.3 Chirp Jammer signal example [7].

The general extent of jammer-induced interference can be defined as: complete receiver loss of GNSS signal tracking abillity, pseudorange measurment errors, also high demodulation error rates and possibility to detect false signals. We can measure how effective interferences caused by jammer can be by comparison of the effective carrier S_c to noise density ratio N_0. The higher the jammer power and the more the jammer signal matches the satellite signal, the higher the noise value will be. It's described as reduction of received signal to noise ratio $\frac{S_c}{N_0}$ and comparison with effective ratio $\left(\frac{S_c}{N_0}\right)_{eff}$ [21].

$$\left(\frac{S_c}{N_0}\right)_{eff} = \frac{S_c \int_{-B/2}^{B/2} G_s(f)\, df}{N_o \int_{-B/2}^{B/2} G_s(f)\, df + J_I \int_{-B/2}^{B/2} G_s(f) G_I(f)\, df} \tag{2.1}$$

$G_s(f)$ defines the spectrum of the satellite signal $s(t)$, $G_I(f)$ defines the spectrum of the interference signal $I(t)$, and B defines the bandwidth. J_I stands for overall interference power.

If we want to calculate only the jammer signal value to GNSS signal, the following formula should be used (Friss equation):

$$\frac{J}{S_T} = P_J + G_J - P_T - G_T + 20\log(d_T) - 20\log(d_J) \tag{2.2}$$

The formula is given in dB. In this case, J is the jamming signal strength (dB), S_t is the transmitter signal strength (dB). P_j to jammer output power (dBW), P_T to transmitter output power (dBW). G_J is jammer antenna gain (dBi), G_T is transmitter antenna gain (dBi). d_J is distance from jammer to receiver (meters), and d_T is distance from transmitter to receiver (meters).

Jammers differ in construction and application, moreover different types of jammers, despite some similarity may have a different impact on a given receiver. Civil PPD jammers can be characterized in terms of their construction, some of them use auxilary power supply provided usually by car lighter and their construction shows this. In addition, there are also those with a rechargeable battery and a group of jammers that differ in the lack of an external antenna (easier to hide). Jammers also distinguish the type of transmitted signal, starting with Class I. Contionous Wave, i.e. a single sinusoidal interference signal within GNSS frequency, which can be represented as:

$$J_{CW}(t) = Acos(2\pi f_{CW} t + \varphi_0) \tag{2.3}$$

where we identify interference signal as J_{CW}, with CW standing for Continous Wave, f_{CW} is interference signal frequency, A is the amplitude and φ_0 is the initial phase of interference signal. Another type of jammer is the Class II. Chirp Signal with Single Saw Tooth Function, a signal where wave interference consists of a sinusoidal signal whose frequency is repeatedly sweeped across certain bandwidth. This type of signal is most often used in the construction of in-car jammers. Next one is Class III. Chirp Signal with Multiple Saw Tooth Functions, this type consists of more than one saw tooth waveform. General mathematical representation for chirp interference can be described as:

$$J_{Ch}(t) = Acos(2\pi f_{Ch}(t) + \varphi_0) \tag{2.4}$$

where in this case J_{CH} is the interference signal and Ch stands for Chirp, $f_{Ch}(t)$ is the instantaneous chirp frequency of the signal at time t. The rest of the notations remain the same

as in 1.8. The frequency span for this type of PPD is commonly between 7 and 60 MHz, the sweep time vary but is usually order of tens of microseconds. The last is Class IV. Chrip Jammer with Frequency Burts, signal is similiar to previous one but the usage of frequency bursts can almost double the bandwidth for a short time period.

Figure 2.4 shows the different signal characteristics of the discussed jammers, the plots on the left side show the time domain of the signals, and the plots on the right side show the frequency domain representations of each of the signals. In Fig. 2.4 (1.), a narrowband CW signal is shown, the frequency of this signal is constant across the plot. Fig. 2.4 (2.) shows a signal composed of three frequency components in its interval. The next signal, visible on Fig. 2.4 (3.) is a type of signal whose instantaneous frequency value changes over time. The last signal of Fig. 2.4 (4.) is a signal representing freqency bursts [31].

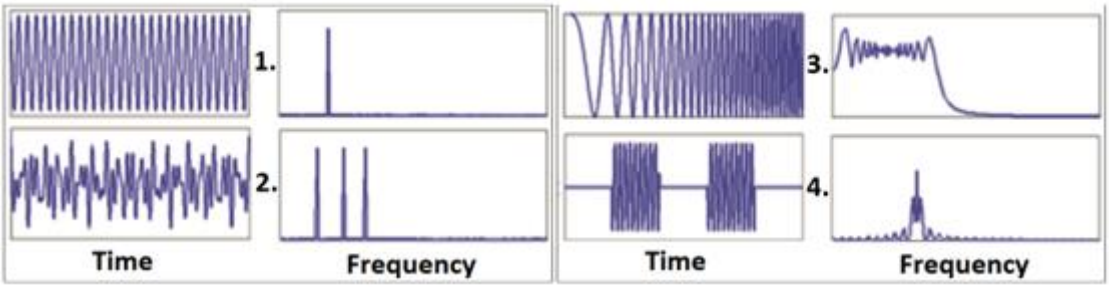

Fig. 2.4 Comparison of jammer signals [31].

Some jammers also generate Gaussian Noise, in this case the source of the jammer propagates wideband noise across the entire frequency of the GNSS target band. Also, disruptions caused by this type of jammer cannot be filtered by Band-stop Filters because the power content value is allocated across all frequency components.

In addition to the normal civilian PPDs, there are also high-power military jammers. In the case of portable utility devices, this type of jammer is often available to the combat units of at various levels. These devices have repeatedly proven their necessity in the face of modern warfare, in addition to the ability to block various types of radio signals and disrupt the operation of positioning systems, they also proved to be very effective in counter-terrorist activities by being able to block the operation of basic detonators of various types of improvised explosives. Unlike civilian jammers, the range of operational frequencies in the case of military devices is much larger.

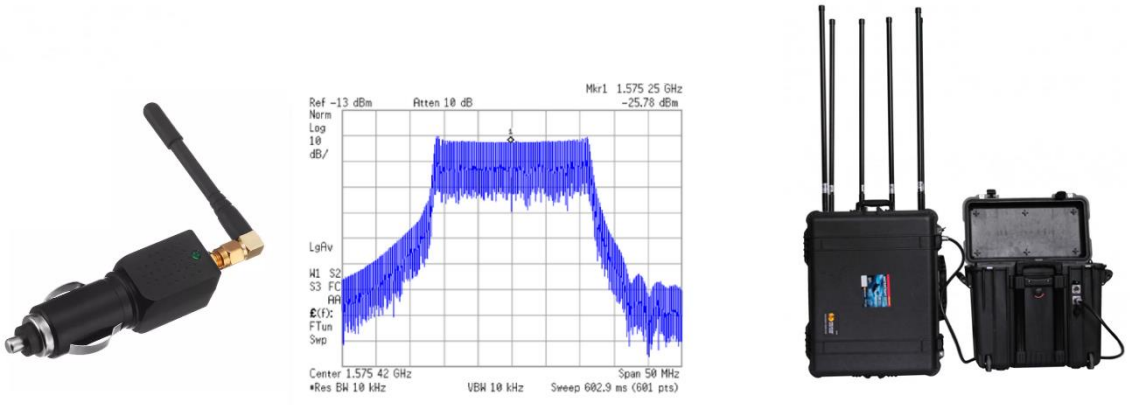

Fig. 2.5 Civilian GP5000 in-car Jammer with signal characteristic (left)
Powerfull Military Falcon Jammer (right)

GP5000 is mainly designed to jam L1 GPS frequencies, while Flacon cover all frequencies used by GNSS, and also AMPS, N-AMPS, DCS, NMT, TACS, GSM, CDMA, TDMA, IDEN, UMTS, VHF, UHF, WiFI, 3G / 4G / 4G LTE and WiMax. The jamming range of the GP5000 is about 15m +, while the Falcon's operating range is about 500-1000 meters. The output power in the case of the GP500 is about 200 mW, in the case of Falcon the output power is adjustable, although the total power is 100W per Band.

2.2 GNSS Jamming impact

Typically, the primary purpose of GNSS jamming is to perform complete GNSS service deny using enough transmitted power. This form of action is usually easily recognizable, although an indirect form of attack may also occur. In this case, the attack strength also depends on the power, the intermediate value of the power causes degeneration of the receiver's operation, but the interference signal strength is not high enough for the receiver to lose the lock or access to satellite signals. [3] The jamming effect on high senstitivity of the GNSS receiver is seen below.

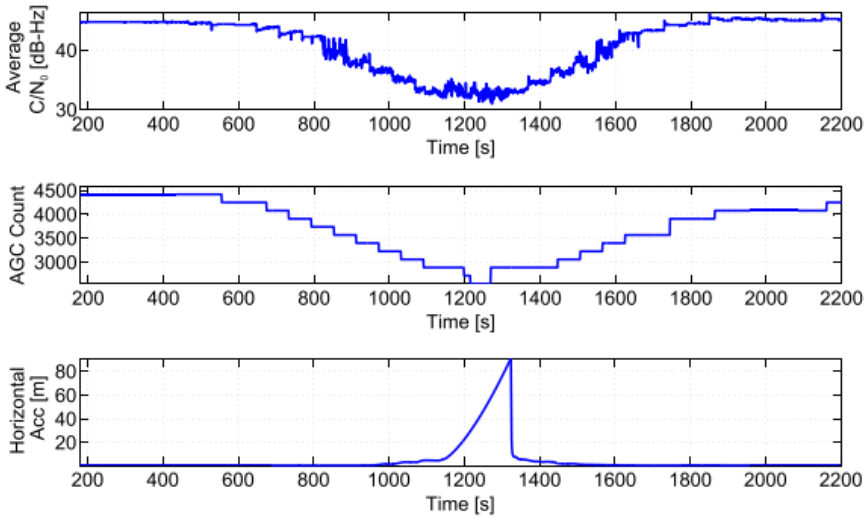

Fig. 2.6 Graphs showing the jammer interference signal impact on high sensititvity GNSS receiver [3]

In this case a typical in-car lighter jammer was used which was controlled by an attenuator and the total jammer to noise ratio was between 55 and 92 dB-Hz.

2.2.1 Impact on Front-End Stage

When discussing the general jammer impact on the receiver, the first element is the Front-End stage. It is an element responsible for filtering the signal in the used band by down-converting it to a selected intermediate frequency by converting the signal from analog to digital. The receivers used in GNSS are multi-bit, therefore they require automatic gain control (AGC) between the analog-digital converter (ADC) and the analog Front-End part [3] . Looking at the graphs of Fig. 2.6, it can be seen how jamming impacts the AGC and how the ADC output is modified becouse of it.

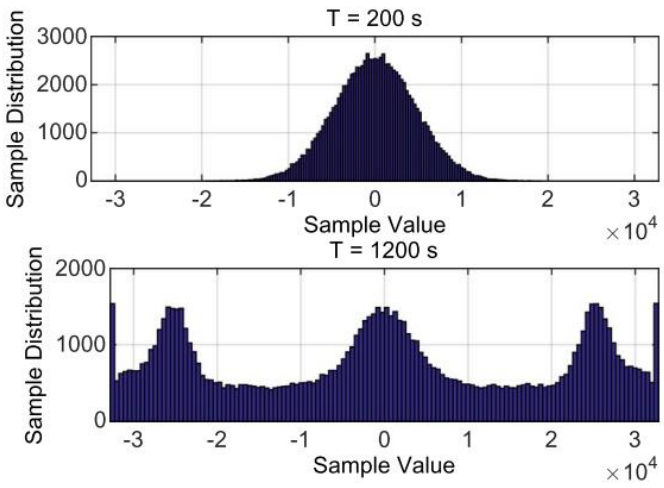

Fig. 2.7 Diagrams showing samples of ADC output without interferences (top) and when affected by swept Jamming signal (bottom) [3]

The effect is shown in Fig. 2.7, where the event shown in Fig. 2.6 is analyzed at instants T = 200 seconds and T = 1200 seconds. When a signal is jammed, the values for the sample statistic are altered and deviations from the Gaussian distribution can be seen. The Front-End stage has many highly non-linear components and in the case of being subjected to a strong jammer signal, various front end elements such as filters or amplifiers can be directed to work outside of their default region.

2.2.2 Impact on Acquisition Stage

Another form of impact is the jammer signal effect on the Acquisition Stage. This is the component responsible for providing the approximate code delay estimation of a given signal and the approximate values of the Doppler frequency estimation. Similarly, correlation of the input signal with local copies of its code and its carrier is the main task performed by the Acquisition block, this is how the cross-ambiguity function (CAF) is evaluated. In general, CAF is a Doppler frequency test with code delays performed by the Acquisition block [3]. Fig. 2.8 illustrates the whole process, in case when GNSS signal is not affected by the interference, only single dominant peak should be visible on the graph.

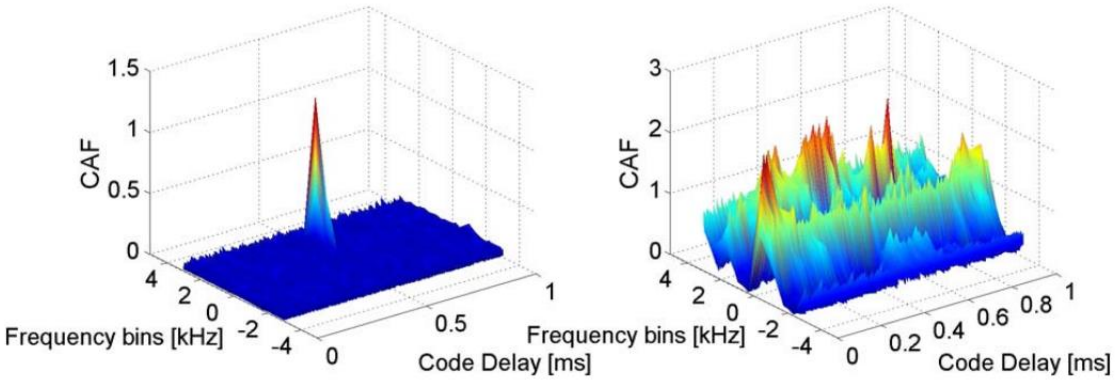

Fig. 2.8 Comparison between the CAF of GPS L1 C/A signal, without interference (left) and affected by -130 dBW Continous Wave signal (right) [3]

2.2.3 Impact on Tracking Stage

When the signal is detected by the Acquisition stage, it is then passed to the Tracking stage. This element is responsible for providing the correct estimates of the signal parameters. It is these parameters that are used in GNSS to calculate things such as pseudo-ranges, phase carriers, and Doppler shifts. The jamming interference impact on the findings of Tracking stage results in erroneous measurments and leads to significant errors. Typically, the tracking stage uses closed-loop architecture, in which case the tracking loops track different elements of the signal. Those tracking loops are built using signal correlators, loop discriminators and loop filters. Loop discriminators use the output signal correlators to determine the error value between the actual signal parameters and the estimated signal parameters [3].

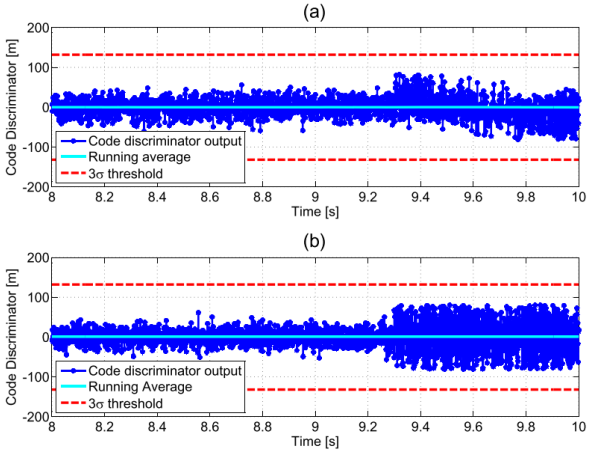

Fig. 2.9 Comparison between code discriminators output, (a) in the presence of -130 dBW Continous Wave Interferences and (b) in the presence of Single Saw Tooth Chirp Signal also at -130 dBW [3]

In the absence of interference and normal operation, the loop discriminator output shown in Fig. 2.9 should be driven to zero.

2.2.1 Impact on Acquired Position

Another GNSS component affected by jamming attack are the GNSS values of acquired position. As it was stated in reference [9], the attack impact using jamming varies depending on the environment in which it is performed. In order to test the jammer's efficiency, a simulation was performed by authors [9]. For free space simulation formula (2.2) was used for the calculations, losses were neglected, so the G_T value was assumed to be 0 dBi, and the P_T receiver power value in the range from 100 W to 1000 W. The entire tests were carried out on the basis of the GPS L1 signal with a value of -157dBW, the values of 47 dB and 27 dB were taken for $\frac{J}{S_T}$ as the respective boundries for tracking and acquisition. In the case of tests in urban areas, the COST-231 Hata model was used, it results from the fact that when there is a blockage in the line of sight, formula (2.2) becomes incipient. Final results are shown in table below:

EIRP (W)	Urban envirnoment (km)		Suburban envirnoment (km)		Free space (km)	
	Acquisition	Tracking	Acquisition	Tracking	Acquisition	Tracking
100	3.495	<1	4.455	1.192	465	41.38
500	5.798	1.576	7.141	1.768	1030	102
1000	6.949	1.700	8.677	2.152	1495	142.3

Tab. 2.2 Results of tests, according to Friss equation for free space envirnoment and COST-231 Hata model for suburban and urban [9]

According to tests, strongest effect should be expected in a free-space environment, in the case of more complex suburban and fully urbanized areas, a reduction in the overall effectiveness of the attack should be expected. Also, considering that jammed signal can still pass the GNSS receiver acquisition and tracking stage, we still get a positioning result. However, this result will be degraded due to the presence of an interference signal in input. The actual value of the positioning error is difficult to estimate.

2.3 GNSS Jamming detection

The most important thing in this case is appropriate preparation and detection of a potential threat. In most cases, jamming detection techniques are characterized in terms of receiver operational characteristics (ROC), which are plotted as a function of false alarms rate [3]. The overall detection probability is based on the probability of the detector detecting interferences due to the presence of jamming. On the other hand, the situation in which there is a probability that the detector will incorrectly present the jammer signal detection is determined by the false alarm rate.

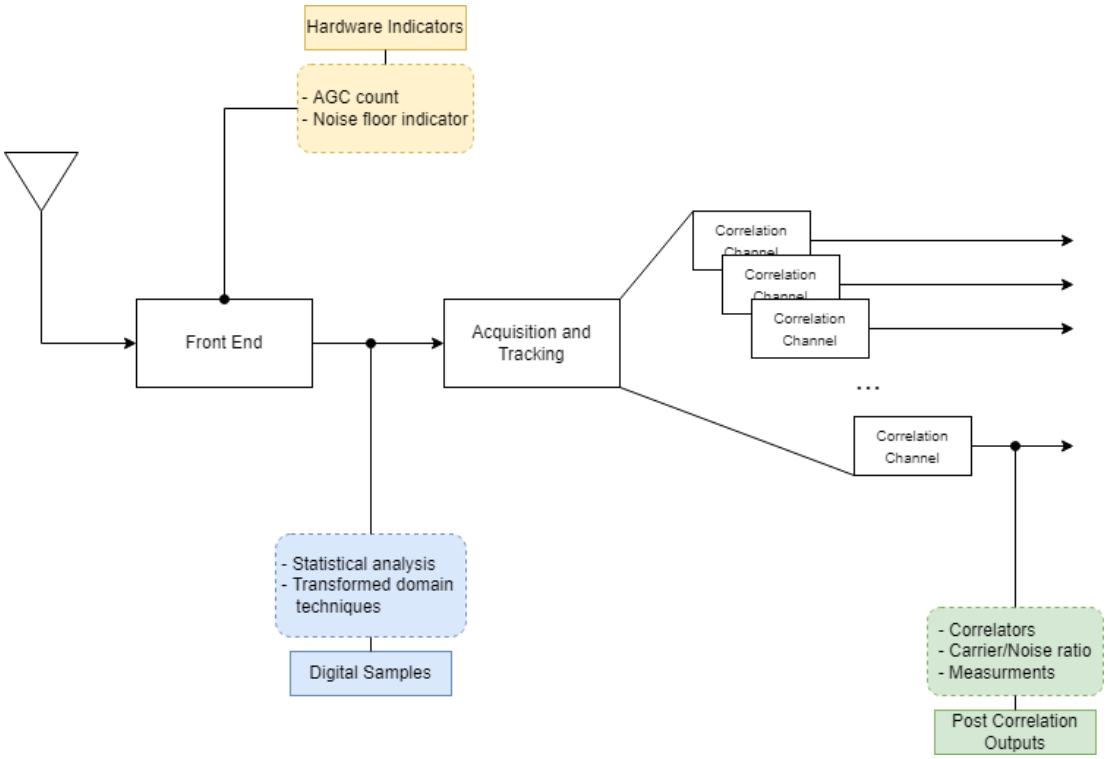

Fig. 2.10 Receiver stages at which jamming detection can be implemented

Fig 2.10 shows various possible receiver stages in which the jamming detection can be implemented, analyzing the measurments of these stages. The last stage of the GNSS receiver responsible for positioning has been omitted because there is no possibility of any countermeasures on this stage, even with correct detection.

2.3.1 Front-End hardware indicators

The influence of jammer signals on the front-end of the receiver has already been discussed. Mainly in this case, we recall how AGC reduces its gain to minimize potential quantization errors, the whole process is to best represent the powerful input signal with a limited amount of bits [3]. This process can be used to monitor interference. For example, let's declare G_{AGC} as the count of auto gain control at some instant of time n. In this case, we can define the jamming detection criterion as a determinant in relation to the number of consecutive samples N of the G_{AGC} count. Therfore if all samples of $G_{AGC}(n)$ are significantly below the declared threshold, a jamming instance can be declared.

2.3.2 Digital signal processing

For the detection method to be effective, the detection of jamming must be early enough. In the case of digital signal processing for detection purposes, samples can be used at the RF Front-End output, at the early stage of the receiver chain. Suppose jamming occurs, in this case the interference signal will be impinging the receiver antenna with a much higher power level than the nominal value for the operational range of the antenna. By using spectral analysis, jamming conditions can be compared with nominal conditions, thus detection of high power jamming signal is possible. The whole process is focused on the fact that under normal conditions the analog to digital converter (ADC) follows the Gaussian distribution. Figure 2.6 shows what it looks like under normal conditions and in the presence of jamming. In the event of jammer interference, the probability density function output samples will deviate from the Gaussian distribution. So the probability density function output samples from the ADC allows the jammer signal presence to be identified.

2.3.3 Post Correlation

In case of jammer signal presence, the effective carrier to noise ratio $\left(\frac{S_c}{N_0}\right)_{eff}$ from formula (2.1) can be reduced [3]. In this case, since we are able to check the values of such an event, we can use $\left(\frac{S_c}{N_0}\right)_{eff}$ measurments as an indicator for jamming presence. Basically, it is

about comparing the $\left(\frac{S_c}{N_0}\right)_{eff}$ value during normal conditions with the interference condition due to the jammer signal. The identification in this case is quite simple due to the enormous influence of visible jammer interference on $\left(\frac{S_c}{N_0}\right)_{eff}$ measurments. An additional advantage of such a solution is the availability of post correlation observables in most receivers available on the market, even in the low-cost ones. The solution also has certain requirements that must be met for proper jamming detection. As a general rule, the $\left(\frac{S_c}{N_0}\right)_{eff}$ values should be checked from all satellites available to the receiver for better detection capabilities. Additionally, this method is not very effective in dynamic conditions. This is because the $\left(\frac{S_c}{N_0}\right)_{eff}$ readings drop in a dynamic situation, both due to the effect of jamming and due to the effect of motion. Efficient adaptation of this method is therefore possible mainly under static conditions.

2.4 GNSS Jamming mitigation

A bit more complicated than detection is the actual mitigation of jamming-induced interference. The risk can be reduced by upgrading the user's inventory by using gain producing antennas and additional jamming rejection. The main method, however, is to increase the strength of the GNSS signals or to use additional functions allowing for greater processing gain. In addition, the use of correlators in the receiver's signal processing stage will provide greater resistance against jamming. An additional improvement is also the integration of the used positioning systems, allowing positioning solutions to be cross checked by other systems. This chapter will be devoted to mitigation techniques.

2.4.1 Adaptive antennas systems

Each type of GNSS receiver uses an antenna to receive the transmitted satellite signals. Antennas vary depending on the system and type of receiver, although the most common type of antenna used in GNSS receivers is a one-piece antenna with fixed pattern. This type of antenna is intended for general use and whether the signal is a real signal, jamming or some other form of interference, the antenna will behave in the same way. A simple solution is to use a multi-element antenna, in this case such an antenna has the ability to shape adaptively pattern

depending on the signal of the environment. These kind of adaptive antennas form deep nulls in their antenna patterns, those nulls are aimed in the directions of the interference sources [43]. However, this solution has several problems, mainly due to the fact that a multi-element antenna is not only more expensive than a single-element antenna, but also much larger. There are several forms of adaptive antenna systems. The first is the so-called Nulling Antenna System.

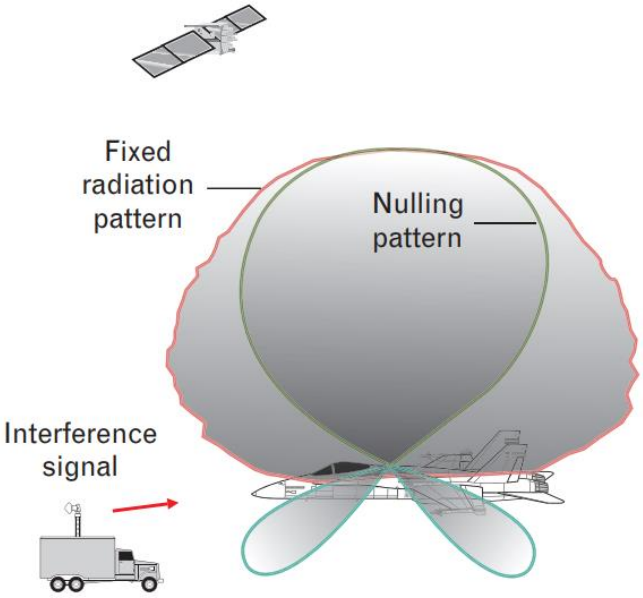

Fig. 2.11 Nulling Antenna System [43]

The structure of the nulling antenna system seen on Fig. 2.11 reduces the gain from the jamming signal direction, unlike the slightly more sophisticated methods in this case there is no additional gain for the GNSS signal.

A slightly different approach is the Beam Former Antenna System, in this case, in addition to directing the null beam towards the jamming sources, the combined real satellite signal visible on each antenna element is additionally used. This method uses this signal to obtain helpful gain of the antenna towards the satellite, thus creating a beam in the directions in which the satellite signals are present.

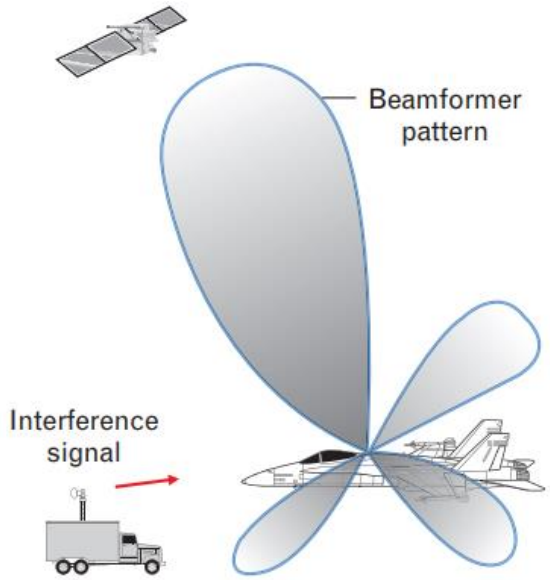

Fig. 2.12 Beam Former Antenna System [43]

Jamming cancellers are also used for additional improvements to antenna systems. It is also one of the simpler methods used to reduce jammer interference. The method consists in using two antennas, one of the antennas is directed towards the jammer (with little or no GNSS signal), while the other antenna is directed towards the GPS signal and the jamming source. The process is to use the gain and phase of output of the first antenna, which are adjusted at weight (W) so that they are equal and opposite to the sum of the output jamming and signal antenna. After both signals are added together, the jammer signal should be canceled out.

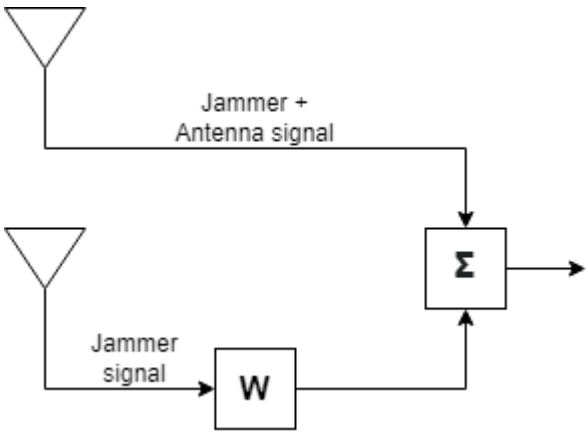

Fig. 2.13 Scheme of Jamming canceller

The standard jamming canceller setup is mostly effective when the jammer signal direction is known and comes from a local source. In case both the GNSS signal and the jammer signal come from the same side, a solution based on two co-sided jamming cancellers would be needed.

Another method based on the improvement of antennas is the use of a polarimeter. In this case, the output of one signal antenna is fed to two output feed elements in order to generate two other polarization outputs. The purpose of such an operation is to produce a signal difference and use it to cancel the jammer signal effect. It should be noted that in the basic form, this method will only be effective against a single jammer.

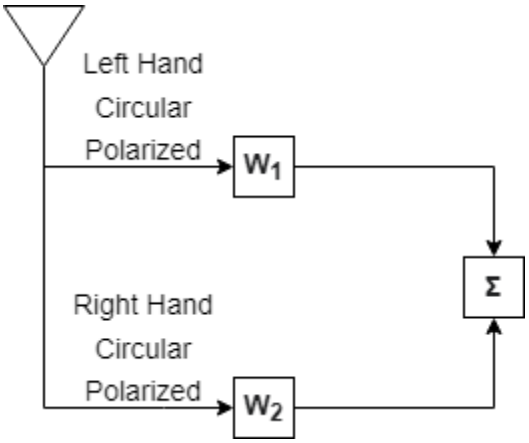

Fig. 2.14 Scheme of polarimeter concept

2.4.2 Adaptive filtering and STAP

Filtering noise from the receiver is essentially the first form of defense against interference. In this case, the so-called notch filters or spectral filters. Such filters are effective in the case of easily identifiable or periodic jamming signals, i.e. they are best for the elimination of Continous Wave interferences. So let's assume Contionus Wave interferences caused by jammer. Fast Fourier Transform (FFT) is made to convert the antenna output signal to the frequency domain, thus otuput will be close to the white noise floor, with single peaks on the jammer frequency. Then the detected peaks on the jammer frequencies are filtered out and the output signal is re-converted to time domain using the inverse transform.

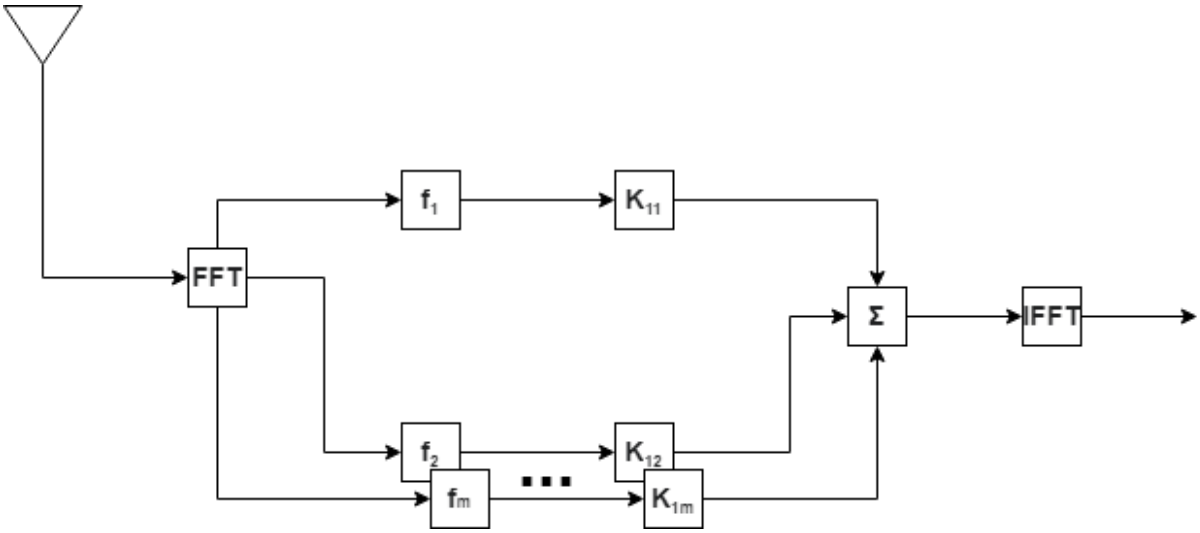

Fig. 2.15 Scheme of notch filter in frequency domain implementation. Where K stays for frequency-bin weights and amount of spectral taps is from 1 to m.

Depending on the implementation, this method is able to deal with the signals of many simple jammers. However, in the case of a broadband jammer, where its signal is not a single peek, but an interference signal spread over the entire GNSS frequency, in the absence of distinct peaks to be filtered, such a filter will prove useless.

The space-time adaptive processor (STAP) is a combination of the effects of earlier methods. It includes both the functionality of adaptive filters to eliminate large amounts of Continuous Wave interferences and the nulling abillity against various types of jammers. The reflection of jammer signals from metallic surfaces near the antennas allows for the use of tapped delay lines. Significant in the method is the fact that each antenna array is electromagnetically different from the other arrays due to the metallic surfaces, and this difference is a function of the frequency. The whole thus becomes a frequency dependent spatial filter, via the tapped delay lines. This method is a bit more complex, STAP can be defined conceptually as a combination of spatial and temporal processing with n antennas and m spectral taps. Recalculation of all $n \times m$ weights is critical for correct implementation, as it allows the use of temporal taps to reduce Continous Wave interferences, while spatial capabilities are reserved in this case to reduce other, more complex interference signals [37].

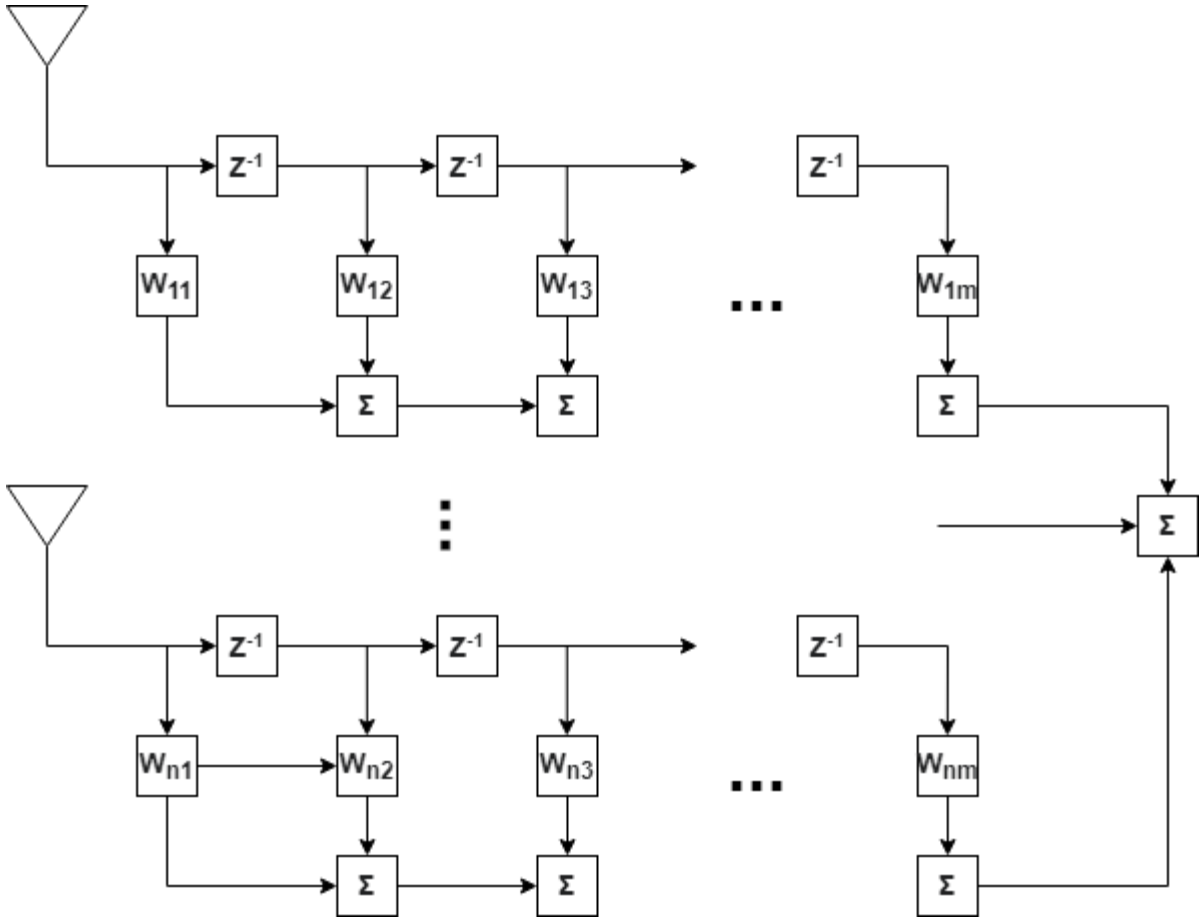

Fig. 2.16 Scheme of STAP. Combining both spatial nulling and time domain implementation of adaptive spectral filtering

2.4.3 Satellites improvements

The main reason why the power received by GNSS receivers is extremely low is because of the enormous distances that the satellite signal must travel. As a result, the presence of even low jamming interference may make it impossible to provide GNSS services over a large area. If the signal strength is increased to significant level, in addition to the need to rebuild the entire system and costs, there will be the problem of the impact of the higher signal strength on other systems. Another type of solution is to mount a high-gain narrow-beam antenna on GNSS satellites. This method relies on the ability of the spot-beam to send a highly concentrated satellite signal. Such a solution is rather unsuitable for civilian use due to the relatively small area of operation of the satellite spot-beam signal. However, this solution may be useful in military applications, in the case of additional possibilities of preserving the functionality of the system in the operational area.

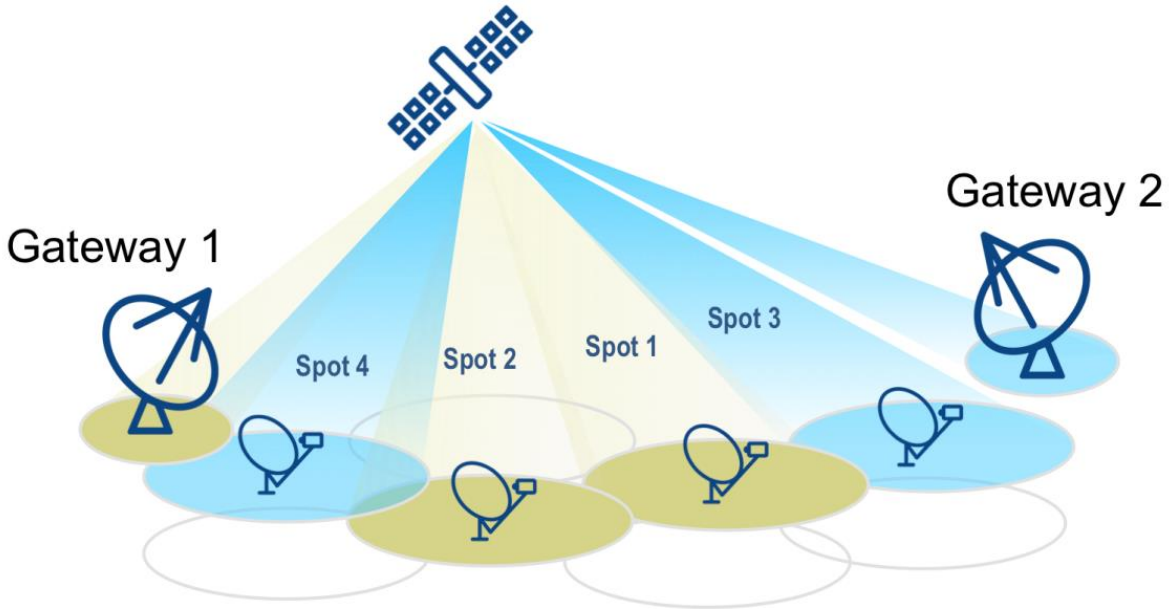

Fig. 2.17 Concept of spot-beam sattelite system. Sattelite signals are impinging only small areas.

Another solution in the field of satellite also applies mainly to military applications. As it has already been said, some of the described solutions can be quite expensive because they require improvements in the utility segment and the users' receivers themselves. Another approach is to create a different architecture segment for regional applications. In this case, a military system based on pseudolites. Such a system will provide a stronger navigation signal in the area of operation, enabling system users to operate even with greater amounts of intentional interference. In order for the system to function, at least four pseudolites platforms are required to operate, each of which will receive a GNSS signal for auto-navigation purposes. All pseudolites will be equipped with efficient, adaptive antenna systems with exceptional robustness. Each pseudo-lithium will be equipped with a GNSS receiver connected to an inertial guidance system, allowing additional correction in the event of stronger interference. The signal transmitted without a pseudo-lithium will be similar to the signals transmitted by GNSS satellites, however, the reception by system users will require minor modifications in order to correctly receive and process pseudolites signals [43].

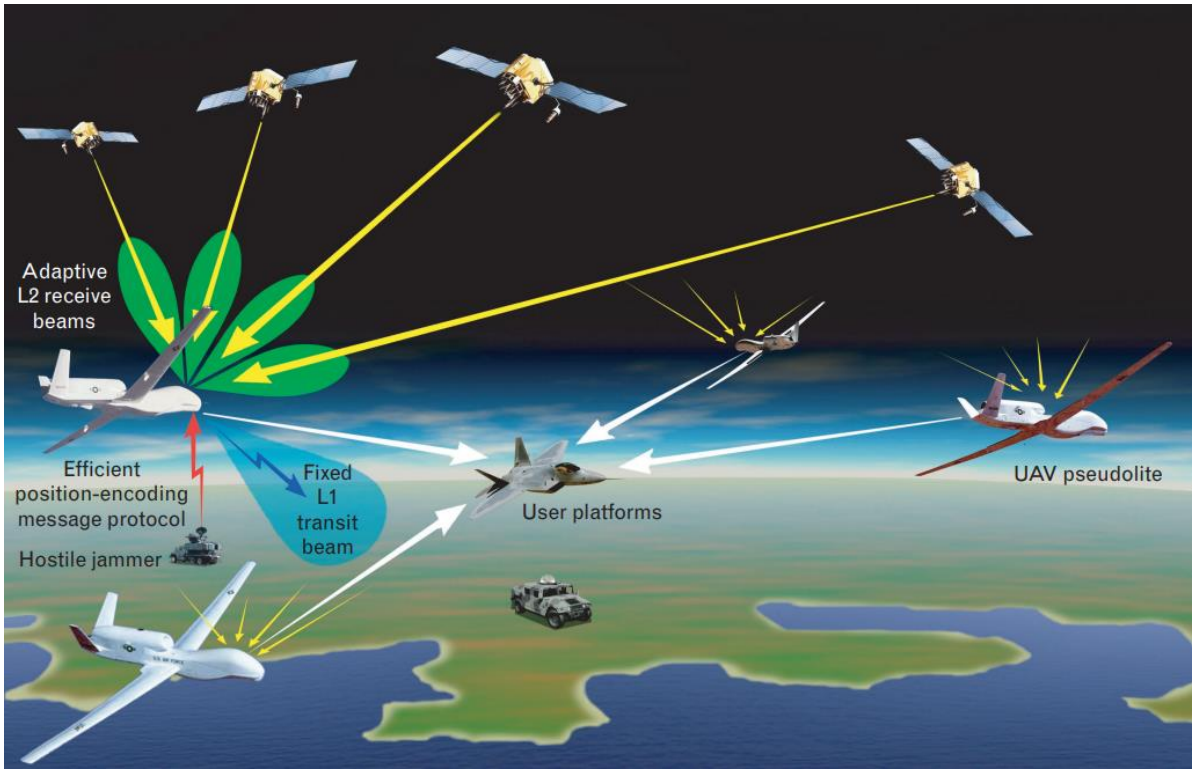

Fig. 2.18 Concept of the military pseudolite GNSS system. Each pseudolite transmits an encrypted signal to system user receivers which decrypt the signal and estimate the position [43].

2.5 GNSS Spoofing

Spoofing is a slightly more complex type of attack. Most GNSS signals are extremely susceptible to in-band interference due to weakness of the transmitted signal over wireless channels. In addition, the way the systems operate enforces backward compatibility to maintain system usability, which makes standard GNSS signals susceptible to distruptive interfering attacks. The main idea of spoofing is to insert your own positioning data into the GNSS receiver (incorrect in relation to the actual system indications). The basic tool in the implementation of spoofing attacks is software defined radio (SDR). That is, a radio communication system that can be adapted to specific requirements, in which the operation of basic electronic components (mixers, filters, modulators, demodulators, detectors) is performed with the help of a computer program. Contrary to jamming, spoofing is by far less frequent electronic attack, and much harder to detect due to its nature of a copy of the real GNSS signal. In general, the spoofing method is more demanding in terms of knowledge and technology of the attacker, and may also

cause significant damage not only to civilian operations, but also to military ones. In the case of attacks on military targets, the case of the successful spoofing of the Iraqi army on the American RQ-170 Sentinel UAV (Unmanned Aerial Vehicle) is quite known, due to the threat of spoofing not much data is freely available for civilian use, and the proliferation of some methods is prohibited.

There are also various techniques used during the spoofing attack. The most basic form is the simulation of a GNSS signal, in this case a simulator capable of transmitting on the appropriate band is used to broadcast a counterfeit GNSS signal. In this type of attack, the generated signal is not fully synchronized with the real GNSS signal (more or less), so for a receiver working in tracking mode, the signal looks like noise. Nevertheless, due to the higher power compared to the actual GNSS signal, such a counterfeit signal can confuse the receiver. This technique is the easiest to perform and the easiest to detect by anti-spoofing methods. The distance from the attacked receiver is also a significant facilitation for the implementation of this type of attack and any other, regardless of the level of complication.

Receiver Based Spoofing is a slightly more advanced technique. In this type of attack, the GNSS receiver is coupled to the signal spoofing transmitter. In contrast to the usual simulation of a GNSS signal, here the system first synchronizes to the value of the real GNSS signal, then gives positioning data and then generates the spoofing signal knowing the 3D pointing vector of its antenna transmit to the target GNSS receiver [6]. In this case, it is much more difficult to distinguish the spoofed signal from the real GNSS signal. The main problem in the implementation of such an attack is the signal spoofing transmission with the appropriate delay and strength of the transmitted signal. During the execution of the attack, the strength of the transmitted spoofing signal should be slightly higher than the actual signal to confuse the GNSS receiver, but not too much that it is not easy to distinguish the spoofing signal from the real one. An additional problem during the execution of the attack is the appropriate adjustment of the frequency and phase of the carrier to be consistent with the real GNSS signal. Additionally, a self-jamming effect or phenomena identical to suppressing relative data bit latencies may occur.

The most advanced types of attacks are based on the full knowledge of the centimeter level postion antenna phase center of the attacked GNSS receiver. This knowledge is used to perfectly synchronize the code and the phase of the spoofing signal carrier with the actual GNSS signal. For such attacks, multiple transmission antennas can be used to confuse anti-spoofing techniques based on the arrival direction of the signal. To achieve this, it is necessary to prepare

the signal array manifold spoofing according to the actual GNSS signal array manifold. Compared to earlier techniques, this type of spoofing is definitely more region-specific. This is due to the fact that the phase alignment of the medium and the synchronization of the array manifold can only be obtained for a small, specific region in which the antenna of the targeted GNSS receiver is located.

Contrary to the jamming interference signal, in the case of spoofing interference waveform has a very similar structure to the actual satellite signal $s_s(t)$ (1.5). In this case, the same shapes will have $G_s(f)$ and $G_I(f)$ (2.1) in the context of the spectrum of the signal for which the maximum overlap can be achieved [21]. Therefore, it is not possible to treat spoofing as a random signal and use the same formula to measure its interference (2.1). Additional problems in determining the correct formula will result from the spoofing attack type, but the basic form of the spoofing waveform formula for one satellite at the reception antenna can be described as:

$$s_I(t) = \sqrt{2P_I} * c_I\big(t - \Delta_I(t)\big) * m_I\big(t - \Delta_I(t)\big) * \cos\Big(2\pi f_{RF}\big(t - \Delta_I(t)\big)\Big) \tag{2.5}$$

Where delay $\Delta_I(t)$ relate to the real delay $\Delta_E(t)$ of the sattelite S with an intentional offest $\tau\Delta(t)$, which concludes:

$$\Delta_I(t) = \Delta_E(t) + \tau\Delta(t) \tag{2.6}$$

2.6 GNSS Vulnerabilities to spoofing

In this context, attention should be paid to several receiver operational layers that may be affected by spoofing. The first in this case is Signal Processing of the GNSS receiver, the second is Data Bit, and the last is Navigation and Postion Solution. In general, it should also be noted that the potential vulnerability depends on the type of receiver used, but not only on this because the level of the attacker's available SDR and its technological capabilities also have a significant impact in determining the vulnerability to specific spoofing attack.

2.6.1 Vulnerability of GNSS Signal Processing

As it was mentioned before, GNSS is a backward compatible technology, due to the need to keep the service fully operational regardless of the innovations introduced. This issue concerns the overall structure of the GNSS signal, including PRN signals, types of modulation used, transmission frequency, Doppler coverage, signal bandwidth and signal strength itself. Most of the standard GNSS receivers in use (especially in the case of the L1 GPS band) are equipped with AGCs, used to compensate for changes in the received signal strength. The problem is that when such an AGC comes into contact with a spoofing signal of a higher strength (which is the standard for such an attack), the receiver's input from the AGC will automatically adjust to the signal with a higher strength. In such a situation, in the case of a standard civil GNSS receiver, the spoofing module may generate a counterfeit GNSS signal with a higher aid, effectively confusing the receiver [6].

2.6.2 Vulnerability of GNSS Data Bit

Most of the GNSS standard payload data is publicly available, including the framing structure. The structure of such a navigation frame consists of telemetry information, almanac and satellite set ephemeris data. The problem is that in use this data does not change very often, for example ephemeris satellite date can be obtained in less than a minute but is permanently stored for 12 minutes and 30 seconds. This fact and duplicate GNSS data frame can be used when constructing an attack. In addition, the health status bits of the satellite can also be used by an attacker to confuse the GNSS receiver and cause it to smack the actual GNSS signals [6].

2.6.3 Vulnerability of GNSS Navigation and Position Solution

The main vulnerability used in spoofing attacks. The attacker uses a counterfeit signal to provide incorrect PRN measurments to the receiver, which causes the wrong output of the positioning solution. Typically, the positioning error is proportional to the rest of the range multiplied by the geometric value. In the work [6] on the analysis of spoofing attacks, the authors created a special index, the vulnerability index against spoofing (VIAS). This index

defined the geometric relationship between the GNSS constellation and the spoofing attack device that resulted in differences in the positioning solution of the GNSS receiver. It shows how the VIAS varies with time and position changes, and that its value is greater when the position dilution of precision (PDOP) value is greater. This is important because it can be used as a determinant for anti-spoofing methods. Some GNSS receivers are used only for time synchronization purposes, such as CDMA / GSM cell phone towers. In this case, the spoofing attack may not so much cause erroneous readings for positioning, but lead to complete disrupt the accuracy of the estimated timing. This situation can cause a chain reaction across the entire network of nearby CDMA / GSM towers.

2.7 GNSS Spoofing attacks characteristics

Different variants of attacks can occur depending on the spoofing delay $\Delta_I(t)$ used and the overall spoofing power P_I. In the event of attacks on Navigation Message, the navigation data message $m_s(t)$ (1.5) will have the necessary information for the receiver to create a correct ranging from the data available from each satellite. The spoofer can demodulate the actual navigation data, predict, modify and retransmit with its own positioning data. If we look at the formula (2.5), the attack on the navigation message will be successful if the value $\tau\Delta_U \sim 0$, and the value of the spoofer signal power will be greater than the real signal $P_I > P_S$. Detection schemes in this type of attack can use the expected time scale to receive a continuous message update and cross-check newly received data with more recent versions. However, the use of this is dependent on the target GNSS system, it may also interfere with the actual daily update of the data for a given GNSS.

Spoofing attacks can also include the PRN Code, a simple illustration of this type of attack is shown in Fig. 2.19. Spoofing attacks can also include the PRN Code, a simple illustration of this type of attack is shown in Fig. 2.19. The upper part shows the real signal tracking point, while the lower part shows the spoofing effect. The values of PRN and Doppler shift for the receiver under the influence of PRN Code spoofing can be calculated by substituting the interference signal value for formula (1.8). Also assuming the knowledge of the correlation value $V_{C,I}(\Delta_S, f_{D,S})$ for the GNSS receiver under the attack:

$$\hat{\Delta}_S(\tau\Delta, f_{D,I}), \hat{f}_{D,S}(\tau\Delta, f_{D,I}) = arg \max_{\Delta_S, f_{D,S}} \left|V_{C,I}(\Delta_S, f_{D,S})\right| \quad (2.7)$$

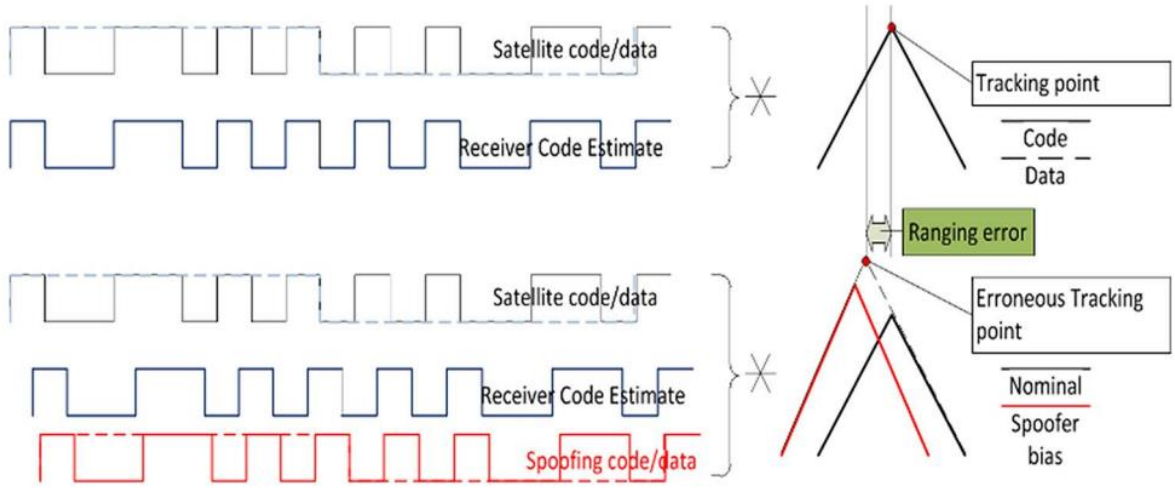

Fig. 2.19 Spoofing of GNSS PRN Code, actual line-of-sight (LOS) tracking point at the top, spoofed tracking point at the bottom [21].

Another spoofing attack type is Lift-Off-Delay (LOD), where the spoofer approaches the actual signal with a relative delay $\tau\Delta_I(\mathrm{t})$ (and Doppler shif $f_{D,I}$ if possible), gradually adjusting the power of the spoofing signal C_I. This situation is shown in Fig. 2.20. At delay $\tau\Delta_I(\mathrm{t}=\mathrm{T2})$, the spoofer approaches the actual signal with a delay and a little less power, causing a further adjustment of the delay value, where at $\tau\Delta_I(\mathrm{t}=\mathrm{T3})\sim 0$ the spoofing signal reaches a delay value almost the same as the actual signal. The spoofing signal power C_I then becomes greater than the actual signal value and the delay value $\tau\Delta_I(\mathrm{t}=\mathrm{T4})$ is further increased to move the tracking point even further away from the actual signal parameters.

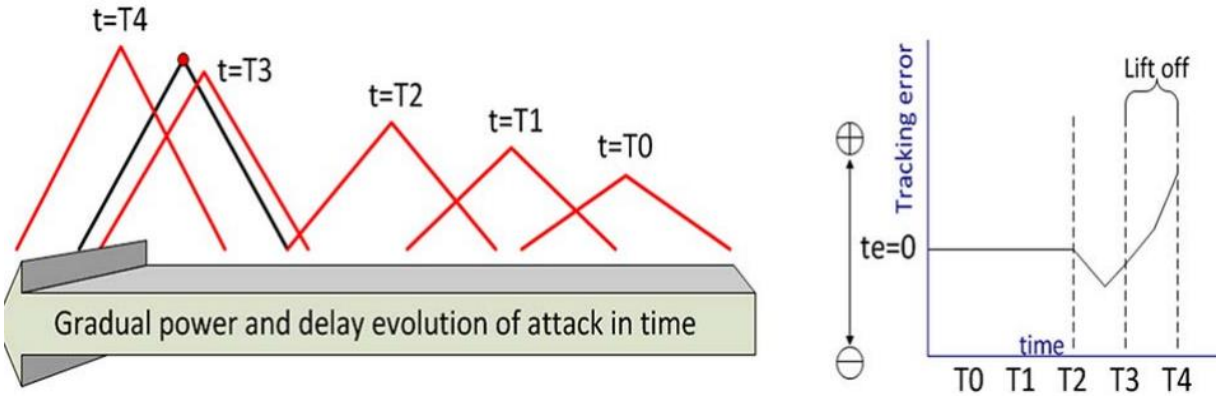

Fig. 2.20 Lift-Off-Delay (LOD) spoofing attack (left) and corresponding tracking error with spoofing attack starting at T2 (right) [21].

Another scenario is Lift-Off-Aligned (LOA) spoofing attack, unlike LOD in this case, the spoofer is aligned with the LOS of the satellite signal, because the value of $\tau\Delta_I(t)$ is always close to zero. This type of attack does not detect at point distant to the prompt correlator, but may create more abrupt changes to tracking parameters in the event that an attack occurs suddenly. Typically, standard GNSS receivers are more vulnerable to this type of attack during signal acquisition, or if they are accomplished with self-spoofing devices, during tracking [21].

Another type of attack is the previously mentioned Meaconing (MEAC) method and Selective Delay (SD). The meaconing itself is a method of recreating the captured GNSS signal. Figure 2.21 shows the course of a meaconing attack, in this case the spoofing signal is a reconstructed replica of a GNSS signal with a fixed delay that can adjust its power value but assumes a constant interference signal delay. A typical GNSS signal repeater can perform this type of attack, whether the signal is encrypted or not. In contrast, Selective-Delay attacks are performed through GNSS chip code estimation. Attacker uses signal at the position and then converts it into a prediction of the signal that would have been received at pretended position by the receiver, then during transmission converted signal is feed into attacked receiver. If in this case the strength of the spoofing signal $C_I < C_S$, a so-called multipath attack occurs because the spoofing signal looks identical to the nearby reflected signal. The issue that distinguishes multipath attack is the fact that this type of attack degrades ranging accuracy, but at the same time in its case the tracking point stays close to the real signal.

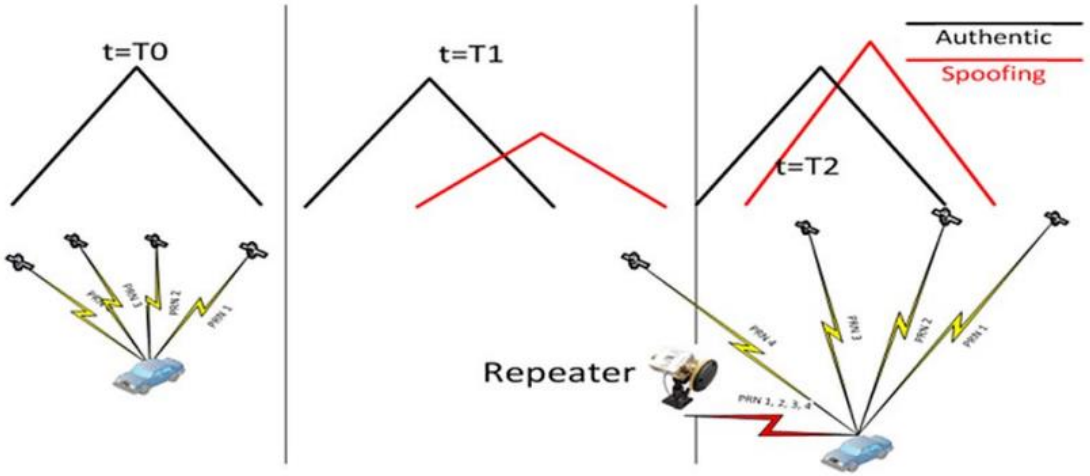

Fig. 2.21 Meaconing attack. Visible delayed replica of signal with varying amplitude [21].

There are also combined methods such as Jam and Spoof (JAS). During such an attack, the spoofer forces the receiver to enter acquisition mode via jamming. This causes the receiver to lose the ability to track the actual signal while signal spoofing is transmitted. The jammer is then disabled when the receiver already acquires spoofing signal.

As it is important for the transmission of signals how urbanized an area is, it is also important for spoofing techniques. In such areas, the receiver is usually not able to track all satellites in the recommended area of operation, and it is also unaware of the surrounding obstacles. This makes it possible to implement No-Line-Sight-Spoofing (NLOSS), enabling the spoofer to block LOS signals within the receiver's range as shown in Fig 2.22. In this way, the spoofer can only transmit a signal for potentially blocked setlites, making the identification of spoofing signals extremely difficult for a GNSS receiver.

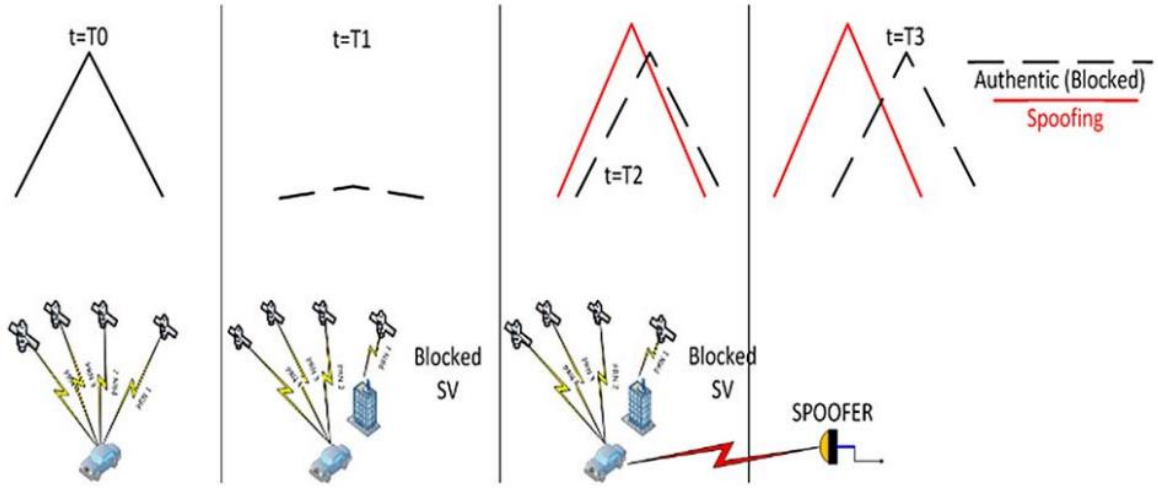

Fig. 2.22 Representation of NLOSS. Spoofing of low elevation satellites [21].

It is also possible to create a Trajectory Spoofing (TS) attack. In all situations except meaconing, spoofing signals can be generated independently of each other. In this type of attack, the spoofer, using SDR or a GNSS signal simulator, tries to recreate the tracking points of all GNSS receiver channels along its entire planned trajectory, forcing the user to follow the spoofed trajectory. In such a situation, all spoofing signals will be generated cohorently with respect to this trajectory, it will cause an error in the method of determining the range consistency of satellites. In the event that the spoofer will spoof the entire parts of the channels, the receiver will simultaneously process both the actual PRN and the spoofing. The analysis of the course and actual effect of such a situation is discussed by the authors in [18].

In conclusion, it should be noted that some types of attacks are specifically prepared for specific situations. For example, LOD would not be feasible against high dynamics users, nor would a multipath attack be effective in the absence of LOS. Therefore, a significant facilitation in creating appropriate countermeasures is determining what type of user or receiver, what type of attack should be expected.

2.8 GNSS Spoofing detection

Similar to the case of jamming, there is a division into sections responsible for the detection and mitigation of threats. Most of the detection techniques are based on the use of the characteristics of the functioning of GNSS systems in order to identify the occurrence of spoofing and, depending on the adapted technique, the possibility of its classification.

2.8.1 Signal power monitoring

The first possibility is to use the $\left(\frac{S_c}{N_0}\right)_{eff}$ value as an identification parameter for spoofing. Most consumer GNSS receivers measure this parameter to check the quality of the signal used. In open sky conditions, only the movement of the satellites and the ionospheric variation can cause gradual smooth changes in the received signal power. In the event that the receiver is spoofed, the $\left(\frac{S_c}{N_0}\right)_{eff}$ measurement may record rapid changes, thus enabling identification of the attack. The anti-spoofing mechanism used in the receiver can constantly monitor the $\left(\frac{S_c}{N_0}\right)_{eff}$ values and check for sudden and non-standard changes. This method is so much more effective that the GNSS receiver can easily store information about the time history of the received signal from each satellite. Figure 2.23 shows a comparison of the real signal SNR and the spoofing of the signal against the Total Spoofing Power (TSP) where the true signal is 10, and the subsequent case of the spoofing signal is 10, 20 and 30. In this test [6], the power value of each real satellite was -158 dBW. and the value of cohorent integration time was $T_c = NT_S =$ 1 ms.

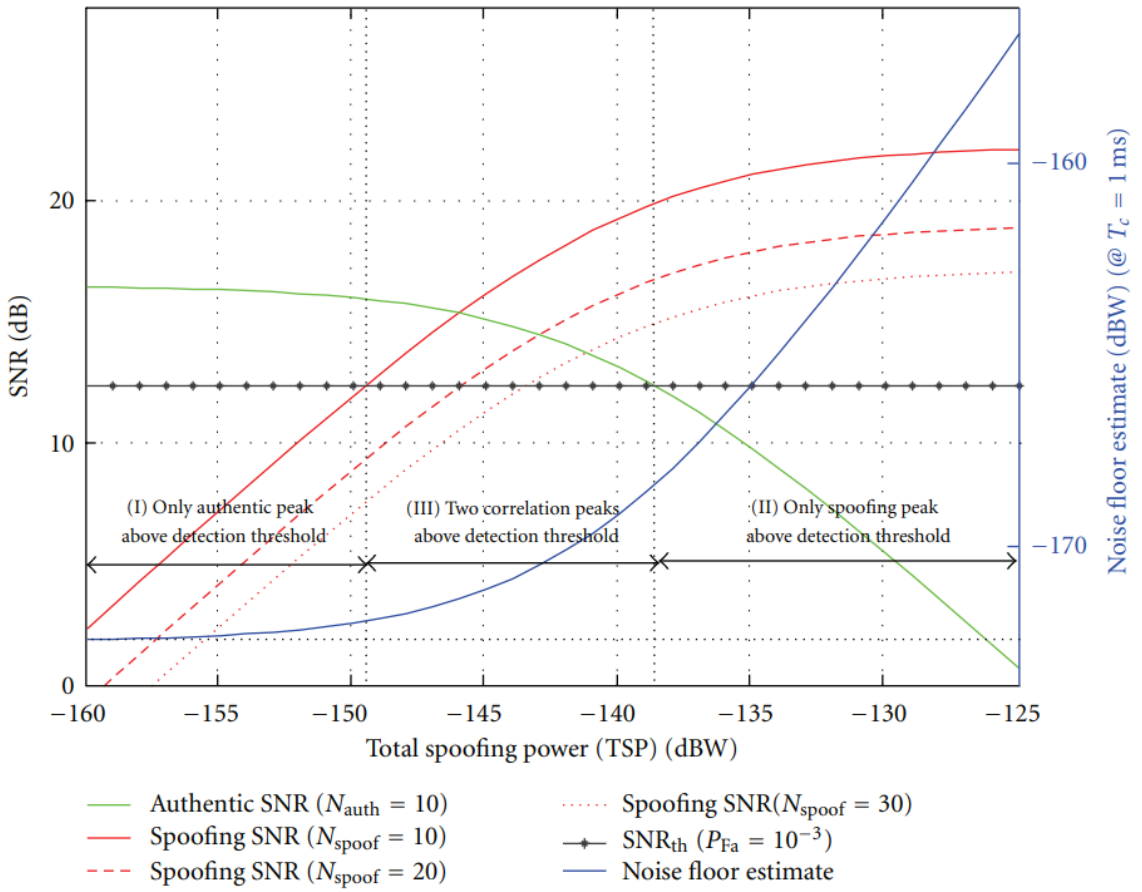

Fig. 2.23 Value of received SNR against TSP, for real and spoofing signal correlation peaks [6].

In the case of monitoring based on signal strength, one should also pay attention to the possibility of monitoring the Total Power value. As the path loss between the spoofing device and the target receiver is highly variable, it is difficult for a spoofer to determine the exact value of the transmit power without going beyond the range of the typical value for GNSS signals. The maximum value of the received GNSS signal strength is in the range of about -153 dBW (GPS L1 frequency). Therefore, the reception of the spoofing signal, the total power of which is much higher than the standard value, enables the detection of the occurrence of an attack.

An additional monitoring criterion is also a frequency based power comparison, for example a comparison of L1 to L2 in the case of GPS. By default, the system has predefined power difference values between GPS signals in different frequency bands, and many GPS receivers have the ability to monitor both L1 and L2 signals. In the case of a low-complexity spoofing attack, there is mainly a signal close to L1. Therefore, the absence of the L2 signal, or

the huge difference in measurement between the L1 and L2 power values, automatically allows the attack to be identified.

2.8.2 Spatial processing

Most devices used to transmit spoofing signals utilize the use of only one antenna to transmit multiple counterfeit signals due to logistical limits. In real GNSS, signals are transmitted in different directions from many different satellites. This allows the use of a spatial processing technique to check the spatial signature of the signals received and to determine which signals are spatially correlated [6].

One possibility according to the information presented in [32] is to use a detection technique based on the analysis of the phase difference between the two fixed antennas over a period of one hour. Knowing the bearing of the antenna array and knowing the trajectory of the satellites, theoretical phase differences can be calculated and compared with the practical phase value differences noted by the antenna array. This allows spoofing to be detected, but the problem with this method is the length of the algorithm execution (about 1 hour) and the necessity to have a calibrated antenna array with a known array orientation. The technique is obviously effective mainly for standard spoofing devices, in the event of an attack using multiple antenna spoofing device this technique could be ineffective.

2.8.3 Time of Arrival

As the spoofing device imitating the receiver has no prior information on the bits of the navigation data, it has to decode the received GNSS signal first and then generate its replica. It occurs by the delay between the spoofing data bit boundaries and the actual signal data. This allows for a time check, if the data bit transition occurs in a time interval other than 20 ms, thus a spoofing attack can be identified. The problem with this method is that the GNSS data frame structure is already known and that it consists of different elements with different update frequencies. Since the update frequency of most parts of the GNSS frame is very low, most GNSS data bits may be predicted by the spoofer. This occurs when the spoofer already acquired GNSS information before it started transmitting the spoofing signal.

Additionally, it is possible to check the relative delay of the signals on two frequency bands. For example, GPS transmits the encrypted P-code on both its L1 and L2 frequencies. Generally, signals received at these frequencies have a relative delay due to the different response of these frequencies to the ionosphere. Due to this, the dual frequency GPS receiver should see only one correlation peak during correlating L1 and L2 signals. The overall propagation delay value is higher for the L2 frequency than for L1, thus the approximate relative delay peaks of the correlation are known to the GPS receiver in question. This technique, however, turns out to be ineffective with more advanced spoofing methods capable of generating signals at both frequencies.

2.8.4 Integration with other systems

Using data from auxiliary equipment of navigation systems, for example, an inertial measurement unit (IMU) can help a GNSS receiver detect the occurrence of a spoofing event. In addition, a GNSS receiver can compare its extraced GNSS solution with that of other positioning and navigation systems such as mobile WiFi stations. If, when comparing the solutions with other systems, there are huge differences, then a spoofing attack can be identified in this way. The main problem of such, apart from the significant increase in costs, is the increase in the complexity of the hardware and software structure of the GNSS receiver. Many of the solutions presented by other systems are not as accurate as the solutions presented by GNSS. In addition, in the case of IMU sensors, it is necessary to calibrate them before using them for positioning purposes. An additional factor is also the very issue of the coverage of other systems used compared to the global scope of GNSS operation.

2.8.5 Authentication and encryption

Depending on the application, some of the GNSS are equipped with authentication methods that allow both to identify and prevent spoofing. This mainly applies to military GNSS applications, although it is planned to use some authentication techniques also in civil applications [42]. As for the use of cryptographic techniques in the construction of GNSS signals, it makes data and code sequences unpredictable from the adversary's side. Application cryptographic functions use encryption, digital signatures and message authentication codes (MAC). As a result, creating a replica of the signal can be very difficult in the case of spoofing.

Before further analysis, it should also be noted that any authentication techniques will be ineffective against certain types of attacks, such as MEAC or NLOSS.

We can distinguish two types of applications of cryptographic schemes in GNSS, symmetric and asymmetric. In the case of symmetrical key schemes, we assume that both the receiver and the transmitter share a secret key, implying that every system user knows that this key can impersonate the satellite signal. In the case of an asymmetric key scheme, we have a private key that shall not be shared and is usually the one that decrypts or signs the message, and the public key used for encryption or signature verification. Public keys are derived from private keys, but no reverse operation is possible. This type of key cryptography, although it does not require security modulo, is slower and requires much longer keys and computing power. When it comes to authentication of the navigation message, we can use digital signature or MAC. Digital signature in this case is based on an asymmetric scheme, where the private key is in the system that uses it to sign the message, completing it with the signature, while system users use the public key and the received message to verify the signature. MACs, on the other hand, are based on a symmetric key schema and can be truncated to provide shorter authentication codes than with asymmetric methods.

Different authentication techniques use different unpredictable features at subcarrier or carrier level of signal, such as frequency hopping or variable pulse shaping. However, the techniques based on Navigation Message Authentication (NMA) seem to be the most effective. Most NMA techniques are based on the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) protocol [52]. TESLA combines the advantages of both symmetric and asymmetric key cryptography, by using one-way hash function to generate a long key chain, disclosing the individual keys in reverse order and in delay to the message and MAC. After the key disclosure K_i, the receiver can verify that the received key is genuine by applying i-times the one-way function verifying the outcome with the root key, which is the last key of the generated key-chain. The root key is signed with a digital signature, since it is the critical verification point and a sophisticated spoofer could otherwise build its own key chain and broadcast spoofed message along with its MAC and the key used to generate the spoofed MAC. The full operation of the TESLA protocol is shown in Fig 2.24

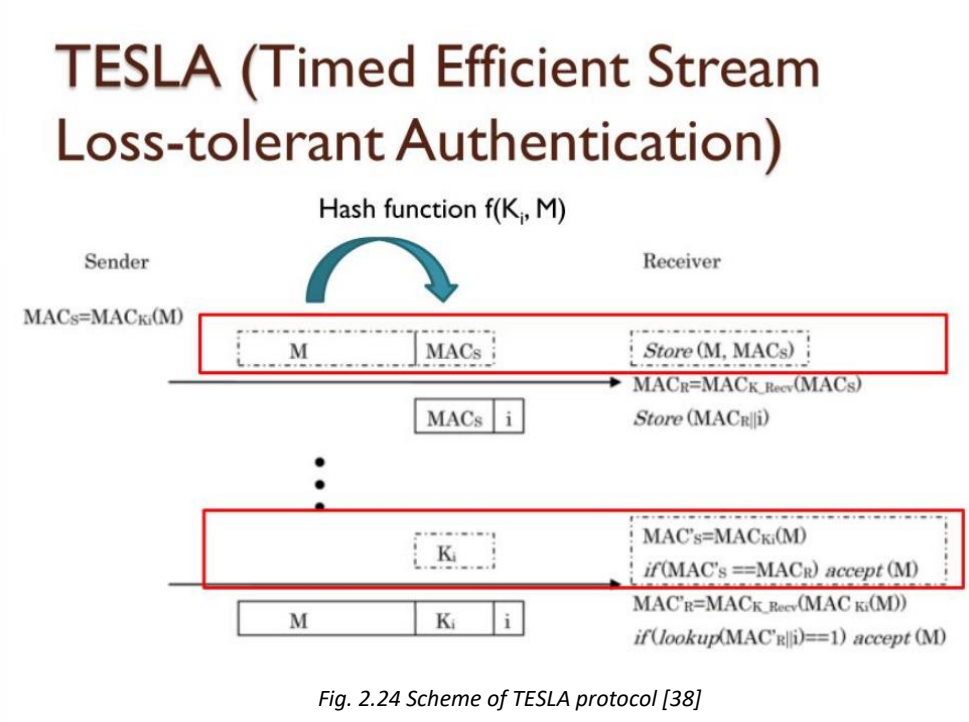

Fig. 2.24 Scheme of TESLA protocol [38]

In the context of encryption, it is about restricting access to the use of a signal, so low-complexity spoofing of such signals is impossible without access to encryption codes and algorithms. Receivers used for such signals must have a classified algorithm, an appropriate key repository, and be certified for use with the given encrypted signal. Such signals are generally very complicated and expensive to deploy, they are practically only used in military applications. An example of such a signal is the GPS M-code.

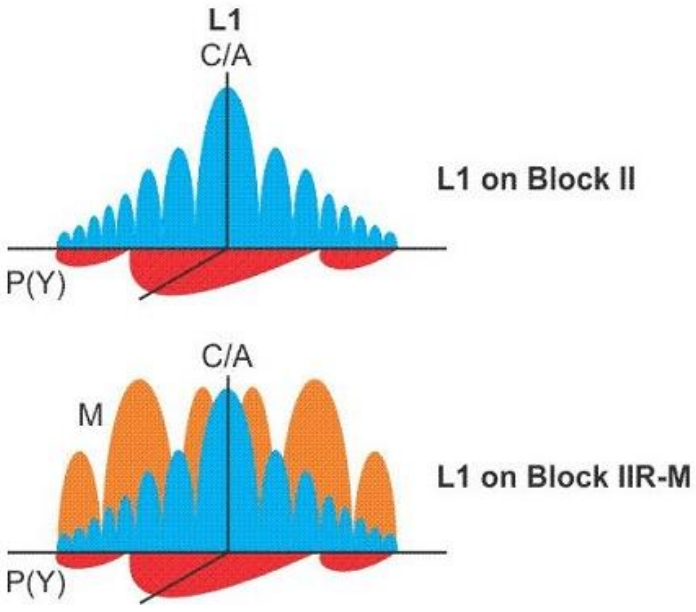

Fig. 2.25 M-code signal

The M-code is a new military signal used in the L1 and L2 bands of the GPS. M-code signals are encrypted and the receivers are able to automatically detect and reject spoofing signals. In addition, one can also mention the greater resistance of this signal to jamming (about 20 dB more than conventional signals) and the possibility of selective jamming of civilian signals, while still being able to fully receive the M-code signal (Blue Force Electronic Attack Compatibility). More direct informations about M-code are presented in reference [1].

2.9 GNSS Spoofing mitigation

In the context of spoofing mitigation, some anti-jamming methods also turn out to be effective, for example Nulling or Beam Forming Antenna Systems. This allows, analogous to jamming, to direct null towards spoofing signal. In addition, additional methods are used to monitor the integration of a GNSS receiver and to detect residual signals. The use of mitigation methods also depends on the type of detection method used in the system, Tab. 2.3 contains a brief summary of the discussed detection methods.

	Spoofing detection method	Spoofing feature	Overall complexity	Method effectivness	Required capability of GNSS receiver	Spoofing scenario generality
Signal power monitoring	Monitoring of Signal-to-Noise value	Higher value of Signal-to-Noise value	Low	Medium	Signal-to-Noise monitoring	Medium
	Monitoring of Total Power value	Higher amplitude	Low	Medium	Total Power monitoring	High
	L1/L2 power comparison	Spoofing not consisting L2 signal	Medium	Low	L2 reception capability	Low
Spatial processing	Direction of arrival comparison	Spoofing signals coming from the same direction	High	High	Multiple antennas	High
Time of Arrival	Time of Arrival discrimination	Spoofing signal delay	Medium	Medium	Time of Arrival analysis	Low
	Signal quality monitoring	Deviated shape of authentic correlation peak	Medium	Medium	Multiple correlators	Low
Integration with other systems	Navigation systems cooperation	All types	High	High	Other navigation systems measurments availability	High
Authentication and encryption	Cryptographic authentication	Not authenticated	High	High	Signal authentication	High

Tab. 2.3 Spoofing detection methods comparison

2.9.1 Residual signal detection

Total suppression of the actual GNSS signal is very difficult to perform during spoofing as it requires precise knowledge of the position of the attacked antenna phase center relative to the spoofer antenna phase center. In most situations, after a successful lift-off, a real signal residue that can be used for spoofing detection and mitigation remains. Such a solution was

presented by the authors in [20]. First, the receiver copies the incoming digitized front-end data into buffer memory. Then, the receiver selects one of the GPS signals being tracked and removes the locally generated version of the signal from the buffered signal. Finally, the receiver performs acquisitions for the same PRN signal on the buffered data. The problem with this method is the standard increase in the complexity of the hardware and processing of the receiver. This is because the da method requires additional tracking channels to track both real and spoofing signals.

2.9.2 Receiver Autonomous Integrity Monitoring

As mentioned, the spoofing signal introduces PRN counterfeit to the receiver measurements during an attack. Depending on the situation, these measurements may not be consistent and consequently not allow a correct positioning solution to be obtained. As indicated in [28], most GPS receivers perform measurements integrity monitoring to detect outlier measurements, this techniques, and known as Receiver Autonomous Integrity Monitoring (RAIM). RAIM can be used as an effective anti-spoofing mechanism at the positioning solution level. The authors in [29] presented an expandability for RAIM to allow receivers to detect and be able to reject outlier measurements detected as a spoofing attack.

3. Spoofing and GPS vulnerability in practice

In order to show the actual course of spoofing, an experiment was performed based on the SDR. The practical aim was to demonstrate the relative ease of carrying out such an attack and the potential secondary effects. The basic assumption of the experiment was to perform the correct spoofing on the GPS receiver contained in the mobile phone. In the case of this experiment, the most basic and simplified spoofing scheme was performed, consisting in generating a signal of a simplified form of the GPS L1 signal based on the available data. It should therefore be taken into account that the experiment is not a real application of electronic warfare means and its solutions are not based on the use of full GNSS signal simulators. Thus, the actual cost of implementation and the actual level of complexity are much lower than in the case of commercial or military attacks. The following subsections contain a description of the hardware and software used, an explanation of the course of subsequent parts of the experiment, along with additional information on the implementation of such attacks.

3.1 Hardware and software

The HackRF One platform was used to perform spoofing, it was created by Michael Ossman for the purposes of commercial applications and security experiments based on radio signals. Several types of phones were used in the tests, and their susceptibility to low-complex spoofing was tested separately, they were Huawei P Smart (model STK-LX1), much older LG K8 2016, and the best secured Iphone XR 64GB. Many devices were selected for the tests in order to present the real difference in the impact of attacks on a specific receiver, in the context of the assumption about the selection of the attack technique for the potential target of the attack and the assumptions of the actual impact of the attack. A standard, cheap GPS antenna with a frequency in the range of 1574-1610 MHz was used as the transmission antenna. Additionally, GPSDO was used for testing purposes related to the adjustment of the appropriate clock values.

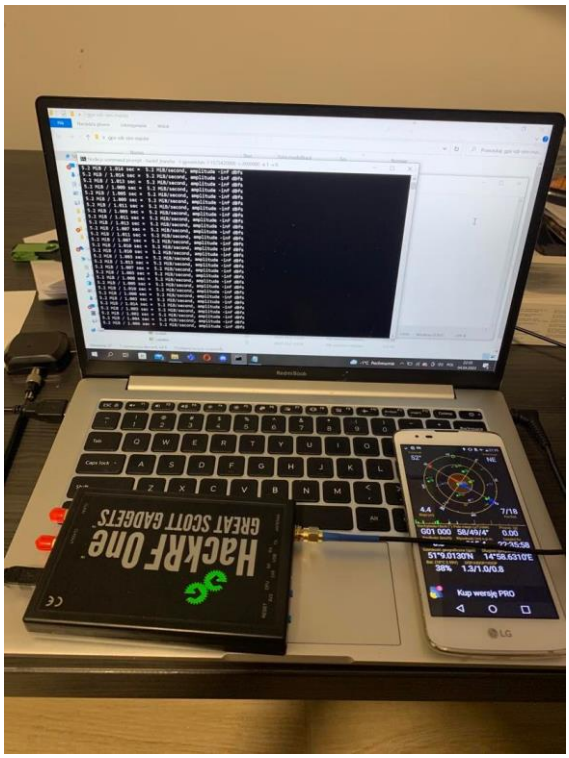

Fig. 3.1 Photo of the setup used for spoofing purposes

In the context of the selection of the platform, the most important thing is that it is able to operate in the range of the GPS signal frequency carrier (1575.42 MHz), bandwidth (2 MHz), and that the output spoofing power value is at a sufficiently high level. Basically we assume the value of the received signal at the level of -130 dBm. In such an experimental environment, the value of the spoofer's signal strength is about 40 dB greater than the actual satellite signals.

The software requires the ability to generate authentic replica of the GPS signal. In addition to the possibility of doing it manually in the programming environment, it’s also possible to use ready-made tool. For the purpose of the experiment, gps-sdr-sim was used, i.e. a ready-made generator that allows to create a GPS baseband signal data streams. It is also necessary to have ephemeris data for a typical GPS satellite. This data is easily accessible with a list of available satellites and their parameters on the CDDIS.NASA website (https://cddis.nasa.gov/Data_and_Derived_Products/GNSS/hourly_30second_data.html), it is necessary to have an account on the website, which can be created by anyone because there are no additional verification mechanisms. Of course, in this case, that's not all, apart from signal generation, we also need to use a tool that allows us to transmit it. As before, you can compile the received GPS signal replica file yourself or use ready-made applications. Since PothosSDR (https://downloads.myriadrf.org/builds/PothosSDR/)software turned out to be compatible with HackRF, the experiment used hackrf_transfer.exe provided by this software.

3.2 The course of the experiment

For the purposes of the experiment, all additional mechanisms allowing to obtain positioning informationsuch as Wi-Fi, additional mobile operator data were disabled on all cell phones. Before the experiment, all phones were reset and "Airplane mode" was turned on.

We start with generating a signal in gps-sdr-sim. We find the coordinates we are interested in that we want to use to generate the appropriate signal and download the file from ephemeris GPS data.

```
C:\Users\cuqier\Desktop\gps-sdr-sim-master>gps-sdr-sim -e brdc1680.22n -l 31.40245035573297,64.500370154274238,100 -b 8
Using static location mode.
Start time = 2022/06/17,00:00:00 (2214:432000)
Duration = 300.0 [sec]
01  111.7  12.2  24288944.3   3.9
05  281.4   5.8  25170014.8   4.5
07   74.1  58.5  20950958.7   1.7
08   43.6  24.3  23232777.7   3.0
09  163.2  19.9  23705692.8   3.3
13  317.1  25.1  23124983.4   2.9
14  293.8  61.0  20846374.0   1.7
17  188.3  36.0  22176481.5   2.4
19  197.9  12.6  24650114.2   3.8
20  252.1   2.6  25355559.2   4.8
21   80.2  14.2  24143091.8   4.0
28  265.2  42.6  21895302.9   2.1
30    2.8  67.0  20601473.1   1.6
Time into run = 300.0
Done!
Process time = 76.6 [sec]

C:\Users\cuqier\Desktop\gps-sdr-sim-master>
```

Fig. 3.2 Generation process using gps-sdr-sim

The generator is quite extensive, but in our case we will only use the basic option. So we pass the ephemeris data file to the generator, we give the selected location coordinates and we set the I / Q data format to 8-bits. After connecting HackRF One, turn on the transfer provided by PhotosSDR and start transmitting the signal generated in gps-sdr-sim. We set the appropriate parameters, the frequency and duration of the transmission we are interested in.

```
C:\Program Files\PothosSDR\bin>hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 0
call hackrf_set_sample_rate(2600000 Hz/2.600 MHz)
call hackrf_set_hw_sync_mode(0)
call hackrf_set_freq(1575420000 Hz/1575.420 MHz)
call hackrf_set_amp_enable(1)
Stop with Ctrl-C
 5.2 MiB / 1.015 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.012 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.013 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.009 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.002 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.013 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.015 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.008 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.009 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.012 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.015 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.014 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.015 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.004 sec =  5.2 MiB/second, amplitude -inf dBfs
 5.2 MiB / 1.015 sec =  5.2 MiB/second, amplitude -inf dBfs
```

Fig. 3.3 Transmission of spoofing signal

From that moment on, the transmitted signal influences the GPS receivers of the antenna. The essential duration of an attack to an effect depends on the device and conditions, the first attempt has no effect on the Apple device, no major changes in the context of operation with or without a signal are visible. In the case of Huawei, it was also possible to get the correct position after a while, as in the case of the LG K8, despite the longer waiting time. In this case, the attack was unsuccessful. The next attempt is made in a room that does not allow access to that number of satellites.

Fig. 3.4 Photo showing a failed attack attempt

The problem in this case is the location, during the trials spoofing took place at a high point with access to a large number of satellites, including GLONASS and Galileo satellites, enabling the obtaining of appropriate positioning data. Therefore, we are changing the location to slightly facilitate the attack.

Fig. 3.5 GPSDO detecting multiple satellites

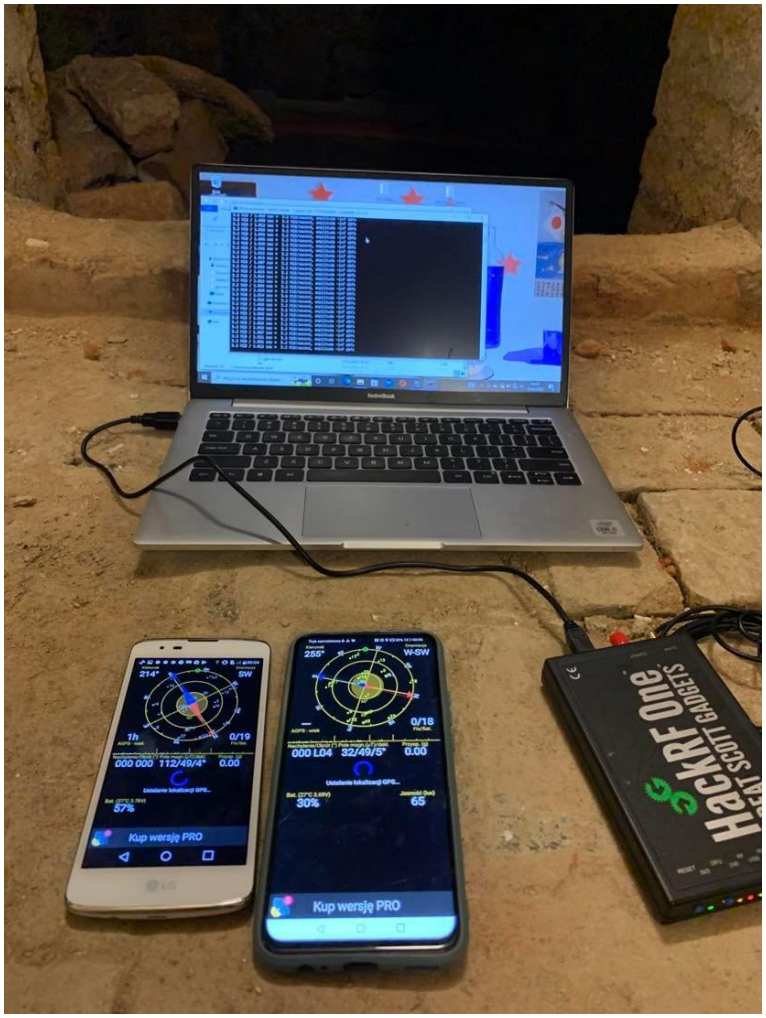

Fig. 3.6 Performing the experiment in the basement

Both devices initially experience a jamming-like effect that prevents them from finding any reasonable positioning solution. This effect is most likely due to too much difference to the actual signal, another replica of signal based on the newer ephemeris was generated to continue the experiment. In the next try, after around 10 minutes, it is possible to fool and spoof properly the least secured phone, i.e. the LG K8 2016. Contrary to the earlier positioning result marking the position in Germany, in Saxony, this time the phone thinks it is in Afghanistan.

Fig. 3.7 Successful spoofing of LG K8 2016

In the face of the signal, Huawei was constantly unable to find any positioning solution (around 30 minutes), only after switching off the signal spoofed transmission he managed to find the right position after 2 minutes. In addition, I did not notice any major changes in the case of the Iphone XR, the positioning results took a bit (up to 30 seconds) longer, but here the reason is the location issue. I assume that the differences in the response of telephones to the spoofing signal result from the quality of the receivers used, which allow to receive a larger number of satellite signals locally. The issue of greater system integration in the case of iOS is probably also important.

Despite initial problems, spoofing was successful. In fact, spoofing can also be performed in the original location, however, it would be initially necessary to use an appropriate jammer to eliminate the remaining satellite signals. The experiment also shows that the localization issue as well as the potential range and influence of the spoofer on the device are extremely important for the course of spoofing.

In the case of AGPS used in both phones, I was not able to get precise technical information, although the Iphone XR is definitely faster than the competition. Most likely, this is due to the novelty of the model, although from previous experience with older models I noticed that in the case of iOS, obtaining a solution was faster than in the Android counterpart.

Conclusion

GNSS is one of the most important means used today for positioning purposes. And the dangers of standard interference, spoofing and jamming are the basic problems that modern researchers are trying to solve. The work discusses the structure of the functioning of GNSS systems and its weaknesses allowing for the implementation of attacks. The scope and scale of the composition and characteristics of the types of jamming and spoofing attacks that modern users have to deal with are given. The impact on specific structures of GNSS functionality and the criteria necessary to launch specific types of attack were also discussed. The work also includes a general list of techniques used for the detection and mitigation of threats, and additional descriptions of improvements for overall GNSS security. Most of the materials used in the work have been presented in the simplest possible way, allowing insight into the topic for people who do not know it fully. Some of the techniques presented in the work are not currently used, yet some of them are very promising and are to be introduced in the near future.

On the other hand, the practical part of the work showed how simple it is to carry out a low-complexity spoofing attack, assuming no access to a larger base of devices. This shows that whether it is spoofing or jamming, an attack of this type can be carried out at home in a dozen or so minutes, and the costs of its implementation are minimal and affordable for everyone.

References:

[1] Barker, C., Betz, J., Clark, J., Correia, J., Gillis, J., Lazar, S., Straton, J. . *Overview of the GPS M Code Signal.* Mitre Corporation.

[2] Bauernfeind, R., Dötterböck, D., Kraus, T., & Eissfeller, B. (2012). *ANALYSIS, DETECTION AND MITIGATION OF INCAR GNSS JAMMER.* University FAF Munich.

[3] Borio, D., Dovis, F., Kuusniemi, H., & Lo Presti, L. (2016). *Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers.* IEEE.

[4] Borio, D., Fortuny-Guasch, J., & O'Driscoll, C. (2013). *mycoordinates.org.* Von https://mycoordinates.org/characterization-of-gnss-jammers/ abgerufen

[5] Borio, D., O'Driscoll, C., & Fortuny, J. (2012). *GNSS Jammers: Effects and Countermeasures.* Ispra, Italy: EC Joint Research Centre, Institute for the Protection and Security of the Citizen.

[6] Broumandan, A., Lachapelle, G., & Nielsen, J. (2012). *GPS Vulnerability to Spoofing and a Review of Antispoofing Techniqes.* International Journal of Navigation and Observation.

[7] Cozzens, T. (2019). *gpsworld.com.* Von https://www.gpsworld.com/highway-gantries-identify-jammers/ abgerufen

[8] Curran, J., Bavaro, M., Closas, P., & Navarro, M. (2016). *On the Threat of Systematic Jamming of GNSS.* Portland Oregon.

[9] de A. Faria, L., de Melo Silvestre, C., Feitosa Correia, M., & Roso, N. (2018). *GPS Jamming Signals Propagation in Free-Space, Urban and Suburban Environments.*

[10] de Abreu Faria, L., Caio Augusto , d., Feitosa Correia, M., & A. Roso, N. (2018). *Susceptibility of GPS-Dependent Complex Systems to Spoofing.* São José dos Campos.

[11] Dixon, C., Smith, S., Hart, A., Keast, R., Lithgow, S., Grant, A., Beatty, C. (2013). *Specification and Testing of GNSS Vulnerabilities.* United Kingdom: Navigation Unlimited.

[12] Fernández-Prades, C. (kein Datum). *Global receiver parameters.* GNSS-SDR.

[13] *Global Navigation Satellite System (GNSS).* (2006).

[14] *GNSS User Technology Report.* (2020). Publications Office of the European Union.

[15] *GPS spoofing using software defined radio.* (2019). Observatoire de Besancon.

[16] Grover, K., Lim, A., & Yang, Q. (2014). Jamming and Anti-jamming Techniques in Wireless Networks: A Survey. *International Journal of Ad Hoc and Ubiquitous Computing*, Volume 17, pp 197–215.

[17] Grzegrzółka, M. (2021). *Wojskowe Systemy Naprowadzania i Śledzenia.* Wrocław: Politechnika Wrocławska.

[18] Günther, C. (2014). A Survey of Spoofing and Counter-Measures. *NAVIGATION*, vol. 61, no. 3, pp. 159-177.

[19] Huang, L., & Yang, Q. (2015). *Low-cost GPS simulator – GPS spoofing by SDR.* DEFCON 23.

[20] Humphreys, T., Ledvina, B., Psiaki, M., O'Hanlon, B., & Kintner, P. (2008). Assessing the spoofing threat: development of a portable gps civilian spoofer. *ION GNSS '08*, pp. 2314-2325.

[21] Ioannides, R., Pany, T., & Gibbons, G. (2016). Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques. *IEEE*, Vol. 104.

[22] Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables. *International Journal of Satellite Communications and Networking*, vol. 30, no. 4, pp. 181–191.

[23] Jansen, K. (2018). *Detection and Localization of Attacks on Satellite-Based Navigation Systems.* Bochum.

[24] Jevtovic, M. (2018). *EFFECT OF PPD TYPE JAMMERS ON AVIATION GPS RECEIVERS.*

[25] Kaplan, E., & Hegarty, C. (2006). *Understanding GPS: principles and applications.* Norwood: Artech House.

[26] Khan, S., Mohsin, M., & Iqbal, W. (2021). *On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions.* Islamabad, Pakistan: Department of Information Security, National University of Science and Technology.

[27] Kožović, D., & Djurdjevic, D. (2021). *Spoofing in aviation: Security threats on GPS and ADS-B systems.*

[28] Kuusniemi, H., Wieser, A., Lachapelle, G., & Takala, J. (2007). User-level reliability monitoring in urban personal satellite navigation. *IEEE Transaction on Aerospace and Electronic Systems*, vol. 43, no. 4, pp. 1305–1318.

[29] Ledvina, B., Bencze, W., Galusha, B., & Miller, I. (2010). An in-line anti-spoofing device for legacy civil GPS receivers. *International Technical Meeting*, pp. 698–712.

[30] Lindroth, N., & Falk, A. (2018). *GPS spoofing at sea.* Gothenburg, Sweden: Department of Mechanics and Maritime Sciences, Charlmers University of Technology.

[31] Lineswala, P., & Shah, S. (2018). *Designing of SDR Based Malicious Act: IRNSS Jammer.* Surat: Department of Electronics and Communication.

[32] Montgomery, P., Humphreys, T., & Ledvina, B. (2009). Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. *International Technical Meeting*, pp. 124-130.

[33] Plessis, W. P. (2018). *Electronic-Warfare (EW) Training with Software-Defined Radio (SDR).* Bangalore, India: Conference: Electronic Warfare International Conference India.

[34] Pu, L. (2015). *A software defined radio experimental platform for GPS/GNSS signal reception alysis.* Texas: Texas A&M University.

[35] Rees, M. (2009). *EUROCONTROL Policy for GNSS In Europe.*

[36] Rosa, T. (2016). *GNSS/GPS Radio Hacking - From Beautiful Equations to Serious Threats.*

[37] Rounds, S. (2004). Jamming Protection of GPS Receivers. *GPS World Magazine*, pp. 38-45.

[38] Ruan, N., & Hori, Y. (2012). *DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things.* International Conference on Selected Topics in Mobile and Wireless Networking.

[39] Rügamer, A., & Kowalewski, D. (2015). *Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!* Sofia.

[40] Sathaye, H., LaMountain, G., Closas, P., & Ranganthan, A. (2022). *SemperFi: Anti-spoofing GPS Receiver for UAVs.* Boston, USA: Northeastern University.

[41] Schmidt, E., Nikolaos, G., & Akopian, D. (2020). *A GPS spoofing detection and classification correlator-based technique using the LASSO.* IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS .

[42] Scott, L. (2003). *Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems.* Portland, USA.

[43] Sklar, J. R. (2003). *Interference Mitigation Approaches for the Global Positioning System pp.167-179.*

[44] Stenberg, N. (2019). *Spoofing Mitigation Using Multiple GNSS-Receivers.* Linköping: Department of Electrical Engineering, Linköping University.

[45] Tanill, C. (2016). *Detecting GNSS Spoofing Attacks using INS Coupling.* Illinois: Illinois Institute of Technology.

[46] Xu, C. (2020). *Defending Against GPS Spoofing by Analyzing Visual Cues.* Blacksburg, Virginia: Virginia Polytechnic Institute and State University.

[47] Yanbing, G., Miao, L., & Zhang , X. (2018). *Spoofing Detection and Mitigation in a Multi-correlator GPS Receiver Based on the Maximum Likelihood Principle.* Beijing: Beijing Institute of Technology.

[48] Zidan, J., Adegoke, E., Kampert, E., Birrell, S., Ford, C., & Higgins, M. (2017). *GNSS Vulnerabilities and Existing Solutions: A Review of the Literature.* Paignton, United Kingdom: Spirent Communications.

[50] gnss-sdr.org. Von https://gnss-sdr.org/docs/sp-blocks/observables/ abgerufen

[51] natronics (2014). Von https://natronics.github.io/blag/2014/gps-prn/ abgerufen

[52] Caparra, G., Wullems, C., Ceccato, S., Sturaro, S., Laurenti, N., Pozzobon, O., Ioannides, R.,T., Crisci, M. (2016). *Navigation Message Authentication Schemes for GNSS Systems*

[53] Prochniewicz, D., Wezka, K., Kożuchowska, J. (2021). *Empirical Stochastic Model of Multi-GNSS Measurements*