Uros Bokan, BSc

Mitigation strategies for GNSS jamming attacks

MASTER'S THESIS

to achieve the university degree of

Diplom-Ingenieur

Master's degree programme: Geomatics Science

submitted to

Graz University of Technology

Supervisor

Univ.-Prof. Dipl.-Ing. Dr.techn. Dr.h.c.mult. Bernhard Hofmann-Wellenhof

Co-supervisor

Dipl.-Ing. Dr.techn. Philipp Berglez

Institute for Geodesy

Graz, November 2018

Affidavit

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master‘s thesis.

Date	Signature

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Das in TUGRAZonline hochgeladene Textdokument ist mit der vorliegenden Dissertation identisch.

Datum	Unterschrift

Abstract

The use of global navigation satellite systems (GNSS) and the associated permanent availability of position as well as precise time measurements become more and more a matter of course in many areas of everyday life. Information from GNSS satellites are used in many applications like civil engineering, energy industry, agriculture, civil protection, telecommunication, banking operations, transport, surveying and many others. Studies show that GNSS services are mainly used for road applications and location based services (LBS). The number of GNSS users is increasing enormously. Due to the rising number of applications and users, it becomes more and more important to consider not only the opportunities, but also the weaknesses and risks of a satellite-based position determination. Due to the great importance, concerning the larger number of potential users, the interest to disturb the signals is increasing as well. Nowadays, radio frequency interference is a big threat in signal processing. Studies show that interference can cause both considerable economic and material damage. The GNSS signals are particularly vulnerable to interference because of the low signal power, which is below the thermal noise floor. In the past years many interference attacks have been reported, although jamming is illegal in the whole European Union. Interference can be divided into unintentional and intentional interference. The biggest threat is intentional interference like jamming, spoofing or meaconing because the signals are transmitted intentionally to cause degraded position and timing determination or to cause a denial of the position, velocity and time (PVT) calculation.

The focus of this thesis is set on jamming. Jamming denotes the masking of GNSS signals with strong signals, which are understood as noise by the GNSS receiver. Jamming has become a serious threat, because jammers can be bought through several websites for a cheap price. Jamming may have fatal consequences for the GNSS receiver. Jamming signals can have a huge impact on the signal processing. Jamming causes a saturation of the analog-to-digital converter, it causes erroneous acquisition results or prevents the receiver of performing an acquisition, it lowers the carrier-to-noise ratio, causes higher variance of the tracking correlators or a loss of tracking. This may cause an inaccurate PVT solution or a denial of the PVT solution. This is very critical for safety critical applications. Therefore, a successful detection and mitigation of jamming signals are needed.

The main topic of this thesis is the investigation and implementation of state-of-the-art mitigation strategies. The impact of jamming signals on a software-defined GNSS receiver is described in detail, taking into account all different stages of the receiver. Within this thesis the jamming signals are characterized and classified based on different properties. Since detecting jamming attacks is a prerequisite for mitigation, different state-of-the-art

detection methods, containing pre- and post-correlation techniques, are analysed and explained in detail. Afterwards different mitigation strategies in the frequency domain, time domain and space-time domain, are described. Two different techniques - adaptive notch filtering and pulse blanking – are investigated in more detail and implemented into existing software-defined GNSS receivers. Based on simulations and real-world data the effect of the implemented mitigation strategies are investigated. Different types of jamming signals, with different spectral characteristics are taken into account. Also different filter and algorithm settings are compared. The assessment and comparison is based on the evaluation of the tracking results, the carrier-noise-ratio, as well as the position, velocity and time solution of the software-defined GNSS receivers.

This thesis provides an insight into state-of-the-art jamming mitigation strategies and analysis the impact of jamming on different stages of the signal processing. The thesis concludes with a summary of the performed work and provides an outlook on future topics.

Zusammenfassung

Der Einsatz globaler Navigationssatellitensysteme (GNSS) und die damit verbundene permanente Verfügbarkeit von Positions- und genauen Zeitmessungen wird in vielen Bereichen des täglichen Lebens zur Selbstverständlichkeit. Die Informationen von GNSS-Satelliten werden in vielen Anwendungen, wie dem Bauingineurswesen, dem Energiesektor, der Landwirtschaft, dem Katastrophenschutz, der Telekommunikation, dem Finanzsektor, dem Transportwesen, dem Vermessungswesen und vielen weiteren eingesetzt. Studien belegen, dass standortbezogene Dienste und Verkehrsanwendungen den größten Anteil von GNSS-Nutzern darstellen. Die Anzahl der Benutzer dieser Dienste steigt stetig. Wegen der zunehmenden Anzahl von Anwendungen und Benutzern wird es immer wichtiger, nicht nur die Chancen, sondern auch die Schwächen und Risiken einer satellitengestützten Positionsbestimmung zu berücksichtigen. Mit zunehmender Wichtigkeit von GNSS steigt auch das Interesse, die Signale zu Stören. Interferenz ist zu einer großen Bedrohung geworden. Studien zeigen, dass Inteferenz sowohl ökonomische als auch materielle Schäden verursachen können. GNSS-Signale sind sehr verwundbar aufgrund ihrer schwachen Empfangsleistung, welche unter dem thermischen Rauschen liegt. In den letzten Jahren wurde über mehrere Inteferenzangriffe berichtet, obwohl das absichtliche Stören von GNSS in der gesamten Europäischen Union verboten ist. Interferenz kann in unbeabsichtigte und beabsichtigke Interferenz unterteilt werden. Die größte Bedrohung stellt die beabsichtigte Interferenz (Jamming, Spoofing und Meaconing) dar, weil die Signale absichtlich ausgesendet werden um die Qualität der Positions- und Zeitbestimmung zu mindern oder um eine Positions-, Geschwindigkeits- und Zeitslösung zur verhindern.

Der Fokus dieser Arbeit liegt auf Jamming. Jamming beschreibt das Maskieren authentischer GNSS-Signale mit starken Signalen, die vom Empfänger als Rauschen angesehen werden. Jamming ist zu einer ernsthaften Bedrohung geworden, weil Störsender leicht über verschiedene Internetseiten zu einem günstigen Preis zu erwerben sind. Die Konsequenzen von Jamming können fatal sein. Jamming verursacht eine Sättigung des ADC, eine fehlerhafte Akquisition bzw. verhindert das Durchführen einer Akquisition, es reduziert das Signal-Rausch-Verhältnis, es verursacht höhere Schwankungen der Tracking-Korrelatoren bzw. den Verlust des Trackings zu Satelliten. Weiters kann es eine ungenauere Positions- und Zeitbestimmung verursachen bzw. eine PVT-Lösung verhindern. Speziell für sicherheitskritische Anwendungen ist dies sehr kritisch und erfordert eine Detektion und entsprechende Gegenmaßnahmen.

Das Hauptthema dieser Arbeit ist die Untersuchung und Implementierung von veschiedenen Mitigationsstrategien. Die Arbeit beschreibt den Einfluss von Störsignalen auf verschiedene

Zusammenfassung

Stufen eines Software-basierten GNSS Empfängers. Basierend auf verschiedenen Signaleigenschaften werden die Störsignale charakterisiert und klassifiziert. Weiters werden unterschiedliche Detektionsalgorithmen beschrieben. Die Detektionsstrategien sind wichtig, weil eine erfolgreiche Erkennung von Störsignalen die Voraussetzung für eine erfolgreiche Abschwächung ist. Danach werden verschiedene Mitigationsstrategien im Frequenz-, Zeit- und Ort-Zeit-Bereich beschrieben. In der Arbeit werden zwei Strategien - der adaptive Notch Filter (ANF) und Pulse Blanking - genauer untersucht und in schon vorhandene GNSS-Softwareempfänger implementiert. Die Auswirkung dieser Strategien wurde auf simulierte und echte Daten angewendet. Es wurden verschiedene Jammer mit verschiedenen spektralen Eigenschaften untersucht. Weiters wurden verschiedene Einstellungen vom Filter berücksichtigt. Zur Bewertung und zum Vergleich der Abschwächungsstrategien wurden die Trackingergebnisse, das Signal-Rausch-Verhältnis und die PVT-Lösung herangezogen.

Diese Arbeit bietet einen Einblick in die Strategien zur Abschwächung von Störsignalen und analysiert die Auswirkung von Störsignalen auf verschiedene Stufen der Signalverarbeitung. Die Arbeit schließt mit einer Zusammenfassung der durchgeführten Arbeit ab und gibt einen Ausblick auf zukünftige Themen.

List of Acronyms

ADC Analog-to-Digital Converter
AGC Automatic Gain Control
AM Amplitude Modulated
ANF Adaptive Notch Filter
ARNS Aeronautical Radio Navigation Service
AWGN Additional White Gaussian Noise
BJ Bump-Jumping algorithm
BMVIT Bundesministerium für Verkehr, Innovation und Technologie (Austrian Ministry for Transport, Innovation and Technology)
BOC Binary Offset Carrier
BPSK Binary Phase-Shift Keying
C/A Coarse/Acquisition
CDMA Code Division Multiple Access
CNR Carrier-to-Noise Ratio
CRC Cyclic Redundancy Check
CW Continuous Wave
CWI Continuous Wave Interference
DC Duty Cycle
DFT Discrete Fourier Transformation
DLL Delay Locked Loop
DME Distance Measuring Equipment
DOP Dilution of Precision
EGNOS European Geostationary Navigation Overlay Service
FDAF Frequency Domain Adaptive Filtering
FDMA Frequency Division Multiple Access
FFT Fast Fourier Transformation
FLL Frequency Locked Loop
FM Frequency Modulated
GDOP Geometric Dilution of Precision
GEO Geostationary Earth Orbit
GLONASS Global'naya Navigationsnaya Sputnikovaya Sistema
GNSS Global Navigation Satellite Systems
GPS Global Positioning System
GUI Graphical User Interface
HAS High Accuracy Service
ICAO International Civil Aviation Organization
IF Intermediate Frequency
IFFT Inverse Fast Fourier Transformation
IIR Infinite Impulse Response

ITU International Telecommunication Union
LFSR Linear Feedback Shift Registers
LNA Low Noise Amplifier
LOP Line of Position
MBOC Multiple Binary Offset Carrier
MGD Multi Gate Delay
NAV Navigation Message
NBI Narrowband Interference
NCO Numerically Controlled Oscillator
NF Notch Filter
OFB Oberste Funkmeldebehörde (Supreme Telecommunication Authority)
OS Open Service
PB Pulse Blanking
PLL Phase Locked Loop
PRN Pseudorandom Noise
PRR Pulse Repetition Rate
PRS Public Regulated Service
PSD Power Spectral Density
PVT Position, Velocity and Time
PW Pulse Width
RDS Running Digital Sum
RF Radio Frequency
RFFE Radio Frequency Front-End
RFI Radio Frequency Interference
RMS Root Mean Square error
SAR Search And Rescue
SBAS Space-Based Augmentation Systems
SCW Swept-Continuous Wave
SDR Software-Defined Receiver
SNR Signal-to-Noise Ratio
SOP Surface of Position
SSB Single Sideband
STFT Short-Time Fourier Transform
SVN Signal-to-Noise Variance estimator
TACAN Tactical Air Navigation
TOA Time Of Arrival
WAAS Wide-area Augmentation system
WBI Wideband Interference

Contents

Abstract iii

Zusammenfassung v

List of Acronyms vii

1 Introduction 2
- 1.1 State-of-the-Art . . . 3
- 1.2 Project PRSAustria . . . 4
- 1.3 Thesis outline . . . 4

2 Global navigation satellite systems 5
- 2.1 GNSS segments . . . 7
- 2.2 Satellite signals . . . 7

3 GNSS receiver 11
- 3.1 Radio-frequency front-end . . . 11
- 3.2 Acquisition . . . 14
- 3.3 Tracking . . . 15
- 3.4 Position, velocity and time computation . . . 18

4 Interference 20
- 4.1 Unintentional interference . . . 20
- 4.2 Intentional interference . . . 22
- 4.3 Classification of jamming signals . . . 23
- 4.4 Impact of jamming on the GNSS receiver . . . 27

5 Jamming detection and mitigation strategies 35
- 5.1 Interference detection strategies . . . 35
- 5.2 Jamming mitigation strategies . . . 38

6 Implementation 47
- 6.1 Used software . . . 48
- 6.2 Implementation of the adaptive notch filter in software . . . 51
- 6.3 Implementation of pulsed interference in software . . . 53
- 6.4 Implementation of the pulse blanking algorithm . . . 55

7 Results 56
- 7.1 Simulations . . . 56
- 7.2 Real-world data . . . 84

8 Conclusions and outlook **94**

List of Figures **96**

List of Tables **100**

Bibliography **101**

Acknowledgments

First, I would like to thank my supervisor Prof. Bernhard Hofmann-Wellenhof and my co-supervisor Philipp Berglez for all the support and guidance during the last year. You gave me an example of a good mentor, researcher and a role model.

I would like to thank all my colleagues at the company Teleconsult Austria for the support during the last 10 months. Special thanks go to the managing director, Andreas Lesch and my co-supervisor and the Head of System Engineering of Teleconsult Austria, Philipp Berglez, who gave me the chance to write my master thesis and to start working at this company. I would also like to give special thanks to Sascha Bartl who was always there for me if I needed help.

I would like to thank all the employees of the Institute for Geodesy and the Institute for engineering geodesy and measurement systems of Graz University of Technology for building up my knowledge during the last five years.

I would like to thank my whole family, especially my parents, Vlasta and Stanko and my grandmother Marta for the love and amazing support they gave me over the whole time of my academic studies. They accepted that I wanted to go my own way in a foreign country. Furthermore, they were always there for me if I had problems. They always lent an open ear to me and comforted me if I was sad or stressed out and they were always available for talking. Moma, rest in peace. Ati, you had the wish to see me graduate, to see my new apartment and you wanted to see how I built up the life on my own after the study. Unfortunately, your illness was stronger than you and you had to give in to it just one month before I finished this thesis. I hope you are proud of me wherever you are now. Rest in peace.

I would like to give big thanks to my fellow students for five amazing five we spent together. A special thanks to “Mathekings” Mathias Duregger, Gernot Kainz, Stefan Laller and Maximilian Schachner-Nedherer. I will never forget our time together through all five years. Without our study group many of my grades would be worse. Without your help and our discussion of the problems I would spend much more time on programming the labs. With your jokes you have improved many of my days. Thank you for everything! I hope we will stay in contact after our academic studies.

Finally, I would like to thank all students and absolvents who were participating the USI-courses Floorball, Ballspiele, Fussball and Volleyball. Doing sports with you was always fun - no matter if we won or lost. It presented a distraction from all the problems I had in those time and a reduction of stress. A special thanks to my friends from the Floorball and Ballspiele courses for the wonderful time we spent together outside the gym.

1 Introduction

The use of global navigation satellite systems (GNSS) and the associated permanent availability of position and precise time measurements as well become more and more a matter of course in many areas of everyday life. The information from GNSS satellites is used in many applications like civil engineering, energy industry, agriculture, civil protection, telecommunication, banking, transport, surveying and many others. Studies show, that the main GNSS markets are road applications and location based services (LBS). The number of GNSS devices is increasing dramatically and forecasts show there will be one device per human in the next few years.

Due to the increasing number of applications and users, it becomes more important to consider not only the opportunities, but also the weaknesses and risks of a satellite-based position determination. Currently, many users are unaware of potential GNSS threats and their impacts. The GNSS signals are particularly vulnerable to interference because of the low signal power, which is below the noise floor. In recent years, GNSS applications have become the target of interference attacks. Studies show that interference can cause both considerable economic and material damage, as interference signals can significantly influence the operation of GNSS. In general, the impact of interference can lead to degraded position and timing accuracies or to a total failure of the positioning. The term interference involves unintentional and intentional interference. Unintentional interference can be caused by the electron concentration in the ionosphere, other GNSS signals or out-of-band signals. In addition to unintentional interference, intentional interference of GNSS signals represents a high threat potential. Jamming, spoofing and meaconing are the known intentional interference types. Spoofing of GNSS signals is the broadcast of counterfeit signals with the intent that the victim receiver misinterprets them as authentic signals. Thus, the victim might deduce a false position and time solution. Meaconing is the interception, delay and rebroadcasting of navigation signals and causes erroneous pseudorange measurements. The objective of jamming is the denial of navigation service by masking the GNSS signals with high power noise. Jamming signals can have a fatal impact on the signal processing. It may cause a saturation of the ADC, false acquisition results, erroneous tracking, lost tracking to certain satellites and thus leads to a denial of service. Because it has an impact on the most receiver stages, it can be detected using different strategies before and after the acquisition stage. The jamming detection is very important, because it is the first step for handling interference. Many applications do not have a back-up in case jamming occurs. Because interference may cause an erroneous position or time estimation or a tracking loss, this can be critical when dealing with banking or energy applications and for applications, which are critical for human lives. Therefore, mitigations strategies have to be applied on the signal. Mitigation strategies have the goal to remove the interfering signal and preserve as much as possible of the useful signal. In

the literature different strategies, which work in the time, frequency domain or in the space-time domain are reported.

The mitigation of jamming signal is the main topic of this master thesis. Within this thesis, state of the art algorithms for mitigating jamming signals. The focus is set on two mitigation strategies in the frequency and time domain: the adaptive notch filter and the pulse blanking algorithm. For the evaluation existing software-defined receivers and simulated as well as real jamming signals are used.

1.1 State-of-the-Art

Interference mitigation is a hot topic in the GNSS community. The mitigation of interference is only possible if the interference is successfully detected. Mitigation is the suppression of the interfering signal. According to Dovis (2015) different mitigation techniques already exist. According to the domain, in which they are implemented, they can be divided into three groups: frequency domain, time domain and in the time-space domain. The implementation of the latter technique requires complex hardware configuration, therefore, it will not be investigated within this thesis. The focus will be set on the time and frequency domain techniques, which can be implemented into existing software.

In general, the frequency domain techniques are widely use. The most common frequency domain techniques are the notch filter and frequency domain adaptive filtering (FDAF). The principle of notch filtering is described in detail in Dovis (2015). The notch filter follows the interfering frequency and mitigates it. But it has two huge drawbacks: the interfering frequency has to be known in advance and has to be constant. Therefore, the adaptive notch filter (ANF), which can adjust itself to the changing frequency, exists. The basic principle of the ANF is described in Dovis (2015). In the literature several implementations of the ANF are presented. Regalia (1991) presents an ANF solution for tracking interfering signals for real data. In Regalia (2010) the ANF, applied on complex data is presented. Another implementation of an ANF can be found in Sugiura (2014) or Mei and Lin (2001). Wheeler (2015) evaluated four already existent ANF solutions and developed an own solution and tested it on multiple sinusoid signals. The implemented ANF are applied on signals with different characteristics. None of the works investigated the impact of the ANF on GNSS signals and on different interference types. In literature the impact of the ANF on the tracking stage is taken into account (Giordanengo 2009). Another frequency domain technique, developed for mitigation of pulsed interference, is the FDAF. It is presented in Dovis (2015) and Raimondi et al. (2006).

The time domain techniques are widely used for mitigation of pulsed interference. In Borio and Cano (2012) the interference cancellation and pulse blanking techniques are analysed and characterized. The interference cancellation is based on the principle of investigating the pulse parameters and predict the pulses in advance. In Niamsuwan et al. (2005) an

asynchronous pulse blanking algorithm for detection and mitigation of pulses with random occurence is presented. Another time domain algorithm is the pulse blanking algorithm, which is presented in Hegarty et al. (2000) and Dovis (2015).

1.2 Project PRSAustria

Parts of this master thesis are based on the project Impacts and Countermeasures of Austrian PRS application scenarios in GNSS denied environments (PRSAustria). The project is managed by the Austrian Research Promotion Agency (FFG) and received funding from the Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program line ASAP. The project is led by TeleConsult Austria, together with its partners Brimatech GmbH and the Austrian Ministry of Defence.

The project has two main goals. First, the thread of intentional interference (jamming, spoofing) has to be investigated. In detail, the effect of interferer characteristics and the interference signal power on the signal design, on tracking performances and on the accuracy of the position, velocity and time information on different receiver types are taken into account. The second task is to elaborate, implement and assess different mitigation strategies on real data and simulated data. The latter is the main topic of this master thesis. Different test campaigns were made during this project. To avoid harming other GNSS receivers or applications the test measurements were performed on the military training ground Seetaler Alpe. Because jamming or spoofing is illegal, an exemption from the Supreme Telecommunication Authority (OFB) of the Austrian Ministry for Transport, Innovation and Technology (BMVIT) was obtained. The PRSAustria project was successfully completed in 2018.

1.3 Thesis outline

The thesis is composed of seven chapters. Chapter 2 provides an overview about the global navigation satellite system, describing the principle of satellite positioning, segments of the global navigation satellite systems and a detailed description of the signal. In Chapter 3 the architecture of a software-define receiver is described in detail. Chapter 4 provides an overview on interference, discussing the sources of unintentional and intentional interference. Furthermore, jamming signals and their impact on a software-defined receiver are presented in detail. Different jamming detection and mitigation strategies are presented in Chapter 5. In Chapter 6 the implementation is discussed. It includes a description of existing software used and of the implementation principles of the mitigation strategies. Chapter 7 shows the results of applying the adaptive notch filter and pulse blanking algorithm on simulated data. Finally, the results of applying the adaptive notch filter on recorded real-world data are shown. Conclusions and the outlook are given in Chapter 8.

2 Global navigation satellite systems

The term Global navigation satellite systems (GNSS) denotes navigation systems based on a global constellation of satellites, which emit ranging signals used for positioning and timing. The positioning can be performed on land, sea, in the air and in the space in every weather condition everywhere on the earth at every time.

The position determination is based on a trilateration using ranges or range rates, measured between the satellite and receiver. The principle is shown in Figure 2.1.

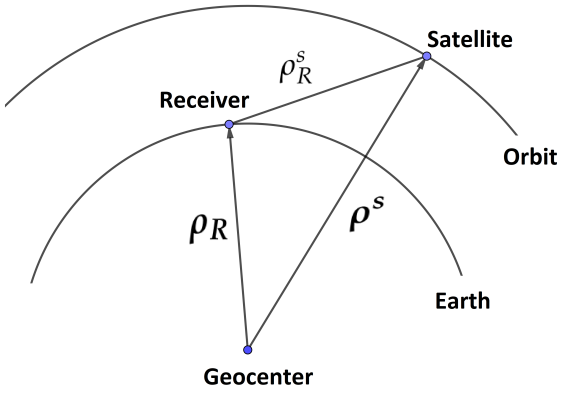


Figure 2.1: Principle of the satellite-based navigation (c.f. Hofmann-Wellenhof et al. 2008)

The position of the satellites, and therefore the vector ρ^s from the geocenter to the satellite, is assumed to be known. The geometric distance between the satellite and the receiver (ρ_R^s) is expressed as range. The range can be derived from the travel time of the signal from the satellite to the receiver. In a 2D space the line of position (LOP) is a cycle, centered at the satellite position, with a radius ρ_R^s. In 3D space the surface of position (SOP) is a sphere. If the ranges between the receiver and 3 satellites are known, the receiver position (the vector between the geocenter and receiver ρ_R) can be calculated. The main task of navigation can be written as

$$\rho_R^s = \|\boldsymbol{\rho^s} - \boldsymbol{\rho_R}\|. \tag{2.1}$$

If ranges are used, it is assumed, that both, the receiver and satellite clocks, are synchronized. But in reality they are not [Teunissen and Montenbruck (2017)]. The satellite clocks are very stable and accurate atomic clocks. Their clock error and clock drift can be estimated and is supposed to be known. On the other side the receiver clocks are mostly crystal oscillators, which are less stable and accurate and have a bias ($\Delta\rho_R$), which is unknown. The delayed ranges are called pseudoranges (R_R^s). They can be represented as

$$R_R^s(t) = \rho_R^s(t) + c \cdot \Delta\delta_R^s(t) + \epsilon_R^s(t) = \rho_R^s(t) + c(\delta_R(t) - \delta^s(t)) + \epsilon_R^s(t), \tag{2.2}$$

where c represents the speed of light, δ^s and δ_R are the satellite and receiver clock errors and ϵ are other error sources like atmosphere, multipath or measurement errors. The LOP are cycles with an error of $\Delta\rho$, and the SOP are spheres with an error of $\Delta\rho$. The receiver position estimation in a 2D space is shown in Figure 2.2.

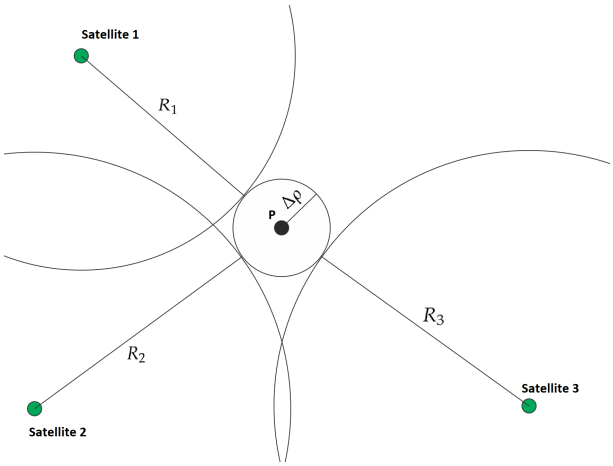


Figure 2.2: The principle of the position estimation in 2D space (c.f. Hofmann-Wellenhof et al. 2008)

Because of the clock errors the navigation equation has to be extended (to 4 unknown parameters), for which reason at least four measurements have to be available to calculate the receiver position. According to Teunissen and Montenbruck (2017) GNSS enables three different types of measurements, which are needed to calculate the position and velocity. Beside pseudoranges carrier phase and Doppler measurements exist. The Doppler is the difference between the transmitted and received frequency due to the Doppler effect. The carrier phase is the instantaneous beat phase and the number of integer number of cycles. The carrier phase is more accurate than the pseudorange. There exist different positioning modes as single point positioning (SPP), precise point positioning (PPP), differential GNSS, relative GNSS etc. They are described in detail in Hofmann-Wellenhof et al. (2008) and Teunissen and Montenbruck (2017).

The term GNSS nowadays summarizes are the U.S. Global positioning system (GPS), the Russian Globalnaya navigationsnaya sputnikovaya sistema (GLONASS), the European system Galileo and the Chinese Beidou. Furthermore, space-based augmentation systems (SBAS) exist, which consist of satellites, which provide integrity information and differential corrections from GNSS satellites to improve the accuracy and integrity. The European SBAS is called european geostationary navigation overlay service (EGNOS), the U.S SBAS is named wide-area augmentation system (WAAS).

2.1 GNSS segments

In general GNSS consists of three segments: space, control and user segment.

The space segment comprises the satellites. The space segment generates and transmits the code and carrier signals and broadcast the navigation message [Subirana et al. (2013)]. The constellation of the satellites has to be designed in a way, that at least four satellites are seen at the same time on everywhere on the earth's surface. For a global coverage at least 24 satellites are needed. According to Hofmann-Wellenhof et al. (2008) the design criteria for the satellite constellation are the user position accuracy, the satellite geometry and size, service coverage, satellite availability, weight and shape of satellites. Another important parameter is the satellite orbit.

The control (or ground) segment is responsible for controlling the whole system. According to Hofmann-Wellenhof et al. (2008) and Subirana et al. (2013) the control segment tracks the satellites, calculates and predicts the satellite position and the satellite clock error, uploads the navigation message for all satellites, controls and maintains the whole system and monitors auxiliary data (as ionosphere parameters) and keeps the GNSS time scale.

The user segment consists of users of the GNSS services, which receive the GNSS signals and process it. According to Hofmann-Wellenhof et al. (2008) the user segment can be classified into different user categories, receiver types and various information services.

2.2 Satellite signals

GNSS signals are electromagnetic waves. They propagate with the speed of light. By means of the transmitted frequency they are located in the L-band. The L-band was chosen because it is a good "compromise between frequency availability, propagation effects and system design" [Hofmann-Wellenhof et al. (2008)]. Because of their high frequency (greater than 30 MHz) they can be classified into line-of-sight waves, which can propagate through the atmosphere. The GNSS signal structure is composed of three different layers: the carrier (physical layer), the ranging code layer and the data-link layer. The signal structure is shown in Figure 2.3.

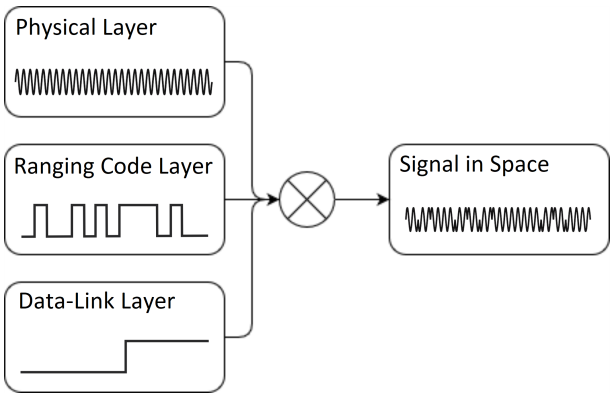


Figure 2.3: Components of the satellite signal (c.f. Hofmann-Wellenhof et al. 2008)

The physical layer is a sinusoidal wave, generated with a certain frequency. The ranging code is a binary sequence of ±1 bits (chips). The sequence is unique for every satellite. The ranging codes are used for pseudorange measurements and for differentiating the single satellites. The satellite signal is characterized with a synchronization of the periodicity of the ranging codes to the system time [Hofmann-Wellenhof et al. (2008)]. The data-link component is a sequence of ±1 bits,representing the navigation data containing information about the ephemeris, time of transmission, clock bias parameters, almanac, integrity and other information. The navigation message has to be decoded by the receiver.

The ranging code and the data-link layer are modulated on the carrier using a phase modulation. If the value of the ranging code or the navigation message changes from $+1$ to -1 or vice versa, the phase of the signal changes between $+\pi$ and $-\pi$. Note, that commonly more ranging codes and navigation message blocks are modulated on one carrier. Figure 2.4 shows the power spectral density (PSD) of different GPS and Galileo signals.

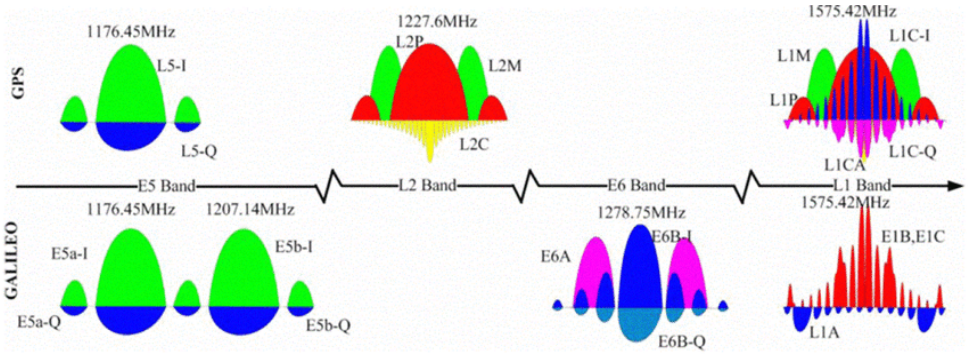


Figure 2.4: GPS and Galileo signal structure [from Arienzo (2010)]

GPS uses three different carrier frequencies. All frequency bands are based on a fundamental frequency of $f_0 = 10.23$ MHz [Subirana et al. (2013)], which is generated by the atomic clocks. The transmitting frequencies are determined by multiplying the fundamental frequency with a certain multiplication factor. The single bands, the multiplication factors, carrier frequencies and the wavelengths are listed in Table 2.1.

Table 2.1: GPS frequency bands

Frequency Band	Multiplication factor	Center frequency $[MHz]$	Wavelength $[cm]$
L1	154	1575.42	19.0
L2	120	1227.60	24.4
L5	115	1176.45	25.5

Different types of pseudorandom noise (PRN) codes are defined for GPS. The coarse/acquisition (C/A) code is a civilian code with a length of 1023 bits and a fundamental frequency of $f_0/10$ (=1.023 Mbps), defined in the L1 band. The duration of one code sequence is 1 ms and one chip wavelength is 293.1 m [Subirana et al. (2013)]. It is generated using two 10-bit linear feedback shift registers (LFSR)[Hofmann-Wellenhof et al. (2008)]. More information about the C/A code generation can be found in United States Department of Defense (2018). The C/A code is modulated only on the L1 band using a binary phase shift keying (BPSK) modulation.

The last layer is the navigation message. The GPS 'legacy' navigation message (NAV) is modulated on L1 and L2 with a frequency of 50 symbols per second (sps). The navigation data consists of different frames. One frame is divided in 5 subframes with the length of 6 s each. To receive all data 12.5 min are needed [Subirana et al. (2013)].

Galileo uses four different frequency bands. Some of the center frequencies coincide with center frequencies of other systems, e.g. GPS L1 or L5. The Galileo frequency bands are listed in Table 2.2.

Table 2.2: Galileo frequency bands

Band	Multiplication factor	Center frequency $[MHz]$	Wavelength $[cm]$
E1	154	1575.42	19.0
E5a	115	1276.45	25.5
E5b	118	1207.14	24.8
E6	125	1287.75	23.4

Note, that E5a and E5b are parts of the E5 carrier frequency on its full bandwidth. Galileo uses 10 different signals on the four carrier frequencies. The different signals are used for four different services [European (2018)]:

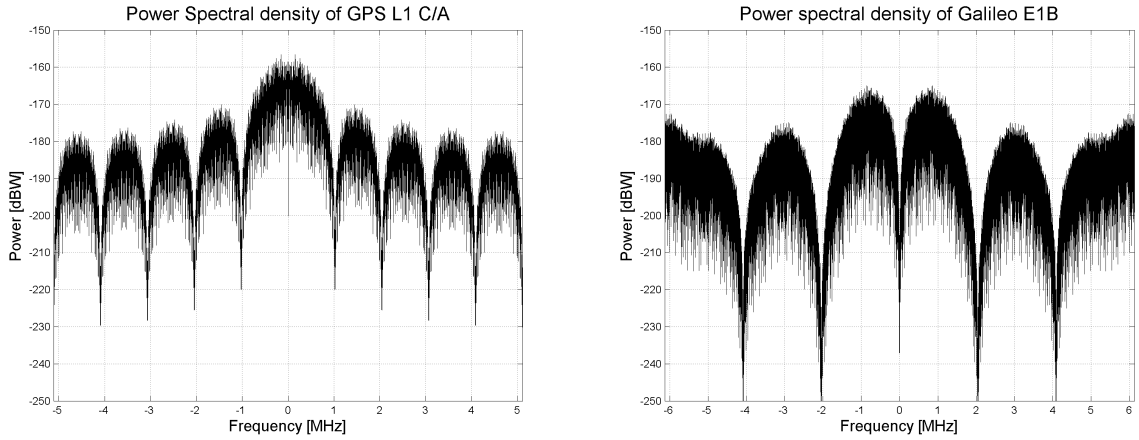
- Open service (OS): This service is unencrypted and free of charge for all users. It includes no integrity information and has no service guarantee [Hofmann-Wellenhof et al. (2008)]. For the OS six signals are modulated onto three carrier frequencies (E1, E5a, E5b). The signal accuracy is comparable to GPS L1 C/A.
- High-accuracy service (HAS): It includes additional encrypted data with a higher data rate than the Galileo OS data. It is located on the E6 carrier frequency, providing added value services by means of extended accuracy and signal authentication.
- Public regulated service (PRS): The signal is located on the E1 and E6 carrier frequencies. It is encrypted and designed for authorized civilian user groups, mostly government agencies and operators of critical infrastructures. The access is restricted by the EU and its member states.

- Search and rescue service (SAR): It contributes to the international COSPAS-SARSAT system for Search and Rescue (SAR) [European (2018)]. If emergency signal is received by the satellites, the emergency message is sent to the SAR ground segment.

The E1 carrier frequency consists of three different signal components. The E1A signal is encrypted and used for the PRS service. E1B and E1C signals are public known and used for the OS and HAS service. The E1B is a data channel, the E1C is a pilot channel. The ranging codes are created using a primary codes and secondary codes. One code consists of 4092 chips, thus, the Galileo E1B code is four times longer than the GPS L1 C/A code. The single codes are available in the European (2016). The code is modulated on the carrier using a multiple binary offset carrier (MBOC) modulation, which consists of two binary offset carrier (BOC) modulations.

The Galileo navigation data consists of navigation data and integrity information. The message has a higher data rate of 250 sps [Teunissen and Montenbruck (2017)].

In this thesis the GPS L1 C/A and the Galileo E1B signal are commonly used. Figure 2.5 shows the PSD of both signals.



(a) GPS L1 C/A

(b) Galileo E1B

Figure 2.5: PSD of the GPS L1 C/A and Galileo E1B signals

The bandwidth of GPS L1 C/A is 10.23 MHz. The spectrum has one main lobe at the center frequency, which is caused by the BPSK modulation. There are many side lobes seen, but their energy is decreasing with increasing frequency. The bandwidth of Galileo E1B is 12.276 MHz. The signal has no main lobe. Two side lobes at ± 1.023 MHz are visible and are the consequence of the BOC(1,1) modulation. Furthermore, additional lobes occur ar ± 6 MHz and are caused by the MBOC(6,1,1/11).

3 GNSS receiver

The main task of a GNSS receiver is to receive the signal in space (SIS) and to process of this signal to provide a position, velocity and time (PVT) solution. A GNSS receiver consists of different components, which can be divided in to hardware and software. The architecture of a software-defined GNSS receiver is shown in Figure 3.1.

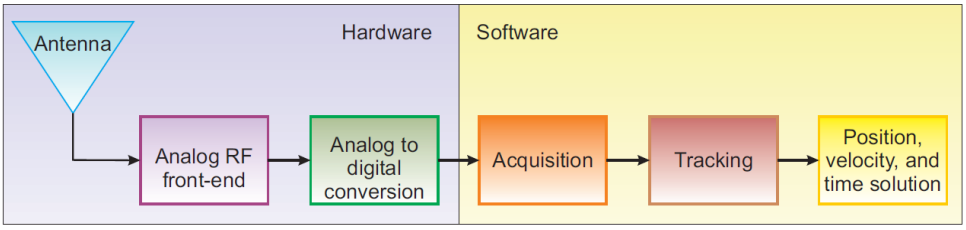


Figure 3.1: Structure of a software GNSS receiver [from Berglez (2013)]

First the signal reaches the GNSS antenna and then it is sent to the radio frequency front-end (RFFE). In the RFFE the signal is amplified, filtered and converted to digital samples. Next the acquisition is performed to identify the satellites in view and to calculate initial estimates of the code phase and the Doppler frequency. These two values change in time and therefore they have to be permanent monitored. This is achieved by the tracking stage. Finally the position, velocity and the time is calculated. The next sections describe the main parts of a software-defined GNSS receiver.

3.1 Radio-frequency front-end

After receiving the incoming signal it is forwarded to the RFFE. According to Teunissen and Montenbruck (2017) the RFFE is the most critical part of a receiver, because it defines the cost, size and power-consumption of the receiver. Therefore, the design is very important. The RFFE consists of different components. The first two components of the GNSS receiver are a bandpass filter and a low noise amplifier (LNA). The bandpass filter eliminates out-of-band signals from the incoming signal, while the LNA increases the magnitude of the received signal for further processing.

The next stage is the mixer/local oscillator. Because of the high carrier frequency and because the Nycquist (Shannon) theorem has to be fulfilled, it is not predicable to use such high sampling frequencies [Berglez (2013)]. Thus, it has to be downconverted to a usable intermediate frequency (IF), which is done by the mixer/local oscillator. Normally the IF

is set to a few MHz, but sometimes the signals are directly downconverted to baseband ($IF = 0$). The downconversion of the signal to a lower IF has an advantage in the quality and the cost component, otherwise expensive and complex narrowband filters for high frequencies would have to be designed [Borre et al. (2007)].

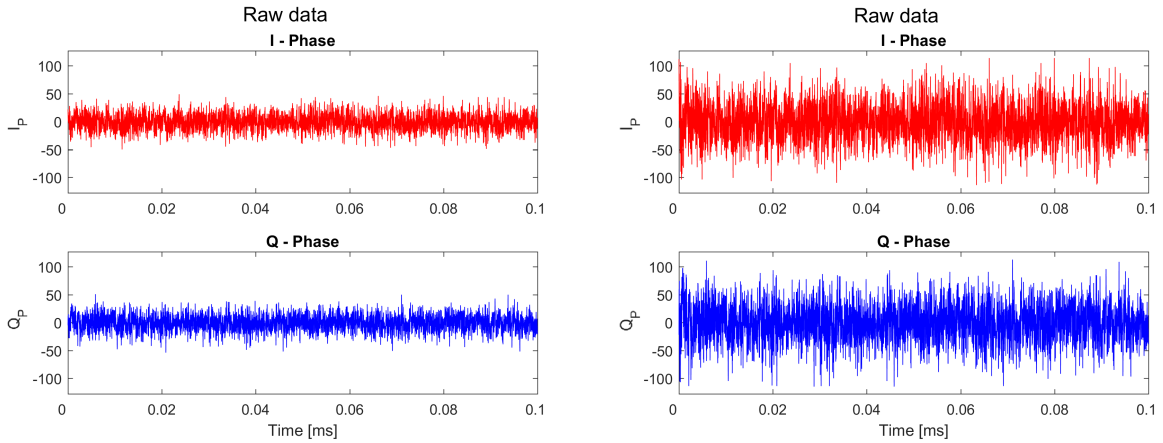
The ADC is the last part of the RFFE, which main tasks are sampling (conversion of the continuous signal to a discrete signal) and quantization (conversion of continuous amplitude to discrete amplitude) [Teunissen and Montenbruck (2017)]. For the quantization a limited number of bits is used. The most ADCs in commercial receivers use 8 bit to convert the analog signal. The ADC output are integer numbers [Pany (2010)]. After the ADC the signal is discrete and can be written as

$$s_{IF}[k] = A \cdot C[k]D[k]cos\Big(\varphi_0 + 2\pi(f_{IF} - f_D)t[k]\Big) + e_{IF}[k], \tag{3.1}$$

where A describes the amplitude of the signal, C is the PRN code sequence, D the navigation message, φ_0 the initial phase, f_{IF} is the IF, f_D the Doppler frequency shift and e_{IF} is the noise component.

After the ADC the AGC can be activated. The AGC is used to control the gain of the incoming signal. The analog input range of the ADC is in most cases too weak [Borre et al. (2007)]. An AGC has the goal to use all bits of the ADC. Therefore it keeps the output's standard deviation on a constant value by multiplying it with a gain [Raimondi et al. (2006)]. If only a few samples are occupied during the ADC, the gain is increased. If the incoming signal strength is too high and the signal occupies the outer values of the ADC, the gain is decreased.

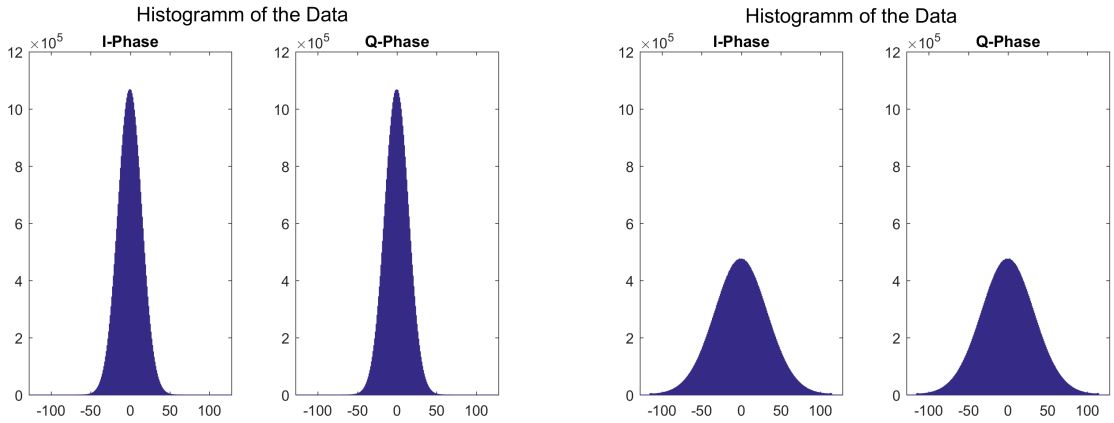
The ADC output are digital signal samples. They can be represented in the time domain, in the frequency domain and as a histogram. The values of the samples in the time domain depend on the number of quantization bits. In case of an 8 bit quantization the samples have 256 (2^8) different values. Figure 3.2 shows the raw data in the in- and quadrature-phase using a sampling frequency of 40 MHz without and with activated AGC. For the ADC a gain of 95 dB was used.



(a) Without AGC (b) With AGC

Figure 3.2: Raw data with and without activated AGC

Figure 3.3 shows the distribution of the received data if AGC is activated (right) and if AGC is not activated (left).



(a) No AGC (b) With AGC

Figure 3.3: Histogram of the input data with (right) and without (left) activated AGC

The distribution of the incoming signal follows the Gaussian distribution if no interference is present. If the AGC is activated, the AGC increases its gain and the histogram gets wider bigger. This offers more signal information.

Because the GNSS signal is below the noise floor, the frequency domain of the incoming signal shows a flat distribution. The PSD of the GPS L1 C/A and Galileo E1B signals were already presented in Figure 2.5.

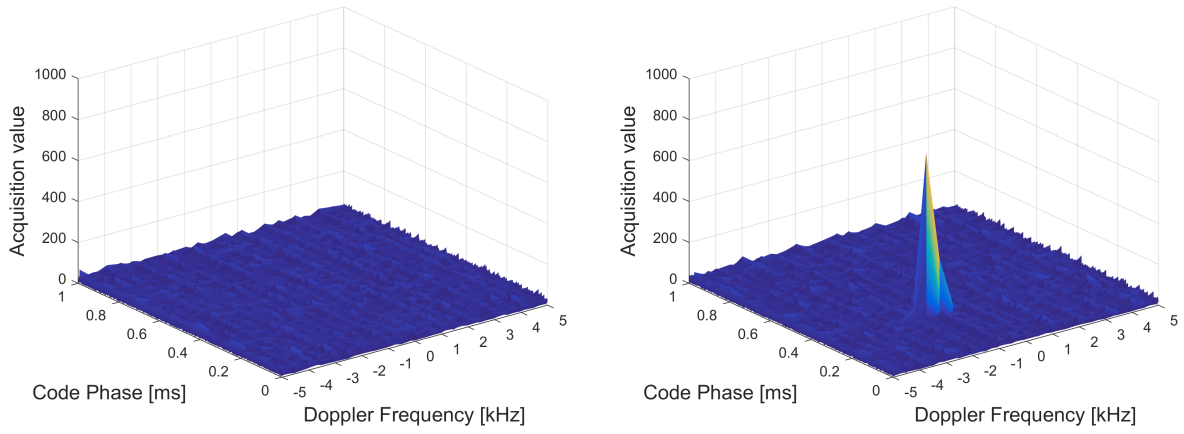
3.2 Acquisition

The acquisition stage is a search process [Berglez (2013)]. It has two main tasks: first, it decides if a signal of a certain satellite is present in the received signal and second, it computes rough estimates of the the Doppler frequency and the code phase.

Because of the relative motion between the satellite and the receiver a frequency shift occurs. The Doppler frequency is propotional to the radial velocity between the satellite and the receiver. The maximal radial velocity of GNSS satellites is 0.9 km/s, which results in a Doppler-shift of ± 4.7 kHz for a stationary receiver [Hofmann-Wellenhof et al. (2008)]. "The code phase denotes the point in the current data block where the ranging code starts" [Borre et al. (2007)]. If the length of one code sequence is taken for acquisition, one code phase is detected. The code phase depends on the distance between satellite and receiver. For the search process replicas of the code and the carrier of the satellite are required. Following Kaplan and Hegarty (2006) for GPS L1 C/A code 1023 different code phases at increments of 1/2 chip are examined. The Doppler search space is depending on the signal integration time, which can vary from less than 1 ms to 10 ms in case of GPS L1 C/A.

Borre et al. (2007) described different acquisition types: serial search acquisition, parallel frequency space search acquisition and the parallel code phase search algorithm.

Figure 3.4 shows the acquisition results of GPS satellites with the PRN 1 and 7. The signal of PRN 1 (left) is not present in the incoming signal, while the signal of PRN 7 (right) is present.



(a) PRN 1 (b) PRN 7

Figure 3.4: The acquisition results for two GPS satellites

If the satellite is present, a peak is detected. The peak is located at a certain code phase and a certain Doppler shift.

3.3 Tracking

The main purpose of tracking is to refine the rough estimates of the Doppler frequency and the code phase, keep track of them and demodulate the navigation data from the signal. The code tracking is usually performed performing a delay locked loop (DLL), while the frequency and phase tracking are usually performed using a frequency locked loop (FLL) and a phase locked loop (PLL).

For the PLL a Costas loop is typically used. Its structure is shown in Figure 3.5.

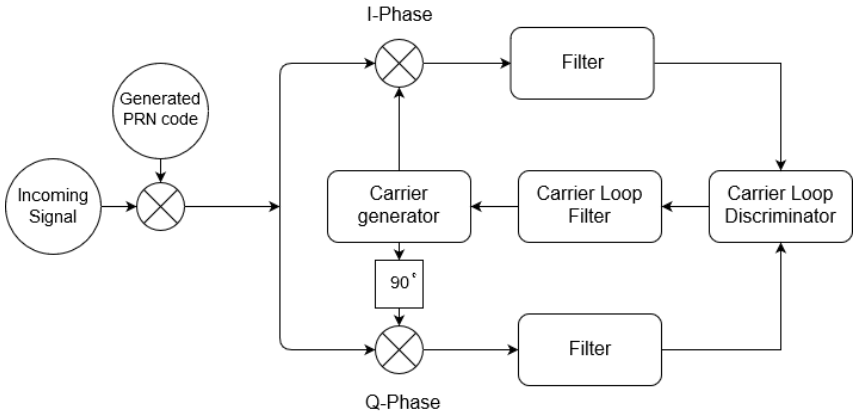


Figure 3.5: Basic structure of a Costas loop [c.f. Borre et al. (2007)]

The Costas loop is insensitive to 180° phase shifts, which appear in case of a navigation bit transition [Borre et al. (2007)]. First the incoming signal is multiplied with a PRN code replica, which removes the code from the signal. Next the numerical controlled oscillator (NCO) generates two carrier replicas, which are shifted by 90° (in- and quadrature-phase) and multiplied with the signal. Next the filtering of the signals in both arms is performed to remove the dependence on the IF [Borre et al. (2007)]. Two signals remain, which are used to calculate a discrimination function. From the discrimination function the phase difference between the input signal and the local carrier replica can be calculated. In Kaplan and Hegarty (2006) different PLL discriminator functions are described.

Code tracking refines the code phase of a code in the received signal. First the input signal is multiplied with a locally generated carrier. If the carrier frequencies of the replica and the incoming signal are aligned, the carrier is removed from the signal and only the code is present. This means that the PLL has to be done before the DLL. Then the code is multiplied with three different code replicas, generated by the PRN code generator. The three replicas are generated using a specific chip spacing δ. A smaller spacing provides more precise results, but introduces noise. A higher spacing is more robust. Often a chip spacing of $\pm\frac{1}{2}$ is chosen [Borre et al. (2007)]. The first replica is aligned with the last known code phase and is called prompt (P), the second is advanced by δ (early - E) and the third replica is delayed by δ (late - L). Figure 3.6 shows the generation of the three replica codes.

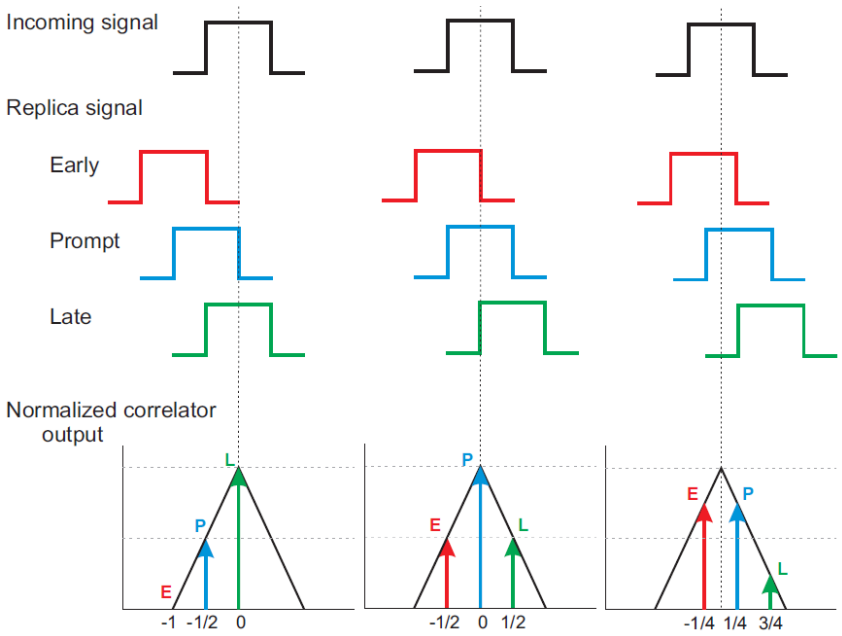


Figure 3.6: The basic principle of a DLL [from Berglez (2013)]

The results of the multiplications between the replicas and the incoming signals are the correlation values between the incoming signal and the replica codes. If the prompt correlator has the highest value and the early and the late correlator show the same values, the replica code is perfectly aligned. If the late correlator has the highest value and the early correlator has the smallest value, a code phase error exists and the code phase of the replica has to be adjusted. The determination of the code phase error is done using a discriminator function. In Kaplan and Hegarty (2006) and Borre et al. (2007) different discriminator functions are mentioned. The most common used discriminator in the receivers is the early-minus-late discriminator [Borre et al. (2007)]. The algorithm, described above, is mostly used for tracking a BPSK modulated signal. Because of autocorrelation function of BPSK generated signal shows only one peak, at least three replicas can be used. A BOC modulated signal shows several peaks in the autocorrelation function. The usage of three correlators would cause multiple zero crossings and a biased tracking and a smaller carrier-to-noise ratio could occur [Teunissen and Montenbruck (2017)]. Therefore, other algorithms have to be used like single sideband (SSB), bump-jumping (BJ) algorithm or a multi-gate discriminator (MGD) [Berglez (2013)].

The carrier-to-noise ratio (CNR) describes the ratio of the received modulated carrier signal power to the received noise power spectral density [Bartl (2014)]. "The measure of CNR provides satellite signal health information in addition to the PVT information" [Falletti et al. (2010)]. There are different methods to estimate the CNR in digital receivers. Falletti et al. (2010) presents five of them. All of them involve processing samples from the correlation output. The signal samples ($r_C[n]$) are given as

$$r_C[n] = \sqrt{P_d}D[n] + \sqrt{P_\eta}\eta[n], \tag{3.2}$$

where $D[n]$ represents the navigation bit samples, η are complex noise samples, P_d and P_n are the powers associated to data and noise.

One of the algorithms is the signal-to-noise variance estimator (SVN). The algorithm is based on the assumption that the imaginary output ($r_{C,Im}[n]$) contains the noise and the real part ($r_{C,Re}[n]$) contains the signal [Bartl (2014)]. Therefore two different estimators are needed. The first one is used for computing the signal power by

$$\hat{P}_d = \left[\frac{1}{N} \sum_{n=1}^{N} \mid r_{C,Re}[n] \mid \right]^2, \tag{3.3}$$

and second computes the signal and noise power by

$$\hat{P}_{tot} = \frac{1}{N} \sum_{n=1}^{N} \mid r_C[n] \mid^2 . \tag{3.4}$$

In Equations 3.3 and 3.4 the symbol N describes the number of observed samples used to calculate one CNR estimate. N has to be high enough to prevent additional estimation bias. Typically a few hundred samples are enough [Falletti et al. (2010)]. Next the noise power is computed as the difference between the total power and the signal power

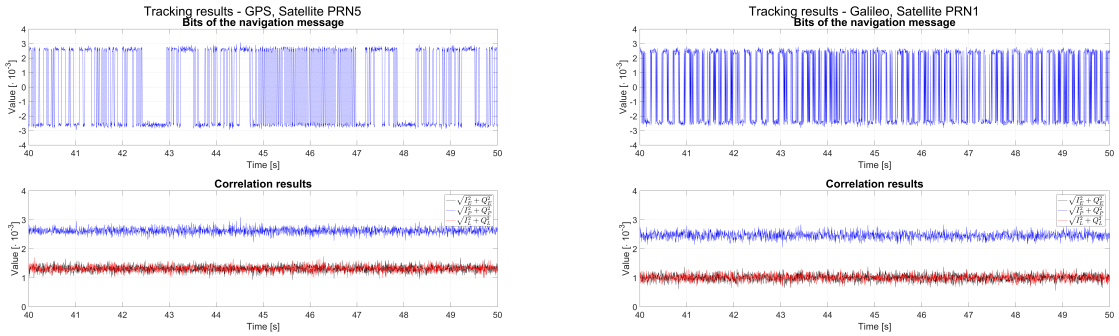
$$\hat{P}_n = \hat{P}_{tot} - \hat{P}_d. \tag{3.5}$$

The relation between the signal power ($\hat{P}_d$) and the noise power ($\hat{P}_n$) is the signal-to-noise ratio (SNR). To determine the CNR the SNR has to be multiplied with the observation bandwidth (B_{eqn})

$$CNR = B_{eqn} \frac{\hat{P}_d}{\hat{P}_n}. \tag{3.6}$$

Bartl (2014) shows, that this algorithm has a good time stability with a very small root-mean-square error (RMS). Furthermore, the complexity of this algorithm is low.

Figure 3.7 shows some of the tracking results for GPS and Galileo satellites. On the upper part of the figures the I_P values are shown. According to Berglez (2013) they represent the bits of the navigation data. Below the correlator functions (early, prompt and late) from the DLL are visualized. The DLL was calculated with three correlators for GPS and five for Galileo. For better comparison the "very-early" and "very-late" correlators for Galileo are not illustrated.



(a) GPS

(b) Galileo

Figure 3.7: Tracking results in case of tracking GPS L1 C/A (left) and Galileo E1B (right) signals

The bits of the navigation data are clearly visible for both systems. In both cases the prompt correlator shows the highest values, whereas the early and late correlator are smaller and of equal magnitude.

3.4 Position, velocity and time computation

After the Doppler frequency, the phase and the code error are successfully tracked, the calculation of the position, velocity and the time (PVT) solution can be performed. The calculation of the receiver position is done using a least squares adjustment. To calculate the receiver position the pseudoranges and the satellite positions have to be determined.

First the recovery of the navigation data has to be done. The bits of the navigation message include i.a. ephemeris, almanac data and time information. The structure of the navigation message is presented in detail in the European (2016) and United States Department of Defense (2018). The navigation data recovery has three steps:

- Bit synchronization: First a mean value over the navigation bit length (20 ms for GPS and 4 ms for Galileo) is made and the navigation bits get thresholded. If the I_P-values are positive, the navigation bit gets a value of $+1$. If the values are negative, they get a value of -1.
- Frame synchronization: Next subframes or pages of the navigation data have to be found. The beginning of every message is marked by a defined preamble [Teunissen and Montenbruck (2017)]. A preamble is a unique order of 8 bits for GPS L1 C/A and 10 bits for Galileo E1B. To find the preambles a correlation between the navigation bits and the predefined preamble is performed. If a preamble is present a correlation maximum is reached. If the preambles were found, the individual subframes are defined.
- Decoding of the navigation message: After defining the subframes the navigation data has to be checked or/and repaired and decoded. The decoding of the navigation

data is made using the Viterbi decoder (Galileo) or the Cyclic Redundancy Check (CRC) algorithm (GPS).

From the navigation data the ephemeris for the current satellite, the almanac data and the time information are decoded. From the ephemerides the satellite position can be calculated. The procedure is described in Hofmann-Wellenhof et al. (2008).

Next the pseudoranges have to be estimated. In Borre et al. (2007) the estimation is divided in two different parts: the computation of the initial set of pseudoranges and in the computation of the subsequent pseudoranges.

Last, the position, velocity and time (PVT) solution can be performed. The calculation of the receiver position is made using a least-squares adjustment. For the calculation the pseudoranges and the satellite positions are needed. Further information is found in Subirana et al. (2013).

4 Interference

The received GPS L1 signal power is -158.5 dBW and the received Galileo E1 signal power is -157 dBW [Teunissen and Montenbruck (2017)], which means, that they are below the noise floor and relative easy to disturb. Disturbing of the signals is linked with the term radio-frequency interference (RFI) or just interference. The thread of disturbing GNSS signals was discussed in the Volpe (2001). According to Dovis (2015) interference is defined as "any electromagnetic source interacting with the signals". Disturbing the authentic GNSS signal can be divided in two groups: unintentional interference and intentional interference [Volpe (2001)]. The first group includes natural sources disturbing the signal, signals, caused by satellites of the same or other GNSS constellations and signals from external systems. The biggest thread for users is intentional interference like jamming, spoofing and meaconing. This chapter describes different interference types and their impact.

4.1 Unintentional interference

Unintentional interference is undesired disturbance of GNSS signal, which happens almost all the time and cannot be prevented that easily. Unintentional interference can be divided into natural interference, intra-system and inter-system interference, multipath and external interference. Some unintentional interference sources are difficult to predict.

During the propagation from the satellite to the receiver the GNSS signal passes the atmosphere. The atmosphere is the most common natural interference source. The atmosphere can be divided into the ionosphere and the troposphere. The ionosphere reaches from 50 to 1000 km altitude and is an charged component of the atmosphere [Hofmann-Wellenhof et al. (2003)]. The content of the ionosphere are free, neutral and charged particles, which have a big influence on the signal propagation. In the ionosphere electron density irregularities cause scintillations. Scintillations are fluctuations in amplitude and phase and cause fading and frequency shifts [Hofmann-Wellenhof et al. (2003)]. The level of scintillations depends on the solar and geomagnetic activity, the geographic location, the local time and the frequency. The troposphere is the nonionized part of the Earth atmosphere. It reaches to an altitude of about 50 km and is nondispersive for frequencies up to 30 MHz [Hofmann-Wellenhof et al. (2008)]. The reason for the caused delays is the weather – temperature, pressure and partial water vapor.

GNSS are differentiated by the PRN code (code division multiple access - CDMA) or by the frequency (frequency division multiple access - FDMA). The only FDMA system

is GLONASS, which will use CDMA in the future too. Theoretically, the codes of the single satellites of the same satellite constellation should be orthogonal to be separated by the receiver. But the orthogonality of the codes is not perfectly and the residual power generates intra-system interference [Dovis (2015)]. This interference type has no major impact on the signal processing. It cannot be prevented, but with careful selection during the design phase it can be minimized.

Inter-system interference occurs because different GNSS share the same carrier frequency. The codes of the different systems are not perfectly orthogonal and the signal power of another system generates interference. An increase of different GNSS systems increases the probability of inter-system interference [Dovis (2015)]. The International Telecommunication Union (ITU) is responsible for the allocation of the frequency bands.

The GNSS signal reaches the GNSS receiver normally via the direct path with a strong signal component. On the other side the signal can be reflected from buildings, trees or other objects and causes delays of the signal. It alters the direction of propagation, amplitude, polarity, and phase of the radio wave [Dovis (2015)]. This path is called the indirect path or multipath. According to Hofmann-Wellenhof et al. (2008) the multipath effect can be reduced or estimated using different methods as antenna based-mitigation, improved receiver technology as well as signal and data processing methods.

External interference is caused by non-GNSS signals. The external signals can be divided into in-band and out-of-band interference. The out-of-band signals are signals from other frequency bands, which collide with the GNSS signals [Dovis (2015)]. Their carrier frequency is located near to the GNSS frequency band. They can be represented by the equation

$$f_{int} < f_{GNSS} - B_{GNSS}/2 \text{ or } f_{int} > f_{GNSS} + B_{GNSS}/2, \tag{4.1}$$

where f_{int} is the frequency of the interferer, f_{GNSS} is the carrier frequency of the GNSS and B_{GNSS} is the bandwidth of the GNSS signal. There are many different systems that cause interference: Analog TV channels, DVB-T, VHFCOM, FM harmonics, personal electronics devices (e.g. cell phones, pagers, laptops, remote control toys), satellite communications, Very high frequency Omnidirectional Range (VOR), instrument landing system (ILS) and mobile satellite service (MSS). More details about out-of-band interference and the influence on GNSS signals are listed in [Dovis (2015)]. In-band-interference are signals that appear in the same bandwidth as the GNSS signals. It can be written as

$$f_{GNSS} - B_{GNSS}/2 < f_{int} < f_{GNSS} + B_{GNSS}/2. \tag{4.2}$$

Such signals can be dangerous for GNSS application, but as reported in Dovis (2015), the amount of interference, caused by in-band signals is smaller than the amount of interference, caused by out-of-band signals. The biggest source of in-band-interference are military or civil aeronautical radio navigation services (ARNS) like the Tactical air navigation (TACAN), distance measuring equipment (DME), secondary surveillance radar (SSR), Joint tactical information distribution (JTIDS) or Multifunction information distribution

system (MIDS), which are located in the Galileo E5 and GPS L5 band. DME and TACAN are the main cause of pulsed interference. Other sources for in-band interference are ultra-wideband (UWB) signals.

4.2 Intentional interference

Intentional interference represents a deliberate attack on the GNSS signal. It is more dangerous for the GNSS receiver as unintentional interference, because the signal is transmitted intentional to cause an erroneous position or prevent the receiver to calculate a PVT solution. In literature three different intentional interference types are reported: jamming, spoofing and meaconing.

Jamming is a big thread for the GNSS applications. It denotes the masking of real GNSS signals with noise. The main goal of jamming is to degrade the receiver position accuracy, prevent signal reacquisition and cause a loss of tracking. It has become a serious thread because jammers, also called personal privacy devices, have become easily available through several websites for a low price. Mitch et al. (2011) states, that most jammers, available on the market, jam the L1/E1 band. Although some devices already jam more different frequency bands. The usage of jammers is illegal in the whole European union. For this master thesis real measurements were performed with a valid certificate from the Supreme Telecommunication Authority (OFB) from the Federal Ministry of Transport, Innovation and Technology (BMVIT).

Spoofing is defined as manipulation, deception and counterfeit of GNSS position, velocity and time information transmitting fake GNSS signals to the receiver. Following Dovis (2015) spoofing attacks can be classified as simplistic, intermediate and sophisticated.

For a simplistic spoofing attack the spoofer broadcasts fake GNSS signals towards a victim receiver. The spoofed signals are not synchronized to the real signals. The received signal looks like noise for the receiver and forces the victim receiver to a loss of tracking or to a reacquisition and to a false position. Such an attack is easy to detect because of the high transmit power and the signals being not synchronized.

The intermediate spoofing attack is more complex. Here the receiver receives synchronized GNSS-like signals from the spoofer and synchronizes itself to these signals. If the spoofing signal is aligned with the authentic signal, its higher power leads the DLL and the PLL to follow the correlation peak from the spoofed signal and not from the authentic. The receiver position, the actual constellation and a precise timing have to be known in advance. Such attacks are hard to detect and to mitigate especially because of its lower power and synchronization.

For a sophisticated spoofing attack more spoofers are connected in a network. The goal of such spoofers is to replicate the alignment of visible signals and the spatial distribution.

Such an attack is very difficult to detect and mitigate.

Meaconing is defined as the rebroadcasting of delayed signal [Dovis (2015)]. The whole spectrum of the GNSS signal is first received by the receiver, then it is delayed and last it is rebroadcast to the target GNSS receiver. The signal reaches the target receiver with a time delay and with a constant amplification factor. Both values are positive.
Meaconing cannot directly manipulate the PVT solution, but it can confuse the receiver and display the PVT solution of the meaconer. Meaconing can be detected if a plausibility check of the clock drift is done. If meaconing signals are received, the clock drift increases rapidly. Thus, for detection an already existing PVT solution is required [Dovis (2015)].

4.3 Classification of jamming signals

In literature different jammer classifications are reported. Dovis (2015) classifies the jammers based on their spectral features with respect to the GNSS signals into in-band and out-of-band signals. Furthermore, Dovis (2015) classifies jamming based on the bandwidth:

- Narrowband interference (NBI): The spectral occupation is small in comparison to the GNSS-band ($B_{int} \ll B_{GNSS}$).
- Wideband interference (WBI): The bandwidth of the interferer is comparable to the GNSS bandwidth ($B_{int} \approx B_{GNSS}$).
- Continuous-wave interference (CWI): It is represented as a single tone in the frequency domain ($B_{int} \Rightarrow 0$).

Another classification can be done based on frequency and amplitude properties of the jamming signal [Bartl (2014)].

Continuous wave (CW) jammers are characterized by a constant frequency and a constant amplitude over the time. The frequency of those jammers lies direct on or near the GNSS center frequency. The frequency and the amplitude of a CW jammers in relation to the time are presented in Figure 4.1.

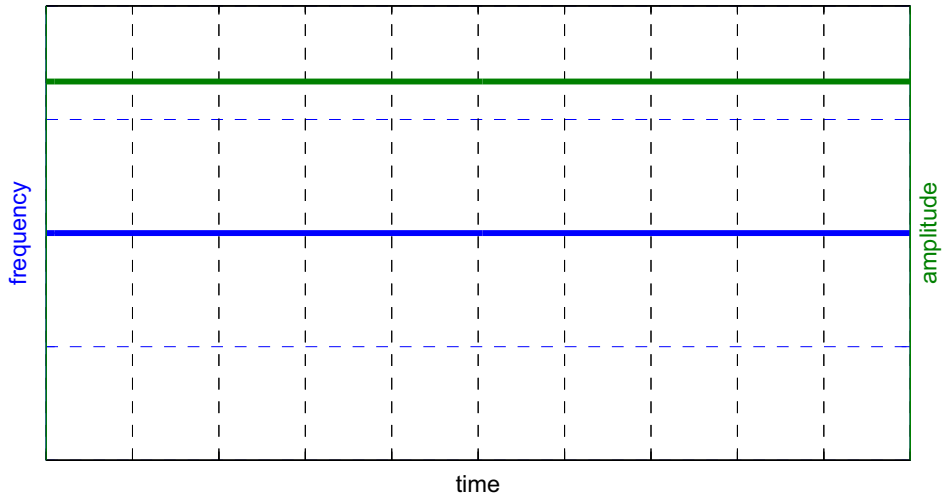


Figure 4.1: Frequency and amplitude characteristics of a CW jammer [from Bartl (2014)]

Swept continuous wave (SCW) jammers are characterized by a constant amplitude and with a changing frequency. The frequency change is periodic using a sawtooth function. The frequency and amplitude representation of a SCW is shown in Figure 4.2.

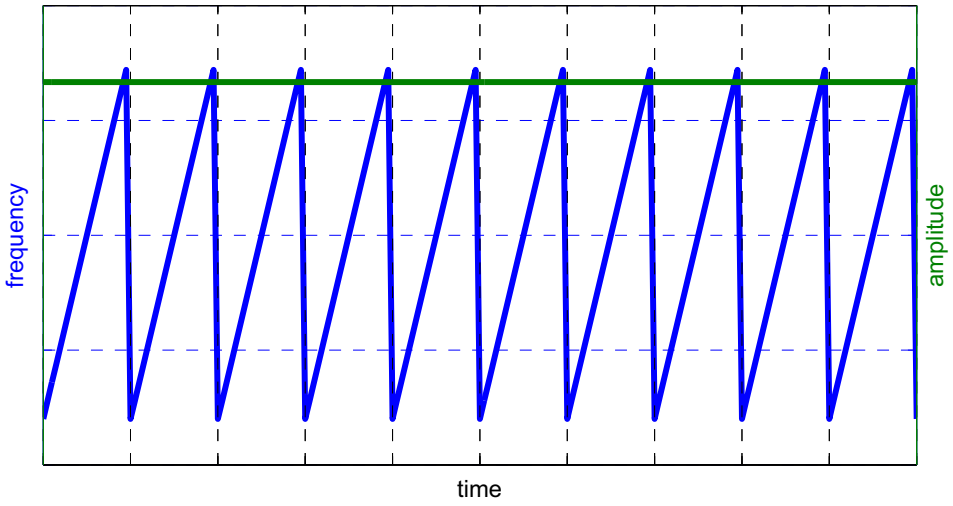


Figure 4.2: Frequency and amplitude characteristics of a SCW jammer [from Bartl (2014)]

SCW interference can be described with three parameters:

- Frequency offset: The difference of the center frequency of the jammer to the carrier frequency of the GNSS signal.
- Sweep bandwidth: The difference between the maximal and the minimal jamming frequency.
- Sweep duration: The time period needed for one complete frequency sweep.

Frequency modulated (FM) jammers are characterized by a constant amplitude and a changing frequency. The frequency change according to a sinusoidal wave. The amplitude and frequency representation of a FM jammer is shown in Figure 4.3.

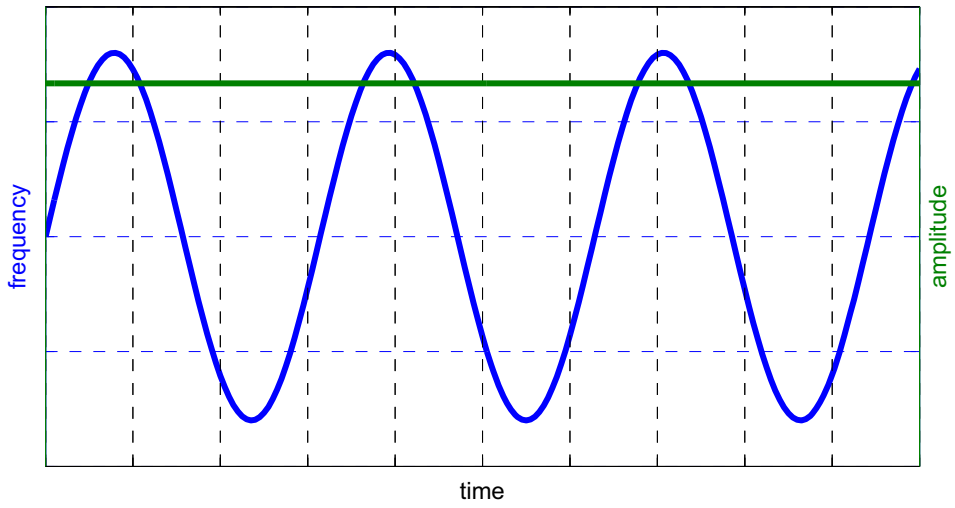


Figure 4.3: Frequency and amplitude characteristics of a FM jammer [from Bartl (2014)]

FM interference can be described with three parameters:

- Frequency offset: The difference of the center frequency of the jammer to the carrier frequency of the GNSS signal.
- Frequency deviation: The amplitude of the sinusoidal wave (the maximal offset of the interfering frequency to the frequency offset)
- Modulation frequency: The frequency of the sinusoidal wave controlling the jamming signal frequency.

Amplitude modulated (AM) jammer are characterized by a varying amplitude and a constant frequency. The amplitude varies by a sinusoidal wave as shown in Figure 4.4.

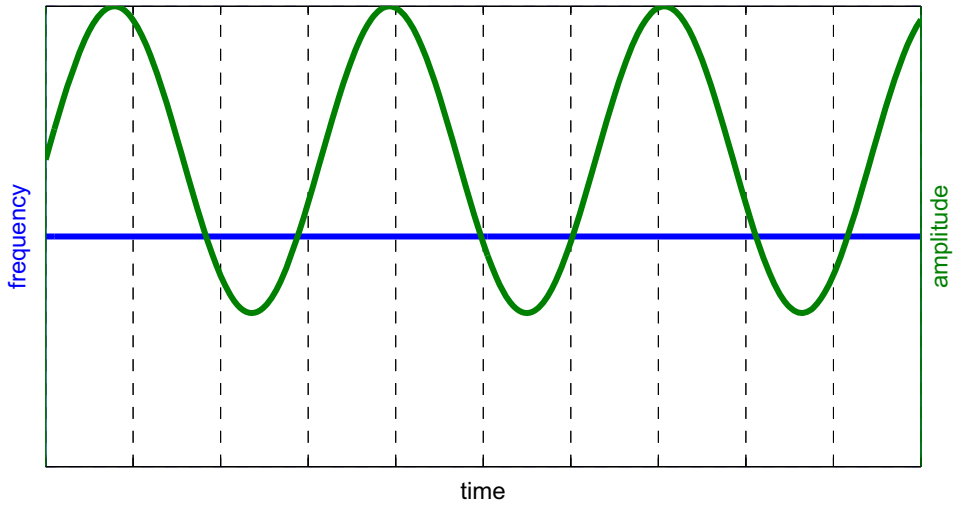


Figure 4.4: Frequency and amplitude characteristics of an AM jammer [from Bartl (2014)]

AM interference can be described with three parameters:

- Frequency offset: The difference of the center frequency of the jammer to the carrier frequency of the GNSS signal.
- Modulation frequency: The frequency of the sinusoidal wave controlling the amplitude.
- Modulation index: The relation of the biggest to the smallest amplitude. The modulation index can reach values between 0.0 and 1.0.

Another special cases of jamming are pseudorandom noise (PRN) jamming (described in Bartl (2014)) and additional white Gaussian noise (AWGN) jamming (described in Karaim et al. (2017)).

In the previous paragraphs continuous jamming signals were presented. In literature another type of interference is mentioned: pulsed interference. "Pulsed interfering signals are characterized by an on-off status of short duration, which alternate in the time domain" [Dovis (2015)]. This interference type occurs often in aviation scenarios. There exist many aeronautical radio navigation services (ARNS), which send pulsed signals. The pulses can be described as NBI. Many of them are located within the GNSS band. The most known examples are DME/TACAN pulses within the GPS L5/Galileo E5 band. They are described in detail in Yin (2007) and Hofmann-Wellenhof et al. (2003). In Dovis (2015) pulsed interference is described by three parameters. The pulse width (PW) describes the duration of one pulse. It is defined in seconds. The pulse repetition rate (PRR) describes the number of pulses per second. The duty cycle (DC) is the percentage of time, that is occupied by the pulses. There exist a connection between these parameters, which is given by

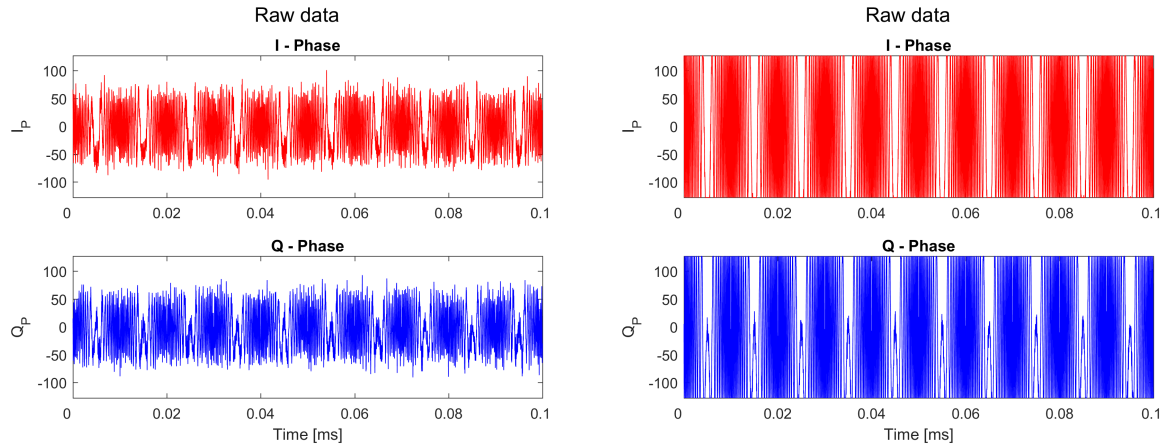
$$PRR = \frac{DC}{PW}. \tag{4.3}$$

There exist different mitigation strategies for pulsed interference like frequency domain adaptive filtering (FDAF) or pulse blanking (PB).

4.4 Impact of jamming on the GNSS receiver

The RF front-end is the first stage of the receiver which is affected by the interferer. If strong interference is present the filters and amplifiers may work outside of their nominal regions. This causes nonlinear effects or clipping phenomenas, i.e. the amplitude exceeds the hardware's capability, which can be mixed with the useful signal and thus degrading the signal quality [Dovis (2015)].

The biggest effect of interference can be observed after the ADC and AGC. The raw data and the histogram of the incoming samples without interference were already shown and discussed in Section 3.1. Figure 4.5 shows 0.1 ms of a received signal during an SCW interference event. The jammer has a sweep duration of 10 μs and a sweep bandwidth of 10 MHz. In this case the AGC was not activated and the samples after ADC were multiplied with a constant gain of 95 dB. In the left figure the power of the jammer was set to -120 dBW, in the right figure the power was set to -110 dBW.



(a) Jammer power -130 dBW

(b) Jammer power -110 dBW

Figure 4.5: I/Q data after ADC with different jammer powers

Interference is an additional signal, causing the samples at the ADC to become higher. The bigger the jammer power, the higher the sample values. In case of a high jamming power a saturation of the ADC happens and the values ± 127, in the case of an 8-bit quantization, are more frequent. Figure 4.6 shows the histogram of 1 s of input data during the SCW interference event with a jamming power of -110 dBW.

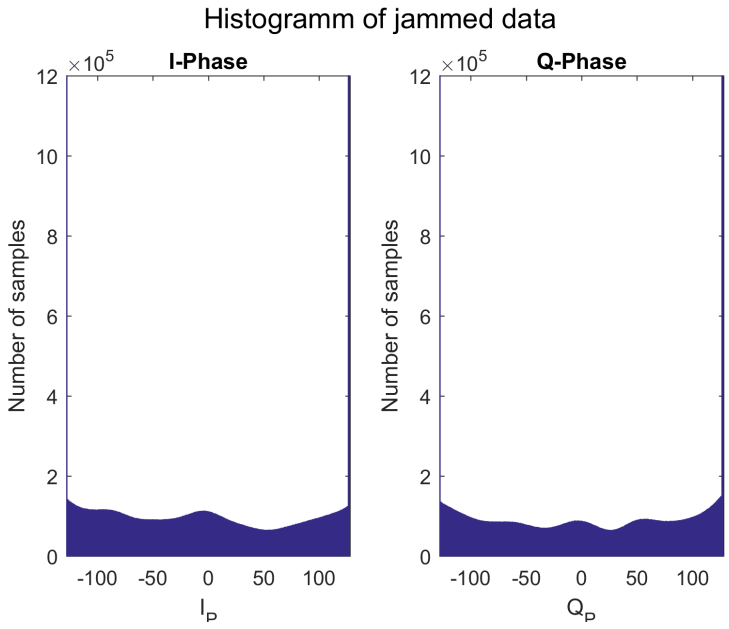


Figure 4.6: Histogram of interfered signal (jammer power -110 dBW without activated AGC)

The AGC is also strongly affected by interference, since it keeps the standard deviation of the incoming signal after the ADC at a constant value. Because the GNSS signal power is below the noise floor, the gain of the AGC is strongly depended on the noise or interference level [Yang et al. (2012)]. If no interference is present the AGC is driven by the noise environment, the temperature, power supply, environmental changes around the antenna etc. [Dovis (2015)]. If a jamming signal appears, the standard deviation of the ADC output increases. The AGC tries to avoid ADC saturation and decreases its gain. This causes a reduction of the amplitude of the useful signal and a loss of information.

Figure 4.7 shows 0.1 ms of the input data of the same SCW jammer as in Figure 4.5b with activated AGC. The AGC suppresses the signal and boundary values are not that frequent anymore.

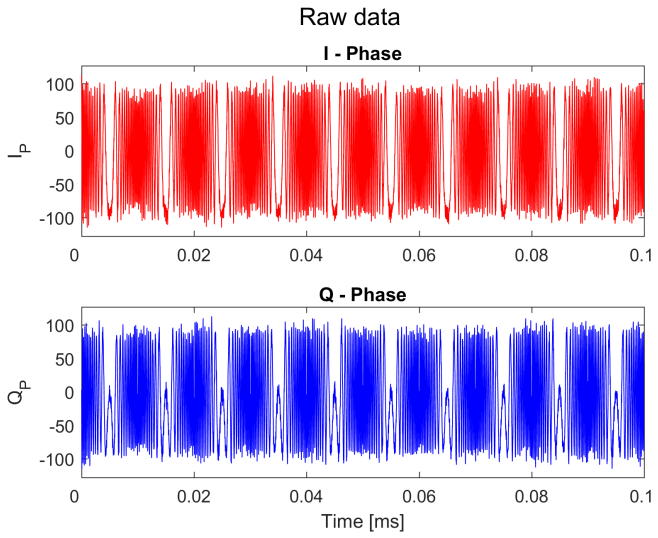
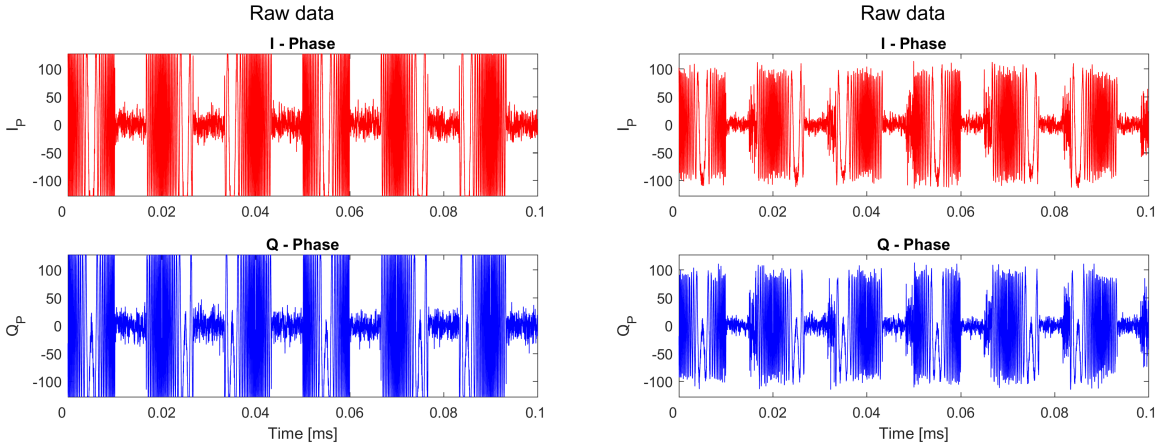


Figure 4.7: I/Q data during an interference event with avtivated AGC

In Hegarty et al. (2000) the effects of pulsed interference on the AGC are described. In the work a boundary between a fast AGC and a slow AGC is set. A fast AGC is almost an ideal AGC. It ignores the higher values at the ADC due to the pulses and provides a gain independent from the interference power. A slow AGC, as used in most receivers, reacts slowly on environment changes. If interference happens, the standard deviation of the ADC output increases and the gain is decreased and thus the useful signal is suppressed. The biggest problem appears if the interference is over. In this case the reaction to this power change is slow which causes a degradation of the useful signal at the ADC output. Figure 4.8 shows pulsed interference without activating the AGC (left) and with activated AGC (right).



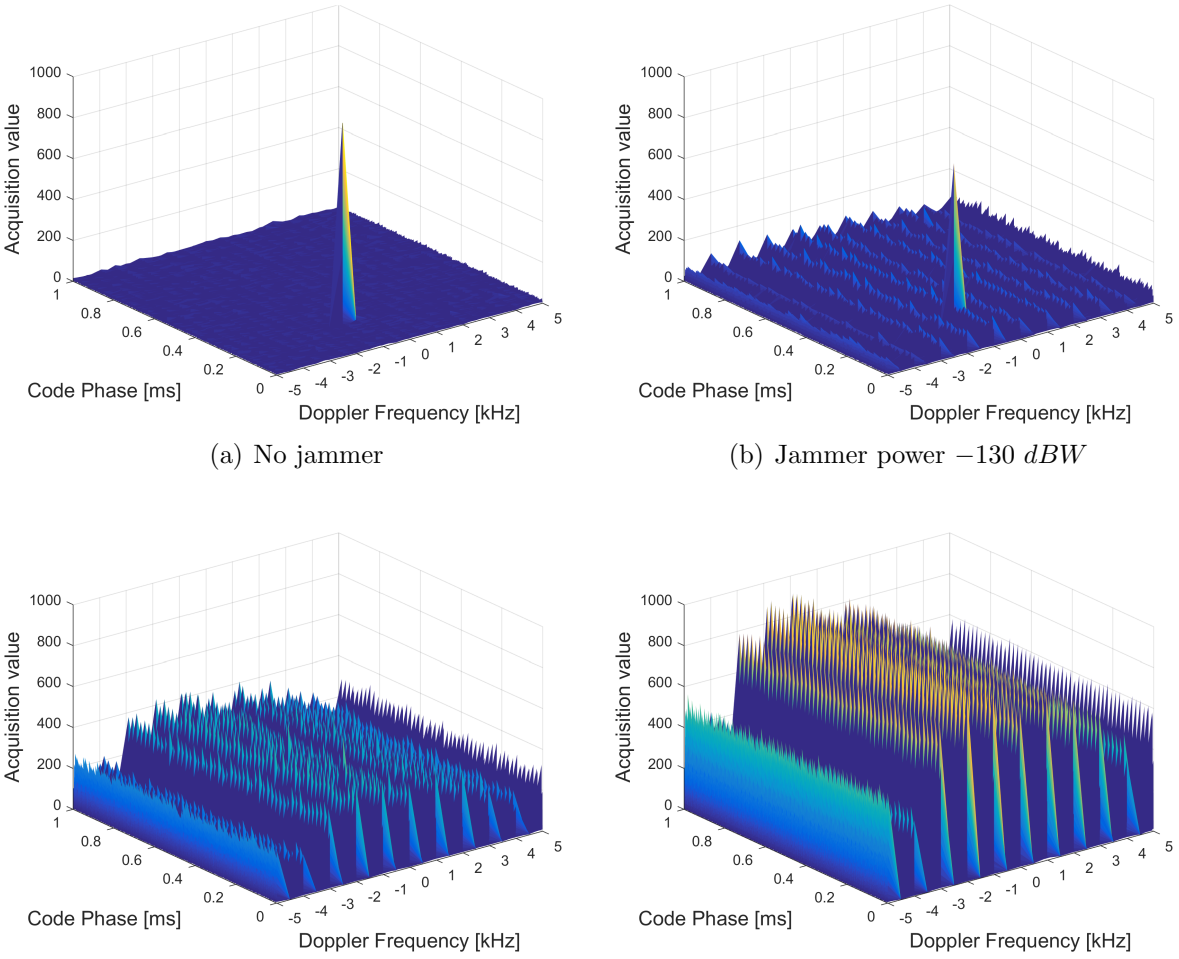
(a) Without AGC

(b) With AGC

Figure 4.8: Pulsed interference with and without using an AGC

The success of the acquisition stage is also depending on the RFFE. If the interference power is weak and the ADC and AGC are not driven to full saturation, an acquisition should still be possible [Dovis (2015)].

The acquisition results of an interference-free event were discussed in Section 3.2. If no interference is present, the acquisition peak is clearly visible and the probability of a false peak detection is therefore very low. Figure 4.9 shows the acquisition results for the GPS satellite PRN 2 during a jamming event with three different jamming signal powers (i.e. −130 dBW, −120 dBW and −110 dBW).



(a) No jammer

(b) Jammer power −130 dBW

(c) Jammer power −120 dBW

(d) Jammer power −110 dBW

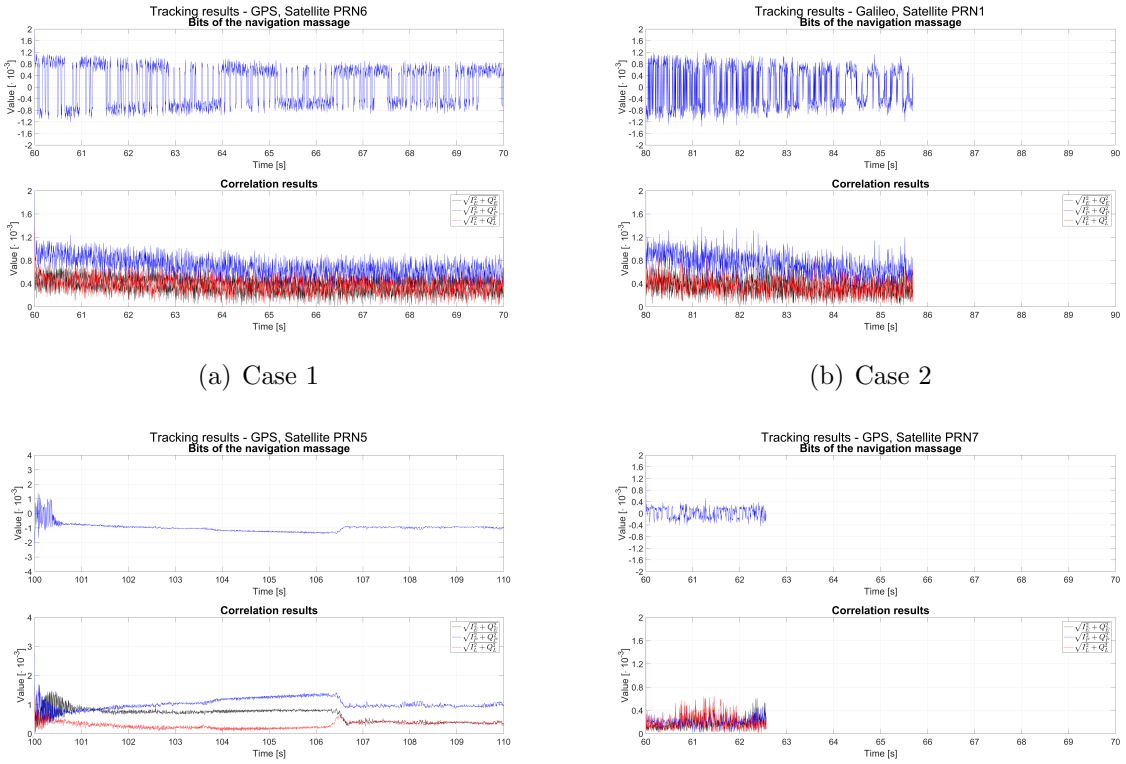
Figure 4.9: Acquisition results during a jamming event with different jamming signal powers

The interference power is an important parameter for the quality of the acquisition. For a jammer power of −130 dBW the acquisition peak is clearly visible and the acquisition provides correct results. However, the noise floor is much higher than for the interference-free event. For a jammer power of −120 dBW a peak is still visible, but it is not that significant as for the interference-free event. For a jammer power of −110 dBW the noise is increased. This means that the acquisition cannot be performed or that the results are wrong. Dovis (2015) investigated the impact of a CWI and a WBI jammer with different

jammer power on the acquisition stage. The quality of the interference was tested using the peak-to-noise floor (PNF). The greater the PNF, the better the peak is visible and the fewer noise appears within the acquisition stage. It was shown, that the WBI has a bigger impact on the acquisition stage than the CWI, because the WBI is spread over a wider spectrum, which causes more noise over the useful GNSS signal bandwidth.

The interference power is not the only parameter, which defines the quality of the acquisition, other parameter, like the interferer type, the center frequency and the bandwidth are also important. In Deshpande (2004) the impact of different interference types, interference parameters and the interference power on the acquisition stage was investigated in detail. The analysis was done with three different parameters: the noise power, the signal-to-noise ratio and the acquisition success percentage. The last describes the percentage of the satellites, for which the correct acquisition results were calculated. Six different jammer types were taken in account: CWI, FM, AM, SCW interference, pulsed interference and AWGN interferer.

The impact of interference on the tracking stage has a consequence on the quality of the pseudoranges and therefore on the PVT solution. Harmful interference increases the variance of the time-of-arrival (TOA), which causes a modification of the discriminator function and therefore false tracking results are caused [Dovis (2015)]. Figure 4.10 shows the tracking results during different interference cases. In the first and second case a SCW interferer with a power between -115 and -110 dBW, a frequency offset of 2.1 MHz, a sweep bandwidth of 1.9 MHz and a sweep duration of 23 μs was used. In the third case a FM interferer with a power between -110 and -100 dBW, a modulation frequency of 100 kHz, a frequency offset of 0 MHz and a frequency deviation of 6 MHz is presented. The last case presents a FM interferer with a power of -100 dBW, a modulation frequency of 200 kHz, a frequency offset of 2.1 MHz and a frequency deviation of 1.9 MHz.



(a) Case 1

(b) Case 2

(c) Case 3

(d) Case 4

Figure 4.10: Different tracking results during interference events

Interference normally causes a higher variance of the tracking output and a change of the correlator values. In most cases the prompt correlator value decreases and the other correlator values increase or stay on the same level. The change of the prompt correlation values causes changes in the navigation bits, which may get flip and therefore the decoding of the navigation message may become unsuccessful. In Figure 4.10a, the receiver keeps tracking. In the case of Figures 4.10b and 4.10d the tracking to the satellite is lost. In Figure 4.10c a false tracking is visible, because the I_P stays the same all the time and for most of the time the late correlator is much higher than the early correlator.

In literature, mostly the RMS code tracking error was investigated when dealing with the effect of RFI on the tracking loop. In Dovis (2015) the variance of the code tracking error for a coherent early-minus-late processing is given by

$$\sigma^2_{s,CELP} = \frac{B_L(1-0.5B_LT)\int_{-\beta/2}^{\beta/2} G_\omega(f)G_s(f)sin^2(\pi f\Delta)df}{(2\pi)^2C(\int_{-\beta/2}^{\beta/2} fG_s(f)sin(\pi f\Delta))^2}, \tag{4.4}$$

where:

- T – integration time
- B_L – one-side bandwidth of the tracking loop
- β_r- Two-sided front-end filter bandwidth
- Δ – early-late spacing [s]

- $G_s(f)$ - GNSS signal PSD, normalized to unit power over infinite bandwidth
- C – received signal carrier power
- $G_\omega(f) = N_0 + C_I G_I(f)$- Noise + interference PSD
- N_0 – flat noise PSD over the received front-end bandwidth
- C_I – interference carrier power ove ran infinite bandwidth
- $G_I(f)$ – normalized interference PSD

Figure 4.11 shows the estimated CNR for GPS satellites during a jamming event. A SCW jammer with a center frequency on the $L1$ centrer frequency and a bandwidth of 40 MHz was simulated. The power of the jammer was increased from -115 dBW to -110 dBW in the first 5 s of interference and then kept constant at -110 dBW.

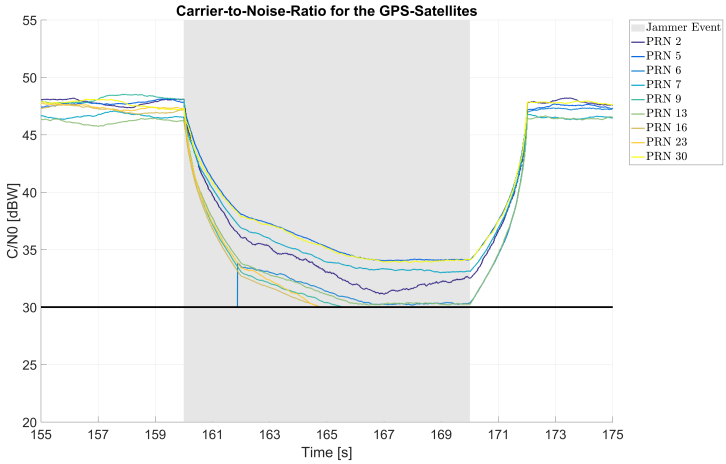
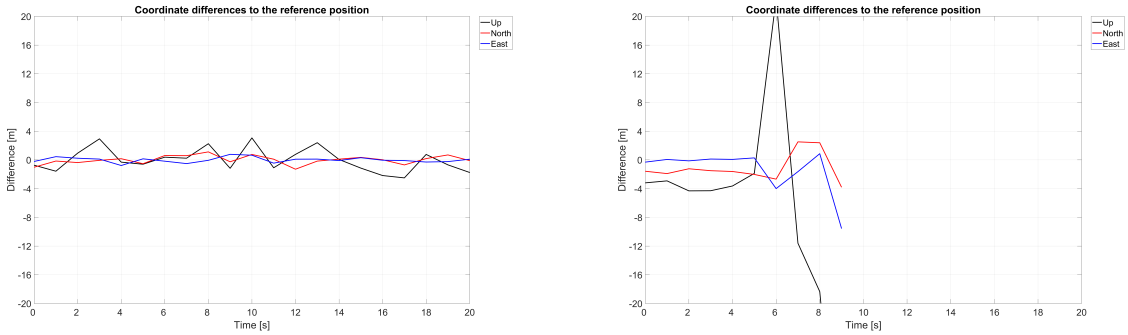


Figure 4.11: Behaviour of the CNR during an interference event

The CNR is quite constant if no jammer is activated. The estimated CNR differentiate from satellite to satellite due to different elevation angles of the satellites or the environment. During an active interferer the noise level increases and the signal level decreases. This leads to a decrease of the CNR of more than 10 dB/Hz. The value depends on the jammer power and on jammer parameters. From the figure it is seen, that the CNR of some satellites drops below 30 dB/Hz and therefore the tracking of this satellite is lost. If the jammer is deactivated, the CNR increases again.

The impact of the interferer on the tracking stage has a direct consequence on the quality of the measured pseudorange and therefore on the PVT solution. As seen in the previous paragraphs jamming causes bigger variance of correlator values, falsifies the navigation bits or may cause a loss of tracking. This affects the pseudorange measurements and the PVT solution. Figure 4.12 shows the difference of the estimated position with respect to the reference position if no interference is present (left) and during an interference event (right).



(a) Without Interference

(b) With interference

Figure 4.12: Difference between estimated position and reference position with (right) and without (left) interference

As shown the interference causes an inaccurate position solution and a total loss of position after a few seconds. In Jost et al. (2008) the effect of different interferer types on the pseudorange estimation was investigated. The pseudorange error for a WBI was about 2 m, for a NBI about 4 m and for a broadcast interferer about 12 m.

5 Jamming detection and mitigation strategies

A successful detection is the first step towards a successful mitigation. Based on the detection the interference can be classified and mitigated. Mitigation aims to reduce the impact of interference as much as possible and maintain normal receiver operation. In this section some detection and mitigation strategies are described in detail.

5.1 Interference detection strategies

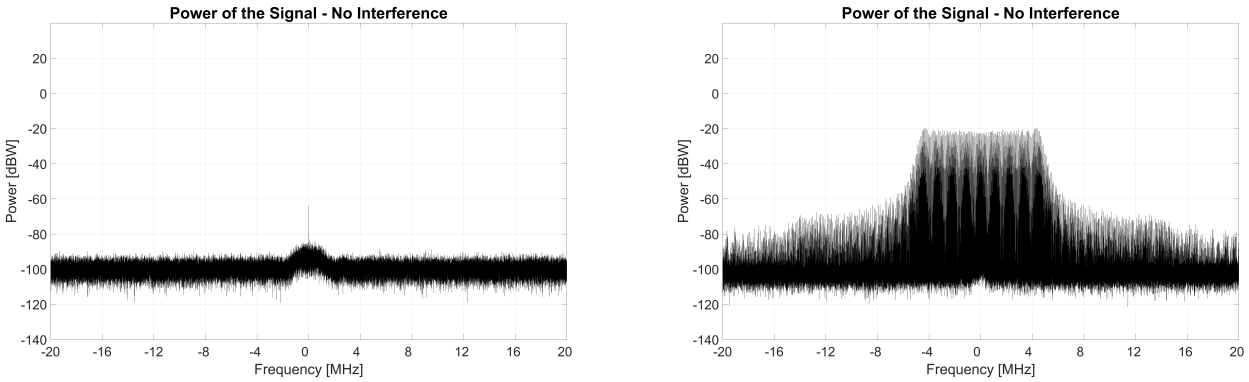
There exist different jamming detection strategies. They are based on observing different quantities at different stages of the signal processing. According to Dovis (2015) and Yang et al. (2012) they can be divided into two main groups: pre-correlation and post-correlation techniques.

The pre-correlation techniques are applied before any signal processing operation (acquisition, tracking or PVT calculation) takes place.

The first presented pre-correlation technique is the AGC monitoring. The AGC is located in the RF front-end. If no interference is present, the gain is almost constant and changes very slowly. If interference occurs, the AGC decreases its gain. The response is not linear [Dovis (2015)] and stays constant during the interference event. This means, that it is very sensitive to all types of RFI [Yang et al. (2012)]. Therefore, monitoring the behaviour of the AGC gain can be used for interference detection. If the gain drops below a certain threshold, interference is detected. This technique was shown to be successful for low-cost front-ends by Dovis (2015).

Another method is the monitoring of the spectral behaviour of the incoming signal. The main principle is to compare the PSD of the received signal with a spectral mask [Dovis (2015)]. In this case the incoming signal is transformed from the time domain into the frequency domain. The transformation is done using a Fourier-transformation. Commonly the fast Fourier transformation (FFT) or a periodigram is used for transformation. More details on periodigrams can be found in [Dovis (2015)]. The FFT is described in Burrus et al. (2012) and Pany (2010). The international civil aviation organization (ICAO) sets different thresholds for interference detection. For detecting narrowband interference a threshold of -150.5 dBW has to be exceeded by a single frequency [TeleConsult Austria GmbH (2015)]. Furthermore, a threshold for detection of wideband interference exists. Figure 5.1 shows the PSD for an interference free-event (left) and a PSD during a wideband-interference

attack (right). A SCW interferer with a bandwidth of 10 MHz at the L1 center frequency was simulated in this case.



(a) Interference-free (b) Interference

Figure 5.1: The Power spectral density in case of an interference-free event and in case of WBI

This method is quite effective, but requires a large computational effort. Very important is the right choice of the parameters, needed for the FFT or for the periodigram computation. A higher number of FFT-points increases the frequency resolution, but also increases the computation complexity. Other pre-correlation techniques, described in literature, are time domain statistical analysis or measurements at the antenna.

Post-correlation techniques are performed after the acquisition stage. Some post-correlation techniques, described in literature, are CNR monitoring, monitoring of the tracking loop accuracies, pseudorange monitoring, PVT monitoring, adaptive notch filter (ANF), phase distortions or running digital sum (RDS). An important advantage of post-correlation techniques compared to the pre-correlation techniques is, that they do not need hardware modifications [Yang et al. (2012)].

The CNR is one of the most important parameters for describing the signal and tracking quality. Interference causes a degradation of the CNR as described in Section 4.4. The biggest advantage of this technique is that the CNR is computed and outputted by most receivers. According to Dovis (2015) and Kemetinger et al. (2013) the drop of the CNR may have multiple reasons as presence of non-line-of-sight (NLOS) signals, low elevation of the satellite, a multipath fading effect, a large Doppler rate not perfectly tracked by the carrier tracking loop or presence of interference. Because different effects can cause a drop of the CNR, detection via CNR monitoring should not be the only interference detection strategy performed.

In the tracking stage the correlator values can be used to compute the CNR estimator. A possible CNR estimator was presented in Chapter 3. On the other hand a theoretical CNR can be computed based on

$$\left(\frac{C}{N_0}\right)_{eff} = \frac{CL_S}{N_0 L_n + I_{total}}. \tag{5.1}$$

The parameter C represents the power of desired signal, L_S is the processing loss in the desired signal, N_0 denotes the noise PSD and L_n the processing loss of the noise. I_{total} is the total level of interference. It consists of all interference sources: intra- and inter-system, external interference, jamming as described in Chapter 4 and reads

$$I_{total} = I_{intra} + I_{inter} + I_{extern} + \cdots + I_{jammer}. \tag{5.2}$$

From Equations 5.1 and 5.2 it follows, that the presence of more interfering sources increases the total level of interference and decreases the effective CNR.

If calculating the effective CNR for jamming detection only the intra-system interference needs to be considered. The power level is calculated by

$$I_{intra} = \sum_{k=1}^{N} C_k L_k \kappa_k, \tag{5.3}$$

where C_k is the received power, L_k is the implementation loss and κ_k is the spectral separation coefficient (SSC).

The SSC describes the overlapping of the spectra of two signals [Wasle et al. (2009)] (e.g. the received GNSS signal and the interfering signal). It indicates the degree of interference [Bartl (2014)]. The SSC can be determined by

$$\kappa_k = \int_{-B/2}^{B/2} G_k(f) G_s(f) df, \tag{5.4}$$

where the parameter B describes the bandwidth, G_k is the PSD of the received signal, including the GNSS signal and different kinds of unintentional and intentional interference, and G_s is the PSD of the desired signal.

For an interference detection via CNR monitoring the theoretical CNR is calculated first. For the calculation of the SSC the PSD has to be known. The processing loss depends on the distance between the satellite and the receiver. Afterwards, the actual CNR is compared to the theoretical CNR. If a certain threshold is exceeded, interference is detected for this satellite. If the CNR of one satellite drops for several dB, this could be due to obstructions in the signal path due to multipath or shadowing [Kemetinger et al. (2013)]. If the CNR drops for several satellites at the same time occur, this indicates interference. Therefore, not only a threshold has to be set, but also the percentage of satellites, whose CNR has to drop under the threshold has to be considered.

Another detection strategy is monitoring the pseudoranges between the satellites and the receiver. Since the accuracy of the correlator output during the tracking stage is directly related to the accuracy of the pseudorange measurements [Dovis (2015)]. Interference causes a degradation of the tracking results and thus, inaccurate or wrong pseudorange measurements. The monitoring of the pseudorange seems to be a good method, but it has to be mentioned, that a change in the pseudorange values may be caused by multipath or ionospheric effects as well.

The influence of jamming on the pseudorange measurements has a direct influence on the PVT solution. Jamming causes a degradation of the PVT solution accuracy and might lead to no solution at all. If the difference between the calculated position and the reference position is larger than a certain threshold, interference is detected. In TeleConsult Austria GmbH (2015) the threshold is calculated using the geometric dilution of precision (GDOP), which can be easily calculated from the elements of the covariance matrix in the least-square adjustment. But interference is not the only influence on the PVT accuracy. Other effects as NLOS, multipath, unexpected dynamics, poor satellite geometry etc. [Dovis (2015)] might degrade the PVT solution as well. Therefore, PVT monitoring should not be the only metric for detection, especially in an environment, where interference is not the only possible disturbing factor.

5.2 Jamming mitigation strategies

The goal of mitigation strategies is to suppress the interfering signal and preserve as much useful signal as possible. Some strategies are defined in the frequency domain and some of them are defined in the time domain. In this chapter different mitigation algorithms are described. First the notch filter (NF) and the adaptive notch filter (ANF) and two realizations of the ANF are presented. They are designed for mitigating wideband and narrowband interference in the frequency domain. Next, the frequency domain adaptive filtering (FDAF) and the pulse blanking (PB), which mitigate pulsed interference, are presented. Note that PB is the only presented mitigation strategy that works in the time domain of the signal.

The notch filter (NF) is a filter used for mitigation of the interfering signal in the frequency domain. A NF is usually designed as a filter with a big "passband frequency response and a very narrow portion of a rejection spectrum" [Dovis (2015)]. The frequency response of a NF is shown in Figure 5.2.

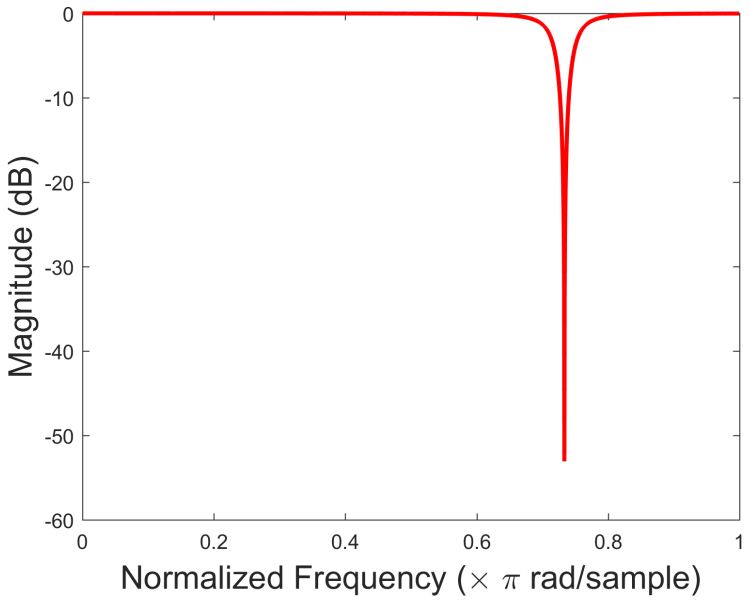


Figure 5.2: The frequency response of a NF

The NF tries to preserve as much as possible of the useful GNSS signal and attenuates the interfering signal. In literature different implementations of the NF are available. Most common implementations of notch filters areinfinite impulse response (IIR) digital filters [Dovis (2015)]. A general expression of a two-pole IIR NF for CWI mitigation is given by

$$H(z) = \frac{1 - 2\,\mathrm{Re}\{z_0\}z^{-1} + \mid z_0 \mid^2 z^{-2}}{1 - 2k_\alpha\,\mathrm{Re}\{z_0\}z^{-1} + k_\alpha^2 \mid z_0 \mid^2 z^{-1}}, \tag{5.5}$$

where z_0 denotes the complex zero, which is placed in on the interfering frequency [Borio et al. (2008)]. The parameter k_α is the pole contraction factor, which determines the width of the notch filter. The closer the contraction factor is to one, the narrower is the NF. "In the presence of multiple tones, a multipole notch filter, based on the use of several two-pole notch filters in cascade, can be used" [Dovis (2015)]. The notch filter is a good method to mitigate interference if the interference carrier frequency is known and constant. But in most cases it is an unknown parameter and changes its value over time. In this case the adaptive notch filter (ANF) has to be used.

"Adaptive notch filtering aims to estimate the unknown frequencies of periodic components buried in noise, and/or retrieve such periodic components" [Regalia (2010)]. For estimating the (changing) frequencies the adaptive unit is used. The basic structure for the two pole ANF coupled with an adaptive unit is presented in Figure 5.3.

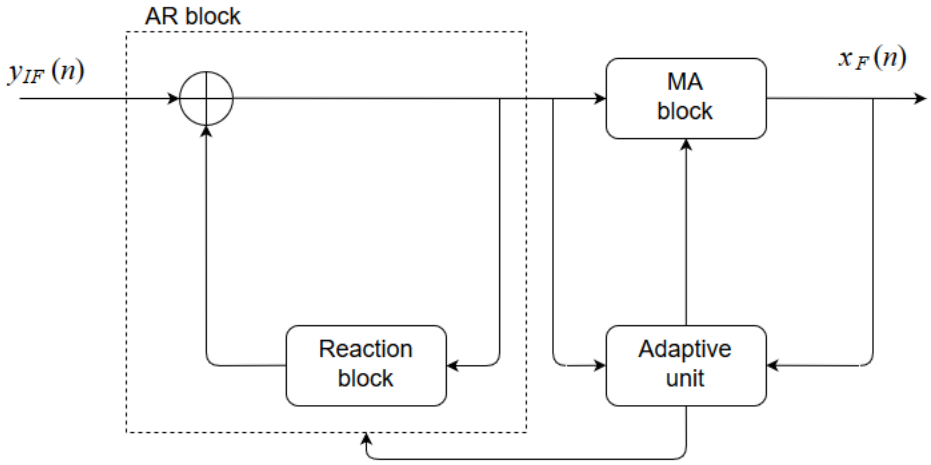


Figure 5.3: The structure of an ANF [c.f. Dovis (2015)]

In Figure 5.3 $y_{IF}(n)$ represents the input (i.e. a signal sample) and $x_F(n)$ describes the filtered signal output. The numerator of the filter transfer function is defined as a moving average (MA) block, the denominator represents the autoregressive (AR) block [Dovis (2015)]. The jammer frequency detection algorithm is based on the removal of the constraint on the location of the filter zeros in the complex plane. Their amplitude is adjusted by the adaptive unit [Dovis (2015)]. For this work the real and complex adaptive filter solutions by Regalia (2010) and Regalia (1991) has been used.

The complex ANF solution is introduced for complex signals. The first order complex all-pass transfer function $C(z)$ for this ANF is given by

$$C(z) = \frac{e^{j\theta} \cdot z^{-1} - \alpha}{1 - \alpha e^{j\theta} z^{-1}}, \tag{5.6}$$

where α is a parameter depending on the attenuation bandwidth of the ANF. The filter transfer function $G(z)$ may be defined as

$$G(z) = \frac{1}{2}[1 - C(z)]. \tag{5.7}$$

In Equation 5.7 the all-pass transfer function and the filter transfer function are depending on $z = e^{j\omega}$. This means that the zeros (or so called "notchs") of the transfer function (ω) are defined at θ. Between $\pm\omega$ a 3 dB bandwidth B is defined. The bandwidth is expressed as

$$B = \frac{\pi}{2} - 2tan^{-1}(\alpha). \tag{5.8}$$

The attenuation bandwidth B is the first of two input parameters for this ANF. It defines the bandwidth in the frequency domain, that is filtered by the ANF. If the bandwidth is chosen too small, only a part of the signal is attenuated. If the bandwidth is chosen too high, useful signal may be suppressed as well. More information about the choice of the

attenuation bandwidth can be found in the next chapters. Once the bandwidth is selected, the parameter α is known. The flow graph of the complex ANF is shown in Figure 5.4.

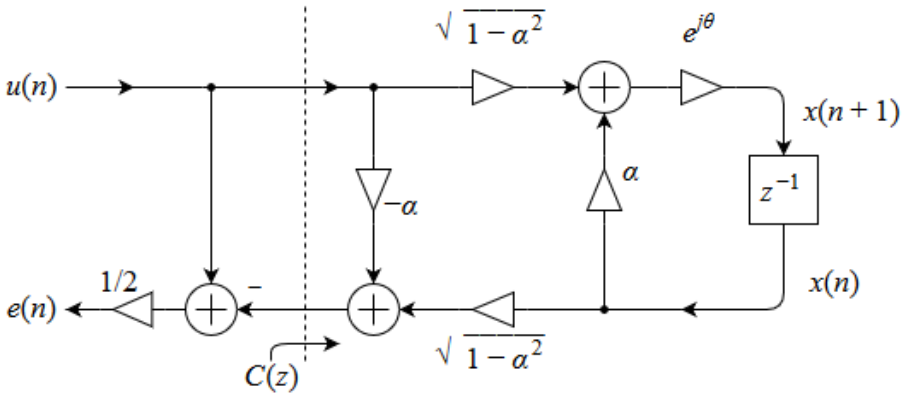


Figure 5.4: Structure of the complex ANF [c.f. Regalia (2010)]

In Figure 5.4 $u(n)$ describes the input signal sample and $e(n)$ describes the output of the filter. In output the jamming signal is suppressed. The connection between the input $u(n)$ and the output $e(n)$ is described by

$$e(n) = -\frac{\sqrt{1-\alpha^2}}{2}x(n) + \frac{1+\alpha}{2}u(n) \text{ and} \tag{5.9}$$

$$x(n+1) = e^{j\theta_1(n)}\alpha x(n) + e^{j\theta_1(n)}\sqrt{1-\alpha^2}u(n), \tag{5.10}$$

where $x(n)$ represents the filtered regressor. For determining the output $e(n)$ the filtered regressor $x(n)$ for the same sample is needed. That means a start value is needed for the calculation. The parameter $e^{j\theta(n)}$ can be rewritten as $e^{j\theta_1(n)} = cos(\theta_1(n)) + j \cdot sin(\theta_1(n))$. The adaptive part of the filter is defined through adaptation of the notch frequency parameter θ_1, which describes the frequency of the interferer in the range between $-\pi$ and π radians. The adaptation algorithm for θ_1 is defined as

$$\theta_1(n+1) = \theta_1(n) + \mu \cdot Im[e(n) \cdot x^*(n)]. \tag{5.11}$$

$x^*(n)$ is the complex conjugate of the filtered regressor. The imaginary part of Equation 5.11 is linked to the change of the notch frequency parameter $\frac{d\theta_1}{dt}$ with respect to the time. For the calculation of $\theta_1(n+1)$ the former value $\theta_1(n)$ is needed. The parameter μ describes the step size of the filter and it is calculated recursively by

$$\mu(n) = \frac{1}{\frac{\lambda}{\mu(n-1)} \cdot \mid x(n) \mid^2}. \tag{5.12}$$

The step size describes the adaptation of the algorithm. The value is always greater than 0. A small μ corresponds to a slow adaptation [Regalia (2010)]. The step size depends on the

second input parameter of the complex ANF - the forgetting factor λ. The value has to be chosen between 0 and 1. It determines how fast the filter can adapt frequency changes and how stable the notch frequency parameter is estimated over time. A forgetting factor of 0 means, that the filter uses no former information of the notch frequency. A forgetting factor of 1 means, that the filter uses only the forward information. A small forgetting factor causes a smaller stability of the notch frequency and a faster reaction on frequency changes. The choice of the forgetting factor will be discussed in the next chapter.

In Regalia (2010) the complex ANF was tested on frequency-hop signal with positive and negative values and for a quadratic polynomial. The complex ANF clearly distinguished between positive and negative frequencies and shows good tracking performances in both cases.

In Regalia (1991) the ANF for real signal samples is presented. The real ANF $G(z)$ is presented with the transfer function

$$G(z) = \frac{1}{2}[1 + C(z)], \tag{5.13}$$

where $C(z)$ represents an all-pass function. A suitable choice of all-pass structure is the planar lattice filter with two tunable planar rotations (θ_1 and θ_2), which provides stability to $G(z)$ and well numerical behaviour in time-varying environments [Regalia (1991)]. The two rotation angles are given by

$$\theta_1 = \omega - \frac{\pi}{2} \text{ and} \tag{5.14}$$

$$\theta_2 = arcsin\left(\frac{1 - tan(B/2)}{1 + tan(B/2)}\right), \tag{5.15}$$

depending on the notch frequency ω and on the 3 dB attenuation bandwidth B. The rotation angle θ_1 is the notch frequency parameter, whereas the rotation angle θ_2 defines the bandwidth parameter. The flow graph of the real ANF is shown in Figure 5.5.

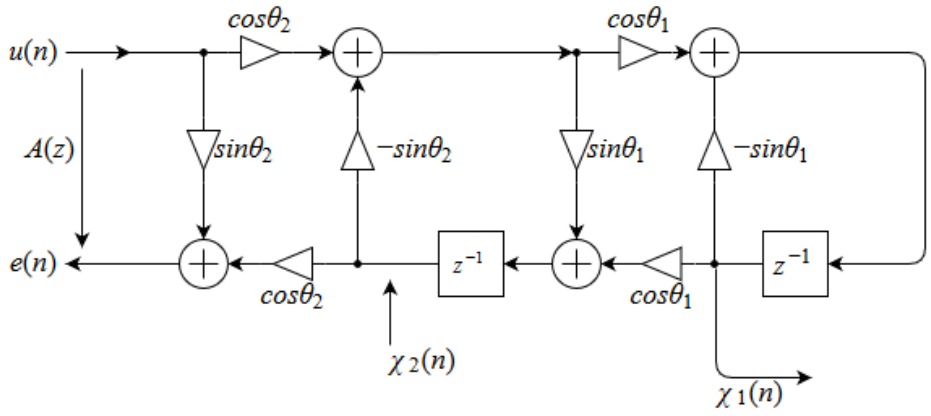


Figure 5.5: Structure of the real ANF [c.f. Regalia (1991)]

For the real ANF two filtered regressors $\chi_1(n)$ and $\chi_2(n)$ exist and both rotation angles are needed for their estimation. They can be written as

$$\chi_1(n) = \frac{z^{-1}cos(\theta_2)cos(\theta_1)}{1 + sin(\theta_1)[1 + sin(\theta_2)]z^{-1} + sin(\theta_2)z^{-2}} \text{ and} \tag{5.16}$$

$$\chi_2(n) = [-\chi_2(n)sin(\theta_2) + u(n)cos(\theta_2] \cdot sin(\theta_1) + cos(\theta_1)\chi_1(n). \tag{5.17}$$

In Equations 5.16 and 5.17 the operator z^{-1} represents the unit delay operator. The filter output is given as

$$e(n) = \frac{1}{2}[cos(\theta_2) \cdot \chi_2(n) + u(n) \cdot (sin(\theta_2 + 1)]. \tag{5.18}$$

The adaptive part of the filter is defined through adaptation of the notch frequency parameter θ_1, which describes the frequency of the interferer in range between $-\pi$ and π radians. For tuning the notch frequency parameter θ_1 the following algorithm is proposed by Regalia (1991):

$$\theta_1(n + 1) = \theta_1(n) - \mu(n)e(n)\chi_1(n). \tag{5.19}$$

The parameter $\mu(n)$ is the step size that describes the adaptation of the algorithm. It can be calculated using Equation 5.11. For some parameters start values are needed: the step size μ, the filtered regressors χ_1 and χ_2 and for the notch frequency parameter θ_1. For the real ANF the same input parameters are needed as for the complex ANF - the attenuation bandwidth B and the forgetting factor λ. The properties of the input parameters are the same as for the complex ANF.

The frequency-domain adaptive filtering (FDAF) is a frequency domain technique suitable for mitigating pulsed interference. This technique is possible because of the narrow frequency representation of pulsed signal (e.g. 1 MHz) relating to GNSS (e.g. 20 MHz) [Raimondi et al. (2006)]. This technique is applied on the signal after the ADC.

First a certain number of samples (N) of the incoming signal are taken and transformed into the frequency domain. From the real and imaginary parts of the FFT the amplitude spectrum is calculated. If no interference is present, the spectrum should be flat (white) because the GNSS signal is below the noise floor. If a pulse with a certain frequency is present, its amplitude is higher. Every amplitude is compared to a certain threshold. If an amplitude exceeds this threshold, this amplitude is set to zero. This mean, that the frequency does not appear in the signal any more. Finally, an inverse FFT (IFFT) is performed on the manipulated data to transform the signal back into the time domain. A graphical representation of the FDAF is shown in Figure 5.6.

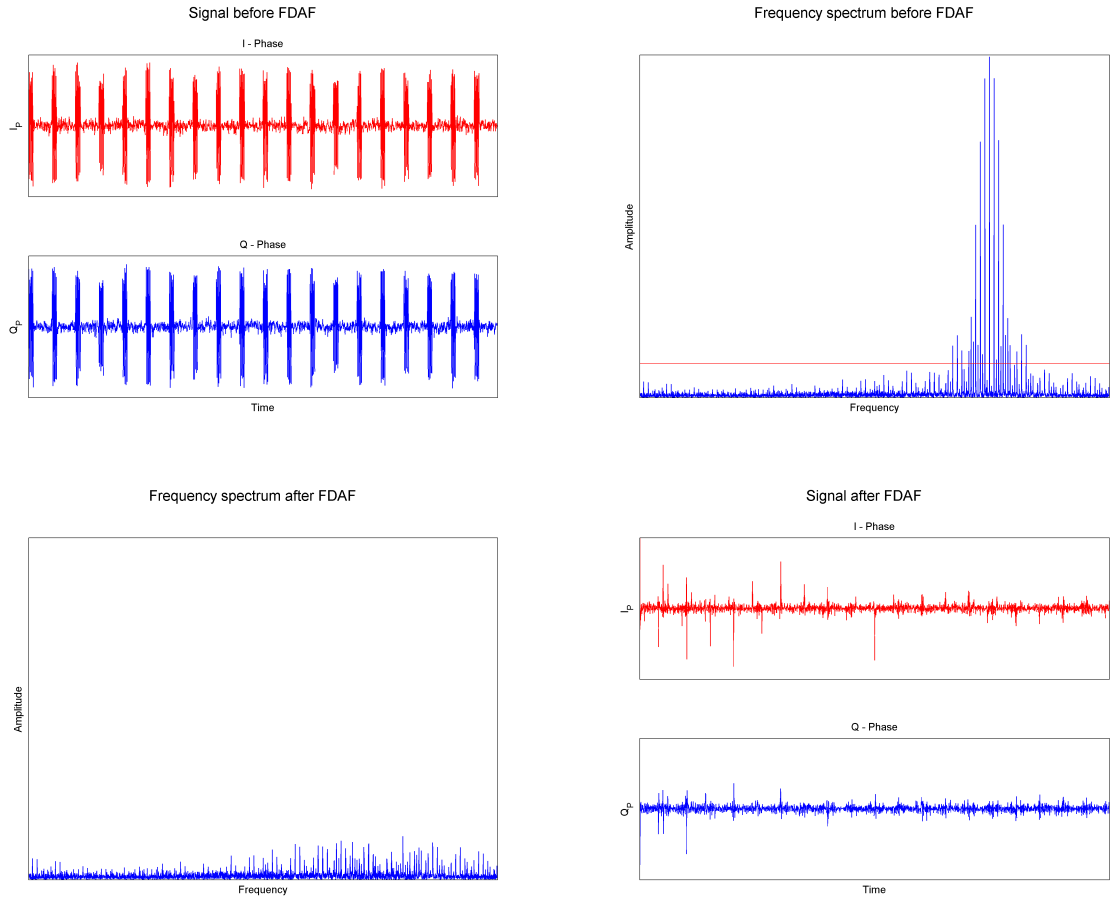


Figure 5.6: Basic principle of FDAF

The effectiveness of this algorithm is strongly related to the effectiveness of the FFT [Dovis (2015)]. According to Raimondi et al. (2006) and Dovis (2015) some remarks have to be considered. A better frequency resolution is achieved using a higher number of FFT points. But a higher number of FFT points also increases the computation effort. If the frequency resolution is too high, the detection of frequency components may not be successful. Furthermore, different window functions can be used for weighting samples, improving the FFT performance and reducing the bias. The number of points in the FFT window should guarantee at least one point in the pulse bandwidth. According to Dovis (2015) the FDAF performance for pulse mitigation is better than the performance of pulse blanking.

As described above, frequency domain techniques can be used for mitigating most continuous interference types. The NF and ANF are used to mitigate CWI, WBI and NBI interference. But they are inappropriate for mitigating pulsed interference, "because the presence of an interfering signal for a limited time is often lost in the phase of the spectral estimation" [Dovis (2015)]. This causes a degradation of useful signal. On the other side time domain techniques exist. The time domain is suitable to detect interference, but for most interference types it is not suitable for mitigating. An exception is pulsed interference,

which can be mitigated using the pulse blanking (PB) algorithm.

The pulse blanking algorithm is a low-cost and low-complexity algorithm, which was first proposed using analog technology and later fully digital [Dovis (2015)]. It is a pre-correlation technique, which means, it has to be applied on the data after the ADC and before the AGC and acquisition. Pulse blanking is zeroing of every sample, containing the interference signal. It is a perfect technique in the presence of ADC saturation. In Borio and Cano (2012) two different situations of pulse blanking are presented:

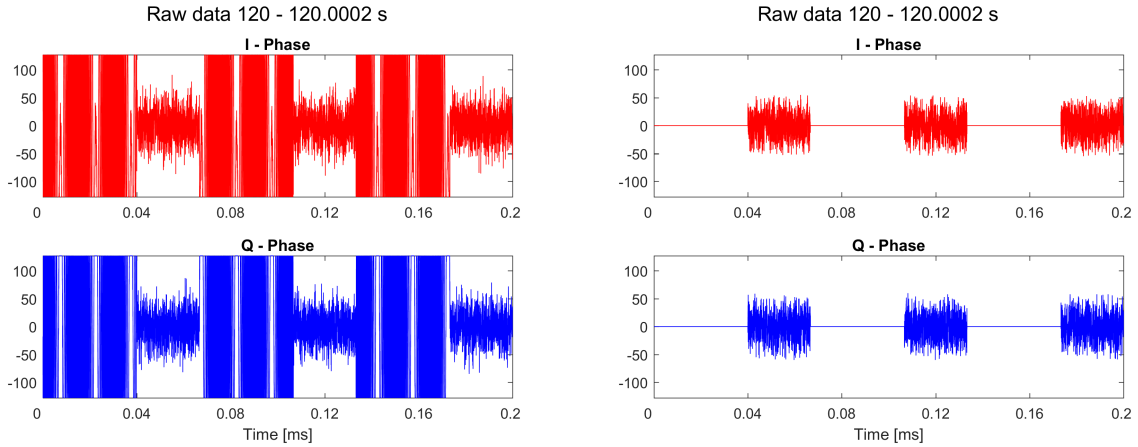
- Ideal blanking: The receiver continuously tracks the signal and estimated and predicts the pulse positions. The pulse positions are assumed to be known and are getting blanked.
- Thresholding: The pulse is determined by comparing the input samples with a certain threshold. This situation is commonly implemented in receivers.

The pulse detection relies on the fact, that the pulses are short and have a higher amplitude than the GNSS signal only. The pulse detection may be done using different techniques: analog power measurements, analysing the histograms of the ADC output levels or by instantaneous power estimates [Hegarty et al. (2000)]. From the input samples ($r_C(t)$) the received power can be calculated and compared to a decision threshold. According to Wesson et al. (2018) the received signal power is calculated using

$$P_k = 10 \cdot \log\left(\frac{1}{T}\int_{t_{k-1}}^{t_k} \mid r_C(t) \mid^2 dt\right). \tag{5.20}$$

The calculation can be performed for a single sample or for a interval $[t_{k-1}, t_k]$. The data can be additionally filtered.

Furthermore, the setting of a threshold is important. The threshold has to be chosen low enough to detect (weak) pulsed interference signals, but it has to be chosen high enough to not zeroise too much of the useful signal. Therefore, a plausible threshold for suppression has to be found. Raimondi et al. (2006) investigated the choice of a decision threshold for pulse blanking. The smallest signal degradation (-8.1 dB) happened at a decision threshold of -117.1 dBW. The pulse blanking method is shown in Figure 5.7 by showing the impact on the I/Q data.



(a) Before PB (b) After PB

Figure 5.7: I/Q samples before and after pulse blanking

The pulse blanking is not the perfect technique because during the pulse zeroing not only the pulse is suppressed, but also the useful GNSS signal. Many pulsed signals have a Gaussian shape, which means, that the pulse borders, which have a smaller power and amplitude, are not suppressed at all [Dovis (2015)]. But it can be considered as near-optimal if all pulses are saturated [Hegarty et al. (2000)].

Pulse blanking has to be done using a multi-bit ADC. If a single bit ADC is used, all samples have the same magnitude and it is not possible to distinguish between interference and useful signal. Furthermore, the pulse blanking should happen before the AGC. The AGC equals the signal samples and thus no pulse detection by amplitude discrimination is possible after that. If it is possible, the AGC can be tuned to map the signal level of a limited number of bits (2 or 3). The higher bits stay for pulse detection [Dovis (2015)]. The pulse blanking is widely-used in aviation scenarios, where pulsed signals are transmitted from ground beacons.

6 Implementation

In the previous chapters the problematic of interference, its impact on the different stages of signal processing and strategies for jamming detection and its mitigation strategies have been described. The mitigation strategies were applied on different data sets, which had to be recorded or simulated. The evaluation of the mitigation strategies is based on the tracking results, on the CNR and on the PVT solution. This means, that the GNSS signals had to be processed in a software-defined receiver or that the mitigation algorithms had to be implemented within a software-define receiver. This chapter deals with the implementation of selected mitigation strategies. The first section describes the software, which was used for simulating GNSS interference and evaluation of the mitigation strategies. The implemented algorithms are presented in the second part of this chapter.

6.1 Used software

In this section two different implementations of a software-defined receiver are presented. Afterwards, a software for signal simulation is described in detail.

Matlab implementation of a software-defined receiver

The Matlab-implementation of the software-defined receiver (SDR) is based on the book and source code of Borre et al. (2007). The SDR is an open-architecture receiver solution and presents an ideal platform for learning the first steps in the signal processing. It is a single-frequency receiver and capable of processing the GPS L1 C/A signals. The source code can be extended with arbitrary functions. This enables the testing of different new algorithms or investigations on different signal processing stages. The flow chart of the SDR is shown in Figure 6.1.

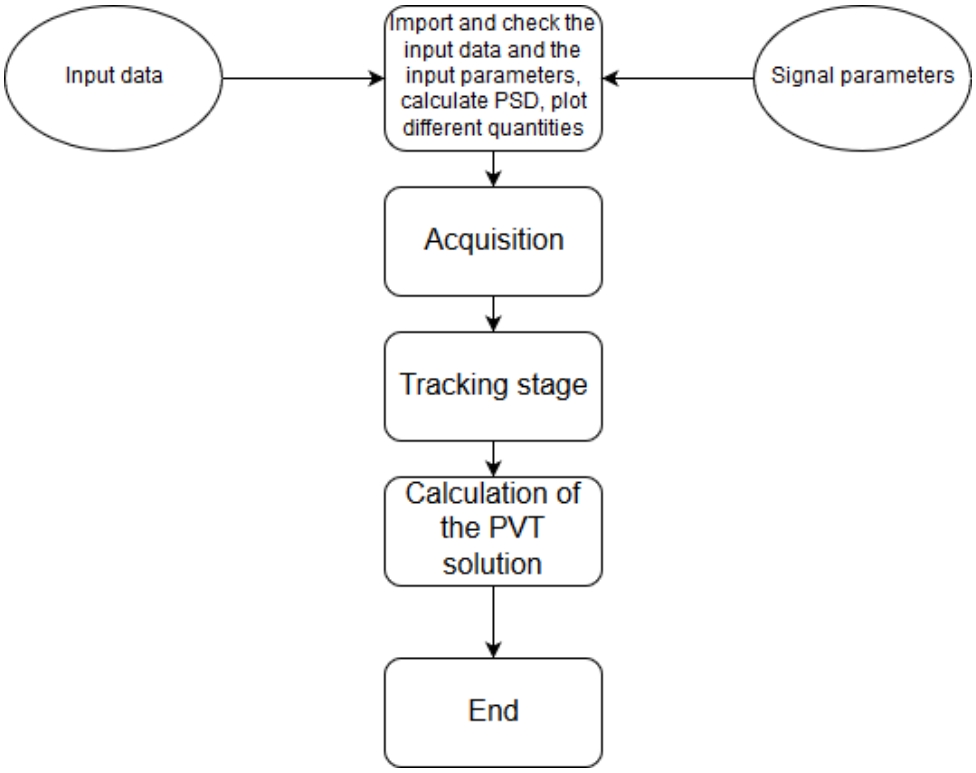


Figure 6.1: Flow chart of the GNSS receiver, implemented by Borre et al. (2007)

The software is composed of three main components: the acquisition, the code/carrier tracking and the calculation of the navigation solution. In the acquisition stage the visible satellites and their code phase and the Doppler frequency using a peak searching are estimated. The tracking stage performs the DLL and the PLL of the data with an integration time of 1 ms. The calculation is performed sequentially for every channel. After the tracking of every satellite, the navigation bits are recovered and decoded, the pseudoranges are calculated and the PVT solution is determined and plotted.

Gaims software

Gaims is a software developed by TeleConsult Austria, which was implemented for the project GNSS airport interference monitoring system (GAIMS). The goal of the project, which was funded by the Austrian ministry for transport, innovation and technology (BMVIT) was to develop a software-defined receiver, which processes the multi-frequency and multi-system GNSS signals and which detects and classifies interfering signal (i.e. jamming and spoofing). The project and its goal as well as the detection implementations are described in Bartl (2014). Figure 6.2 shows the graphical user interface of the software.

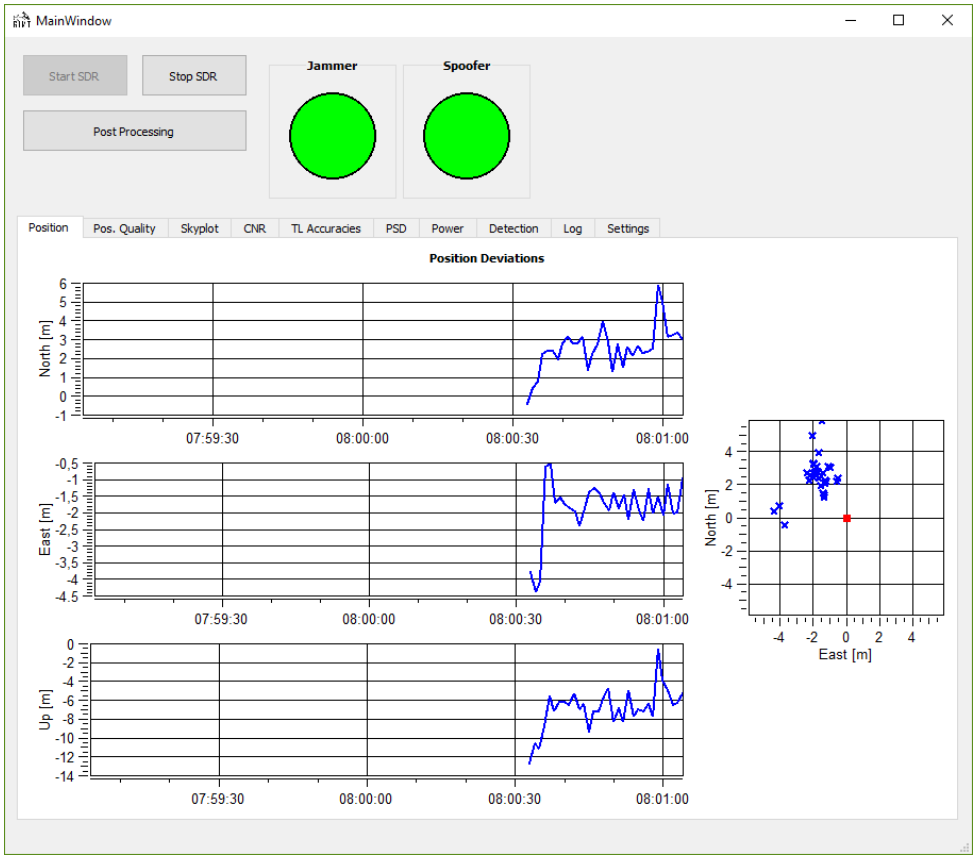


Figure 6.2: Graphical user interface of the software GaimsGUI

If the signal processing is started, different quantities like the position, position accuracy, CNR, tracking loop (TL) accuracies, PSD and the number of interference detection parameters, are shown. For jamming detection seven different algorithms are implemented: the detection via position accuracy, CNR behaviour, DLL and PLL accuracy, received signal power and the PSD in the narrow- and wideband. The flow chart in Figure 6.3 shows the principle of the jamming detection and mitigation strategies implemented in the software Gaims.

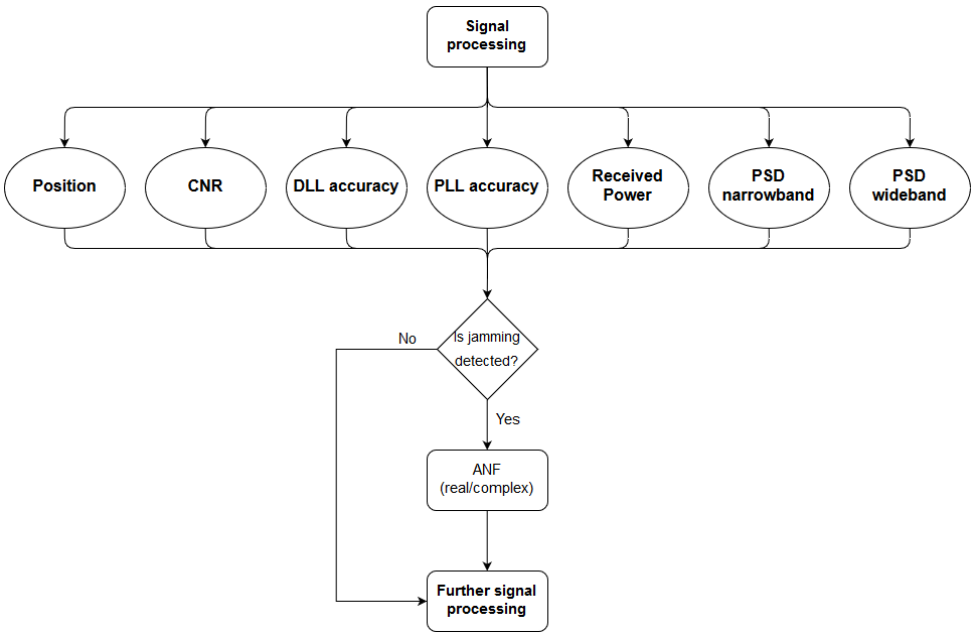


Figure 6.3: Flow chart of the jamming mitigation strategies, implemented in the software Gaims

If jamming is detected by one of the algorithms, a warning is raised and if two or more algorithms detect a jammer an alarm is raised. Details can be found in Bartl (2014).

Software GIPSIE®

The GNSS multisystem performance simulation environment (GIPSIE®), developed by TeleConsult Austria, is capable of simulating GNSS intermediate frequency (IF) signals. It supports all GNSS, regional systems and augmentation systems, which are currently available for satellite-based navigation. It enables the simulation of IF signals of multiple systems, of more different signal bands, different raw measurements, the simulation of path delays, caused by the troposphere or ionosphere, the simulation of jamming, spoofing and multipath signals. Furthermore, different RF front-ends with arbitrary parameters can be simulated. There exists a graphical user interface (GUI) version and a console version of the software. The GUI is shown in Figure 6.4.

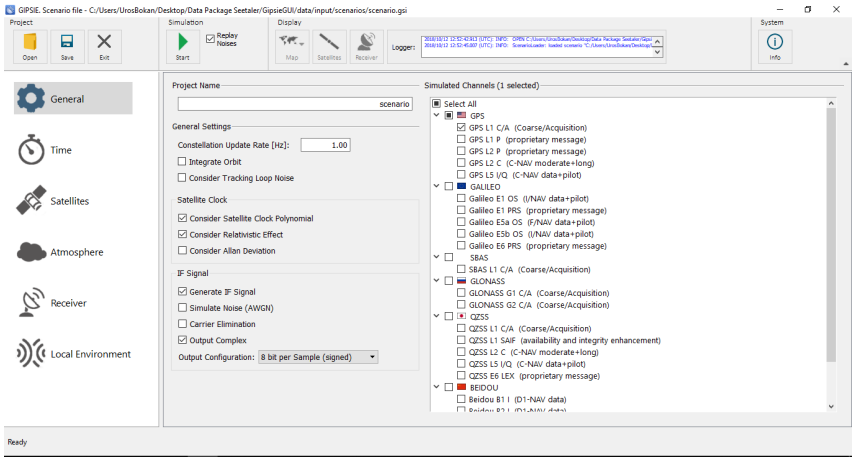


Figure 6.4: Graphical user interface of GUI version of GIPSIE

The user can define the simulation parameters in the user interface or in an arbitrary scenario-file. The GIPSIE® software is implemented in C++. It was used in this master thesis for simulating different jamming signals on top of GPS L1 C/A and Galileo E1B signals.

6.2 Implementation of the adaptive notch filter in software

An important tool for evaluating the satellite signal is the short-time-Fourier transform (STFT). The ANF was implemented in the Matlab-version of the SDR and in the existing software Gaims.

Short-time-Fourier transformation

The short-time-Fourier-transform (STFT) is a simple and effective tool for computing time frequency representations [Khan et al. (2011)]. Mathematically the signal energy for a time t and for a frequency ω is obtained by correlating a signal $s(\tau)$ with a modulated window function (h) and can be written as

$$STFT\{s(\tau)\}(t,\omega) = \int_{-\infty}^{\infty} s(\tau) \cdot h(\tau - t) \cdot e^{-j\omega\tau} d\tau. \tag{6.1}$$

For the computation of the STFT with a discrete signal a short section of a signal is chosen. Afterwards the section is multiplied with a window function and then a transformation into the frequency domain is performed via the DFT discrete- Fourier transformation (DFT) or FFT. The resulting amplitude is squared to determine the PSD of the signal. This procedure is repeated with new data. The shift between two consecutive data blocks is called overlap period.

Window functions are used for non-periodic signals as GNSS signals. The usage of a window reduces the leakage effect when dealing with non-periodic signals. But it cannot eliminate the leakage effect. Ideally, the window should be an impulse in the time frequency plane [Khan et al. (2011)]. In reality different window functions are used. According to [Bartl (2014)] the Hann window is an appropriate choice for the filter function because it causes a small error.

Implementation in Matlab R2016b

In a first step a Matlab implementation was made for analysing the signals and the effects of the ANF. The signal was analyzed considering raw data or calculating a STFT. The ANF implementation was done using the Equations 5.6 to 5.12 for the complex solution and the Equations 5.13 to 5.19 for the real ANF. To evaluate the ANF the filtered data, the spectrogram of the filtered data and the frequency response of the ANF are compared.

The effect of the ANF on the signal processing was investigated using SDR. The software and its structure were presented in Section 6.1. The ANF implementation was done within the tracking stage. The flow chart of the implementation is shown in Figure 6.5.

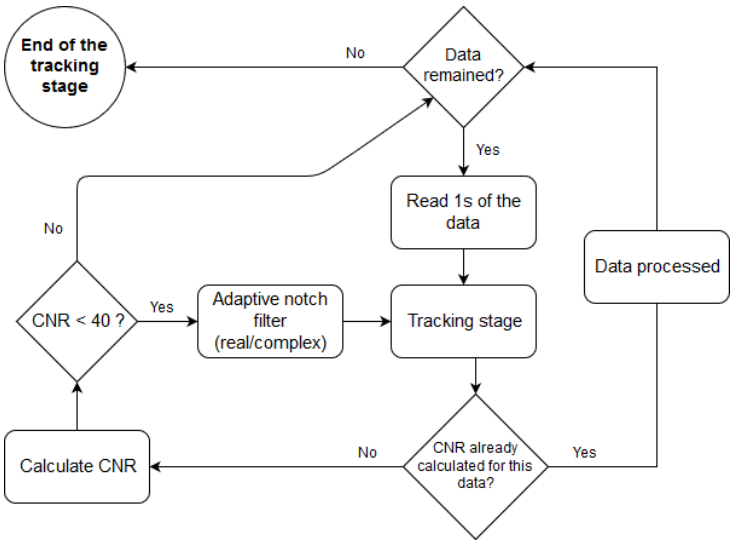


Figure 6.5: Flow chart of the implemented ANF in the SDR

First, 1 s of the data are read from the dataset and processed in the tracking stage. The interference detection is performed using the CNR estimator, which can be calculated at the tracking output from the correlator values. In this case the SVN approach, which is described by Equations 3.2 to 3.6, was used. If the CNR would be calculated for every integration, the values would show large variations. To avoid this the data can be smoothed using a moving average [Bartl (2014)] or the CNR can be calculated for a longer period. In this case the calculation was made for every second. If interference occurs, a drop of the CNR is observed. If the CNR for the last processed second exceededs a predefined threshold, interference is detected and the ANF is performed on the data and the tracking

stage is repeated with the filtered data. If the threshold is not exceeded, the next 1 s of data are read and processed. This is done for every satellite for every second. The threshold for interference detection was set to 40 dB/Hz.

As explained in Chapter 5.1, a CNR drop for a single satellite can be caused by multipath, low elevation of the satellite an so on. Therefore it is better to apply the ANF on the data if more satellites are affected at the same time. The software SDR calculates the tracking stage sequential for every satellite. Therefore, it was only used for first tests. The implementation of the ANF and the evaluation of the results were performed using the Gaims software.

Implementation of the ANF into the software Gaims

The ANF was implemented into the existing Gaims software. The principle is shown in Figure 6.3. If only one algorithm for interference detection for the actual integration interval raises an alarm, the ANF is activated and applied on the data. The input values for the ANF (the forgetting factor λ and the attenuation bandwidth B) can be defined by the user. Other quantities like the notch frequency θ_1 and the step size μ have the start values of 0. The filtered signal is then used for further processing.

6.3 Implementation of pulsed interference in software

To perform the pulse blanking, first the pulsed interference had to be implemented into the GIPSIE software. In literature (Dovis 2015) three parameters are mentioned, which describe the pulsed signal: the pulse width (PW), the duty cycle (DC) and the pulse repetition rate (PRR). The parameters have been already described in Section 4.3. Only two quantities are needed to describe the pulsed signal. For this implementation the PW and the DC were chosen.

The assumption was made, that every implemented interference type (AM, FM or SCW) with arbitrary input parameters can be simulated as pulsed interferer. The implementation strategy is presented in Figure 6.6.

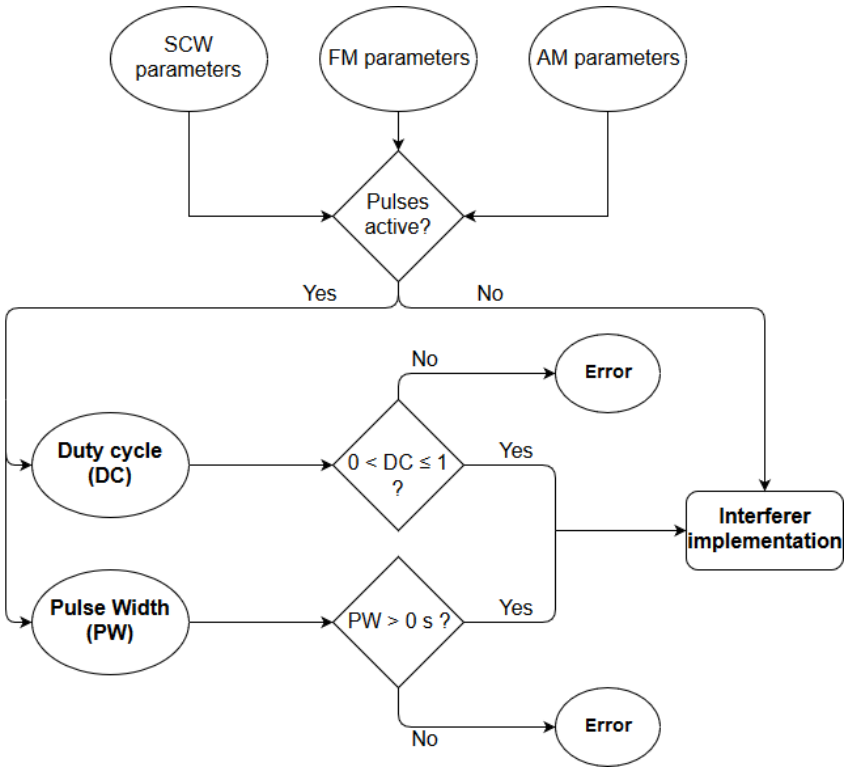


Figure 6.6: Flow chart of the validation of pulsed interference

After the input values are validated, the interference signal is, based on the interferer parameters, calculated and added to the raw signal. The amplitude of the interfering signal depends on the predefined jamming power and the distance between the jammer and the receiver. The algorithm of the single interferer types was already implemented in GIPSIE® and will not be discussed in detail. The principle of adding pulsed interference to the raw signal is shown in Figure 6.7.

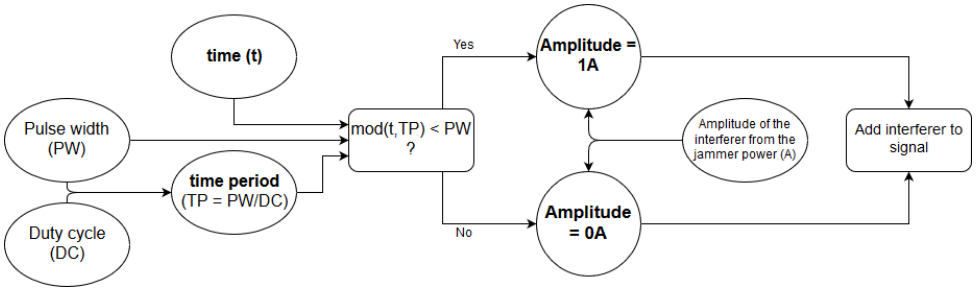


Figure 6.7: Flow chart of the validation of pulsed interference

For evaluation, if the signal sample is located within the pulse, the time period (TP) of the pulsed signal was used. The TP is the inverted PRR and describes the period between the start of two consecutive pulses. The next parameter, used for the implementation is the time t. It is increased for every sample within the interference event. If the remainder of the division of t and TP is smaller than the PW, the current sample is detected within a pulse and its amplitude factor is set to 1. If the remainder is greater as the PW, the sample is registered outside the pulse and the amplitude factor is set to 0 and no interference is

added to the raw data.

6.4 Implementation of the pulse blanking algorithm

The implementation was done within the software Matlab R2016b. The algorithm zeroises signal samples which exceed a certain threshold. The flow chart of the algorithm is shown in Figure 6.8.

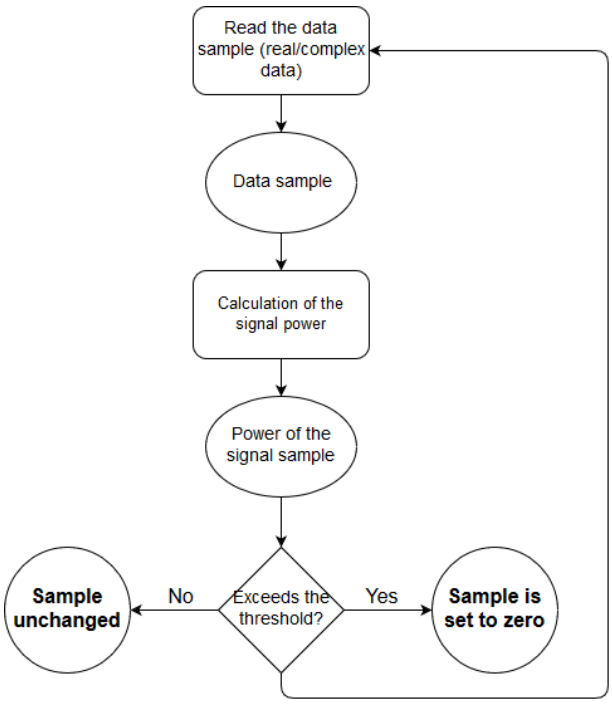


Figure 6.8: Flow chart of the pulse blanking algorithm

Based on the single sample the signal power is calculated. The calculation is based on Equation 5.20. The higher the values of the signal sample, the higher the signal power. Furthermore, the value was converted into dBW using the equation

$$P[dBW] = 10 \cdot log10(P_k). \tag{6.2}$$

Afterwards, the calculated receiver power was compared to a certain threshold. In Raimondi et al. (2006) it is mentioned, that the less degradation of useful signal is caused using a threshold of -117.1 dBW. If the power of the signal sample exceeds this threshold, the signal sample is set to 0.

The calculation of the signal power for a single sample has its drawback: the results are very noisy. Therefore, Raimondi et al. (2006) recommends to filter the data with a bandwidth of 0.25 μs. This smooths the data and prevents the PB algorithm of zeroising healthy signal samples. If the signal is filtered using a moving average (MA) the calculation can still be performed in real-time.

7 Results

The main objective of this thesis is to investigate different jamming mitigation techniques. In this case two ANF solutions and the pulse blanking algorithm were implemented and tested. To determine the effectiveness, different datasets with different jamming signal properties were used. The evaluation of the results is based on the spectrograms, raw data and filtered data. To evaluate the tracking results, the PVT solution and the CNR, the signals were processed using the software Gaims. For the GNSS signal processing the following properties were chosen:

- Number of coherent integrations: 2
- Number of non-coherent integrations: 4
- Coherent integration time for GPS: 4 ms
- Coherent integration time for Galileo: 4 ms
- Number of GPS correlators: 3
- GPS correlator spacing: 0.5
- Number of Galileo correlators: 5
- Galileo correlator spacing: 0.2

In the first section, the results of applying the ANF and PB on data, simulated using GIPSIE®, are shown. Afterwards the ANF was applied on the real data.

7.1 Simulations

The purpose of the simulations was to test the implementation of the different algorithms in a well-controlled environment using the GIPSIE® simulator. Using the software, different jamming signals with different spectral characteristics were simulated and analysed using different processing settings. Overall, two different simulations were made. In the first simulation, continuous interference was simulated to evaluate the performance of an ANF. In the second one pulsed interference was simulated to evaluate the performance of the PB algorithm.

Performance of the adaptive notch filter

The properties of the simulated IF signals are listed in Table 7.1.

Table 7.1: Properties of simulated IF signals

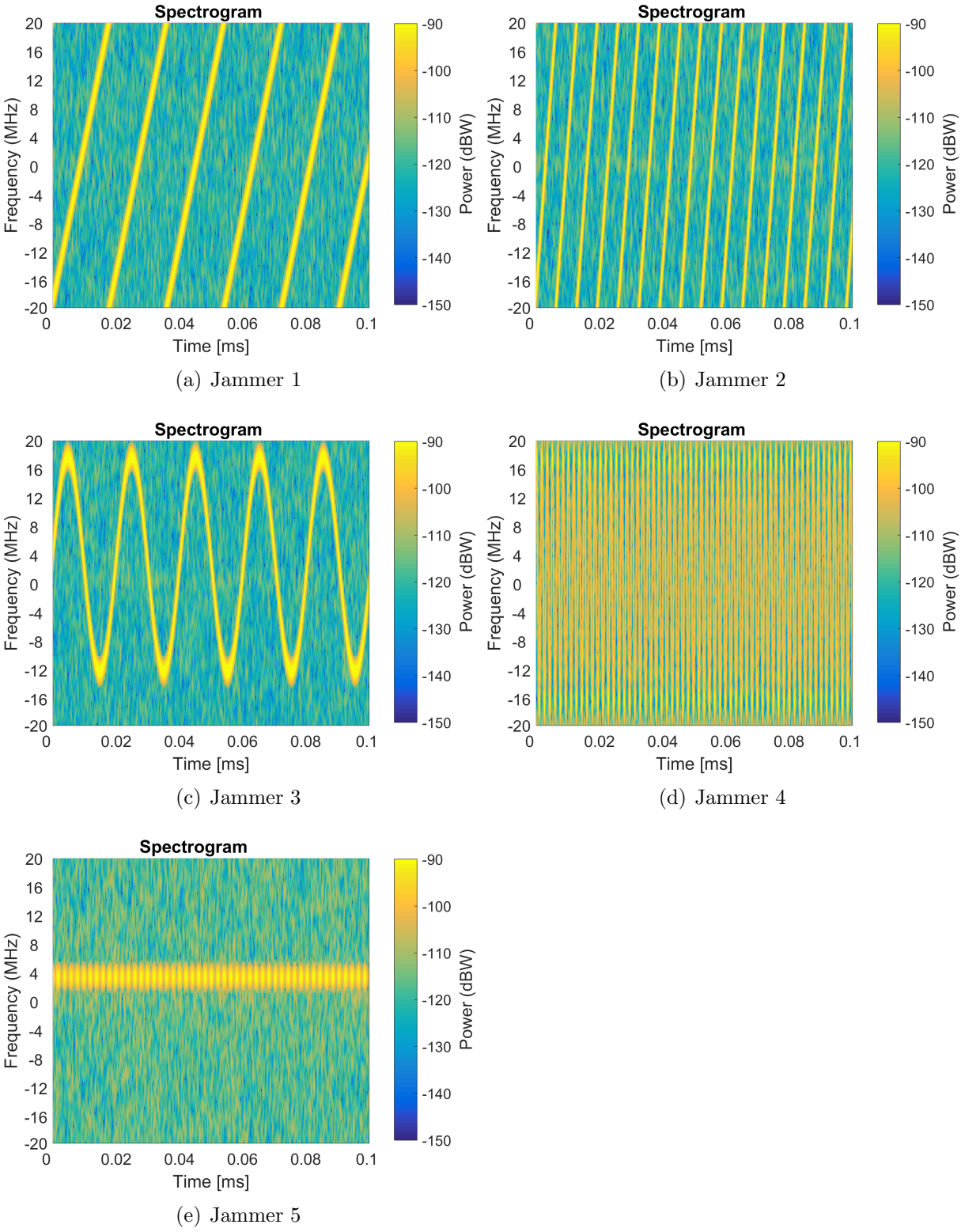
Sampling frequency(f_s):	40 MHz
Intermediate frequency (f_{IF}):	0 MHz
Number of quantization bits:	8 (256 different values)
Activated AGC:	Yes
Visible GPS satellites:	PRN 2, 5, 6, 7, 9, 13, 16, 23, 30
Visible Galileo satellites:	PRN 1, 2, 6, 8, 9, 15, 16, 17, 18, 19, 27

Overall five different jammers were simulated. Every interferer was simulated for 10 s. The properties of the simulated jammers are listed in Table 7.2:

Table 7.2: Characteristics of the simulated jammers

	Jammer 1	**Jammer 2**	**Jammer 3**	**Jammer 4**	**Jammer 5**
Type:	SCW	SCW	FM	FM	AM
Duration:	10 s	10 s	10 s	10 s	10 s
Power $[dBW]$**:**	-120, -110	-120, -110	-120, -110	-120, -110	-120, -110
Frequency offset $[MHz]$**:**	0	0	2.3	0	3
Sweep Bandwidth $[MHz]$**:**	40	40	-	-	-
Sweep duration $[\mu s]$**:**	18	6.5	-	-	-
Frequency deviation $[MHz]$**:**	-	-	15	18	-
Modulation frequency $[kHz]$**:**	-	-	50	600	500
Modulation index [ ]:	-	-	-	-	0.7

The power of all simulated jammers was the same for better comparison. At the beginning it was set to -120 dBW. The power is increased in the first five seconds to -110 dBW and then stayed constant till the end of the interference event. Two of the jammers are SCW jammers, two of them are FM jammers. The last simulated interferer is an AM jammer. Figure 7.1 shows the spectrograms of the different interferers. The STFT was calculated for 0.1 ms with a FFT window length of 0.8 μs and an overlap period of 0.2 μs.



(a) Jammer 1

(b) Jammer 2

(c) Jammer 3

(d) Jammer 4

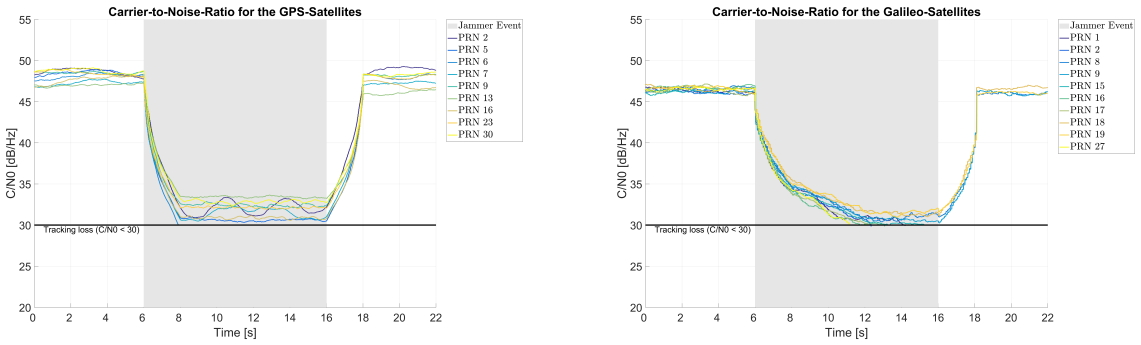
(e) Jammer 5

Figure 7.1: Spectrograms of the simulated jammers

The SCW jammers are WBI, centred at the L1/E1 center frequency and spread over the whole spectrum. They differ from each other by the sweep duration. The sweep duration of jammer 1 is set to 10 μs, the sweep duration of the second jammer is almost a third of

it (6.5 μs). The FM jammers are WBI interferers as well. The most markable difference between them is their modulation frequency. Jammer 3 has a modulation frequency of 50 kHz, while jammer 4 has a modulation frequency of 600 kHz. The AM jammer was simulated to prove, if the ANF can follow a constant frequency. The jammer is centred 3 MHz from the L1/E1 center frequency.

First, the SCW jammers will be taken into account. The CNR during the first interference event for GPS (left) and Galileo (right) satellites is presented in Figure 7.2.



(a) GPS (b) Galileo

Figure 7.2: Estimated CNR for GPS and Galileo when processing the simulated jammer 1

No markable differences between GPS and Galileo during an interference-free event are visible. All satellites have a CNR between 45 and 50 dB/Hz. Satellites of the same constellation do not show differences in the CNR to each other because no atmospheric noise was simulated. During the interference event, the CNR decreases its value. The value strongly depends on the jammer power. The stronger the jamming power, the smaller the CNR. The receiver loses track of six satellites (1 GPS satellite and 5 Galileo satellites). The tracking loss happened a few seconds after the start of the interference. The reasons for a tracking lost are the jammer characteristics and the high jammer power. If the CNR for GPS and Galileo during interference events is compared, it can be seen that the values are lower for Galileo satellites. The reason can be found in the integration time. For Galileo, the integration time had to be set to 4 ms, which equals the length of one code and a navigation bit. An integration time of 4 ms for GPS means that, for the tracking, four code lengths were used, which causes more accurate and better results.

Figure 7.3 shows the correlator values and the navigation bits during 10 s of interference event 1 for the GPS satellite PRN 5.

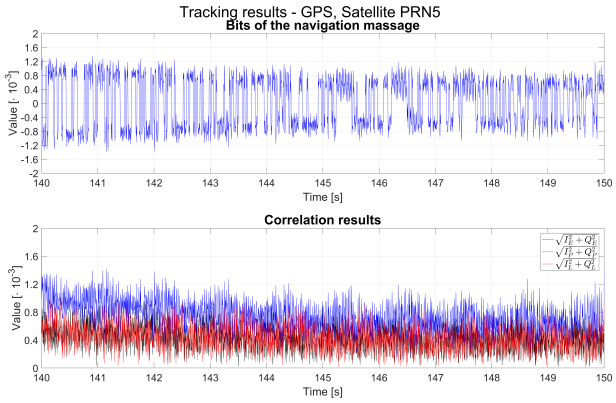


Figure 7.3: Tracking results during the first simulated interference event for the GPS satellite PRN 5

The correlator values depend on the jammer power. With higher jammer power the correlator values decrease. Noticeable is the large variance of the correlator values, which has an impact on the pseudorange estimation. A less stable discriminator function causes a false code phase estimation and thus an erroneous pseudorange estimation. The navigation bits are clearly higher than 0 and are still detectable.

The calculation of the PVT solution was performed for every second. Note that the position calculation can be only done after the receiver successfully tracks four or more satellites and if the navigation data have been successfully decoded for these satellites. First, a reference position was calculated. The reference position is the mean value of every coordinate till the first interference event. Afterwards, the difference of every coordinate to the reference position was calculated. In Figure 7.4 the coordinate differences to the reference position during the first interference event are presented.

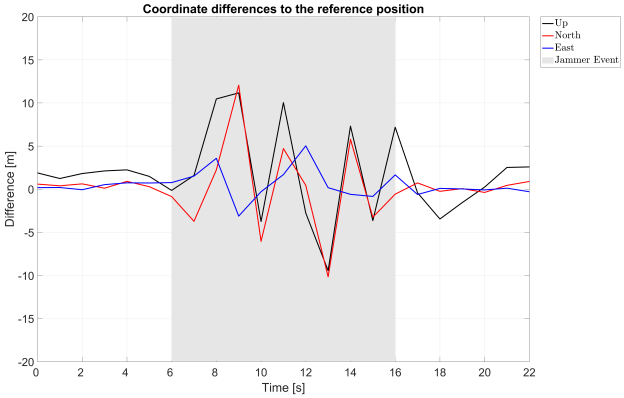
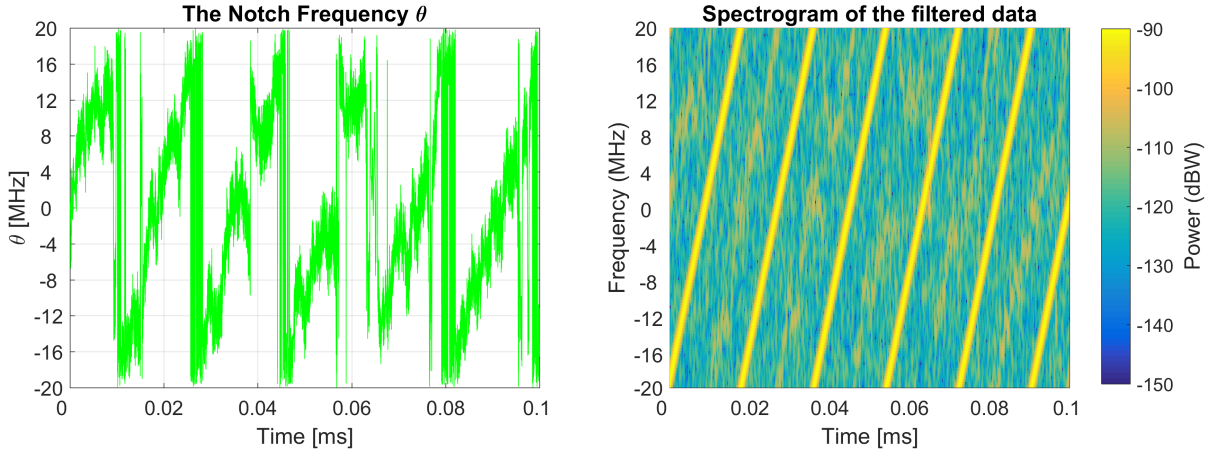


Figure 7.4: Navigation solution during the simulated jamming event 1 without applying the ANF on the data

As shown in Figure, the smallest variations appear in the east-component. The biggest variations are visible in the up-component because of the satellite geometry. It can be seen that the coordinate differences to the reference position get higher during the interference event. This is mostly caused by an inaccurate tracking stage, causing erroneous pseudorange estimation for all satellites. Furthermore, during this jamming attack tracking to

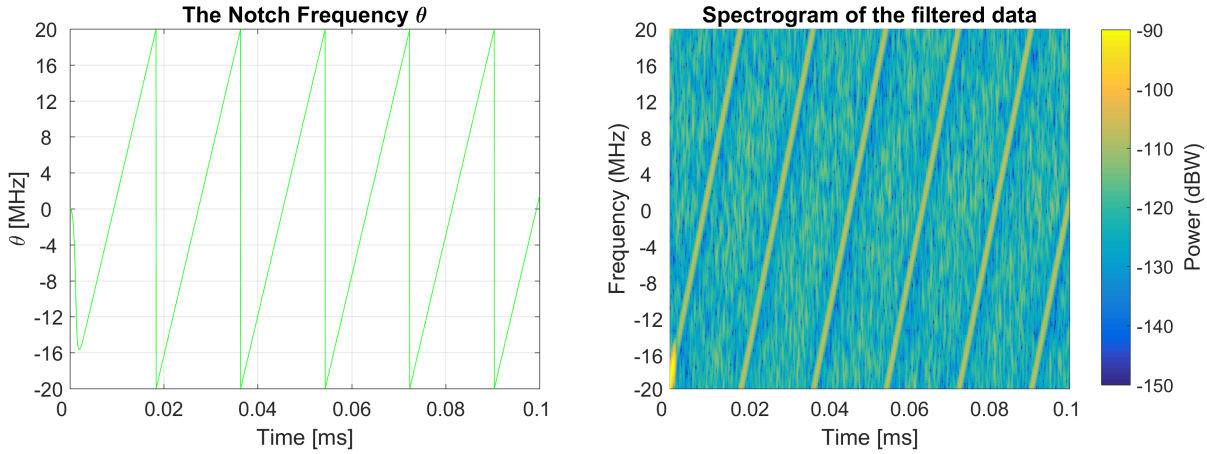
some satellites is lost by the receiver. A loss of satellites means less observations for the least-squares-adjustment and in general a worse satellite geometry and a less accurate PVT solution.

In the next step the ANF was applied on the data. As described in Section 5.2, the ANF is characterized by two input parameters: The forgetting factor λ and the attenuation bandwidth B. To evaluate the effect of the ANF on the data, different combinations of both parameters were made. Figures 7.5, 7.6 and 7.7 show the notch frequency parameter and the spectrogram of the filtered data for the interference event 1 after applying the ANF with three different combinations of ANF input parameters on the data. Every figure shows a different combination of input parameters.



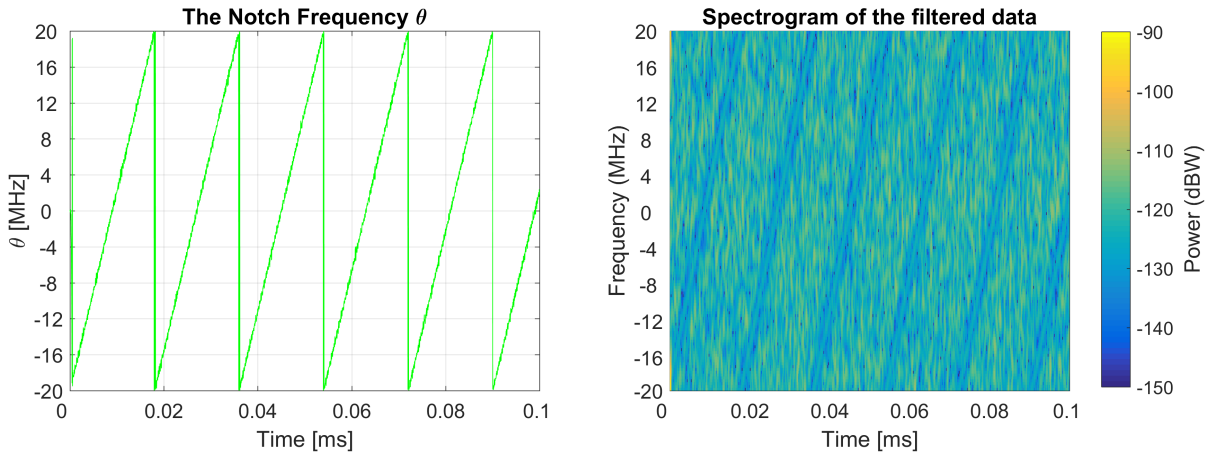
(a) θ (b) Spectrogram

Figure 7.5: Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 1 ($\lambda = 0.3$, $B = \pi/50$)



(a) θ (b) Spectrogram

Figure 7.6: Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 1 ($\lambda = 0.9$, $B = \pi/3$)



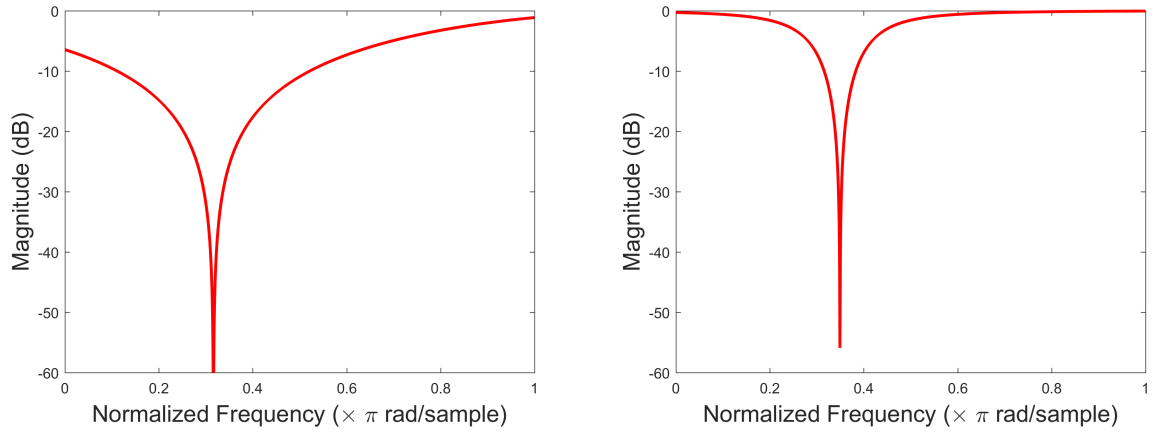
(a) θ (b) Spectrogram

Figure 7.7: Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 1 ($\lambda = 0.3$, $B = \pi/3$)

A forgetting factor of 0 means, that the ANF uses no information of the previous jamming frequency for the computation of the current jamming frequency. A forgetting factor close to 1 means, that the ANF uses only information from the previous epoch to compute the current notch frequency. A smaller forgetting factor causes a faster reaction on frequency changes. This is very important for SCW jammers, because they are characterized by fast frequency changes. On the other hand, the variance of the notch frequency is increased, which causes a smaller stability of the ANF and a smaller quality of the estimation of θ_1. A bigger forgetting factor may cause spikes in the notch frequency or it reacts on the jamming frequency with a certain delay. The best result is obtained, if a smaller forgetting factor is chosen (as seen in Figure 7.7).

The attenuation bandwidth is an important parameter and a right choice of the attenuation bandwidth is needed for a successful mitigation. An ANF with a small bandwidth mitigates

only a small part of the interfering signal. The remaining interfering signal is not mitigated or suppressed for only a few dB. The choice of a higher B mitigates a higher amount of interfering signal. But if the attenuation bandwidth is chosen too large, not only the interfering signal is mitigated, but also parts of the useful signal may be suppressed too. Figure 7.8 shows the frequency response for attenuation bandwidths $\pi/2$ (left) and $\pi/10$ (right). A higher attenuation bandwidth attenuates more frequencies around the center frequency. The center frequency of a greater bandwidth is mitigated more intensively than the center frequency of a smaller bandwidth.



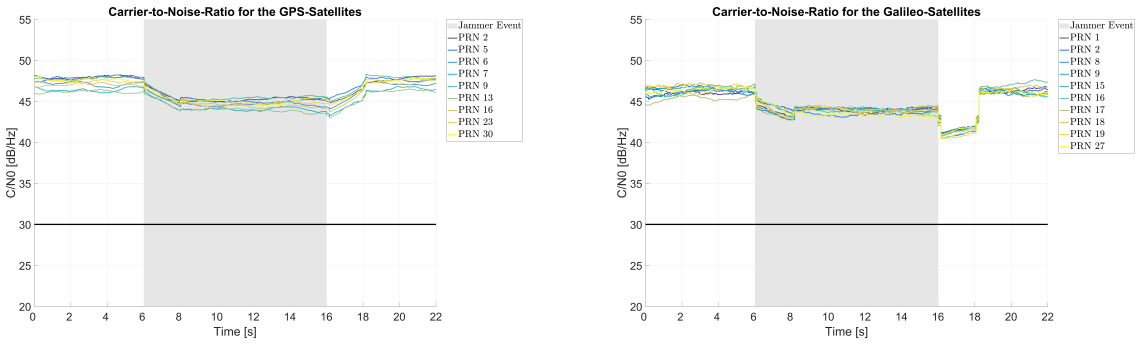
(a) $\pi/2$ (b) $\pi/10$

Figure 7.8: Frequency response of the ANF with two different attenuation bandwidths B

Different combinations of the input parameters were teste and more of them successfully filtered out the interfering signal. The optimum solution, which was chosen for further calculations, was

- $\lambda = 0.3$
- $B = \pi/3$.

Afterwards, the signal was processed with activated ANF once interference was detected. Figure 7.9 shows the CNR during interference event 1 after ANF was applied on the data.



(a) GPS (b) Galileo

Figure 7.9: Calculated CNR after applying the ANF on the data

By comparing Figures 7.2 and 7.9 the effect of the ANF is visible. The ANF filters out the interference part of the incoming signal, which increases the CNR values. In some cases this prevents the receiver from losing tracking to certain satellites. But nevertheless, the CNR is smaller as for the interference-free event. The reason for that is that the ANF suppresses not only the interfering signal, but it suppresses also a part of the useful signal. This reduces the carrier power and decreases the CNR. It can be seen that the CNR values are higher for GPS satellites than for Galileo satellites. The reason for that are the processing settings.

Figure 7.10 shows the tracking results (bits of the navigation message and the correlator values) of the GPS satellite PRN 2 during the interference event 1 after applying the ANF on the data.

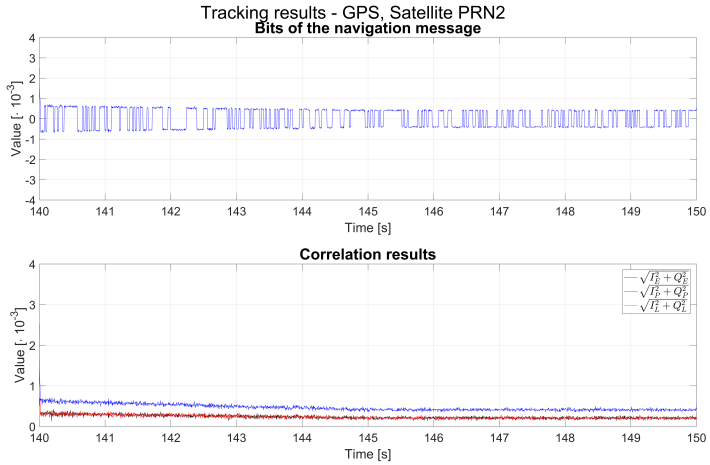


Figure 7.10: Tracking results during the first simulated interference event for the GPS satellite PRN 2

By comparing Figures 7.3 and 7.10 the effect of the ANF on the tracking values can be seen. The ANF causes smaller correlator values, but they are more stable as without ANF. This increases the accuracy of the pseudorange estimation and of the PVT solution. Furthermore, the prompt-correlator is higher than the other two, which means that the tracking is stable. The small correlator values have an influence on the value of the bits

of the navigation message. The bits have a lower value, but in this case they are clearly above zero, which enables a successful bit synchronization and decoding of the navigation message.

Figure 7.11 presents the PVT solution during the jamming event 1 after the ANF was applied on the data. Note that for the calculation, both GPS and Galileo satellites were taken.

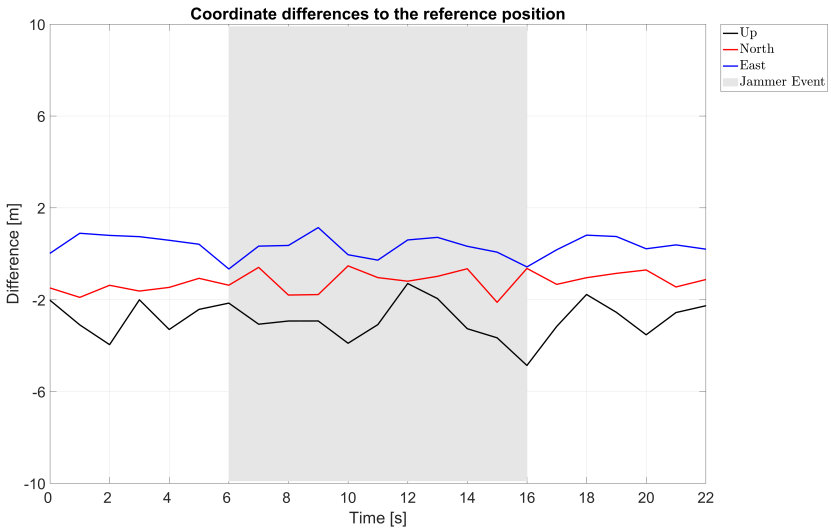


Figure 7.11: Navigation solution for jammer 1 after applying the ANF on the data

By comparing Figures 7.4 and 7.11 the effect of the ANF can be seen. The ANF causes smaller coordinate differences to the reference position. This is due to a more accurate pseudorange estimation and by the tracking of more satellites. It can be concluded that the ANF successfully mitigates the SCW jammer 1 and causes better results.

In the next step, the effect of the ANF on the simulated jammer 2 was investigated. The spectrogram of the filtered data, using the input parameters $\lambda = 0.3$ and $B = \pi/3$, is presented in Figure 7.12.

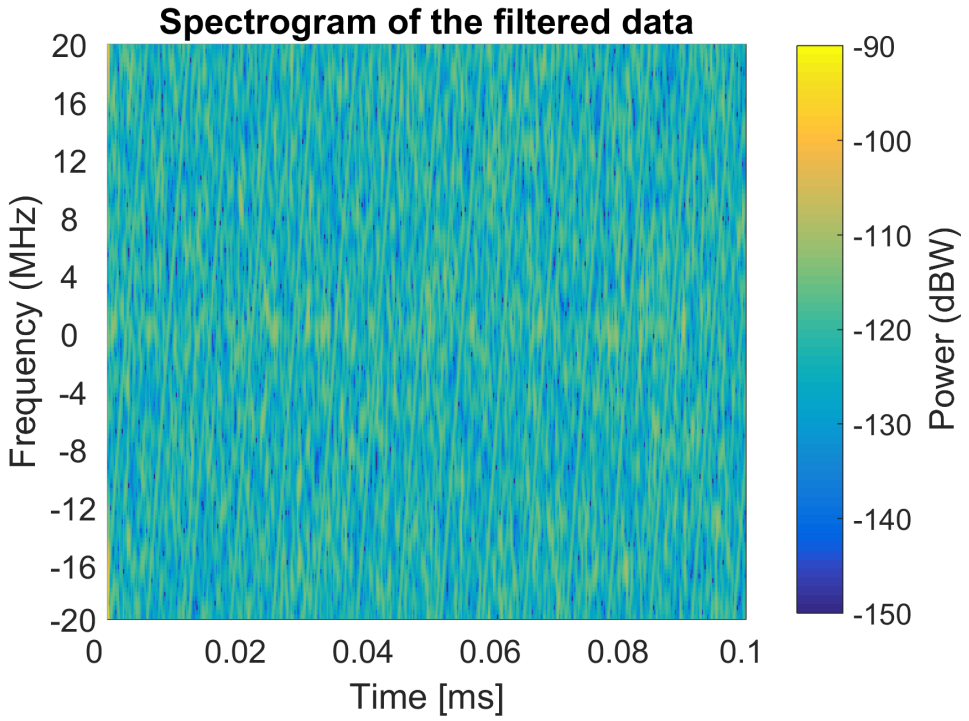
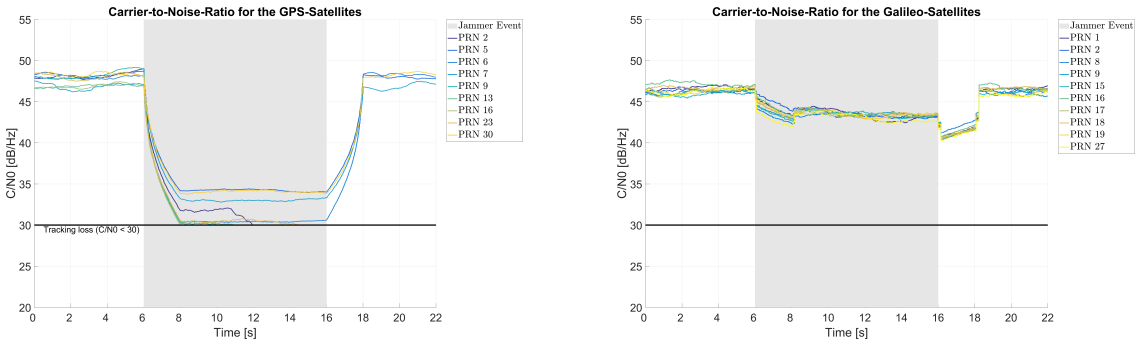


Figure 7.12: Spectogram of the filtered data of the simulated jammer 2 after applying the ANF on the data ($\lambda = 0.3$, $B = \pi/3$)

The ANF, using the previous settings, is able to mitigate the signal.

Figure 7.13 shows the CNR of all GPS satellites before (left) and after (right) applying the ANF on the data.



(a) Without ANF

(b) With ANF

Figure 7.13: Calculated CNR during the jamming event 2 before and after applying ANF on the data

As for the interferer 1, the ANF increases the CNR of all satellites and prevents the receiver from losing the tracking. The CNR before applying the ANF on the data is between 30 and 35 dB/Hz. The receiver loses tracking of four GPS satellites. After the ANF is activated,

the CNR occupies values between 42 and 46 dB/Hz and all satellites are being tracked. By comparing the CNR to jammer 1 (Figure 7.9) it can be seen that during jamming event 2, the CNR is lower by about 2 dB/Hz. This is related to the sweep bandwidth of the jammer. A higher sweep bandwidth means that a large part of the spectrum is covered by interference. The amount of useful signal is already smaller than for a jammer with a higher sweep bandwidth. The ANF suppresses a higher amount of signal, which results in a lower CNR.

The third and fourth jammers in the simulation are FM jammers, which have different modulation frequencies. The modulation frequency of the third jammer is 50 kHz, the modulation frequency of the fourth jammer is 600 kHz. The spectrograms of both jammers are shown in Figure 7.1. Both of them are WBI jammers, spread over the whole spectrum. Due to a high modulation frequency, the frequency behaviour of the fourth interferer is barely recognizable.

Again the signal was processed without activating the ANF first. Figure 7.14 shows the CNR of the GPS satellites during interference event 3 without applying the ANF on the data.

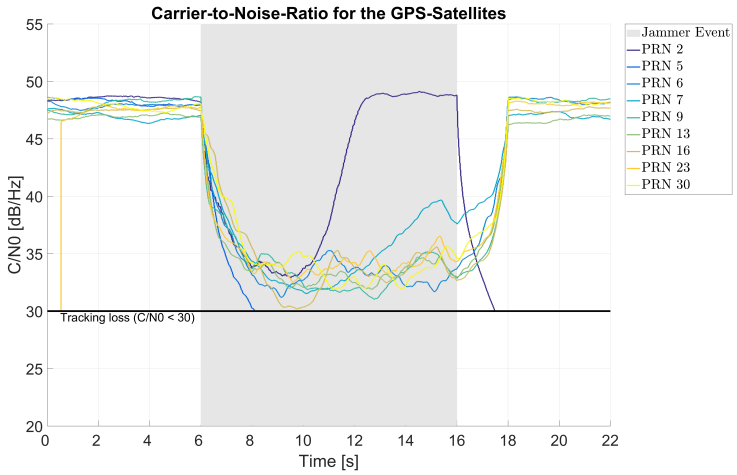
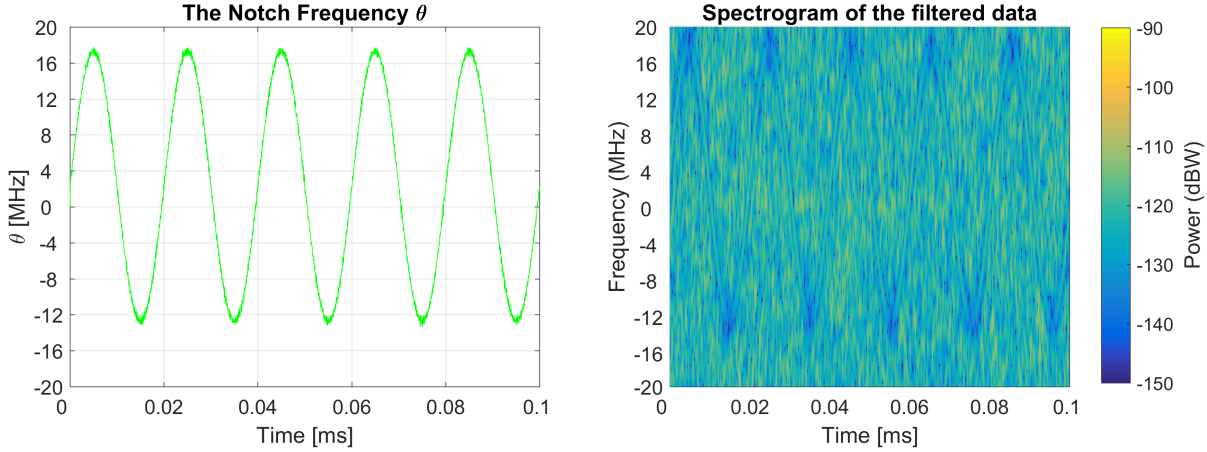


Figure 7.14: CNR of GPS satellites during the simulated jammer 3 without applying the ANF on the data

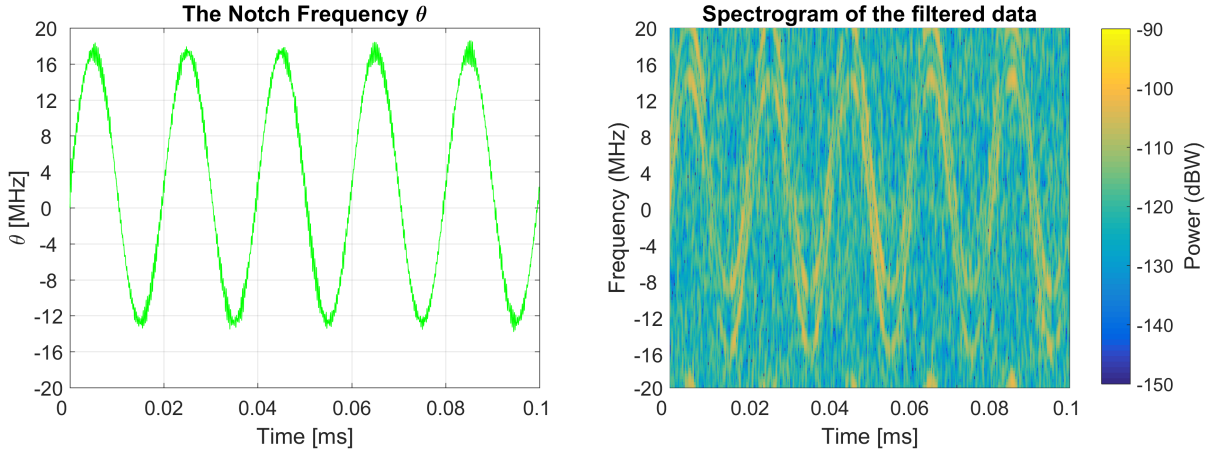
The figure shows that the GPS satellite PRN 2 has actually a higher CNR during the interference event. This cannot be interpreted as a successful tracking, but it is the consequence of a systematic error, happening in the tracking stage. This causes an erroneous discriminator function and erroneous correlator values. The CNR of all other satellites is strongly decreased. The receiver also loses tracking to some satellites.

Afterwards, the ANF was applied on the different jammers. To evaluate the effect of the ANF on the data more different combinations of ANF setting parameters were made. Figures 7.15, 7.16 and 7.17 show the notch frequency parameter and the spectrogram of the filtered data for interference event 3 after applying the ANF with three different combinations of input parameters on the data. Every figure shows a different combination of input parameters.



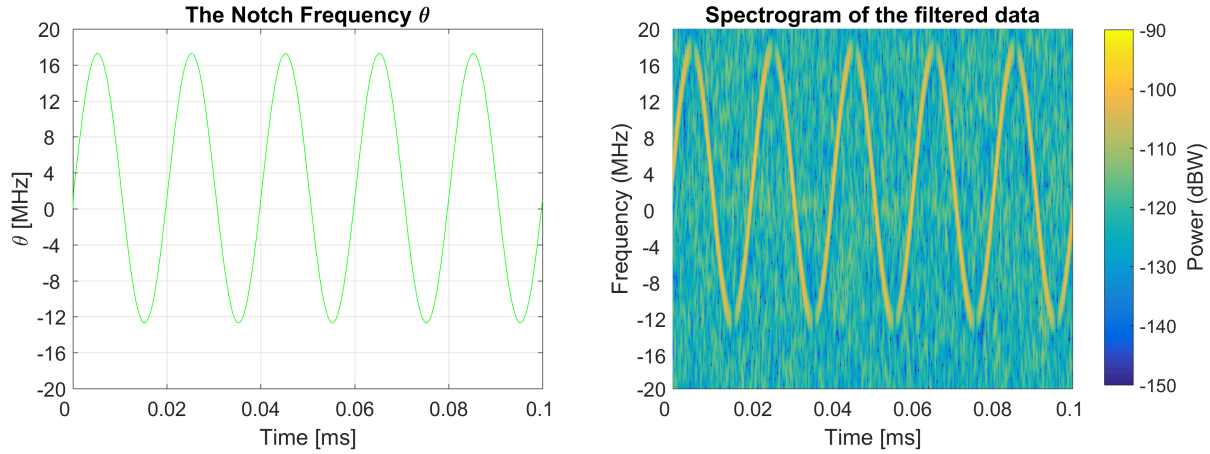
(a) θ (b) Spectrogram

Figure 7.15: Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 3 ($\lambda = 0.3$, $B = \pi/3$)



(a) θ (b) Spectrogram

Figure 7.16: Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 3 ($\lambda = 0.3$, $B = \pi/10$)



(a) θ (b) Spectrogram

Figure 7.17: Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 3 ($\lambda = 0.9$, $B = \pi/5$)

The notch frequency follows the jamming frequency for all combinations. The interfering frequency shows no jumps. Jumps are, as seen for the SCW jammers, the biggest problem of the ANF, because it needs a certain response time to follow it. A FM jammer has no such fast changes of the interfering frequency and the notch filter has no problems to follow. The effect of the ANF can be seen when considering the spectrogram. Here, similar results to the SCW jammer are visible. A larger forgetting factor reacts slowly on frequency changes, it causes a delay and it does not mitigate the whole jamming signal. Thus, a smaller forgetting factor should be chosen when dealing with FM jammers with a higher frequency deviation. The bandwidth should be chosen to be high. As the optimum solution

- $\lambda = 0.3$
- $B = \pi/3$

was found. Once jamming was detected, the ANF with the optimum filter parameters was applied on the signal. Figure 7.18 shows the CNR of the GPS (left) and Galileo (right) satellites after the filtering of the jammed data 3.

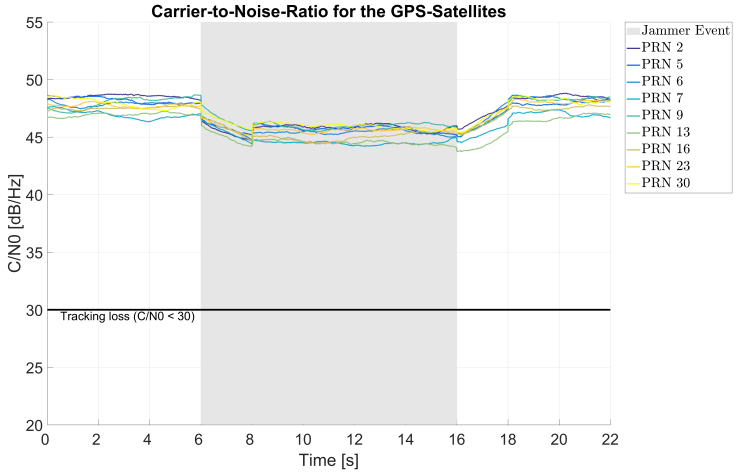


Figure 7.18: CNR of GPS satellites during the simulated jammer 3 after applying the ANF on the data

The usage of ANF increases the CNR of all satellites and prevents the receiver of losing track to the satellites. The CNR values, after applying the ANF on the data, are between 40 and 45 dB/Hz, which means a good quality of the signal.

Figure 7.19 shows the CNR of GPS satellites during the interference event 4 without activating the ANF.

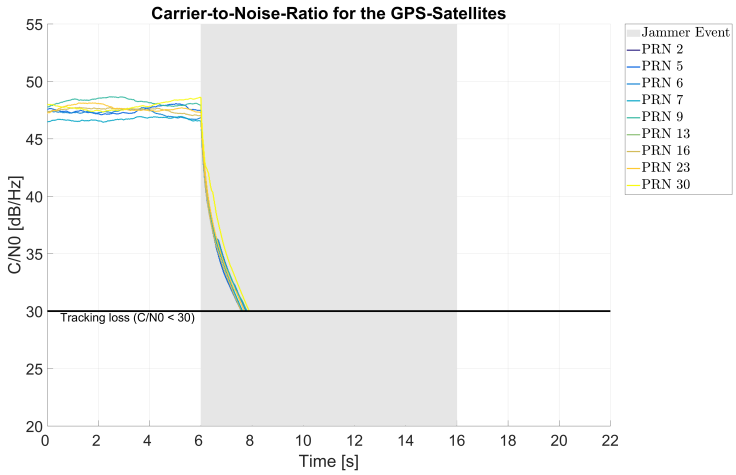
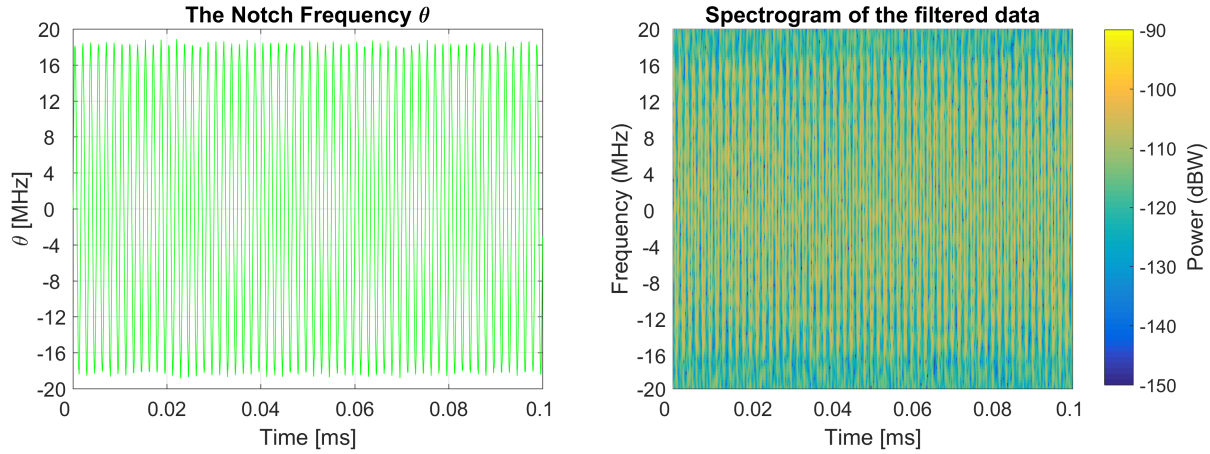


Figure 7.19: CNR of GPS satellites during the simulated jammer 4 without applying the ANF on the data

The receiver loses track of all satellites during this jamming event. The main reason for such behaviour are the jammer characteristics. Because of the high modulation frequency and the high frequency deviation the whole spectrum is covered by interference, which disables a successful tracking and a PVT solution.

Figure 7.20 shows the notch frequency parameter and the spectrogram of the filtered data after applying the ANF with the optimal choice of the input parameters on the simulated jammer 4.



(a) θ (b) Spectrogram

Figure 7.20: The notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 4 ($\lambda = 0.3$, $B = \pi/3$)

It can be seen that the ANF successfully follows the jamming frequency. But, as shown in the spectrogram, not the whole jamming signal is mitigated. The main reason for this is the high modulation frequency. At a sampling frequency of 40 MHz, a modulation frequency of 600 kHz means that a sine wave of the jammer is represented by 67 samples. The ANF has to follow the sine wave to mitigate it. If a high forgetting factor is chosen, the reaction of the ANF is very slow, the ANF follows some values, but stays at the same frequencies. This disables a successful mitigation. Therefore, the choice of a low λ is the best solution in this case.

After that the ANF was applied on the jammer 4 with a high modulation frequency. The CNR of GPSsatellites after applying the ANF on the data is shown in Figure 7.21

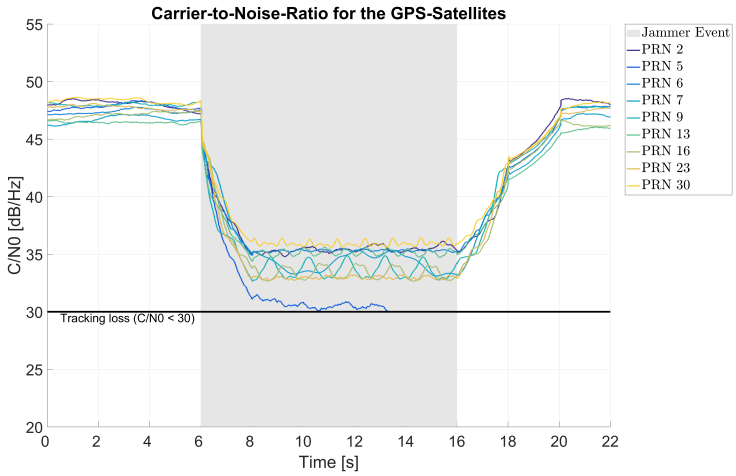


Figure 7.21: CNR of GPS satellites during the simulated jammer 4 after applying the ANF on the data

The CNR is between 35 and 40 dB/Hz and is lower than for jammer 3 with modulation frequency of 50 kHz (c.f. Figure 7.18). The receiver loses track of only one satellite. It can be concluded that the modulation frequency has a huge impact on the tracking quality. The higher the modulation frequency, the worse the CNR and tracking results. A modulation frequency close to 1 MHz or higher may be one method for outflanking the ANF.

The AM jammer is characterized by a constant frequency behaviour. This means that, if the frequency is known, a NF can be used for mitigating this interference type. In this case, the ANF was applied on the data to prove that it can also mitigate a signal with a constant frequency. An AM jammer can be represented by three parameters: the frequency offset, the modulation frequency and the modulation index. The simulated AM jammer was set 3 MHz from the L1 center frequency. The spectrogram of the AM interferer is shown in Figure 7.1.

The spectrogram shows a constant frequency behaviour of the jammer. In the spectrogram some variations in the magnitude during the jamming event are visible. The variations represents the amplitude of the incoming signal, which varies over time.

Figure 7.22 shows the CNR of all Galileo satellites during the fifth interference event without applying the ANF on the signal.

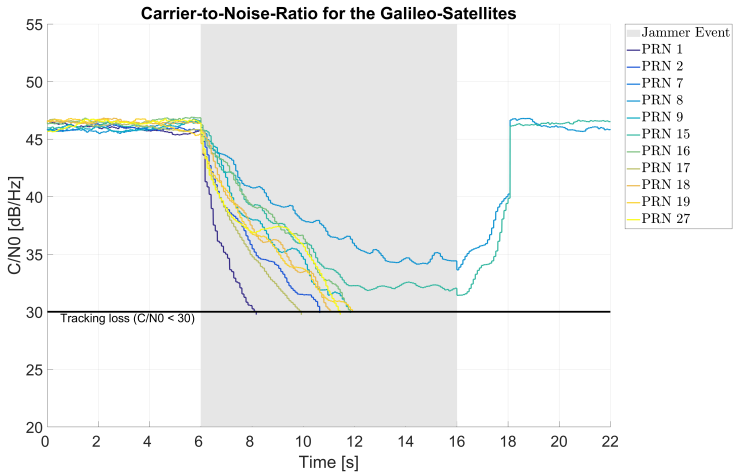


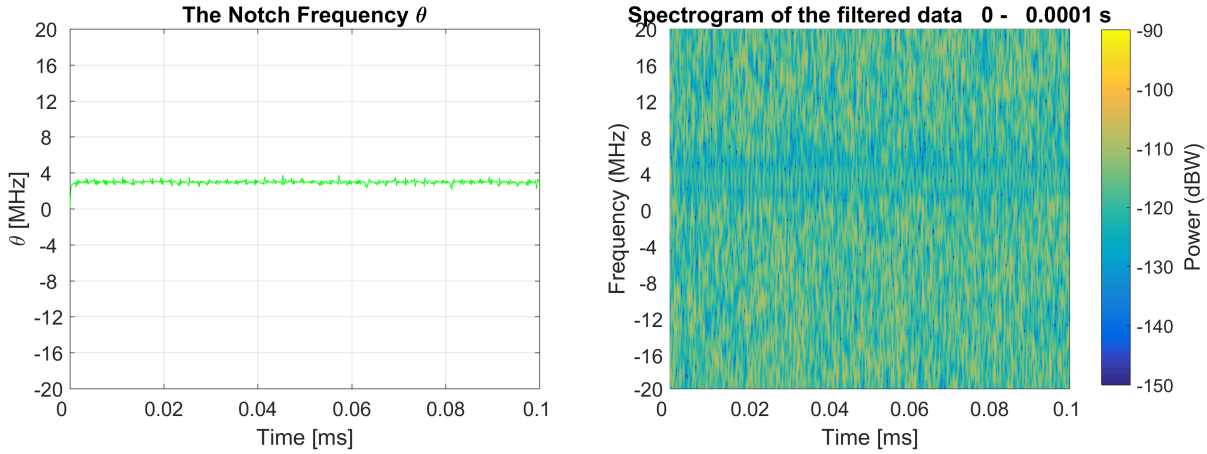
Figure 7.22: Estimated CNR of the AM interferer without applying ANF on the data

The interferer has an impact on the estimated CNR. The main reason is the high interference power. The higher the jamming power, the lower the estimated CNR. The receiver loses track of eight Galileo satellites during the jamming event and continuous track of two of them. Note, that the interferer is not located on the main lobe of the Galileo E1B signal.

In a next step an ANF was applied on the data. Different combinations of ANF input parameters were investigated. The following combinations was found to be suitable for mitigating such interference type:

- $\lambda = 0.9$
- $B = \pi/5$

Figure 7.23 shows the notch frequency (left) and the spectrogram of the filtered data (right) after applying the ANF on jammer 5.



(a) θ (b) Spectrogram

Figure 7.23: Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 5

The ANF is following the constant interfering frequency correctly and for the whole time. Because of the constant frequency, a higher forgetting factor is advantageous for mitigation. It causes a lower variance of the notch frequency. The attenuation bandwidth has to be high enough to mitigate the whole jamming signal.

Figure 7.24 shows the CNR of all Galileo satellites during the jamming event 5. In this case, the ANF was activated once jamming was detected.

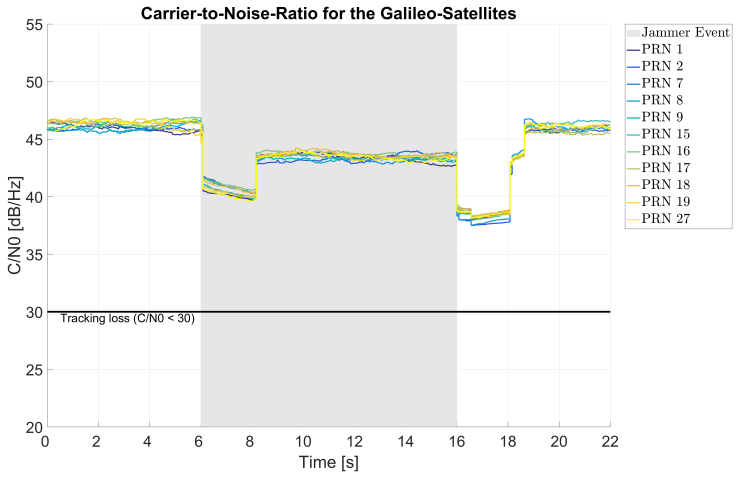


Figure 7.24: Estimated CNR of the AM interferer after applying ANF on the data

As for the SCW and FM interferer, the ANF increases the CNR during the AM interference event and prevents the receiver from losing track to eight Galileo satellites. The receiver can successfully track all the Galileo satellites for the whole interference event. The CNR is lower as for the interference-free event. The reasons are the same as for the other two interference events. It can be concluded that the ANF is able to mitigate AM jamming signals and prevent the receiver of losing track of some satellites.

Performance of the pulse blanking algorithm

The effect of the PB algorithm on pulsed data was investigated in the next step. Therefore, four different pulsed jammers were simulated. The properties of the simulations are listed below:

- Sampling frequency: 40 MHz
- Intermediate frequency: 0 MHz
- Simulated channels: GPS L1 C/A
- Number of quantization bits: 8
- AGC active: No
- Filtering of the signal: No
- ADC gain: 95 dB

The simulation properties are very similar to the properties of the simulation for evaluation of the ANF. The PB algorithm in GNSS receivers is implemented after the ADC and before the AGC. The AGC equals the signal's standard deviation, which does not allow thresholding, which is the main purpose of PB. To simulate the signals in the correct way and hypothetically implement the PB after the ADC, the AGC had to be turned off. An important parameter for PB is the ADC gain. The gain is multiplied to the signal samples before the ADC output. The higher the gain, the higher the sample values. Because the samples are used for calculating the received power, the ADC gain has an influence on the signal power calculation. In this case, it was set to 95 dB, which is a default value in GIPSIE®. As mentioned before, pulsed signals can be added to all in GIPSIE® implemented interferer types. In all cases, a SCW interferer was implemented with the parameters, listed in Table 7.3

Table 7.3: Parameters of the simulated SCW jammers with pulsed behaviour

Power:	−100 dBW
Frequency offset:	0 MHz
Sweep bandwidth:	10 MHz
Sweep duration:	15 μs

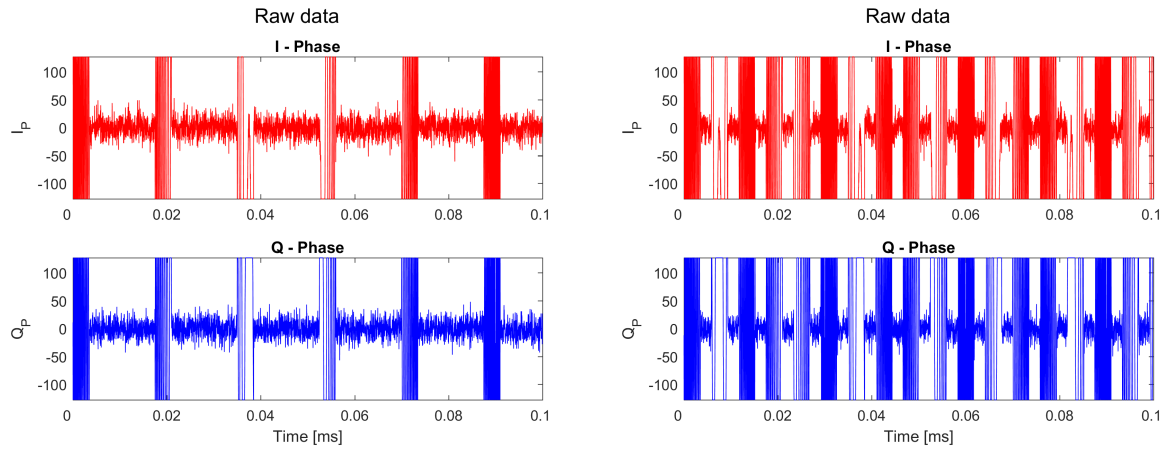
The simulated jammer is a WBI jammer and not a NBI as the most pulsed signals (DME/TACAN) are. To make the situation as realistic as possible, the frequency of the jammers was set on the L1 center frequency. In the simulations, the effect of the pulse width and the duty cycle was investigated. The properties of the four simulated jammers are listed in Table 7.4

Table 7.4: Characteristics of the simulated pulsed jammers

	Jammer 1	**Jammer 2**	**Jammer 3**	**Jammer 4**
Pulse width $[ms]$**:**	3.5	3.5	20	300
Duty Cycle [ ]:	0.2	0.6	0.2	0.2

First, the impact of the DC on the results will be taken into account. The first and the second simulated jammer differ only by the DC. The DC of the first jammer is set to 20 %, the DC of the second jammer is 60 %. Both jammers have the same PW of 3.5 μs. Note

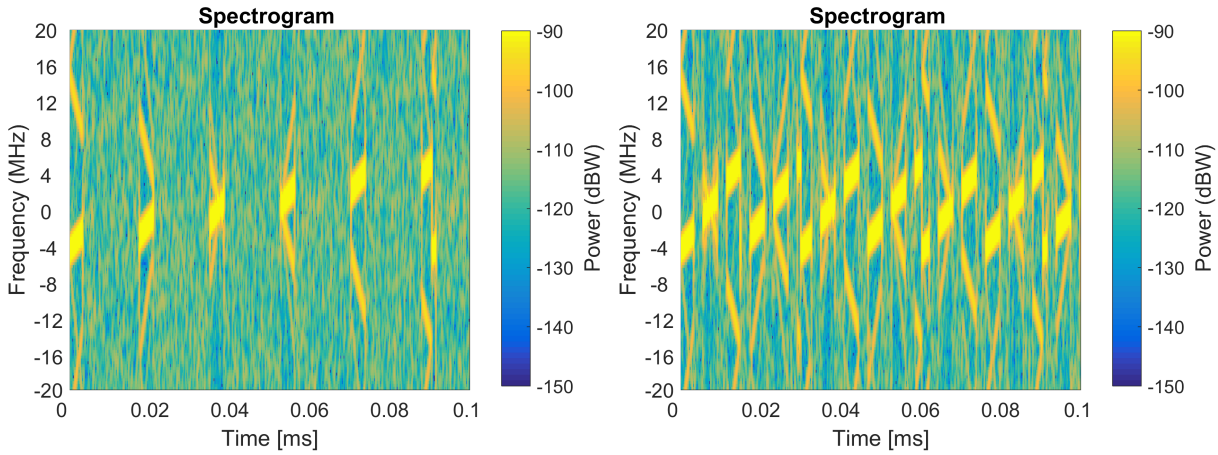
that the chosen duty cycles are much above the DCs of real ARNSs. Figure 7.25 shows 0.1 ms of raw data, which represents a pulsed signal with a duty cycle of 0.2 (left) and 0.6 (right).



(a) Duty cycle 0.2 (b) Duty cycle 0.6

Figure 7.25: Raw data of pulsed signals with different duty cycles

Because of the high jammer power, the pulses are very markable and the border values (± 127) are more frequent. Figure 7.26 shows the spectrograms of both signal sequences.

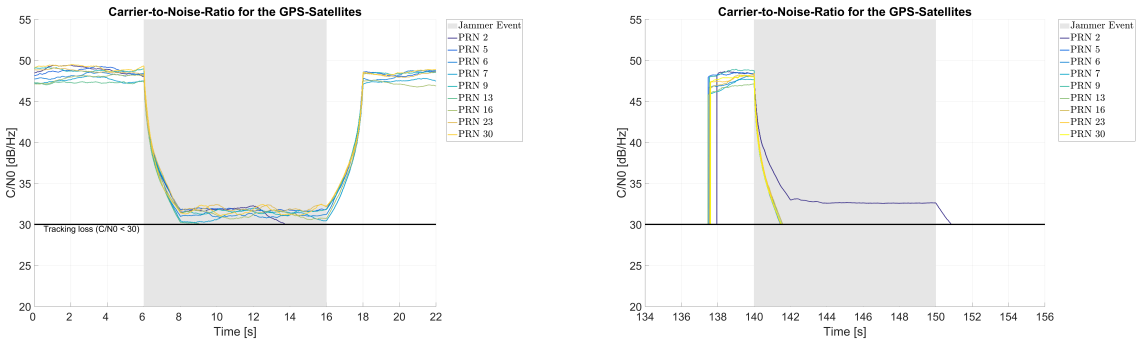


(a) Duty cycle 0.2 (b) Duty cycle 0.6

Figure 7.26: Spectrograms of pulsed signals with different duty cycles

In the right figure, the SCW frequencies are better recognizable due to the higher DC. In the spectrograms some additional frequencies are visible. These additional frequencies are caused by the saturation of the ADC and the deactivation of the AGC.

Figure 7.27 shows the CNR of all GPS satellites during the first (left) and the second (right) interference event without performing PB on the data



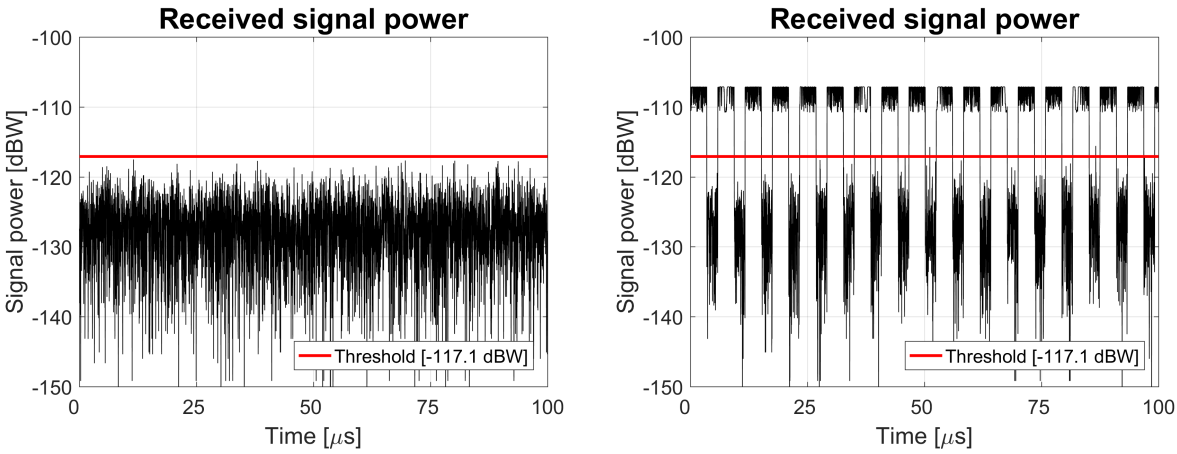
(a) First interferer (DC = 0.2)

(b) Second interferer (DC = 0.6)

Figure 7.27: CNR of the first and second pulsed jammer without performing PB

The CNR strongly depends on the duty cycle. The greater the duty cycle, the lower the CNR. For a DC of 0.2, tracking of all satellites is possible, but the CNR is almost at the border value of 30 dB/Hz. If the DC is set to 0.6 the receiver loses track of all GPS satellites. The border duty cycle to successfully track the GPS satellites is between 20 and 30 %. Note that the tracking properties are highly correlated with the interferer power. For a lower interference power, the DC has to be higher in order to lose track.

Figure 7.28 shows the estimated signal power of 0.1 ms of the data once during an interference-free event (left) and during a pulsed interference with a DC of 0.6 (right).



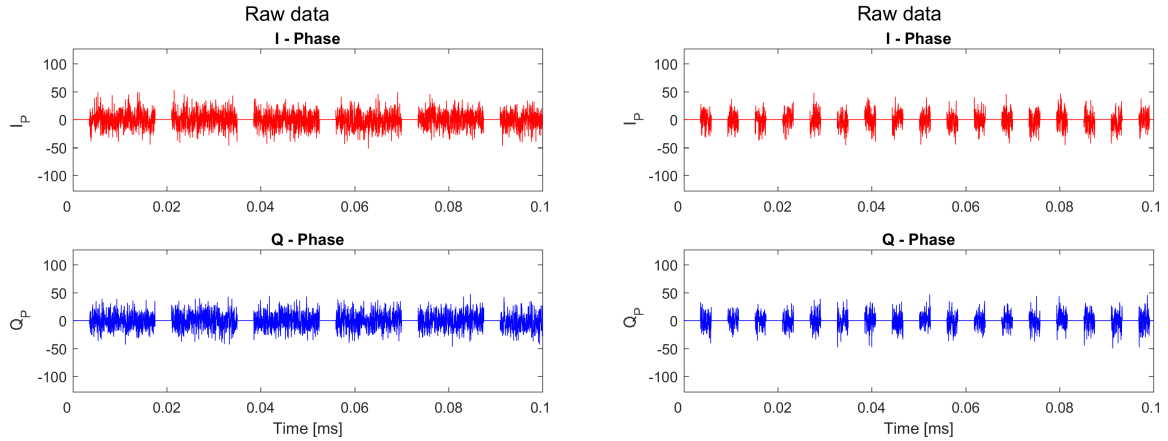
(a) No Interference

(b) Duty cycle 0.6

Figure 7.28: Estimated signal power

The estimated signal power shows large variations. The variations are due to the fact that no filtering of the data was performed. For the interference-free event, no significant overrun of the signal power is seen. The PB algorithm blanks only 0.0457 % of the useful signal, which has no impact on the signal processing quality. In case of a higher ADC gain and a lower interference power, it would be advantageous to filter the data with a moving average. During interference events, significant exceedings of the threshold during the pulsed events occur. The pulses are clearly visible because of the high interference

power. Because the received signal power is relatively constant, it is expected that the signal during the whole pulse is zeroized. Based on the data an estimation of the pulse parameters could be performed. The estimated jammer power is about −108 dBW, which is 8 dBW lower than the simulated interferer power. The reason for such behaviour are the signal samples. Because of the strong interference, a saturation of the ADC happens, which disables the estimation of the real power, based on signal sample values. The signal samples after the PB for interference events are presented in Figure 7.29.

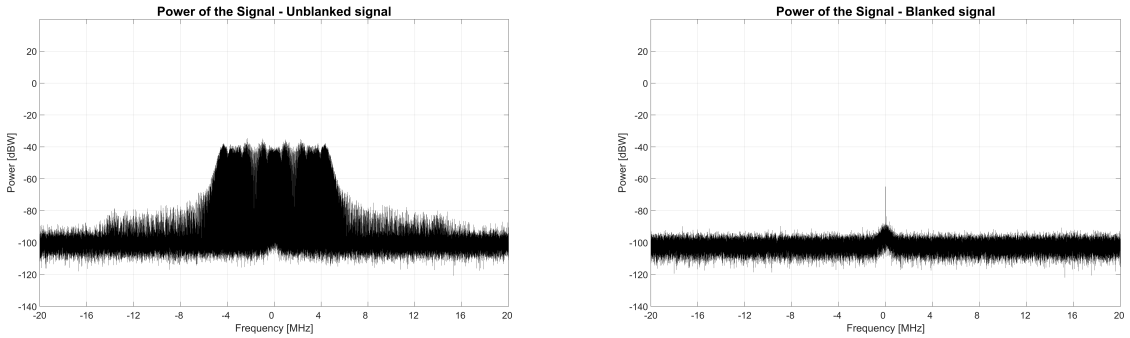


(a) Duty cycle 0.2

(b) Duty cycle 0.6

Figure 7.29: Blanked data of pulsed signals with different duty cycles

In the figure the effect of the PB is seen. Once the signal power exceeds the defined threshold, the signal samples in the I- and Q-phase are set to zero. Because of the constant jammer power, which always exceeds the given threshold (Figure 7.28), whole pulses are blanked and the signal samples are set to zero for the pulse duration. To prove the quality of the PB algorithm, the PSD from the data before and after the blanking can be considered. The PSD of 100 ms of the data during the first interference event is shown in Figure 7.30. On the left, the PSD of the original signal is presented and on the right, the PSD of the blanked signal is presented.



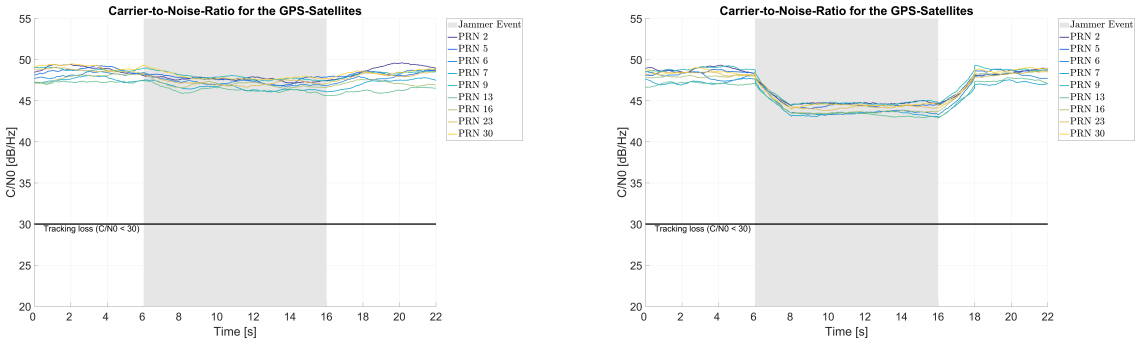
(a) Unblanked data

(b) Blanked data

Figure 7.30: PSD of unblanked (left) and blanked (right) data during the second interference event

In the left part of Figure 7.30, the spectral characteristics of the simulated jammer can be seen. The frequencies between -5 and 5 MHz have an increased magnitude. After the PB the PSD corresponds to the PSD of GPS L1 C/A signal, but with a decreased magnitude. It can be concluded that the PB algorithm is successful, because it zeroises the interfering signal. Because of zeroing of a part of the useful signal, a smaller power of the remaining signal is visible.

The CNR of all GPS satellites during both interference events after applying PB on the data is shown in Figure 7.31.



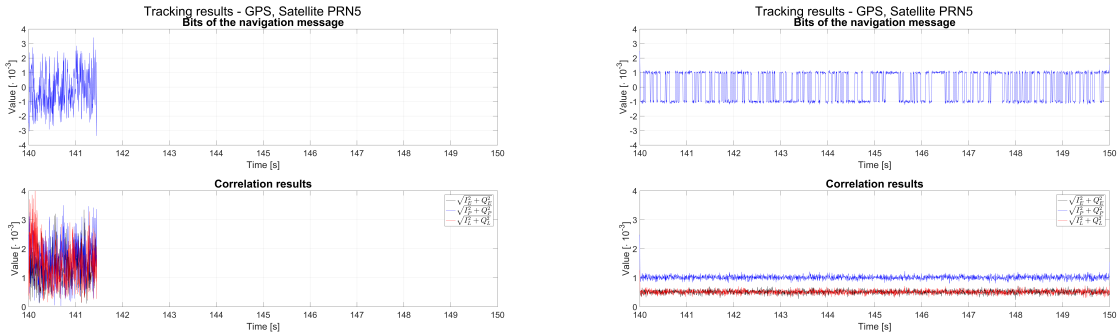
(a) First interferer (DC = 0.2)

(b) Second interferer (DC = 0.6)

Figure 7.31: CNR of the first and second jammer after performing PB on the data

By comparing Figures 7.27 and 7.31, the effect of the PB can be seen. If the interfering signals are removed, the CNR gets greater, the receiver keeps track and a position solution is possible for both jammers. For the first interfering event, the CNR is less than 3 dB lower than the CNR during a non-interference event. The CNR of the second interferer is lower than the CNR of the first interferer. This is caused by a higher DC, thus, a higher amount of signal is zeroed and a smaller amount of useful signal remains.

Afterwards, the tracking results of the GPS satellite PRN 5 during the second interference event, both before and after applying PB on the data, were investigated. The correlator values and the bits of the navigation message are shown in Figure 7.32



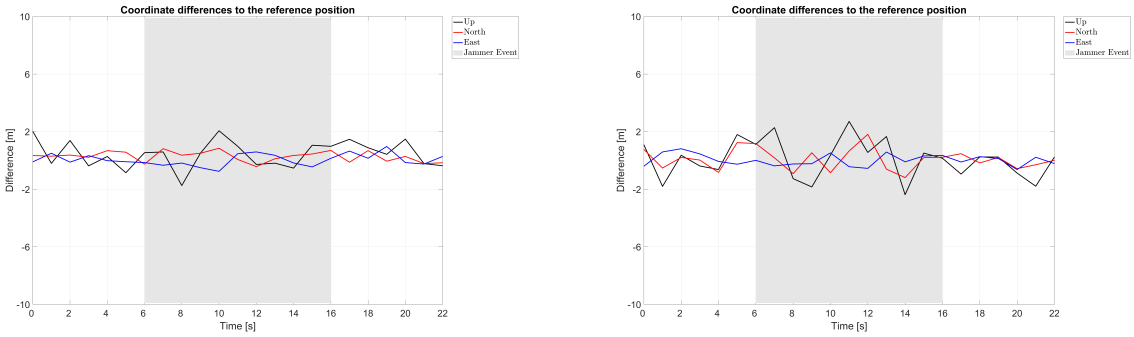
(a) Without PB

(b) With PB

Figure 7.32: Tracking results using different duty cycles with and without applying PB on the data

Due to the jammer characteristics and the high jammer power, the correlator values and the navigation bits get very noisy and the correlators are not well aligned. In many cases, the early or late correlator are higher than the prompt correlator. After a few seconds, the receiver loses track of this satellite because of the bad signal quality. After applying PB on the data, the correlator values become smaller compared to the interference-free event, but it can be seen that the prompt correlator is higher than the other two. The variance of the correlators is much smaller and that the navigation bits are well visible. This provides an accurate pseudorange estimation and a correct parsing of the navigation message.

Finally, the PVT solution was calculated for both jammers with different DCs. The differences to the reference position for the first and the second jammer are presented in Figure 7.33.



(a) Jammer 1 (DC = 0.2)

(b) Jammer 2 (DC = 0.6)

Figure 7.33: Comparison of the PVT solution of pulsed jammer 1 and 2 after applying PB on the data

Without performing PB on the data, the receiver loses track of all satellites during the second jamming event. Because the receiver can still track all satellites during the first interference event, a PVT solution is possible, but, because of the poor signal quality and worse tracking quality, the coordinate differences are higher than during an interference-free event. As seen in Figure 7.31, the PB enables the receiver to keep track of satellites and a PVT solution during both interference events is possible. It can be seen that for the second interferer with a higher DC, the differences to the reference position are greater

than for the first interferer.

Next, the impact of the PW on the PB algorithm and on the signal processing was investigated. The third and the fourth simulated jammers differ only by the pulse width. The pulse width of the third jammer was set to 20 μs and the PW of the fourth jammer is 300 μs. Both jammers have a DC of 0.2.

Figure 7.34 shows 0.2 ms of the raw data during the third interference event.

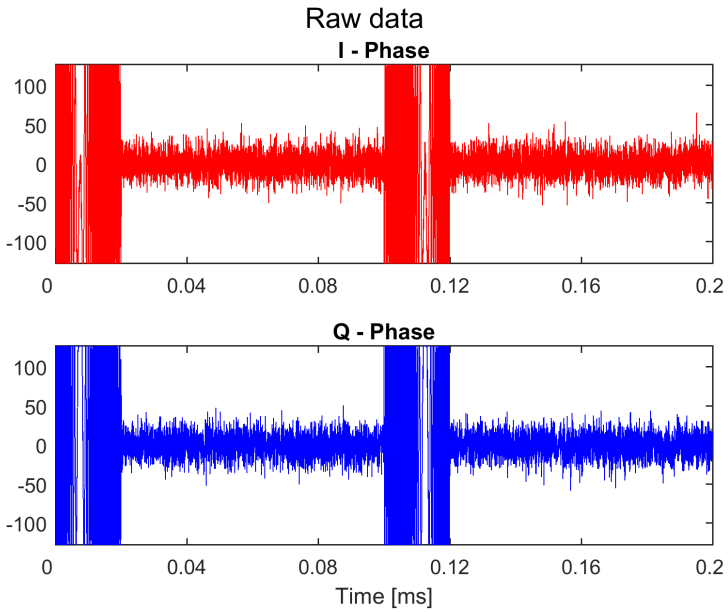
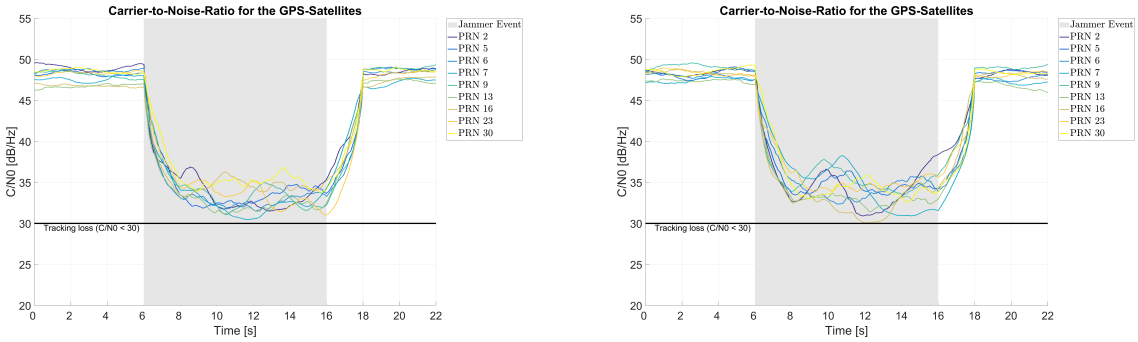


Figure 7.34: I/Q data for the third pulsed interferer event

The appearance of the pulse depends on both parameters, the PW and the DC. A longer PW for the same DC means that the pulse happens less often. The percentage of the time with pulsed signals stays the same. In the presented time period of 0.2 ms two pulses with a PW of 20 μs appear. If the PW would be set to 5 μs, eight pulses would be visible.

In Figure 7.35, the CNR for the third (left) and the fourth (right) interference event without applying PB on the data is shown.



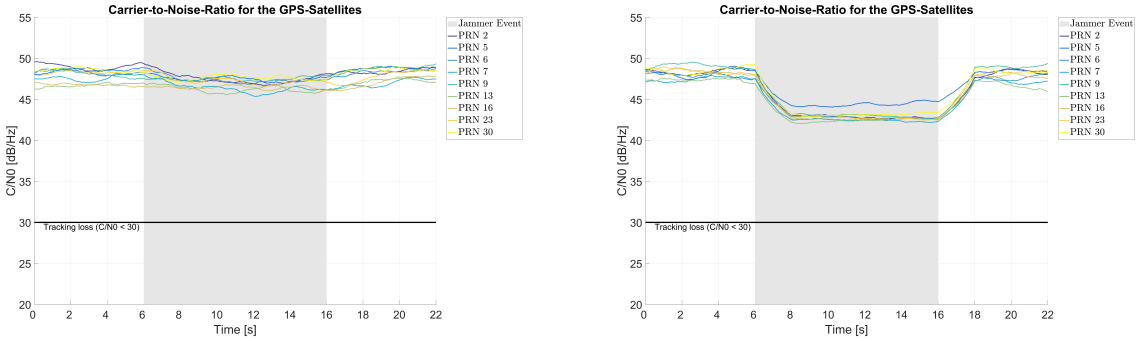
(a) Third interferer (PW = 20 μs)

(b) Fourth interferer (PW = 300 μs)

Figure 7.35: CNR of the third and fourth pulsed jammer without performing PB

When considering the CNR values, no significant impact of the PW on the CNR is seen. The ratio is between 30 and 37 dB/Hz during both interference events. The similar values make sense because of the same duty cycle. A higher PW causes more pulses per second, but the amount of time, covered by pulsed signals, is the same for all PWs. The PW only has an influence on the tracking quality if it is chosen to be close to the integration time.

Figure 7.36 shows the CNR for the third (left) and the fourth (right) interference event after applying PB on the data.



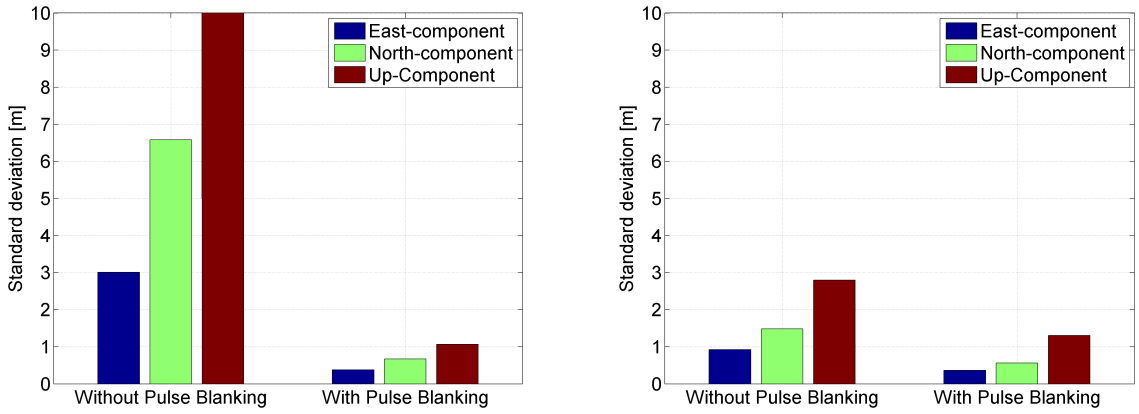
(a) Third interferer (PW = 20 μs)

(b) Fourth interferer (PW = 300 μs)

Figure 7.36: CNR of the third and fourth pulsed jammer after performing PB on the data

The PB increases the CNR of all satellites during both interference events. The CNR is smaller during interference events than during interference-free events, because the PB suppresses a part of the useful signal. When no PB was applied on the data, the CNR shows a constant value during both interference events. After the pulse blanking differences in the CNR between jammers 3 and 4 can be seen. The CNR of the blanked interferer four is clearly lower than the CNR of the blanked interferer three. The reason for it is the pulse width and the PB algorithm.

Last, the PVT solution with and without applying PB on the data was calculated. To evaluate the results, the standard deviations of the coordinate differences to the reference position were calculated. The standard deviations are presented in Figure 7.37.



(a) Third interferer (PW = 20 μs)

(b) Fourth interferer (PW = 300 μs)

Figure 7.37: Standard deviation of the coordinate differences before and after applying the PB on the data

Although no markable differences of the CNR between the third and fourth interference event without PB are seen, differences in the standard deviation of the coordinate differences occur. The standard deviation if higher for the fourth interference event. The highest standard deviation occurs in the up-component (10.2 m) during the fourth interference event. Pulse blanking increases the accuracy of the PVT solution. During the fourth interference event, the standard deviation of the up-component decreases to 1.0666 m, which is very important in case of applications with a high accuracy demand. After the PB, no markable difference between the two scenarios occur.

7.2 Real-world data

In the previous section it was shown that the presented mitigation strategies can be applied on jamming signals with different spectral, time, frequency/amplitude characteristics and different jamming power. All of the presented signals were simulated using the software GIPSIE®. In this section, the impact of mitigation strategies on real-world recorded data is presented.

The jamming signals were recorded on 4.10.2017 at the Truppenübungsplatz Seetaler Alpe in the western part of Styria, Austria. As GNSS interference is illegal in the European Union, all tests were performed under a valid certificate of exemption by the Supreme Telecommunication Authority (OFB) from the Austrian Ministry for Transport, Innovation and Technology (BMVIT). For the campaign, different jammers were used. All of them are SCW jammers and are available on the internet. Two of them are cigarette lighter jammers, the other three have a power supply and can be used everywhere, either inside or outside a car. The used jammers are shown in Figure 7.38.

Figure 7.38: Jammers used for the test measurements

The measurements were performed at different distances between the jammer and the receiver. The distance is highly correlated to the received jammer power. For the evaluation, two distances were chosen: 150 and 300 m. Table 7.5 summarizes the recording settings.

Table 7.5: Properties of the performed measurements

Simulation duration:	305 s
Sampling frequency (f_s):	40 MHz
Intermediate frequency (f_{IF}):	0 MHz
Number of quantization bits:	8 (256 different values)
Activated AGC:	Yes
Visible GPS satellites	PRN 5, 7, 13, 15, 20, 28, 30
Visible Galileo satellites:	PRN 7, 19, 20, 30

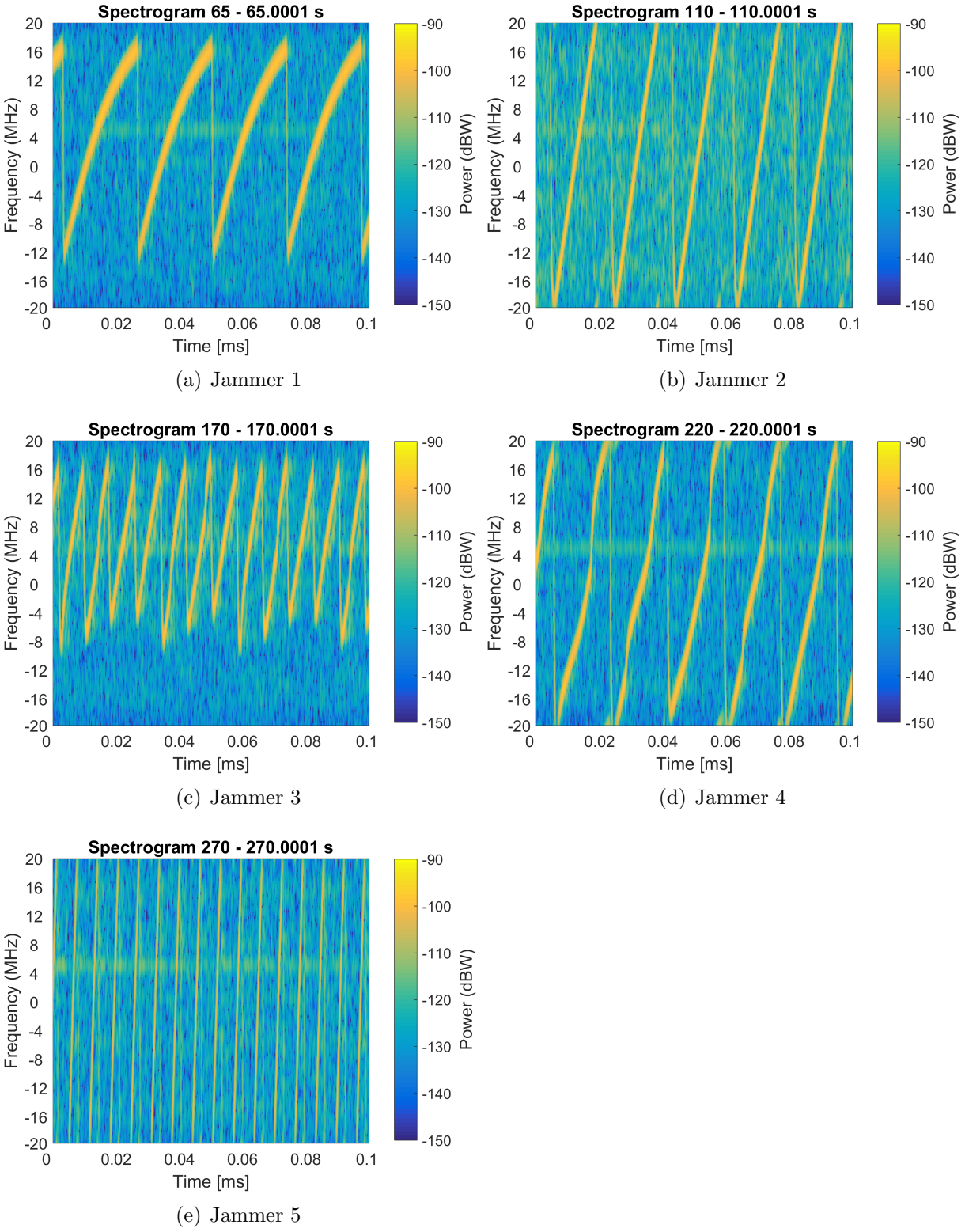
Table 7.6 provides information on the characteristics of the used jammers. The characteristics were determined using the Gaims software. The interference classification and the estimation of jammer parameters were implemented by Bartl (2014).

Table 7.6: Characteristics of the used jammers

	Jammer 1	**Jammer 2**	**Jammer 3**	**Jammer 4**	**Jammer 5**
Duration	$\sim$ 24 s	$\sim$ 23 s	$\sim$ 20 s	$\sim$ 20 s	$\sim$ 20 s
Central frequency [MHz]	2.3	0	5.45	0	0
Bandwidth [MHz]	30.625	> 40	24.75	40	> 40
Sweep duration [μs]	23	19	7.4	18	6.5

All of the jammers can be classified as WBI jammers and have a continuous behaviour. The latter means that the ANF has to be applied on them for mitigation. Three of the interferers are spread over the whole spectrum.

Figure 7.39 shows the spectrograms of all used jammers. The calculation of the STFT was performed using a window length of 0.8 μs and a overlap period of 0.2 μs.



(a) Jammer 1

(b) Jammer 2

(c) Jammer 3

(d) Jammer 4

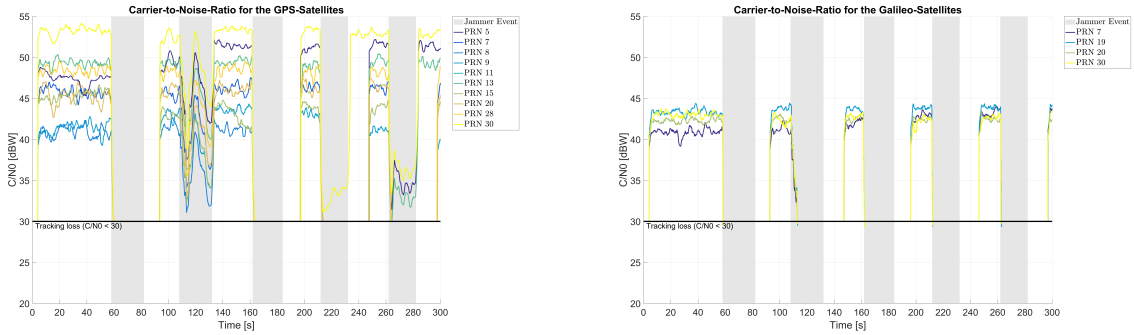
(e) Jammer 5

Figure 7.39: Spectrograms of the used jammers

The jammer frequency of the jammer 1 is not rising linearly, but shows a certain curvature when reaching the positive maxima. In this region, the jamming signal also has a larger standard deviation. Jammer 2 is a wideband jammer and exceeds the bandwidth of the

RFFE (40 MHz). Because the AGC reacts very slowly on changes of the received signal power (which decreases when the jammer does not effect the GNSS frequency band), a pulsed effect in the raw data is visible. The signal of jammer 2 shows a linear behaviour. Jammer 3 has the smallest bandwidth of all tested jammers. It shows a linear frequency behaviour, but the frequency of the jammer is not stable. Especially the lower jamming frequencies vary for more than 5 MHz. Jammer 4 and 5 show similar properties. Both of them are spread over the whole bandwidth. The bandwidth of the jammer 5 is much larger than 40 MHz and disturbs other frequency bands as well. The frequency of the jammer 5 increases linearly with a constant standard deviation, while jammer 4 shows variations in the standard deviation. The frequency of jammer 4 increases as a hysteresis function. It can be concluded that the presented jammers have similar properties. All of them are SCW jammers, affecting the L1 band. They use cheap components, causing variations of the minimal/maximal jamming frequencies, hysteresis functions or different standard deviations in the jamming frequencies.

First, the signal was processed without applying the ANF on the data when detecting interference. The CNR estimator, calculated from the correlator outputs for the whole time period and for GPS and Galileo, is presented in Figure 7.40.



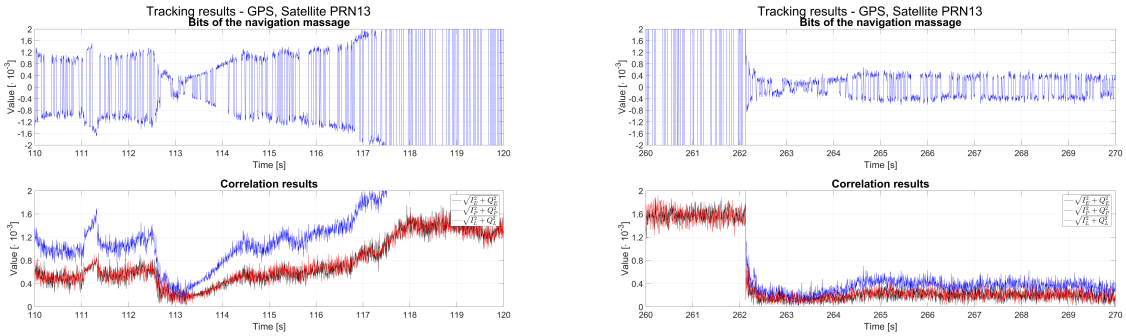
(a) GPS

(b) Galileo

Figure 7.40: Calculated CNR when processing the measured data

The CNR for GPS satellites is higher than for Galileo satellites. The CNR during a interference-free event varies for GPS satellites between 40 and 54 dB/Hz and for Galileo between 40 and 45 dB/Hz. As mentioned in Section 4.4, the carrier-to-noise ratio depends on different parameters. The most probable reason for such high variations is the elevation angle of the satellites. Jamming causes a loss of tracking of all Galileo satellites. For the GPS satellites, the tracking to all satellites is only continued during interference event 2. Some satellites keep track also during interference event 4 and 5. The reasons, why the receiver does not lose tracking, may be the jamming power and the jammer characteristics. In most cases, the lock is kept for the satellites with a higher CNR.

The correlator values and the bits of the navigation message to the GPS satellite PRN 13 during interference event 2 and interference event 5 are presented in Figure 7.41.



(a) Interference 2

(b) Interference 5

Figure 7.41: Correlator values and navigation bits for GPS PRN 13 during two interference events

The correlators show varying behaviour. In particular, the values during interference event 2 show large variations. At epoch 113 s, the prompt correlator is almost as big as the early and late correlator, and the navigation bits are very small. At this point, the CNR is also very small and comes very close to the value 30 dB/Hz and almost a loss of tracking occurs. Four seconds later, the square of the in- and quadrature-phase value and the navigation bits exceed the plot limits. For this time period a high CNR is also visible. The possible reason for such varying behaviour is the varying jamming power, caused by low-cost oscillators in the jammer.

Finally, the PVT solution was calculated without applying the ANF on the data. The coordinate differences to the reference position for the whole dataset are shown in Figure 7.42.

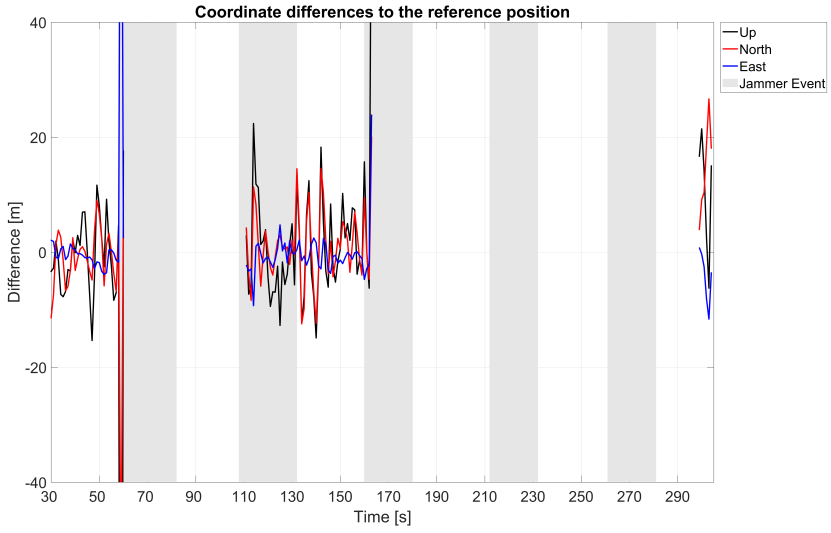
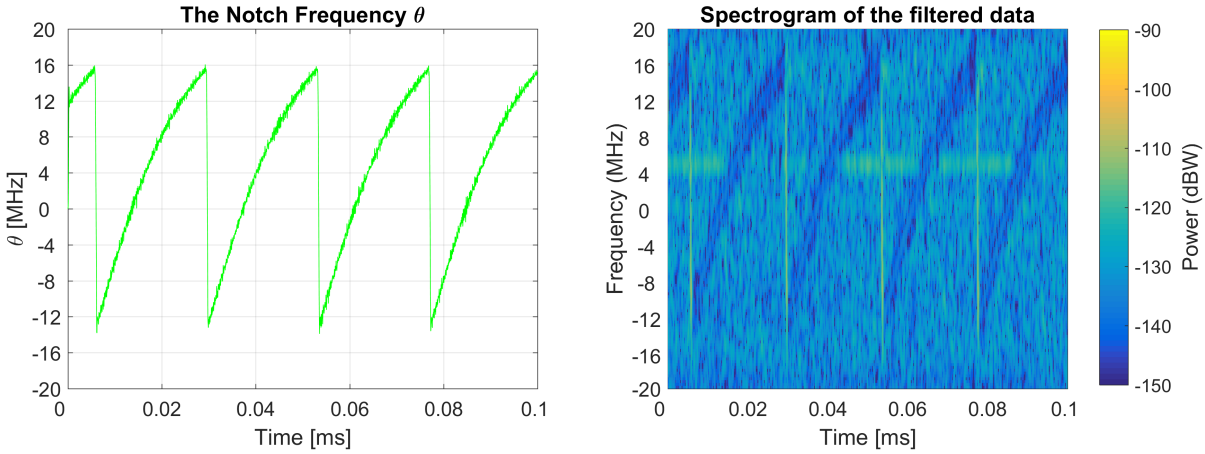


Figure 7.42: Navigation solution for the real dataset without applying ANF on the data

Because the receiver loses track of almost all satellites during jamming events 1, 3, 4 and 5, no PVT solution is available at these epochs. During interference event 2, a PVT solution is possible, but showing higher coordinate differences. The coordinate differences to the reference position are much higher as in the case of the simulated jammers. The

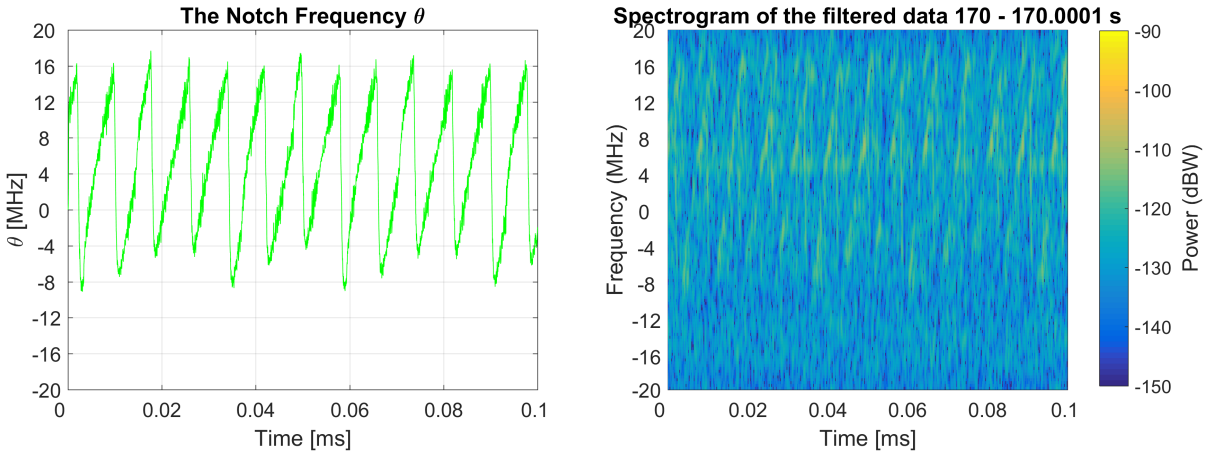
reason can be found in the atmosphere or in the multipath effect, which cause delays in the pseudorange estimation.

In a next step, the ANF was applied on the data. Many combinations of input parameters were applied on the raw data and many of them mitigated the interfering signal at all. As the optimum solution, the combination $\lambda = 0.3$ and $B = \pi/3$ was chosen. Figures 7.43 and 7.44 show the notch frequency parameter and the spectrogram of the filtered data of the jammers 1 and 3.



(a) Notch frequency θ (b) Spectrogram

Figure 7.43: Notch frequency and the spectrogram of the filtered data after applying the ANF on the SCW jammer 1



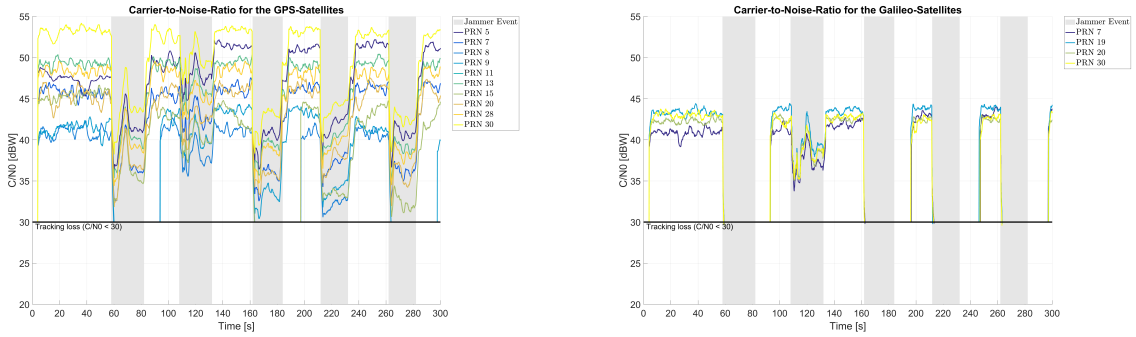
(a) Notch frequency θ (b) Spectrogram

Figure 7.44: Notch frequency and the spectrogram of the filtered data after applying the ANF on the SCW jammer 3

In both cases, the notch frequency parameters follow the interfering frequency. In the case of the interferer 1, the higher standard deviation of the jammer at the maximum frequency causes higher variations of the notch frequency. The small forgetting factor produces fast

changes on frequency sweeps and the attenuation bandwidth of $\pi/3$ causes suppression of the whole jamming signal.

After applying the ANF on the data the signal was processed. Figure 7.45 shows the CNR for the GPS and Galileo satellites.



(a) GPS (b) Galileo

Figure 7.45: Calculated CNR after applying the ANF on the real data

If the ANF is activated, the receiver keeps track of almost all GPS satellites. But nevertheless, the CNR is smaller as for the interference-free event. The receiver loses tracking of some GPS satellites despite the ANF. It loses tracking of two GPS satellites during jamming events 1, 3 and 5. During jamming events 2 and 4, no GPS satellites are lost. The tracking is mostly lost to satellites with a small elevation and a small CNR before the jamming. The tracking was lost to all Galileo satellites, which also had a lower CNR.

In Figure 7.46, the tracking results (correlator values, bits of the navigation message) of the GPS satellite with the PRN 30 at the beginning of the interference event 3 are presented.

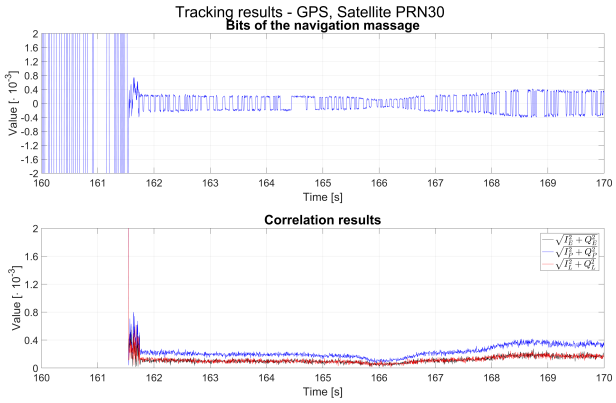


Figure 7.46: Tracking results after applying the ANF on the jammed data for the GPS satellite PRN 30

Note that the jammer was activated at about 161.4 s. In the first 1.4 s of this representation, no interference was present. If the ANF is applied on the data, the receiver keeps track. The correlator values are much smaller as without interference. The prompt correlator is higher as the early and the late correlators, which have similar values. The only exception is a few milliseconds after activating the jammer. There might be two reasons for such behaviour. First, shortly after activating the jammer, the jamming power may be higher than afterwards. As seen in the previous sections, the jamming power is an important parameter for the signal quality. Secondly, the jamming was not yet detected and the ANF was not activated.

In a final step the PVT solution was calculated. The coordinate differences to the reference position are shown in Figure 7.47.

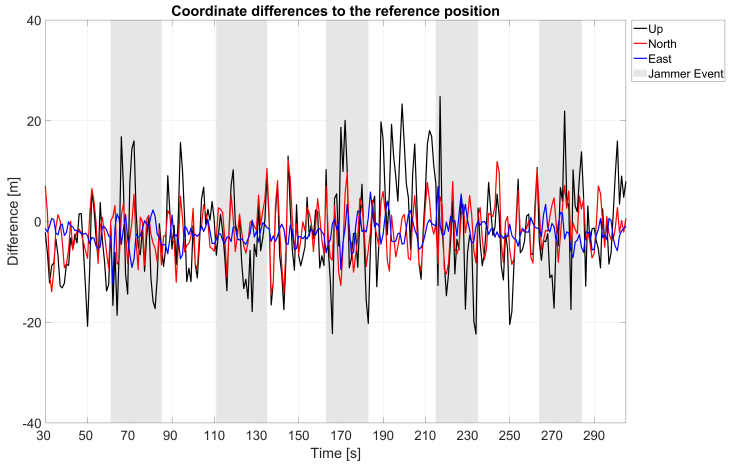


Figure 7.47: Navigation solution for the real dataset after applying the ANF on the data

Because at every epoch tracking of at least four satellites is ensured, a PVT solution over the whole measurement period can be calculated. Because of the atmospheric influences and multipath, the variances of the coordinate differences are higher than for the simulated data. The smallest variations appear in the east component. The biggest variations are seen, as usual in the GNSS, in the up-component because of the satellite geometry. During

the interference events, higher variations of the coordinate differences appear. The higher variations are strongly connected to the quality of the tracking stage and to the number of visible satellites.

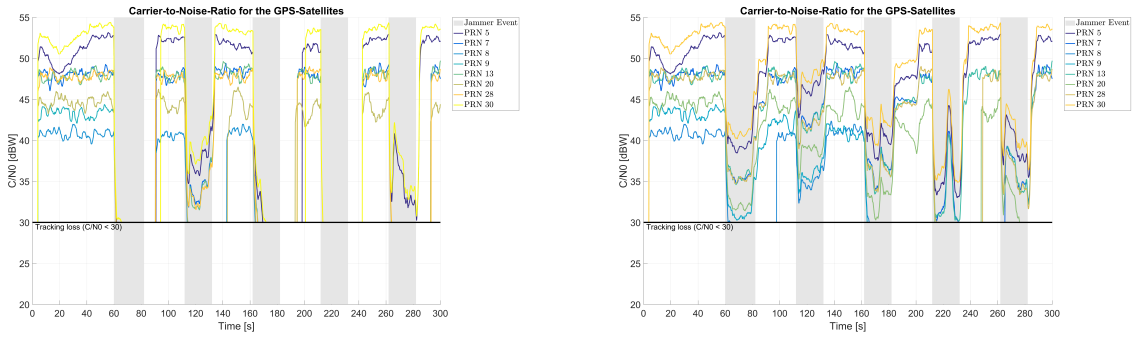
For evaluation, the mean difference to the initial position and the standard deviation during the single jamming events and for the interference-free case were calculated. The values are listed in Table 7.7:

Table 7.7: Deviation from the reference position and standard deviation of the coordinate differences

	μ_E [m]	μ_N [m]	μ_U [m]	σ_E [m]	σ_N [m]	σ_U [m]
Interference-free	0,0	0,0	0,0	2,7	5,0	7,8
Interference 1	-3,2	-2,3	-2,5	3,0	4,2	9,9
Interference 2	-3,1	-1,2	-4,8	1,4	5,8	8,0
Interference 3	-1,7	-1,9	-0,5	3,5	5,8	10,5
Interference 4	-0,9	-2,2	-6,6	2,3	5,2	7,4
Interference 5	-3,4	0,6	0,0	2,4	4,3	10,1

The mean value for the interference-free event equals zero because the mean value over the non-interference events is used for the calculation of the reference position. During the interference events, the standard deviation of the differences to the reference position increases. The mean difference to the reference position increases too. This is highly correlated to the smaller amount of useful signal and to a smaller CNR.

Finally, the dataset with a smaller distance between interferer and the receiver (150 m) was processed and evaluated. The distance is highly correlated to the jamming power. Figure 7.48 shows the CNR of all GPS satellites without (left) and with (right) applying ANF on the data.



(a) Without ANF

(b) With ANF

Figure 7.48: Calculated CNR when processing the measured data with a distance of 150 m

If jamming is activated, the tracking of all satellites during the interference events 1, 3, 4 and 5 is lost. This disables the calculation of the PVT solution. Furthermore, it is visible that during interference event 2, the receiver loses some GPS satellites. For a smaller jammer power, the tracking of all GPS satellites was kept (c.f. Figure 7.40). Once the ANF is applied on the data during an interference event, the most GPS satellites are kept

in tracking. The smaller distance between the jammer and the receiver causes a smaller CNR during almost every jamming event. But the biggest difference between the two measured datasets can be seen during interference event 4. In the case of the distance 300 m, no satellites were lost if applying the ANF on the data. For the distance of 150 m, the receiver loses its lock on four satellites. The receiver was able to track only three remaining satellites, which is not enough for a PVT solution.

The navigation solution after applying the ANF on the data is shown in Figure 7.49.

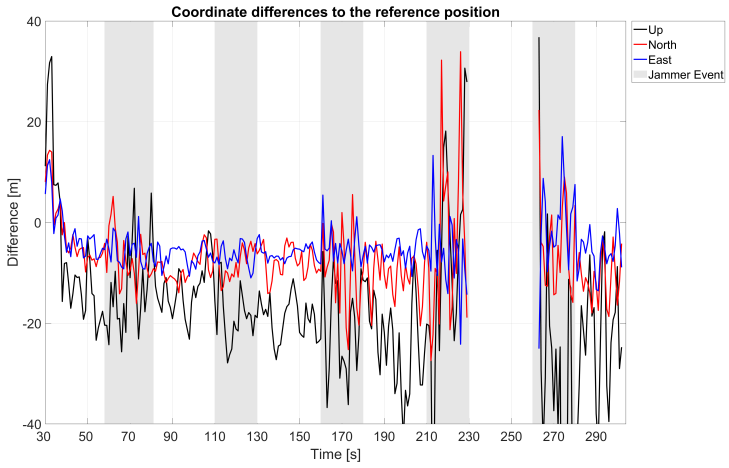


Figure 7.49: Navigation solution for the dataset 150m after applying the ANF on the data

Note that if the ANF was not applied on the data, the position solution was possible only before the first interference event and during the second interference event. During the other interference event, no position solution was possible, because the receiver lost tracking to almost all satellites. If applying the ANF on the jammed data, the navigation solution is possible for most of the interferers. The only exception is at the end of interference 4. As mentioned above, the receiver kept track of only three satellites, which disables the calculation of the PVT solution till a reacquisition is performed. It is visible, that during the interference events the difference to the reference position is higher as during an interference-free event. If comparing Figures 7.47 and 7.49 the variances to the reference position is higher for a smaller jammer-receiver distance. It can be concluded that the jammer power is an important parameter for mitigating interference.

8 Conclusions and outlook

This thesis focuses on the impact of different jamming signals on the GNSS signals and the impact of jamming signals on the signal processing. Furthermore, it investigates different mitigation strategies to overcome jamming attacks.

The usage of global navigation satellite systems and the associated permanent availability of position and time measurement become more and more a matter in many areas of everyday life. The GNSS services are used in many applications. Studies show that the number of GNSS applications and GNSS users is increasing rapidly. Therefore, it is important to not only consider the opportunities, but also the weaknesses of satellite based position and time determination. The GNSS signals are vulnerable to interference because of the low signal power which lies below the thermal noise floor. In the last few years years many interference attacks (civil and military) were reported. While unintentional interference is of minor concern, intentional interference, such as jamming, spoofing or meaconing, can have severe impacts on the application, especially on safety-critical applications. The goal of GNSS receivers should be the detection of interference, followed by mitigation of the interfering signal.

The thesis starts with an overview of the satellite-based navigation and of existing GNSS, tailored to GPS and Galileo. Afterwards, a brief introduction to the software-defined receiver is provided. The main functional blocks are described in detail and the basics of the signal processing are given. Afterwards, the focus was put on interference. First, unintentional interference, which is divided into natural interference, intra-system and inter-system interference, multipath and external interference. Then the thesis focuses on intentional interference which represents a deliberate attack on the GNSS signal. It is dangerous, because the signal is transmitted to the receiver intentionally to cause an erroneous position or prevent the receiver to calculate a PVT solution. According to literature the intentional interference is divided into jamming, spoofing and meaconing. This master thesis deals with jamming signals. Jamming is the masking of GNSS signals with noise. It has become a serious threat, because jammer can be bought on diverse websites for a cheap price, although jamming is illegal in the whole European Union. Jammer can be classified based on different properties like bandwidth, spectral features or amplitude and frequency behaviour. Furthermore, special types of jamming, like pulsed interference, additional white Gaussian noise jamming or PRN jamming exist. Afterwards, the impact of jamming on the main functional blocks of a software-defined receiver was presented in detail. Starting with the impact on two stages of the radio frequency front end the impact of jamming signals on the acquisition and tracking stage, on the carrier-to-noise ratio and on the PVT solution are explained. Jamming may have a fatal impact on the receiver. It causes a saturation of the ADC, it causes erroneous acquisition results or prevents the receiver of performing acquisition, it lowers the CNR, causes higher variance

of the tracking correlators or a loss of tracking. This may cause an inaccurate PVT solution or a denial of the PVT solution. Afterwards, detection strategies, which are divided into pre- and post-correlation strategies, are discussed. The jamming detection is a prerequisite for mitigation. In a next step, some state-of-the-art jamming mitigation strategies in the frequency domain, in the time domain and in the space-time domain, are explained in detail. Since for the space-domain techniques a complex hardware is needed, only the other two techniques were addressed in this thesis. Two different techniques - adaptive notch filtering and pulse blanking – are investigated in more detail. The adaptive notch filtering works in the frequency domain. It is characterized by a big passband frequency response and a narrow portion of rejection spectrum. The adaptive notch filter consists of an adaptive unit which estimates the varying jamming frequency and tries to follow and remove it over time. In the thesis two solutions of the ANF - for real and complex signals - were implemented. Pulse blanking is a mitigation strategy in the time domain. It is mainly used for mitigating pulsed interference. Based on thresholding interfering signals are detected and the affected signal samples are set to zero. For performing the investigations the real and complex solution of the ANF were implemented into existing software. For the realization a Matlab implementation of the software-defined receiver and Gaims, a software developed by Teleconsult Austria, were used. The Matlab implementation was used for testing, while the Gaims software was used to assess the impact of the mitigation strategies. The pulse blanking was implemented in Matlab. For the pulse detection the signal power was used, which is calculated based on the signal samples. After blanking the jamming signals the data was processed using the Gaims software. To perform pulse blanking pulsed interference had to be implemented into the software GIPSIE®, a software developed by TeleConsult Austria.

First, the ANF and the PB were performed on simulated data. For generating the IF signals, containing GPS L1 C/A and Galileo E1B signals, the software GIPSIE® was used. The software is also capable of simulating jamming signals. For the evaluation of the ANF five different continuous jammers were simulated. Two of them were SCW jammers, two of them FM jammers and the last simulated jammer was an AM jammer. The SCW jammers differed by the sweep bandwidth, the FM jammers differed by the modulation frequency. All of them were wide-band interferer, spread over the whole front-end spectrum. The AM jammer was simulated to prove, that the adaptive notch filter can follow jamming signal with a constant frequency as well. For comparison, all jammers had the same power. The ANF showed good performance on mitigating continuous signal. It estimates the interfering frequency and filters it out. The choice of the input parameters of the ANF, the forgetting factor and the attenuation bandwidth, was very important. A lower forgetting factor reacts faster on frequency changes which is very important in case of a fast sweeping jammer. A higher forgetting factor reacts slowly on frequency changes but enables a stable notch frequency estimation. A higher value can be used for mitigating an AM jammer. The attenuation bandwidth should be high enough to mitigate the whole interfering signal, but low enough not to mitigate a huge amount of useful signal. The filtering of a jammed signal reduces the noise level of the signal and causes an increase of the CNR and better tracking results. In many cases it prevents the receiver from losing lock to the satellites and enables a calculation of the PVT solution. The limitating factors of the ANF are the sweep bandwidth and the modulation frequency. For evaluation of the PB algorithm four different pulsed interferer were simulated. All of them were SCW interferer with a

constant power. The first two jammers differed by the duty cycle of the pulsed signal, the third and the fourth jammer differed by the pulse width. The PB algorithm showed good results for mitigating pulsed interference. After the interfering signal was removed from the useful signal, the receiver was able to track the satellites and calculate a more accurate PVT solution. The main problem of PB is the pulse detection. In the simulated case the power was set relatively high to detect it easily. If the power is set lower, the amount of interfering signals, exceeding a threshold, is smaller and the receiver calculates a PVT solution with an interfering signal.

Afterwards, the performance of the algorithms was tested on real-world jamming signals. The jamming signals were recorded at the military training ground Truppenübungsplatz Seetaler Alpe in the western part of Styria, Austria. The measurements were performed under a valid certificate of exemption by the Supreme Telecommunication Authority (OFB) from the Austrian Ministry for Transport, Innovation and Technology (BMVIT). The measurements were performed with different distances between the jammer and the receiver. The distance highly correlates with the received signal power. In this work two distances were considered. For the campaign five different jammers were used. All of them were SCW jammers. By applying the previously mentioned mitigation strategies to the real-world data it was shown that the strategies show a good performance as well. The limiting factor of the mitigation strategies is the jamming signal power. Once the jamming power gets too high, the amount of the useful signal gets too low and it is not possible anymore to track the signal successfully after mitigation.

For future work the implemented algorithms will be refined and further tested. An automatic computation of the forgetting factor and the attenuation bandwidth, needed for a successful and autonomous mitigation, will be implemented and will be based on the spectral characteristics of the signal. Furthermore, the mitigation of two other interference types (PRN jamming and AWGN jamming) should be developed and evaluated. In literature another time domain technique is described - interference cancellation. This algorithm estimates the pulse characteristics, predicts the pulse position and suppresses it. In the future this algorithm should be implemented and evaluated for pulsed signals. The parameter estimation based on the incoming signal power, as used in this work, seems to be a plausible approach.

List of Figures

2.1 Principle of the satellite-based navigation 5
2.2 The principle of the position estimation in 2D space 6
2.3 Components of the satellite signal 8
2.4 GPS and Galileo signal structure 8
2.5 PSD of the GPS L1 C/A and Galileo E1B signals 10

3.1 Structure of a software-defined GNSS receiver 11
3.2 Raw data with and without activated AGC 13
3.3 Histogram of the input data with (right) and without (left) activated AGC 13
3.4 The acquisition results for two GPS satellites 14
3.5 Basic structure of a Costas loop 15
3.6 The basic principle of a DLL 16
3.7 Tracking results in case of tracking GPS L1 C/A (left) and Galileo E1B (right) signals 18

4.1 Frequency and amplitude characteristics of a CW jammer 24
4.2 Frequency and amplitude characteristics of a SCW jammer 24
4.3 Frequency and amplitude characteristics of a FM jammer 25
4.4 Frequency and amplitude characteristics of an AM jammer 26
4.5 I/Q data after ADC with different jammer powers 27
4.6 Histogram of interfered signal (jammer power $-110\ dBW$ without activated AGC) 28
4.7 I/Q data during an interference event with avtivated AGC 29
4.8 Pulsed interference with and without using an AGC 29
4.9 Acquisition results during a jamming event with different jamming signal powers 30
4.10 Different tracking results during interference events 32
4.11 Behaviour of the CNR during an interference event 33
4.12 Difference between estimated position and reference position with (right) and without (left) interference 34

5.1 The Power spectral density in case of an interference-free event and in case of WBI 36
5.2 The frequency response of a NF 39
5.3 The structure of an ANF 40
5.4 Structure of the complex ANF 41
5.5 Structure of the real ANF 42
5.6 Basic principle of FDAF 44
5.7 I/Q samples before and after pulse blanking 46

6.1 Flow chart of the GNSS receiver, implemented by Borre et al. (2007) . . . 48
6.2 Graphical user interface of the software GaimsGUI 49
6.3 Flow chart of the jamming mitigation strategies, implemented in the software Gaims 50
6.4 Graphical user interface of GUI version of GIPSIE 51
6.5 Flow chart of the implemented ANF in the SDR 52
6.6 Flow chart of the validation of pulsed interference 54
6.7 Flow chart of the validation of pulsed interference 54
6.8 Flow chart of the pulse blanking algorithm 55

7.1 Spectrograms of the simulated jammers 58
7.2 Estimated CNR for GPS and Galileo when processing the simulated jammer 1 59
7.3 Tracking results during the first simulated interference event for the GPS satellite PRN 5 60
7.4 Navigation solution during the simulated jamming event 1 without applying the ANF on the data 60
7.5 Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 1 ($\lambda = 0.3$, $B = \pi/50$) 61
7.6 Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 1 ($\lambda = 0.9$, $B = \pi/3$) 62
7.7 Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 1 ($\lambda = 0.3$, $B = \pi/3$) 62
7.8 Frequency response of the ANF with two different attenuation bandwidths B 63
7.9 Calculated CNR after applying the ANF on the data 64
7.10 Tracking results during the first simulated interference event for the GPS satellite PRN 2 64
7.11 Navigation solution for jammer 1 after applying the ANF on the data . . . 65
7.12 Spectogram of the filtered data of the simulated jammer 2 after applying the ANF on the data ($\lambda = 0.3$, $B = \pi/3$) 66
7.13 Calculated CNR during the jamming event 2 before and after applying ANF on the data 66
7.14 CNR of GPS satellites during the simulated jammer 3 without applying the ANF on the data 67
7.15 Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 3 ($\lambda = 0.3$, $B = \pi/3$) 68
7.16 Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 3 ($\lambda = 0.3$, $B = \pi/10$) 68
7.17 Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 3 ($\lambda = 0.9$, $B = \pi/5$) 69
7.18 CNR of GPS satellites during the simulated jammer 3 after applying the ANF on the data 70
7.19 CNR of GPS satellites during the simulated jammer 4 without applying the ANF on the data 70
7.20 The notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 4 ($\lambda = 0.3$, $B = \pi/3$) 71
7.21 CNR of GPS satellites during the simulated jammer 4 after applying the ANF on the data 72

7.22 Estimated CNR of the AM interferer without applying ANF on the data . 73
7.23 Notch frequency and the spectrogram of the filtered data after applying the ANF on the simulated jammer 5 74
7.24 Estimated CNR of the AM interferer after applying ANF on the data . . . 74
7.25 Raw data of pulsed signals with different duty cycles 76
7.26 Spectrograms of pulsed signals with different duty cycles 76
7.27 CNR of the first and second pulsed jammer without performing PB 77
7.28 Estimated signal power 77
7.29 Blanked data of pulsed signals with different duty cycles 78
7.30 PSD of unblanked (left) and blanked (right) data during the second interference event 79
7.31 CNR of the first and second jammer after performing PB on the data . . . 79
7.32 Tracking results using different duty cycles with and without applying PB on the data 80
7.33 Comparison of the PVT solution of pulsed jammer 1 and 2 after applying PB on the data 80
7.34 I/Q data for the third pulsed interferer event 81
7.35 CNR of the third and fourth pulsed jammer without performing PB 82
7.36 CNR of the third and fourth pulsed jammer after performing PB on the data 82
7.37 Standard deviation of the coordinate differences before and after applying the PB on the data 83
7.38 Jammers used for the test measurements 84
7.39 Spectrograms of the used jammers 86
7.40 Calculated CNR when processing the measured data 87
7.41 Correlator values and navigation bits for GPS PRN 13 during two interference events 88
7.42 Navigation solution for the real dataset without applying ANF on the data 88
7.43 Notch frequency and the spectrogram of the filtered data after applying the ANF on the SCW jammer 1 89
7.44 Notch frequency and the spectrogram of the filtered data after applying the ANF on the SCW jammer 3 89
7.45 Calculated CNR after applying the ANF on the real data 90
7.46 Tracking results after applying the ANF on the jammed data for the GPS satellite PRN 30 91
7.47 Navigation solution for the real dataset after applying the ANF on the data 91
7.48 Calculated CNR when processing the measured data with a distance of 150 m 92
7.49 Navigation solution for the dataset 150m after applying the ANF on the data 93

List of Tables

2.1 GPS frequency bands 9
2.2 Galileo frequency bands 9

7.1 Properties of simulated IF signals 57
7.2 Characteristics of the simulated jammers 57
7.3 Parameters of the simulated SCW jammers with pulsed behaviour 75
7.4 Characteristics of the simulated pulsed jammers 75
7.5 Properties of the performed measurements 85
7.6 Characteristics of the used jammers 85
7.7 Deviation from the reference position and standard deviation of the coordinate differences 92

Bibliography

Arienzo L (2010): RF Interference Vulnerability Assessment for GNSS receivers. In: JRC scientific and technical report. DOI: 10.13140/RG.2.2.29051.52002.

Bartl SM (2014): GNSS Interference Monitoring - Detection and classification of GNSS jammers. Master thesis, Institute of Navigation, Graz University of Technology, Austria.

Berglez P (2013): Development of a multi-frequency software-based GNSS receiver. PhD dissertation, Institute of Navigation, Graz University of Technology, Austria.

Borio D, Camoriano L, Presti LL (2008): Two-Pole and Multi-Pole Notch Filters: A Computationally Effective Solution for GNSS Interference Detection and Mitigation. In: IEEE Systems Journal 2(1): 38-47.

Borio D, Cano E (2012): Evaluation of GNSS Pulsed Interference Mitigation Techniques Accounting for Signal Conditioning. In: Proceedings of the European Navigation Conference 2012. Gdansk, Poland.

Borre K, Akos DM, Bertelsen N, Rinder P, Jensen SH (2007): A software-defined GPS and Galileo receiver, a single-frequency approach - applied and numerical harmonic analysis. Birkhäuser, Boston Basel Berlin.

Burrus CS, Frigo M, Johnson SG, Pueschel M, Selesnick I (2012): Fast Fourier Transforms. CONNEXIONS, Houston, Texas.

Deshpande SM (2004): Study of Interference Effects on GPS Signal Acquisition. Master thesis, Department of Geomatics Engineering, University of Calgary, Canada.

Dovis F (2015): GNSS Interference Threats and Countermeasures. Artech House, Boston London.

European Commision (2016): Galileo open service. Signal in space interface control document (OS SIS ICD). Issue 1.3, September. Available at www.gsc-europa.eu/system/files/galileo_documents/.

European Commision (2018): Galileo System Services. More information on www.gsa.europa.eu/galileo/services.

Falletti E, Pinni M, Presti LL (2010): GNSS Solutions: Carrier-to-Noise Algorithms. In: Inside GNSS 2010(01): 20-27.

Giordanengo G (2009): Impact of Notch Filtering on Tracking Loops for GNSS Applications. PhD dissertation, Faculty of Information Engineering, Politecnico di Torino, Italy.

Hegarty C, Dierendonck AJ Van, Bobyn D, Tran M, Kim T, Grabowski J (2000): Suppression of pulsed interference through blanking. In: Proceedings of the IAIN World Congress and the 56th Annual Meeting of The Institute of Navigation (2000), San Diego, California, June 26 - 28: 399 - 408.

Hofmann-Wellenhof B, Legat K, Wieser M (2003): Navigation: Principles of Positioning and Guidance. Springer, Wien New York.

Hofmann-Wellenhof B, Lichtenegger H, Wasle E (2008): GNSS - Global Navigation Satellite Systems: GPS, GLONASS, Galileo and more. Springer, Wien New York.

Jost T, Weber C, Schandorf C, Denks H, Meurer M (2008): Proceedings of the Radio interference effects on commercial GNSS receivers using measured data. In: 2008 IEEE/ION Position, Location and Navigation Symposium,Monterey, California, May 5-8: 459 - 467.

Kaplan ED, Hegarty CJ (2006): Understanding GPS: Principles and Applications. 2nd Edition. Artech House, Boston London.

Karaim M, Elghamrawy H, Tamazin M, Noureldin A (2017): Investigation of the effects of White Gaussian Noise jamming on commercial GNSS receivers. In: Proceedings of the 12th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt , December 19-20: 468-472.

Kemetinger A., Hinteregger S., Berglez P. (2013): GNSS Interference Analysis Tool. In: Proceedings of the European Navigation Conference 2013, Vienna, Austria, April 21-23.

Khan NA, Jafri MN, Qazi SA (2011): Improved resolution short time Fourier transform. In: Proceedings of the 7th International Conference on Emerging Technologies, Islamabad, Pakistan, September 5-6: 1-3.

Mei S, Lin K (2001): Adaptive Notch Filter for Single and Multiple Narrow-band Interference. Bachelor Thesis, Faculty of Communications, Healt and Science, Edith Cowan University, Australia.

Mitch R, Dougherty R, Psiaki M, Powell S, O'Hanlon B (2011): Signal characteristics of civil GPS jammers. In: Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, Oregon, September 20-23: 1907-1919.

Niamsuwan N, Johnson JT, Ellingson SW (2005): Examination of a simple pulse-blanking technique for radio frequency interference mitigation. In: Radio Science 40 (05): 1-11.

Pany T (2010): Navigation Signal Processing for GNSS Software Receivers. Artech House, Boston London.

Raimondi M, Julien O, Macabiau C, Bastide F (2006): Mitigating pulsed interference using frequency domain adaptive filtering. In: Proceedings of the 19th International

Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2006), Fort Worth, Texas, September 26 - 29: 2251 - 2260.

Regalia PA (1991): An improved lattice-based adaptive IIR notch filter. In: IEEE transactions on signal processing 39 (9): 2124-2128.

Regalia PA (2010): A complex adaptive notch filter. In: IEEE Signal Processing Letters 17 (11): 937-940.

Subirana JS, Zornoza JM Juan, Hernández-Pajares M (2013): GNSS Data Processing. Volume I: Fundamentals and Algorithms. ESA Communications, Noordwijk, Netherlands.

Sugiura Y (2014): A fast and accurate adaptive notch filter using a monotonically increasing gradient. In: Proceedings of the 22nd European Signal Processing Conference (EUSIPCO), Lisbon, Portugal, September 1-5: 1756-1760.

TeleConsult Austria GmbH (2015): GNSS Airport Interference Monitoring System - Austrian Space Applications Programme, 9th call for proposals, Final Report.

Teunissen PJG, Montenbruck O (2017): Springer Handbook of Global Navigation Satellite Systems. Springer, Cham, Switzerland.

United States Department of Defense (2018): GPS Signal in Space Interface Specification (IS-GPS-200J). Available at `www.gps.gov/technical/icwg/IS-GPS-200J.pdf`.

Volpe J (2001): Vulnerability assessment of the transportation infrastructure relying on the global positioning system. National Transportation Systems Center, U.S. Department of Transportation.

Wasle E, Berglez P, Seybold J, Hofmann-Wellenhof B (2009): RNSS signal modeling for interference analysis. In: Proceedings of the 22nd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2009), Savannah, Georgia, September 22-25.

Wesson KD, Gross JN, Humphreys TE, Evans BL (2018): GNSS signal authentication via power and distortion monitoring. In: IEEE Transactions on Aerospace and Electronic Systems 54 (2): 739-754.

Wheeler PT (2015): Adaptive notch filtering for tracking multiple complex sinusoid signals. PhD dissertation, Advanced Signal Processing Group, Loughborough University, United Kingdom.

Yang J Hwan, Kang C Ho, Kim S, Park C Gook (2012): Intentional GNSS Interference Detection and Characterization Algorithm Using AGC and Adaptive IIR Notch Filter. In: International Journal of Aeronautical and Space Sciences 13 (4): 491-498.

Yin T (2007): Simulator of Pulsed Interference Environment of an Airborne GNSS Receiver. Master thesis, Department of Signals and Systems Chalmers University of Technology, Göteborg, Sweden.