Sascha M. Bartl, BSc

GNSS Interference Monitoring

Detection and classification of GNSS jammers

MASTER'S THESIS

to achieve the university degree of

Master of Science
(Diplomingenieur)

Master's degree programme: Geomatics Science

submitted to

Graz University of Technology

Institute of Navigation

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

Co-supervisor
Dipl.-Ing. Dr.techn. Philipp Berglez

Graz, November 2014

This document was written in TEXstudio and compiled with pdfLATEX2e and BIBTEX. For the creation of this document the version control system `git` was used. Figures that are not explicitly cited have been created with MATLAB or DIA Diagram Editor or taken as screenshots from the developed software.

Statutory declaration

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.

Graz, ____________________ ____________________

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 Masterarbeit identisch.

Graz, am ____________________ ____________________

Datum Unterschrift

Abstract

Interference of GNSS signals can be problematic for many kinds of applications relying on these signals as it leads to distorted measurement results or denial of service. The number of interference incidents disturbing GNSS signals is rising continually over the past years. This thesis describes the development of a GNSS airport interference monitoring system (GAIMS) capable of reliably detecting and classifying GNSS interferer such as jammer or spoofer. This is an important topic, especially for safety-critical applications, as these sources of intentional interference may deteriorate the performance of GNSS or cause a complete denial of service.

The thesis starts with an overview of the current situation regarding interference of GNSS signals, where different application scenarios for GAIMS are described. The benefit and innovative elements of the GAIMS are investigated during a discussion on current state-of-the-art systems for interference monitoring. A critical evaluation of the advantages and disadvantages of each system is discussed.

A major part of this thesis is the formulation of the theoretical background of possible methods to detect and classify GNSS jammer and spoofer. The second chapter explains the concept of a GNSS receiver together with the advantages of a software-defined radio as used for the development and contains a discussion on the impact that interfering signals have on different measurement quantities.

Based on this theoretical background and knowledge on the types of GNSS jammer and spoofer, the development of the GAIMS is described embedded in the framework of a software-defined radio. In chapter 3, different algorithms for detection and classification are implemented to work simultaneously and independent from each other, which ensures that the results are reliable.

The developed system for detection and classification of GNSS interferer is tested and evaluated using simulated data as well as recorded data from a GNSS front-end. The simulations are used to prove the functioning of the implemented algorithms and a measurement campaign evaluates the system based on recorded real-world data. During the measurement campaign it was possible to detect a real GNSS jammer in the vicinity of the airport Graz Thalerhof, which is the first incident of intentional interference that has been documented in Austria.

The thesis concludes with a critical review of the developed system including suggestions for further developments to enhance the detection and classification accuracy. An outlook is given regarding the practical use of the system and the next steps that will be made to further improve the developed GAIMS.

Zusammenfassung

Interferenz von GNSS Signalen kann für verschiedenste Anwendungen problematisch sein, die auf GNSS basieren, da dadurch die Messungen verfälscht werden können oder die Dienste nicht mehr zur Verfügung stehen. Aus verschiedenen Gründen steigt die Zahl an Störungen von GNSS Signalen immer weiter an.

Die vorliegende Arbeit beschreibt die Entwicklung eines GNSS airport interference monitoring system (GAIMS), welches die zuverlässige Detektion und Klassifikation von GNSS Störsendern ermöglicht. Dies ist speziell für sicherheitskritische Anwendungen ein wichtiges Thema, da solche Störsender die Funktion von GNSS Anwendungen verschlechtern oder sogar gänzlich verhindern können.

Die Arbeit beginnt mit einem Überblick über die aktuelle Situation bezüglich Interferenz von GNSS Signalen. Die unterschiedlichen Anwendungsszenarien von GAIMS werden in Bezug auf die derzeitige Situation beschrieben. Der Innovationsgehalt von GAIMS wird im Vergleich zu aktuellen Systemen gezeigt. Es werden die Vor- und Nachteile der unterschiedlichen Systeme im Hinblick auf die Überwachung solcher Störungen beschrieben.

Ein wichtiger Teil der vorliegenden Arbeit ist die theoretische Betrachtung möglicher Methoden zur Detektion und Klassifikation von Störsendern. Das zweite Kapitel erklärt das generelle Konzept eines GNSS Empfängers und zeigt die Vorteile, die ein Software-basierter Empfänger für die Entwicklung bringt. Eine Betrachtung der Auswirkungen unterschiedlicher Arten von Störsendern auf unterschiedliche Messgrößen rundet das Kapitel ab.

Basierend auf der erarbeiteten Theorie und dem erworbenen Wissen über GNSS Störsender, wird die Entwicklung von GAIMS in Kapitel 3 beschrieben. Unterschiedliche Algorithmen zur Detektion und Klassifikation werden verwendet um gleichzeitig und unabhängig voneinander die GNSS Signale zu überwachen. Diese Kombination unterschiedlicher Algorithmen garantiert die bestmöglichen Resultate.

Das entwickelte System wird mit Hilfe einer Simulation, sowie mit aufgezeichneten realen Daten eines GNSS Empfängers, getestet und evaluiert. Die Simulation wird verwendet, um die Funktion der eingebauten Algorithmen zu validieren, wobei die im Zuge einer Messkampagne aufgezeichneten Daten die Eignung des Systems für den realen Betrieb zeigen. Im Zuge dieser Messkampagne konnte zum ersten mal in Österreich ein aktiver GNSS Störsender entdeckt und dokumentiert werden.

Die vorliegende Arbeit schließt mit einer kritischen Betrachtung des entwickelten Systems. Vorschläge für weitere Verbesserungen der Detektion und Klassifikation werden diskutiert. Ein Ausblick über den praktischen Nutzen und die nächsten Schritte in der Weiterentwicklung von GAIMS rundet die Arbeit ab.

Contents

Acknowledgment

At this point I want to mention the people, who supported me within the development of this thesis. I would like to acknowledge scientific input as well as private support which was important for me.

First, I would like to mention my supervisor Univ.-Prof. Dipl.-Ing. Dr.h.c.mult. Dr.techn. Bernhard Hofmann-Wellenhof and thank him for his critical review and supervision of this thesis. His review is a motivating scientific input for this thesis as well as further developments and improvements.

I really appreciate the support from Dipl.-Ing. Dr.techn. Philipp Berglez and Dipl.-Ing. Stefan Hinteregger, who gave valuable input regarding references, reviewed this thesis and helped me solving problems concerning different topics. The structure and implementation of the developed software as well as this thesis were revised and enhanced as a result of numerous inspiring discussions. Their help is always motivating and improved my understanding of important aspects of this work.

Additionally, I want to thank the whole team of TeleConsult Austria GmbH for heartily integrating me into their community and office routines from the first day on. While technical conversations inspired me, the coffee breaks and tabletop soccer matches sufficiently distracted me to regain energy and motivation.

I want to thank my family for privately supporting me and giving me the opportunity and necessary recourse to finish my work. Throughout the past years they kept me grounded and helped me out whenever necessary. Personal discussions and conversations with them are always motivating to aim at higher goals.

Last but definitely not least, I want to especially thank my fiancé Christina for her unapologetic support in every situation. She indeed is the most important person in my life and therefore an essential private support for my work. Always caring about me and finding the right words and actions, motivating me to reach the best I can do, my everlasting thank and acknowledgment belongs to her.

Abbreviations

ADC	Analog to digital converter
AGC	Automatic gain control
AM	Amplitude modulation
ANF	Adaptive notch filter
ARNS	Aeronautical radionavigation service
ASAP	Austrian space applications programme
ASCII	American standard code for information interchange
bmvit	Ministry for transport, innovation and technology
BOC	Binary offset carrier
BPSK	Binary phase shift keying
BW	Bandwidth
C/A	Coarse/acquisition
CBOC	Composite binary offset carrier
$\mathrm{C/N_0}$	Carrier-to-noise ratio
$(\mathrm{C/N_0})_{\mathrm{eff}}$	Effective carrier-to-noise ratio
CS	Commercial service
CW	Continuous wave
DFT	Discrete Fourier transform
DLL	Delay locked loop
FFG	Austrian research promotion agency
FFT	Fast Fourier transform
FM	Frequency modulation
FPGA	Field programmable gate array
GAIMS	GNSS airport interference monitoring system
GBAS	Ground-based augmentation system
GIAT	GNSS interference analysis tool
GIMT	GNSS interference monitoring tool
GIPSIE®	GNSS multisystem performance simulation environment
GNSS	Global navigation satellite system
GPS	Global Positioning System
GPU	Graphics processing unit
GUI	Graphical user interface

IF	Intermediate frequency
IFS	Intermediate frequency signal simulator
IOV	In-orbit validation
ITU	International Telecommunication Union
NBP	Narrowband power
NCO	Numerically controlled oscillator
NP	Noise power
OS	Open service
P	Precision
PLL	Phase locked loop
PPD	Personal privacy device
PRN	Pseudorandom noise
PRS	Public regulated service
PSD	Power spectral density
PVT	Position, velocity and time
RF	Radio frequency
RMS	Root mean square
RNSS	Radionavigation satellite service
SCS	Satellite constellation simulator
SCW	Swept continuous wave
SDR	Software-defined radio
SNR	Signal-to-noise ratio
SSC	Spectral separation coefficient
STFT	Short time Fourier transform
USB	Universal serial bus
WBP	Wideband power

1. Introduction

Modern global navigation satellite systems (GNSSs) gained more and more importance throughout the past years. Not only position and velocity, but also timing information is constantly derived from systems like Global Positioning System (GPS), Galileo and others and is also used as basis for safety-critical applications.

Satellite systems nowadays are the most used positioning method for almost every navigational task. In flight and especially aircraft landing though this evolution is yet not quite so far, which is because of the fatal aftereffects of system malfunctions and thus high security requirements. Aircraft landing systems are quite expensive and need a lot of maintenance compared to GNSS-based augmentation systems for use at an airport. More details on instrument landing systems as an example for the working principle of terrestrial radio navigation can be found in Hofmann-Wellenhof et al. (2003). Therefore especially small airports in developing countries could benefit from a GNSS providing highly reliable results with a high level of integrity. Integrity in this sense means the ability of the system to independently report a potential malfunction to its user.

This thesis deals with interference of GNSS signals, which is one of the main threats to these systems, reducing the reachable level of performance. Interference cannot be fully avoided, because of the general working principle of GNSS relying on radio signals traveling all the way through the atmosphere from the satellites to the users, but this thesis covers ways to detect and classify interfering signals. The classification results could be useful for the development of strategies to reduce the impact of interference on the measurement results.

1.1. Motivation

GNSS interference monitoring is a useful tool for providing measurement results (e.g. position, velocity and time) with a high level of integrity and will therefore become more and more important throughout the next years. This is because of two main factors: First, the number of safety-critical applications based on GNSS (where integrity is a crucial factor) for all kinds of purposes is rising continually (Volpe (2001)), which increases the need for reliable results. Second, the usage of electromagnetic waves for many different systems has increased quite a lot over the past years, which leads to a higher probability of interfering signals from other systems. This higher level of interference cannot be avoided, which means that receivers for applications that need a high level of integrity must be able to deal with interfering signals.

In addition to this unwanted disturbances of the GNSS signals, the portion of intentional

interference - for different reasons - is becoming a more and more relevant factor even for civil applications and can lead to huge measurement errors or even full denial of service (Johnston (1999)).
This has been demonstrated e.g. in Scott (2011) at Newark Liberty International Airport as truck drivers regularly used GNSS jammers plugged into the cigarette lighters of their trucks. The usage of these jammers on the freeway near the airport interfered with the installed ground-based augmentation system (GBAS), which lead to sporadic outages and unreliable results until an interference detection system in combination with multiple surveillance cameras made it possible to detect the source of this offense. This incident is an excellent example for the damage that these so-called personal privacy devices (PPDs) could cause and how their usage increased during the last years. Embedded in the ongoing discussion concerning the fear of losing personal privacy rights through technologisation it can be assumed that the number of used PPDs will rise dramatically in the near future.
According to Scott (2011), personal privacy is one of the main, but not the only motivation for civilians to use GNSS jamming technologies. Another reason, why jammers have presently become more popular, is a financial one: modern road tolling systems use GNSS trackers in cars to observe the utilization of the monitored roads and compute the toll that a driver has to pay based on the actual covered distance. Even insurance companies have plans for car insurance schemes that are based on the amount of usage of the insured car, which could easily be realized by GNSS tracking systems in the cars.
Following Volpe (2001) a breakdown of GPS for just one day would cost the transportation and all dependent markets an enormous amount of money. Therefore also terrorists can see a rising motivation in disturbing the signals of GNSSs and it is important to be prepared for such offenses.

1.2. State-of-the-art

According to Butsch (1999), the task of GNSS interference monitoring refers to the observation of unwanted signals that could degrade the quality of GNSS measurements. For the purpose of interference monitoring, the signal properties as well as some derived quantities from the measurements have to be evaluated periodically. Interference detection algorithms can therefore be applied directly on the received signal (pre-correlation detection techniques) or after the tracking process (post-correlation detection techniques). The working principle of a GNSS receiver including tracking and correlation will be explained in section 2.1. Current state-of-the-art detection algorithms include the following as a short introduction to interference monitoring systems.

Interference threshold mask: The power spectral density (PSD) of the incoming signal from the antenna can be used to start the (pre-correlation) interference monitoring. A monitoring station as introduced in Butsch (1999) could use specific interference threshold masks to compare the computed spectra with. Figure 1.1 shows a PSD together with a threshold mask, where interference by narrowband signals can be ruled out.

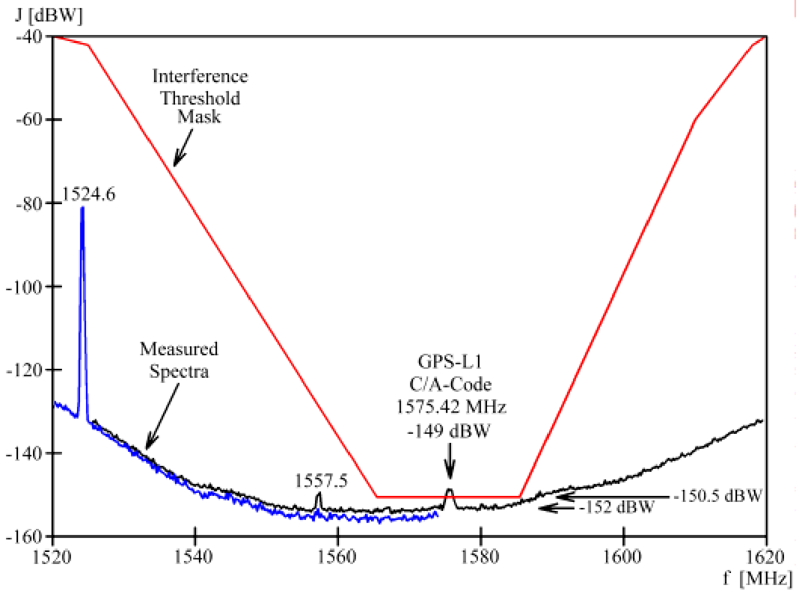


Figure 1.1.: PSD with interference threshold mask (from Butsch (1999))

Automatic gain control: Another possibility to detect GNSS interference is to use the automatic gain control (AGC), that is used at the analog to digital converter (ADC) in order to extract the maximum amount of information from the satellite signal (Isoz et al. (2011)). Figure 1.2 shows the AGC level over a period of 24 hours for one monitoring station near Kaohsiung International Airport in Taiwan. There were several incidents of heavy radio frequency (RF) interference during the measurements, which let the AGC level drop significantly. The monitoring algorithm detects an interferer if the AGC level drops below a specified level.

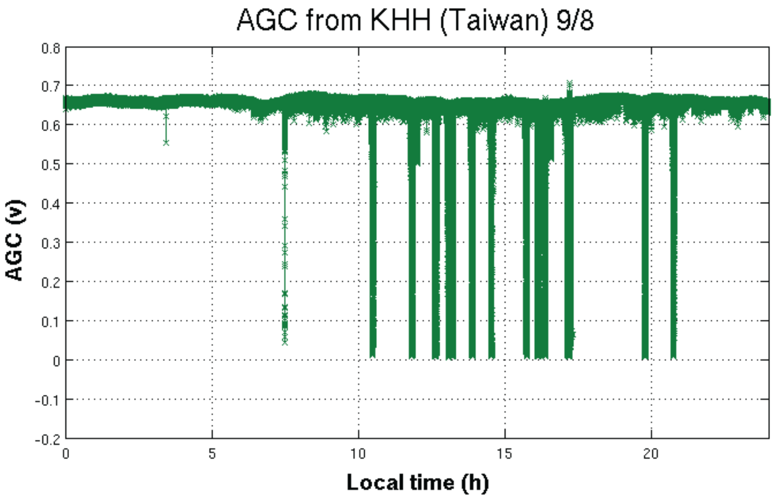


Figure 1.2.: Heavy interference in Kaohsiung on the 9th of August (from Isoz et al. (2011))

Adaptive notch filter: Apart from the AGC it is also possible to use the parameters of an adaptive notch filter (ANF) for interference detection and classification. Where the AGC - according to Yang et al. (2012) - is the better choice for detection of an interferer, a combination of different ANF parameters allow a classification of the type of interference. A combined approach as in Yang et al. (2012) is able to easily distinguish between different types of interference.

Carrier-to-noise ratio: Modern post-correlation techniques for interference detection use correlator output power in the form of carrier-to-noise ratio (C/N$_0$) as in Balaei et al. (2006), because it shows quite consistent performance under different levels of RF interference. In Balaei and Dempster (2009), this technique is investigated, using a statistical approach. Figure 1.3 shows an example for the impact of interference on the C/N$_0$ measurement. It can be seen that the C/N$_0$ drops significantly in the case of RF interference.

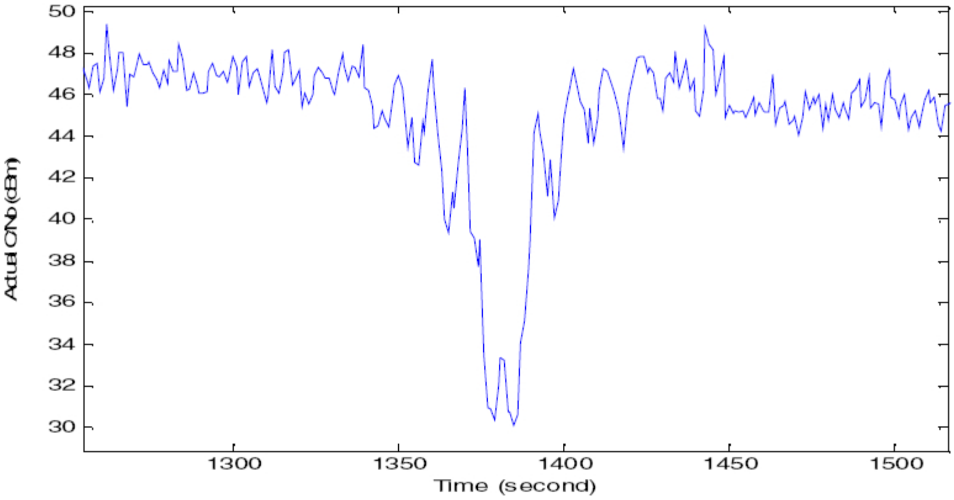


Figure 1.3.: C/N$_0$ measurement during RF interference (from Balaei et al. (2006))

Evaluation: Each of these monitoring techniques has certain advantages and disadvantages. The pre-correlation methods are generally faster in detection, because no additional signal processing is needed and the sampling for the detection can be higher. The post-correlation methods suffer from a delay caused by the baseband signal processing and are generally applied to longer parts of the signal, but on the other hand allow a more reliable detection. A monitoring system therefore should generally consist of a combination of pre-correlation and post-correlation techniques to enable the best possible results in matters of detection delay and reliability.

1.3. Project GAIMS

GNSS airport interference monitoring system (GAIMS) is a research project funded by the ministry for transport, innovation and technology (bmvit) in Austria and managed by the Austrian research promotion agency (FFG) as part of the ninth call for proposals of the Austrian space applications programme (ASAP). The GAIMS project is lead by TeleConsult Austria GmbH in cooperation with BRIMATECH Services GmbH and the Institute of Navigation at Graz University of Technology.

The aim of the project is to develop a system, which reliably detects sources of interference (i.e. jammer or spoofer) within the GNSS signal bands. These interferers are then analyzed to classify them into jammer and spoofer and further details, like interferer power, bandwidth or repetition rate are estimated.

State-of-the-art detection algorithms are investigated for their suitability, if necessary improved and implemented in the framework of a software-defined radio (SDR). The detection is based on the combination of different algorithms, including pre-correlation as well as post-correlation methods.

The project is amongst others interesting for the airport Graz Thalerhof, because a highway is next to the runway, which leads to a higher risk of being disturbed by an interferer in case of GNSS approach. For further information on the project GAIMS please refer to TeleConsult Austria GmbH (2013).

1.3.1. Innovative elements

Innovative in the project GAIMS is the combination of different approaches for the detection of interfering signals. The combination includes different independent approaches including pre-correlation and post-correlation techniques as well as the position of the reference station itself. Reliable automatic detection of interferers is really gaining importance. The classification and storage of different interferers can be a valuable and innovative tool for an airport or other users that need a high level of integrity to analyze the trend of interference in the surroundings and develop algorithms to further improve the reliability of the detection.

1.3.2. Contributions to the project

This thesis contributes to the GAIMS project with two different tasks: The first part of this practical development is the detection of GNSS interferers based on C/N_0 measurements, while the second part is the classification of the detected interferers.

C/N_0 based detection: This detection method is based on the comparison of the actual and the theoretical C/N_0 for each satellite that can be tracked. Therefore this detection method can only be applied after tracking (post-correlation) and has a higher computational burden and a greater time lag than the pre-correlation detection methods, but shows consistent performance for wide ranges of interferer power down to the complete loss of the desired signal. This thesis covers the estimation of the actual C/N_0 for each measurement epoch based on the tracking results as well as the development of a detection algorithm that is based on the actual values and the comparison to the theoretical ones.

Classification: The classification of the detected interferer can be done using several techniques. The algorithm used in the GAIMS project is based on the computation of a short time Fourier transform (STFT), the parameters of an ANF and an estimation of the interferer power and stores the estimated jammer parameters. This thesis covers the whole classification process including comparison with stored jammers and storage of the data.

Tests and validation: The implemented algorithms are tested and validated using simulated as well as recorded real-world data. The test results are used to assess the performance of the developed algorithms as well as the overall GAIMS.

2. Theoretical background

This chapter explains the theoretical background of GNSS receiver design with particular attention to interference and gives some details about the C/N$_0$ as well as the respective signal processing techniques that can be used for interference monitoring. The impact of interfering signals on the GNSS measurements is discussed with respect to the threat that such signals represent in the special case of safety-critical applications as for example in the environment of an airport.

2.1. GNSS receiver design

Figure 2.1 shows the overall structure of a GNSS receiver, according to Hofmann-Wellenhof et al. (2007). The receiver can generally be divided into three processing blocks and a RF antenna. The RF front-end processes the analog RF signal coming from the antenna and uses an ADC together with an AGC to convert the signal to digital samples at a given intermediate frequency (IF). This IF signal is then processed in the second block - the signal processing block - to acquire and track all possible satellites in view and compute the pseudoranges to the satellites along with some other measurements that are important for the application. The position, velocity and time (PVT) block uses the measurements of the signal processing block to compute the final results - position, velocity and time in general.

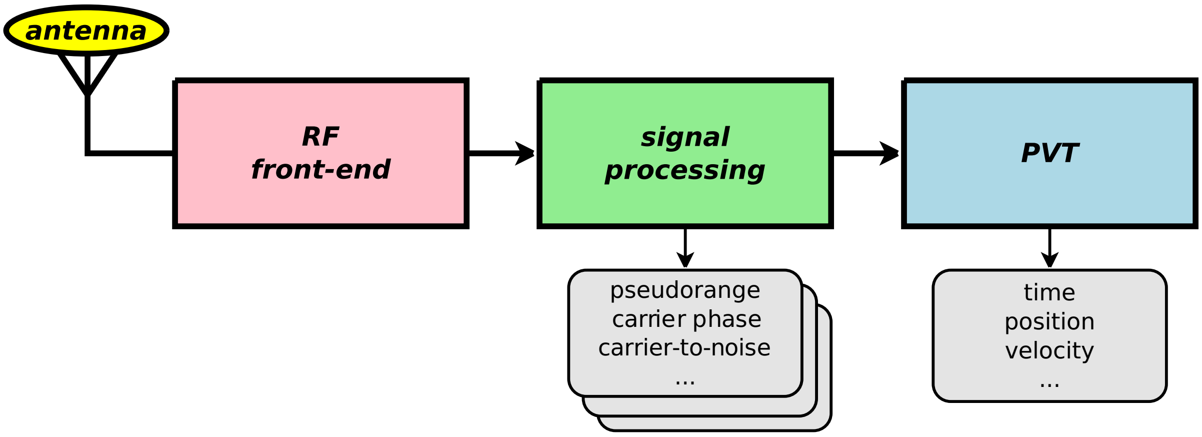


Figure 2.1.: Generic GNSS receiver structure

While the signal processing (especially tracking) in standard receivers is done by hardware correlators in multiple channels at the same time, a software-defined radio as introduced for example in Berglez (2013) or Krumvieda et al. (2001) has a software implementation of all receiver parts after the RF front-end. Because of the computational burden related to the correlation of the tracked codes, such a SDR requires quite powerful hardware. But on the other hand it has the big advantage of flexibility for the development of new computation algorithms, because they can easily be tested and implemented without the need to change any hardware parts.

2.1.1. Tracking

The basic principle of GNSS measurements is the correlation of the received signal with a replica code that is generated in the receiver (e.g. Kaplan and Hegarty (2006)). Figure 2.2 shows the modulation scheme for the creation of a GNSS signal. Tracking a satellite signal in the sense of GNSS means a constant adaption of the estimated code or phase offset and Doppler frequency according to the correlation results of the input with the replicated signal. After acquisition (first estimation of these values during search for satellites in view) this is the main task of the signal processing unit.

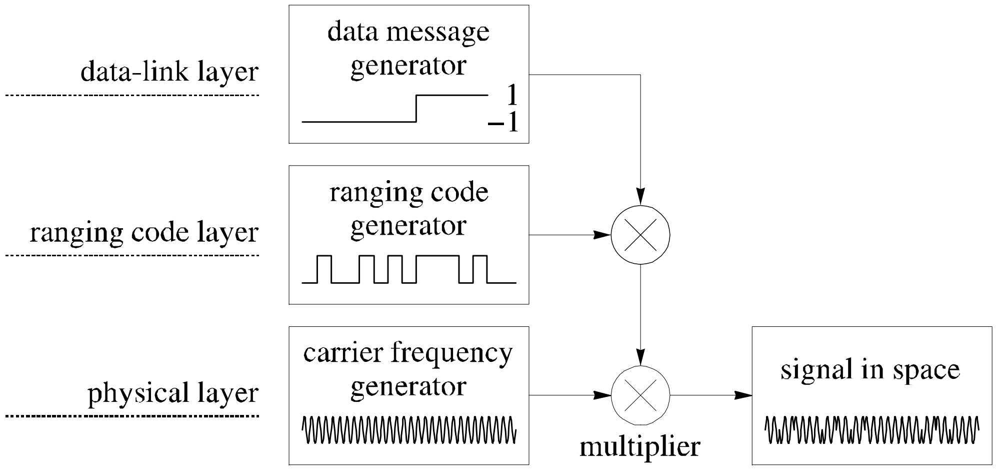


Figure 2.2.: GNSS signal generation (from Hofmann-Wellenhof et al. (2007))

Figure 2.3 shows the typical structure of a signal processing unit (according to Hofmann-Wellenhof et al. (2007)) consisting of one channel for each satellite. If the front-end's output is a complex signal then it is split into it's real and imaginary part and afterwards correlated with the replica signal (carrier wave and code), which is timed by a numerically controlled oscillator (NCO) according to the signal processing results. The correlation results are then evaluated in the discriminators to estimate carrier phase and code offset as well as Doppler frequency shift of the incoming signal. For more details on the acquisition and tracking of satellites refer to Dierendonck (1996) or Kaplan and Hegarty (2006). The correlation result is also used to estimate the current C/N_0 as a measure for the tracking accuracy, which will be explained in detail in section 2.3.3.

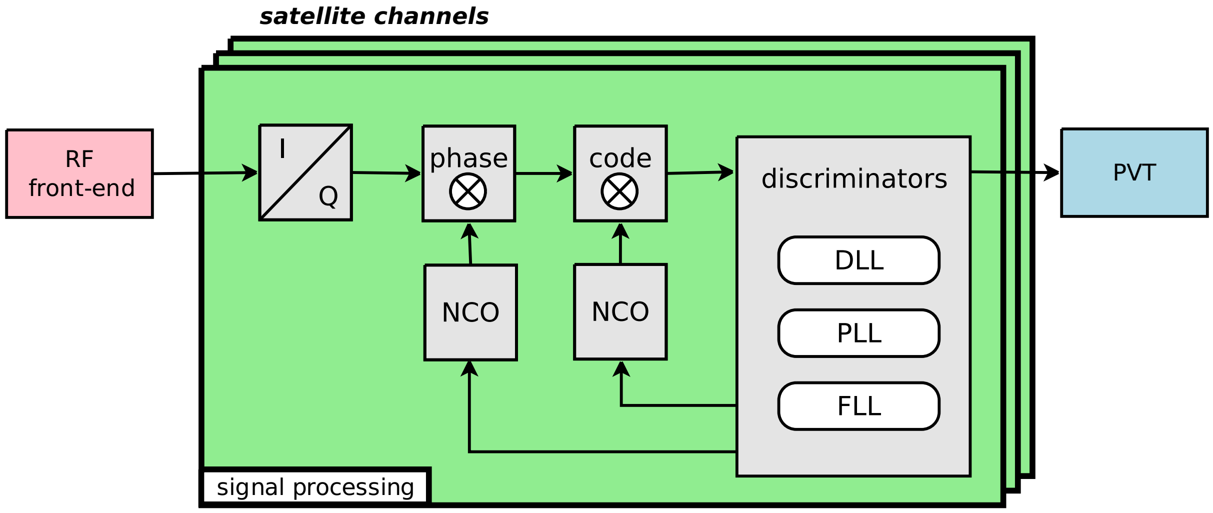


Figure 2.3.: GNSS receiver signal processing

2.1.2. Measurements

The measurements used to estimate the receiver's position, velocity and time (mainly code and phase pseudoranges as well as Doppler frequency) derived from the correlation results are explained in detail in Hofmann-Wellenhof et al. (2007). Code and phase pseudoranges are the computed distances between receiver and satellites without taking the receiver's clock error into account. The Doppler frequency denotes the shift of the signals frequency due to the relative motion between satellite and receiver and will typically be in the range of about ±5000 Hz. Also a general error model for these quantities as well as useful data combinations to minimize the effects of the systematic errors can be found in Hofmann-Wellenhof et al. (2001).

The signal processing results that are described in the following two sections including the C/N_0 can also be seen as GNSS receiver measurements, where the C/N_0 can be used for integrity and interference determination.

2.2. Signal processing

In a SDR it is quite easy to implement different methods of signal processing to analyze the tracking quality and therefore estimate the accuracy of the measurements. The frequency bands used by GNSS signals (summarized in Figure 2.4) are located in the L-band and are part of the aeronautical radionavigation service (ARNS) and radionavigation satellite service (RNSS). Therefore they are strictly protected and regulated by the International

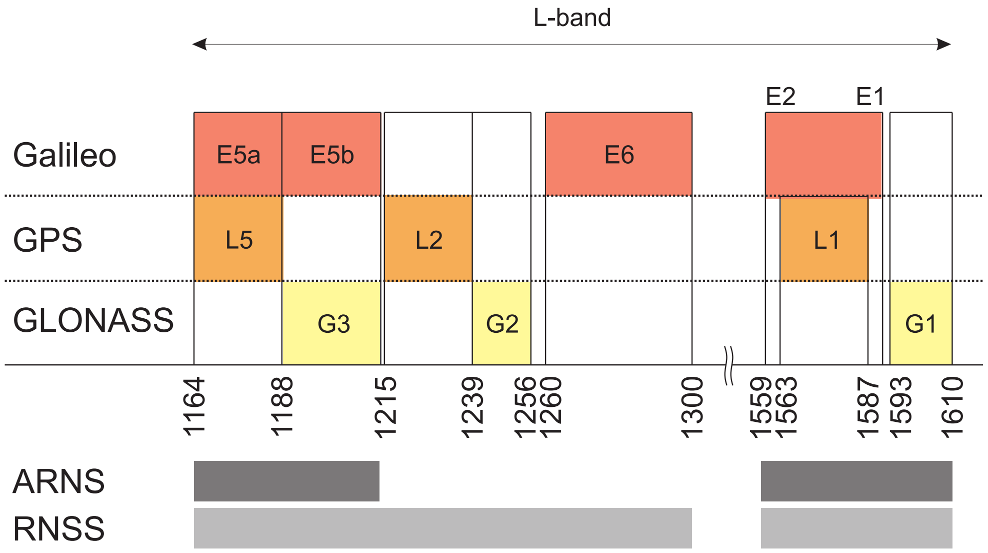


Figure 2.4.: GNSS frequency band allocation (from Turner et al. (2002))

Telecommunication Union (ITU). Analyzing the spectrum of the received signal at the antenna therefore is a possible method to estimate the noise level. Also interfering signals can be found and separated in the spectrum. The preferred way to compute the spectrum of a discrete signal is the fast Fourier transform (FFT) as introduced in Walker (1996).

2.2.1. Power spectral density

The power spectral density of a signal shows the distribution of the signal power over the allocated frequencies. According to Wasle et al. (2009) the estimation of the power spectral density of a GNSS signal can be computed based on the frequency domain representation, generated by a FFT. The PSD is generally computed using the Fourier transform

$$X(f) = \int_{-\infty}^{\infty} x(t) e^{-\imath 2\pi f t} \, dt \tag{2.1}$$

of a continuous signal $x(t)$ as introduced in Oppenheim et al. (1999). Using the autocorrelation function $\Gamma_{xx}(t)$, which can be expressed as

$$\Gamma_{xx}(t) = X^*(f) X(f) \ , \tag{2.2}$$

using the complex conjugate $X^*(f)$ of the spectrum $X(f)$, the power spectral density $S_{xx}(\omega)$ can be computed by

$$S_{xx}(\omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \Gamma_{xx}(t) e^{-\imath \omega t} \, dt \tag{2.3}$$

for each frequency ω of the monitored signal.

As the frequency spectrum used by GNSS is strictly regulated, changes in the PSD of the signal can be used to detect the presence of interfering signals. Figure 2.5 shows an example of the analytic PSD of a GPS coarse/acquisition (C/A)-code. The PSD shows the typical structure of a binary phase shift keying (BPSK) modulated signal. As can be seen, the main signal power is concentrated at the center with small side lobes when using this type of modulation.

Galileo on the other hand uses a different kind of modulation, called binary offset carrier (BOC) for its signals (e.g. composite binary offset carrier (CBOC) for the open service (OS)). This modulation scheme has the advantage that the maximum power is not concentrated at the center frequency, but split into two main lobes symmetrically around the center frequency as can be seen in Figure 2.5. This leads to a higher robustness with respect to incidents of narrowband interference like from GNSS jammers.

One of the main reasons for this choice of modulation was the consideration of inter-system interference between GPS and Galileo as they use the same frequency band (L1/E1 with 1575.42 MHz) for their civil/open signals. As the figure shows, the BOC modulated signals transmit the highest power in frequency ranges where the BPSK modulated signals transmit the lowest power and vice versa.

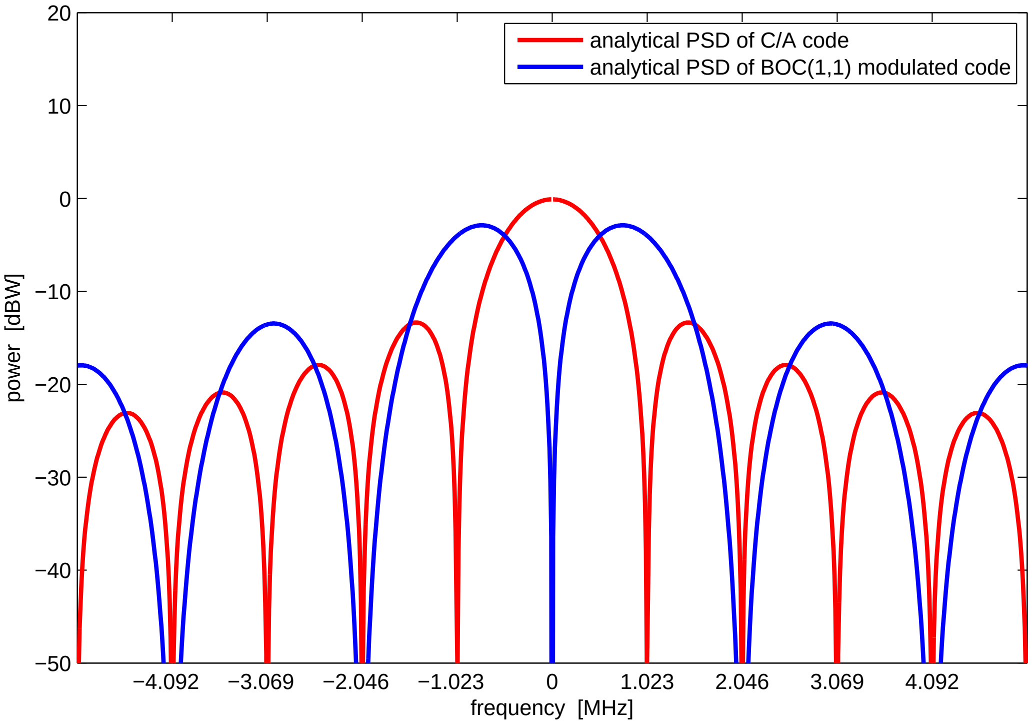


Figure 2.5.: Analytic PSDs of GPS (C/A) and Galileo (BOC(1,1)) codes

2.2.2. Short time Fourier transform

The short time Fourier transform as introduced for example in Allen (1977) consists of many Fourier transforms over short time periods of the incoming signal. These can be computed by a fast Fourier transform (FFT). Therefore for each time step the full spectrum is computed with a rather low frequency resolution due to less samples per FFT. The STFT thus shows how the frequency components of a signal change over time. When displayed as an image, with color indicating the power for each time/frequency bin, a STFT is an excellent tool to visually analyze the trend of power and frequency of the examined signal and to classify the type of interference.

2.2.3. Adaptive notch filter

A notch filter can be used to remove the power in a certain frequency range from an incoming signal. Based on the theory discussed in Regalia (1991) and Regalia (2010), the underlying complex all-pass transfer function $C(z)$ of a notch filter is written as

$$C(z) = \frac{e^{j\theta} z^{-1} - \alpha}{1 - \alpha e^{j\theta} z^{-1}} \; . \tag{2.4}$$

The filter transfer function $G(z)$ with $z = e^{j\omega}$ is defined as

$$G(z) = \frac{1}{2} \left(1 - C(z)\right) \tag{2.5}$$

and has a notch (zero value) at filter frequency $\omega = \theta$. It therefore removes the signal parts with this frequency from the incoming values. The 3 dB attenuation bandwidth Ω around θ depends on the filter parameter α as

$$\Omega = \frac{\pi}{2} - 2 \tan^{-1} \alpha \tag{2.6}$$

and controls the width of the notch. The filtering of the input signal $u(n)$ based on the explained transfer function can be written in it's state-space description as

$$\begin{aligned} x(n+1) &= e^{j\theta(n)} \alpha x(n) + e^{j\theta(n)} \sqrt{1-\alpha^2} u(n) \; , \\ e(n) &= -\frac{\sqrt{1-\alpha^2}}{2} x(n) + \frac{1+\alpha}{2} u(n) \end{aligned} \tag{2.7}$$

to obtain the filter output $e(n)$ from the filtered regressor $x(n)$.

An adaptive notch filter (ANF) is such a filter with a variable notch frequency $\theta = \omega_0$, that is adapted based on the filtered signal itself and the filter output. An ANF is used in a GNSS receiver to automatically estimate and filter out unknown frequencies such as interfering signals that could degrade the receiver performance. The adaption of the filter's notch frequency $\theta(n+1)$ can be obtained from the filter output $e(n)$ and the filtered regressor $x(n)$ by

$$\theta(n+1) = \theta(n) + \mu \cdot \mathrm{Im}\left[e(n)x^*(n)\right] \ , \tag{2.8}$$

using a stepsize μ, which can be expressed depending on the so-called 'forgetting factor' λ in the form of

$$\mu(n) = \left(\sum_{k=0}^{n} \lambda^{n-k} x^2(n)\right)^{-1} \ , \tag{2.9}$$

with $0 < \lambda \leq 1$. The choice of λ determines how fast the filter can adapt to frequency changes or how stable the notch frequency is estimated over time.

2.3. Carrier-to-noise ratio

According to Petovello et al. (2009), the $\mathrm{C/N_0}$ is the ratio of received carrier power to noise density and therefore can be used as a measure for the tracking quality. A high carrier-to-noise ratio indicates good tracking quality and thus measurements with low noise.
The magnitude of the $\mathrm{C/N_0}$ mainly depends on the carrier power of the tracked code and the transmission loss due to the atmosphere, which leads to values in the range of 47 to 51 dBHz (Spilker (1996)). RF interference can lead to a significant drop of this value.

2.3.1. Difference between SNR and $\mathrm{C/N_0}$

The terms $\mathrm{C/N_0}$ and signal-to-noise ratio (SNR) are often used interchangeably, but there is a fundamental difference between the two. As stated in Petovello and Joseph (2010) SNR refers to the ratio of the signal power (usually carrier power in dBW) to noise power (dBW) in a given bandwidth and is usually expressed in dB whereas $\mathrm{C/N_0}$ is the ratio of the carrier power to noise power per unit bandwidth (1 Hz) and is usually expressed in dBHz. The SNR can be theoretically computed using

$$\mathrm{SNR} = S - N, \tag{2.10}$$

where S is the signal power in dBW and N represents the noise power in dBW. $\mathrm{C/N_0}$ on the other hand can be computed by

$$\frac{\mathrm{C}}{\mathrm{N_0}} = C - (N - BW), \tag{2.11}$$

using the carrier power C and bandwidth BW of the observation. Therefore the relation between $\mathrm{C/N_0}$ and SNR follows

$$C - N_0 = \mathrm{SNR} + BW \tag{2.12}$$

for the theoretical values by means of dB.

Estimation of signal-to-noise ratio

According to Petovello et al. (2009), the relation between the estimated SNR and $\mathrm{C/N_0}$ can be written as

$$\frac{\mathrm{C}}{\mathrm{N_0}} = \mathrm{SNR} + 10\log_{10}\left(\frac{2\mathrm{NBW}}{f_s\tau}\right), \tag{2.13}$$

with a noise bandwidth NBW, a sampling frequency f_s and a coherent integration time τ. Note that the definition of the estimated SNR in this equation does not fully correspond to the theoretical value stated above.

2.3.2. Theoretical $\mathrm{C/N_0}$

Theoretical the $\mathrm{C/N_0}$ can be written as

$$\frac{\mathrm{C}}{\mathrm{N_0}} = S_r + G_a - 10\log_{10}(k_B) - 10\log_{10}(T_{sys}) - L, \tag{2.14}$$

where S_r describes the received signal power, G_a is the antenna gain in the direction of the specified satellite, k_B stands for the Boltzman's constant, T_{sys} is the system noise temperature, composed of source and receiver noise temperature, and L denotes the implementation loss, which will typically be in the range of about 2 dB according to e.g. Petovello et al. (2009). Taking the presence of interfering signals into account, the effective carrier-to-noise ratio $(\mathrm{C/N_0})_{\mathrm{eff}}$ can be computed as

$$\left(\frac{\mathrm{C}}{\mathrm{N_0}}\right)_{\mathrm{eff}} = \frac{CL_s}{N_0L_n + I_{\mathrm{total}}}, \tag{2.15}$$

using the desired signal power C in combination with the corresponding processing loss L_s, the noise power N_0 with processing loss L_n and the total level of interference I_{total}. Following Prim et al. (2008), equation 2.15 can be expressed more detailed, including the specific effects of the RF front-end in form of the filter function $H(f)$. Using the power spectral density of the desired signal G_s and interfering signals G_I^j, the equation can be written as

$$\left(\frac{\mathrm{C}}{\mathrm{N_0}}\right)_{\mathrm{eff}} = \frac{C \cdot \int_{-\infty}^{\infty} G_s(f)H(f)\,df}{N_0 \cdot \int_{-\infty}^{\infty} G_s(f)H(f)\,df + \sum_j C_I^j \cdot \int_{-\infty}^{\infty} G_s(f)G_I^j(f)|H(f)|^2\,df}, \tag{2.16}$$

where C_I^j denotes the power of the interfering signals. This equation contains the definition of the total interference as in equation 2.38 in section 2.6.1 based on the spectral separation coefficient (SSC), but using the custom front-end filter characteristics instead of a combined bandwidth limitation. Note that the Doppler offset has been omitted here for readability.

2.3.3. Estimation of actual $\mathrm{C/N_0}$

The receiver estimation of actual $\mathrm{C/N_0}$ can be computed using different algorithms, which will be summarized here and are taken from Petovello et al. (2009) and Falletti et al. (2011). The computations are based on the correlator output samples $r_C[n]$, given as

$$r_C[n] = \sqrt{P_d}D[n] + \sqrt{P_\eta}\eta[n], \tag{2.17}$$

where $D[n]$ stands for the navigation bit samples and $\eta[n]$ are the complex noise samples with the corresponding powers P_d and P_η.

Beaulieu's method: This method was introduced in Beaulieu et al. (2000), motivated by an intuitive formulation of the signal and noise power estimates. The C/N$_0$ can be computed from

$$\frac{\mathrm{C}}{\mathrm{N}_0} = \frac{1}{T_{\text{int}}} \cdot \left[\frac{1}{N} \sum_{n=1}^{N} \frac{\hat{P}_n}{\hat{P}_d} \right]^{-1} , \tag{2.18}$$

using the integration time T_{int}. $\hat{P}_d$ denotes the signal-plus-noise power of the correlator output and $\hat{P}_n$ is the noise power. These quantities can be computed using the relations

$$\hat{P}_d = r^2_{C,\text{Re}}[n] + r^2_{C,\text{Im}}[n] \tag{2.19}$$

and

$$\hat{P}_n = \left(|r_{C,\text{Re}}[n]| - |r_{C,\text{Im}}[n]| \right)^2 \tag{2.20}$$

based on the real and imaginary parts $r_{C,\text{Re}}[n]$ and $r_{C,\text{Im}}[n]$ of the correlator output.

Signal-to-noise variance estimator: The (squared) signal-to-noise variance estimator is analog to the variance summing method (e.g. Sharawi et al. (2007)) and is based on the fact that the imaginary output of the correlator contains noise only, while the real part corresponds to the signal. It uses the total power of signal and noise $\hat{P}_{\text{tot}}$ estimated as

$$\hat{P}_{\text{tot}} = \frac{1}{N} \sum_{n=1}^{N} |r_C[n]|^2 \tag{2.21}$$

in relation to the signal power $\hat{P}_{\text{d}}$ according to

$$\hat{P}_{\text{d}} = \left[\frac{1}{N} \sum_{n=1}^{N} |r_{C,\text{Re}}[n]| \right]^2 , \tag{2.22}$$

to compute the estimated noise power $\hat{P}_{\text{n}}$ as

$$\hat{P}_{\text{n}} = \hat{P}_{\text{tot}} - \hat{P}_{\text{d}} \ . \tag{2.23}$$

The C/N$_0$ in this case can be computed as

$$\frac{\mathrm{C}}{\mathrm{N}_0} = \frac{1}{T_{\text{int}}} \cdot \frac{\hat{P}_{\text{d}}}{\hat{P}_{\text{n}}} \ . \tag{2.24}$$

Real signal complex noise method: This method is quite analog to the signal-to-noise variance estimator explained above and also exploiting the fact that the imaginary correlator output should contain just noise. The noise power $\hat{P}_\mathrm{n}$ can be estimated using

$$\hat{P}_\mathrm{n} = \frac{2}{N} \sum_{n=1}^{N} |r_{C,\mathrm{Im}}[n]|^2 \ , \tag{2.25}$$

while the total power (corresponding to equation 2.21) is computed from

$$\hat{P}_\mathrm{tot} = \frac{1}{N} \sum_{n=1}^{N} |r_C[n]|^2 \ . \tag{2.26}$$

The signal power $\hat{P}_\mathrm{d}$ follows from

$$\hat{P}_\mathrm{d} = \hat{P}_\mathrm{tot} - \hat{P}_\mathrm{n} \ , \tag{2.27}$$

which again leads to a carrier-to-noise ratio like in equation 2.24.

Moments method: According to Falletti et al. (2011) it is possible to estimate the actual $\mathrm{C/N_0}$ for complex signals using the second- and fourth-order statistical moments ($\hat{M}_2$ and $\hat{M}_4$) of the tracking result to estimate signal and noise power using

$$\begin{aligned} \hat{P}_\mathrm{d} &= \sqrt{2\hat{M}_2^2 - \hat{M}_4} \ , \\ \hat{P}_\mathrm{n} &= \hat{M}_2 - \hat{P}_\mathrm{d} \ , \end{aligned} \tag{2.28}$$

where the $\mathrm{C/N_0}$ can be estimated as

$$\frac{\mathrm{C}}{\mathrm{N_0}} = \frac{1}{T_\mathrm{int}} \cdot \frac{\hat{P}_\mathrm{d}}{\hat{P}_\mathrm{n}} \ . \tag{2.29}$$

The statistical moments are computed by their time averages using

$$\begin{aligned} \hat{M}_2 &= \frac{1}{N} \sum_{n=1}^{N} |r_C[n]|^2 \ , \\ \hat{M}_4 &= \frac{1}{N} \sum_{n=1}^{N} |r_C[n]|^4 \ . \end{aligned} \tag{2.30}$$

Power ratio method: The total power of the correlator output $r_C[n]$ (which can be seen as a stationary stochastic process) in this algorithm (introduced in Dierendonck (1996)) is summed over two different bandwidths. The wideband power measure WBP_k is based on the common noise bandwidth of $1/T_{\mathrm{int}}$ and estimated from

$$\mathrm{WBP}_k = \sum_{m=1}^{M} |r_C[kM+m]|^2, \quad \text{where} \quad k = 0, 1, \dots, \left(\frac{N}{M} - 1\right) \ , \tag{2.31}$$

while on the other hand the narrowband power measure NBP_k is based on the noise bandwidth $1/(MT_{\mathrm{int}})$. This measure can be estimated from

$$\mathrm{NBP}_k = \left(\sum_{m=1}^{M} r_{C,\mathrm{Re}}[kM+m]\right)^2 + \left(\sum_{m=1}^{M} r_{C,\mathrm{Im}}[kM+m]\right)^2 \ . \tag{2.32}$$

The noise power NP_k can be estimated as the ratio between the narrowband and wideband power measure

$$\mathrm{NP}_k = \frac{\mathrm{NBP}_k}{\mathrm{WBP}_k}, \tag{2.33}$$

whose estimated statistical mean value $\hat{\mu}_{\mathrm{NP}}$, computed from

$$\hat{\mu}_{\mathrm{NP}} = \frac{M}{N} \sum_{k=0}^{N/M-1} \mathrm{NP}_k \ , \tag{2.34}$$

can be used the compute an estimate for the $\mathrm{C/N_0}$ according to

$$\frac{\mathrm{C}}{\mathrm{N_0}} = \frac{1}{T_{\mathrm{int}}} \cdot \frac{\hat{\mu}_{\mathrm{NP}} - 1}{M - \hat{\mu}_{\mathrm{NP}}} \ . \tag{2.35}$$

Constraints

The real part of the correlator output values varies in its sign according to the navigation bits that are modulated onto the signal. Therefore the $\mathrm{C/N_0}$ estimation algorithms that are based on summing the (not squared) correlator output values over a specific time would be strongly affected by a summation over a navigation bit transition where the real part of the correlator output changes its sign. It is therefore necessary to choose the summation interval as an integer fraction of the navigation bit length of e.g. 20 ms for the GPS C/A-code to avoid distorted carrier-to-noise ratio estimates.
According to the chosen summation interval (with a maximum of e.g. 20 ms) the estimated values for the $\mathrm{C/N_0}$ may show relatively large variations during the measurement interval. In general it is recommended to smooth the estimated $\mathrm{C/N_0}$ using a low-pass filter (e.g. moving average) to obtain a better estimate.

2.3.4. Performance of C/N_0 estimators

The previously described estimators for C/N_0 show quite different performances in terms of estimation stability, implementation complexity, asymptotic behavior and their reaction to RF interference.

Stability of solution over time: Figure 2.6 shows the estimated C/N_0 for one GPS satellite using C/A-code tracking. The figure clearly shows that the estimates without any smoothing suffer from rather large variations over short time periods as stated in the section above.
The C/N_0 estimation gets much better when smoothing the data with a moving average filter, which can be seen in Figure 2.7 using a window size of 3 seconds for the averaging. Here it can be seen that different algorithms show a little offset compared to each other, but in general the estimates correspond quite well. The remaining differences between the previously discussed estimators arise from the different impact that the noise in the signal has on each estimator. Figures 2.6 and 2.7 suggest the power ratio method is the steadiest over short time periods.

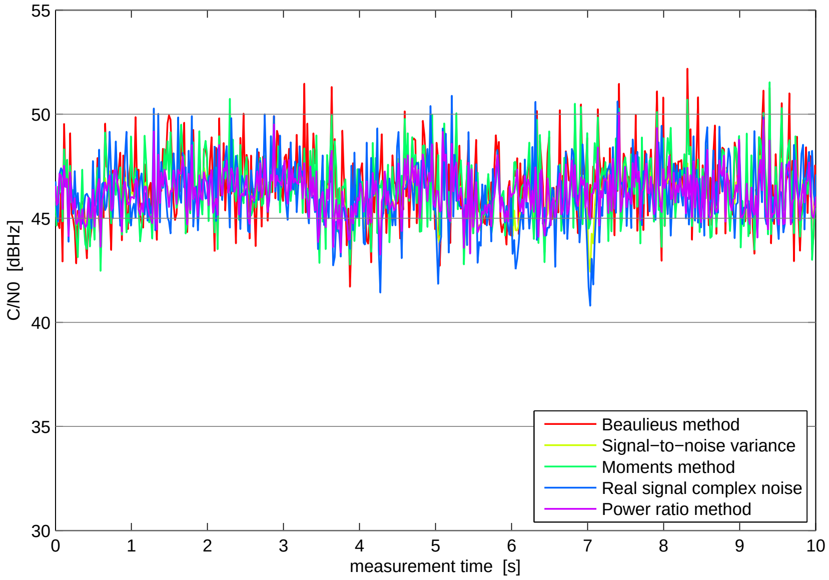


Figure 2.6.: Comparison of raw C/N_0 values from 5 different estimators

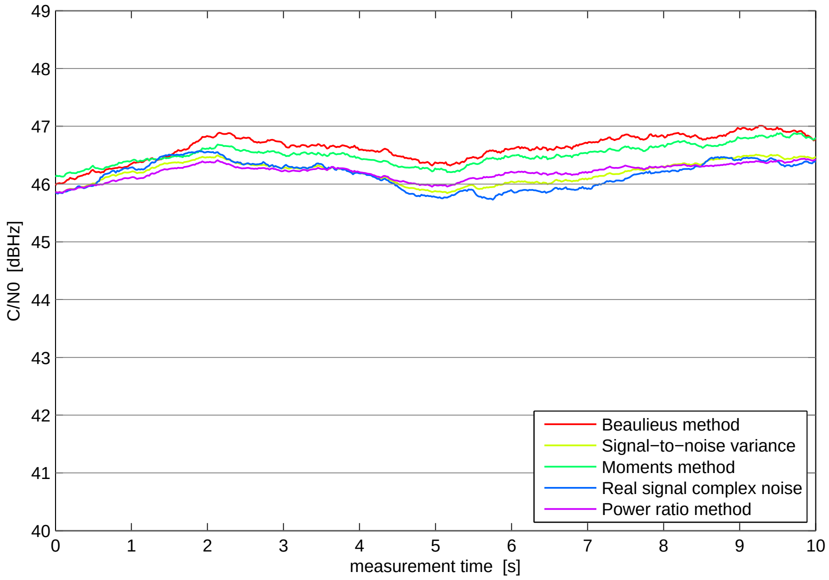


Figure 2.7.: Comparison of smoothed C/N_0 values obtained from 5 different estimators

Table 2.1.: RMS error of C/N_0 estimates [dBHz]

Computation method	**original**	**smoothed**
Beaulieu's method	1.78	0.22
Signal-to-noise variance	1.12	0.19
Moments method	1.57	0.17
Real signal complex noise	1.58	0.24
Power ratio method	1.08	0.13

Table 2.1 contains the root mean square (RMS) errors of the different estimates from their mean values in dBHz. The table confirms that the power ratio method results in the steadiest values of all investigated methods, showing the smallest RMS error for the original as well as the smoothed values. Therefore this computation algorithm is an appropriate choice for the task of interference monitoring.

Implementation complexity: According to Falletti et al. (2011), the implementation complexity can be evaluated by using the number of arithmetic operations required to estimate the C/N$_0$. Table 2.2 contains the number of additions, multiplications and divisions of real numbers for each estimation method (N being the number of samples used for one estimate and $K = N/M$ is the ratio between the two noise bandwidths in the power ratio method). The table shows the power ratio as well as the moments method are the most complex related to the others. When implementing a real-time solution for estimation of the C/N$_0$ one should pay attention to this fact, even though the tracking itself is far more computationally complex in a software-defined radio.

Table 2.2.: Complexity of different C/N$_0$ computation methods (Falletti et al. (2011))

Computation method	**Additions**	**Multiplications**	**Divisions**
Beaulieu's method	$3N + 1$	$3N + 3$	$N + 1$
Signal-to-noise variance	$3N - 1$	$2N + 4$	1
Moments method	$4N$	$5N + 5$	1
Real signal complex noise	$3N + 1$	$3N + 3$	1
Power ratio method	$4N - K + 1$	$2N + 2K + 2$	$K + 1$

Asymptotic behavior: The performance of the different estimation methods for increasing C/N$_0$ values can be represented by it's asymptotic bias, for the signal power $P_\mathrm{d} \to \infty$. The equations for this bias have been derived in Pini et al. (2008) and Falletti et al. (2011), assuming the residual phase noise θ_n as a zero-mean random variable with a uniform distribution in $\left[-\sqrt{3}\sigma_\theta, +\sqrt{3}\sigma_\theta\right]$ and a variance of σ_θ. Table 2.3 shows the derived expressions for the asymptotic biases for each computation method. The choice of a uniform distribution for the phase noise allows the derivation of this rather simple expressions in a closed form. Interesting about this equations is that the moments method is not biased by a residual phase error, because the signs in the real and imaginary values vanish because of the squaring. The analysis of the asymptotic behavior is interesting because the development of future GNSSs and improvements lead to higher C/N$_0$ values.

Table 2.3.: Asymptotic biases of the C/N$_0$ estimation

Computation method	**Asymptotic bias**
Beaulieu's method	$\frac{P_\mathrm{d}}{P_\mathrm{n}}\left[\frac{1}{2} + \frac{\sin\left(2\sqrt{3}\sigma_\theta\right)}{4\sqrt{3}\sigma_\theta}\right]$
Signal-to-noise variance	$\frac{\sin^2\left(\sqrt{3}\sigma_\theta\right)}{3\sigma_\theta^2 - \sin^2\left(\sqrt{3}\sigma_\theta\right)}$
Real signal complex noise	$\frac{\cos\left(\sqrt{3}\sigma_\theta\right)\sin\left(\sqrt{3}\sigma_\theta\right)}{\sqrt{3}\sigma_\theta - \cos\left(\sqrt{3}\sigma_\theta\right)\sin\left(\sqrt{3}\sigma_\theta\right)}$
Moments method	$\frac{P_\mathrm{d}}{P_\mathrm{n}}$
Power ratio method	$\frac{\sin^2\left(\sqrt{3}\sigma_\theta\right)}{3\sigma_\theta^2 - \sin^2\left(\sqrt{3}\sigma_\theta\right)}$

Reaction to interference: Additive white Gaussian noise as the simplest form of interference degrades the C/N$_0$ estimates with increasing power. Table 2.4 shows the estimated C/N$_0$ values together with the respective variance in dependence of different noise values for the signal-to-noise variance as well as the power-ratio method. The table shows that the different estimates for C/N$_0$ values are degraded with a similar performance, showing a maximum difference of the mean value of about 0.3 dBHz. The variance on the other hand is significantly smaller using the power ratio method and less influenced by interference.

Table 2.4.: C/N$_0$ estimation with additive white Gaussian noise (Sharawi et al. (2007))

Noise σ^2	**Signal-to-noise**	**Variance**	**Power ratio**	**Variance**
[dBW]	[dBHz]	[dBHz]	[dBHz]	[dBHz]
0	49.6	1.05	49.5	1.06
6	48.4	1.71	48.0	1.23
10.7	44.7	1.44	44.5	1.02
15.6	41.8	1.52	41.6	0.97
18.1	39.6	1.58	39.5	1.78
20	37.7	1.88	37.6	1.39
26	31.7	3.44	31.4	1.74

The degradation of C/N$_0$ caused by narrowband interference depends on the difference between the IF and the continuous wave (CW) interference frequency. Also the impact is more significant when the CW interference overlaps with a code spectral line. In Sharawi et al. (2007) it is shown that the performance of the two investigated methods differs with high CW interference power levels and the power ratio method suffers less from stronger interference.

2.4. Interference

The superposition of electromagnetic waves leads to a change in the resulting energy (positive or negative), which is in general called interference and a main threat to GNSS signals. Any two signals with similar enough frequencies will result in interference and degrade the desired system performance. This is the reason why the ITU strictly regulates and protects the use of the aeronautic frequency band, where the signals of GNSSs are situated.

2.4.1. Types of interference

Interference, according to Volpe (2001) or Kaplan and Hegarty (2006), can be unintentional or intentional. Unintentional interference can be divided into intra-system, inter-system or external interference depending on the source of the interfering signal and cannot be fully avoided. Intentional interference on the other hand is usually referred to as jamming, spoofing or meaconing and is meant to deliberately degrade the positioning accuracy or completely prevent a position solution.

Unintentional interference: Different signals of one system (e.g. GPS coarse/acquisition (C/A) and precision (P) code or signals from different GPS satellites) interfere each other even tough they are designed to have the smallest possible effects on each other. This effect is called intra-system interference. Interference between two different GNSS (e.g. GPS and Galileo) is also minimized by different code structures as shown in section 2.2.1 but still existing and denoted as inter-system interference. All other influences of non-GNSS signals that should not deliberately degrade the performance of the receiver (e.g. from neighboring frequency bands) are summarized as external interference. A quite natural form of unintentional interference is the effect of multipath. The additional delayed arrival of a signal due to a reflection in the environment of the receiver leads to a distortion in the received signal and can be seen as environmental interference.

Intentional interference: Jamming is the most popular - as well as easiest - form of intentionally degrading the performance of a GNSS receiver. The GNSS signals transmitted from the satellites arrive very weak at the receiver (with a power of about -160 to -155 dBW depending on the signal propagation loss) and can therefore be easily overpowered by small devices. This has the effect that the signals that already are below the thermal noise level are fully drowned in the noise and cannot be recovered by the receiver anymore (refer to section 2.5 for more details on jamming devices). Spoofing refers to the generation and transmission of signals that appear as legitimate GNSS signals and therefore mislead the receiver with false information. The reception and delayed rebroadcasting of real GNSS signals is called meaconing and has an effect similar to environmental multipath, where the signals are delayed because of their longer path due to a reflection.

2.5. GNSS jammers

GNSS jammers in contrast to spoofing or meaconing work with relatively high transmitting power and try to drown the GNSS signal in a high noise level. Based on the frequency and amplitude characteristics, five different kinds of jammers can be distinguished.

Continuous wave: Continuous wave (CW) jammers use a signal with constant frequency and amplitude (CW signal) to disturb the GNSS measurements. The frequency of this kind of jammers is generally directly on or near the L1/E1 band as most of the civilian GNSS receivers only receive signals in this frequency band. Figure 2.8 shows the characteristics of a CW jammer.

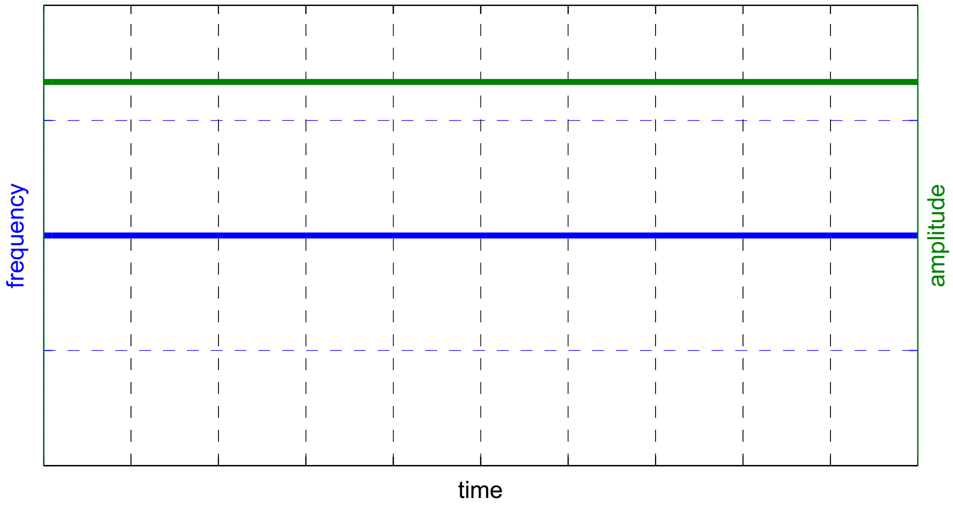


Figure 2.8.: Characteristics of a CW jammer

Swept continuous wave: These jammers use a signal with a specific bandwidth in which the frequency varies over time with a certain sweep duration while the amplitude is constant, which is called swept continuous wave (SCW). The frequency of a SCW signal changes periodically according to a sawtooth function around a certain center frequency and the amplitude is constant as in the CW signal (see Figure 2.9).

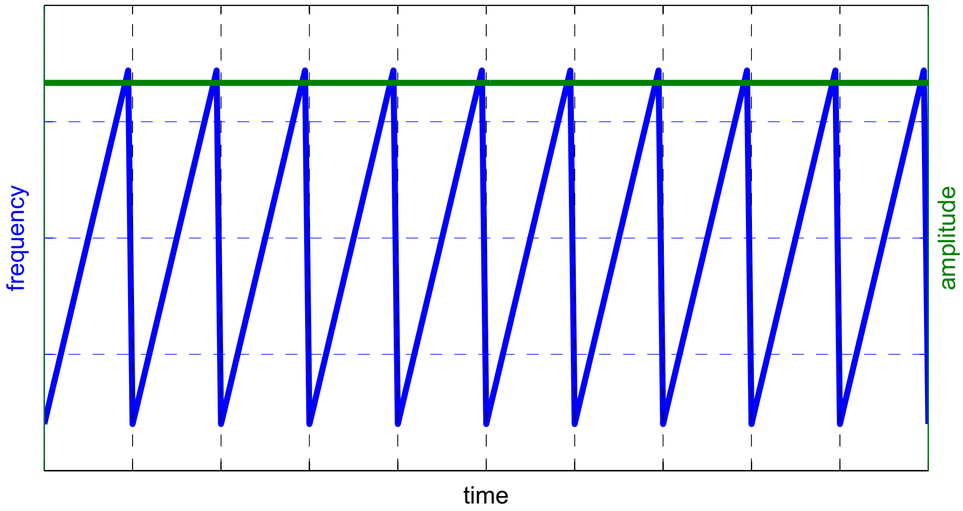


Figure 2.9.: Characteristics of a SCW jammer

Amplitude modulation: The amplitude modulation (AM) jammers show a constant frequency over time, but use a modulation by a sinusoidal wave to vary their amplitude (see Figure 2.10). The so called modulation index determines the percentage by which the original amplitude of the wave varies.

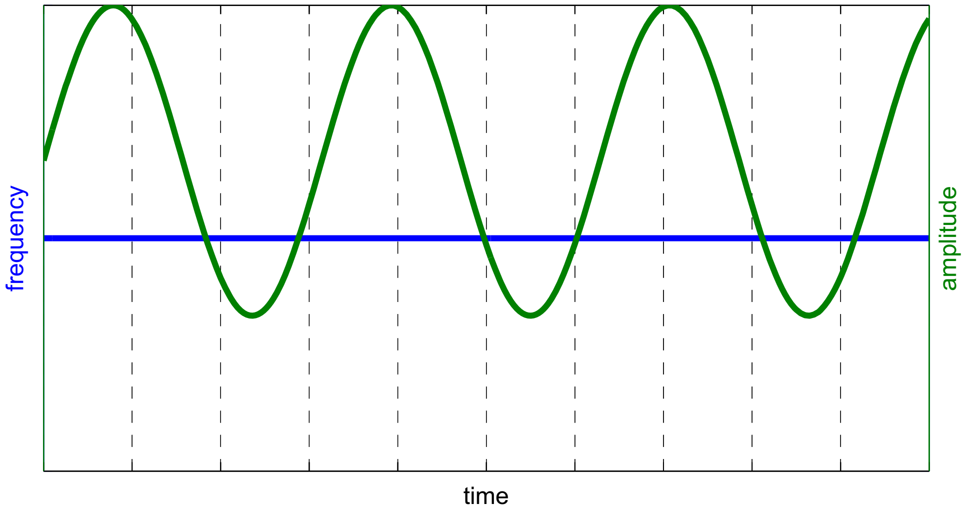


Figure 2.10.: Characteristics of an AM jammer

Frequency modulation: A frequency modulation (FM) jammer can be understood analog to the AM jammer, but here the frequency instead of the amplitude is changed over time as seen in Figure 2.11. The modulation is determined by the frequency of the modulating wave (modulation frequency) and the bandwidth (difference between maximum and minimum frequency) of the variation.

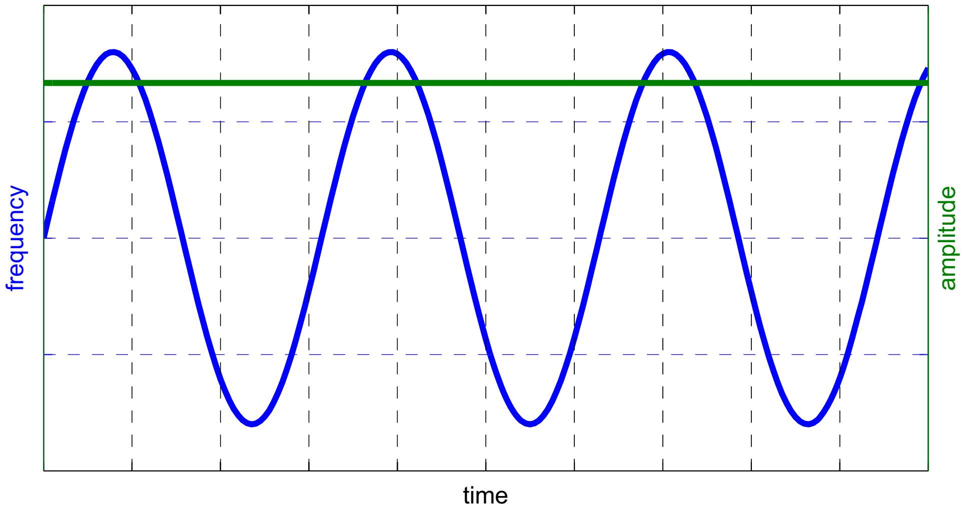


Figure 2.11.: Characteristics of a FM jammer

Pseudorandom noise: A so-called pseudorandom noise (PRN) jammer uses the code of an existing satellite (PRN) with a certain delay to interfere with the real signal from that satellite and prevent the receiver from tracking the correct code. The amplitude/frequency characteristics of such a jammer therefore are quite similar to those of the real signals. PRN jammers are no jammers following the classic definition, but can be understood as first stage of spoofing or meaconing.

The effects of CW and SCW jammers on a single-frequency GPS receiver have been investigated in Johnston (1999). The paper shows that the position errors due to CW and SCW interference are significant and remain undetected by a commercial off-the-shelf receiver only tracking C/A-code. Also different civil GNSS jammers have been tested for the signal characteristics in Mitch et al. (2011), which shows that most of them were some kind of SCW jammers that are powered by a battery or car cigarette lighter. Such jammers can be bought easily (and relatively cheap) over the Internet, but are nonetheless quite effective.

2.6. Interference monitoring

Interference monitoring aims to detect the presence of interfering signals and inform the user of the system whether GNSSs can safely be used or not. In the case of a positive detection of an interferer, a distinction between jammer or spoofer should be made.

2.6.1. Impact of interference

According to Kaplan and Hegarty (2006) the RF front-end of a GNSS receiver uses one or more AGC stages for the root mean square (RMS) amplitude of the thermal plus jamming noise to remain constant over time. During an event of high RF interference the AGC reduces the gain to keep the original RMS level at the ADC. This can be critical, especially when considering limited quantization levels at the ADC, and lead to complete drowning of the already weak GNSS signal. At any rate, the tracking performance will be degraded by jamming events because of a higher noise affecting the correlation function.
Following Wasle et al. (2009) the carrier tracking accuracy σ_{PLL} within the phase locked loop (PLL) can be estimated using

$$\sigma_{\mathrm{PLL}} = \frac{\lambda}{2\pi}\sqrt{\frac{B_{\mathrm{L}}}{\frac{\mathrm{C}}{\mathrm{N}_0}}\left(1 + \frac{1}{2T\frac{\mathrm{C}}{\mathrm{N}_0}}\right)} \ , \tag{2.36}$$

depending on the $\mathrm{C/N_0}$, wavelength λ of the GNSS signal, loop bandwidth B_{L} and coherent integration time T. The code tracking accuracy σ_{DLL} within the delay locked loop (DLL) has been derived in Betz and Kolodziejski (2009) and also depends on the $\mathrm{C/N_0}$, but has an additional dependency on the discriminator characteristics leading to more complicated formulas, which are omitted here for readability. The $\mathrm{C/N_0}$ itself in the form of

$$\left(\frac{\mathrm{C}}{\mathrm{N}_0}\right)_{\mathrm{eff}} = \frac{CL_s}{N_0 L_n + I_{\mathrm{total}}} \tag{2.37}$$

(according to equation 2.15) depends on the total interfering power I_{total} computed as

$$I_{\mathrm{total}} = \sum_{k=1}^{M} C_k L_k \kappa_k \ , \tag{2.38}$$

where C_k is the received power, L_k is the implementation loss and κ_k denotes the SSC between the desired and the interfering signal. The SSC, which represents the mean power of the cross-correlation function, indicates the degree of interference caused by the interfering signal and can be computed by

$$\kappa_k = \int_{-B/2}^{B/2} G_k(f) G_s(f)\, df \ , \tag{2.39}$$

using the PSDs of the received (G_k) and the desired (G_s) signal.
RF interference thus leads to a higher noise floor in the PSD of the signal (caused by the lower AGC gain), worse tracking accuracy at PLL/DLL and a lower C/N$_0$. It can also lead to a complete loss of lock, if the interference is strong enough. According to equation 2.38, the impact of the interferer mainly depends on its amplitude and on the SSC.

2.6.2. Monitoring techniques

There exist a few methods to detect interfering signals during GNSS measurements. Automatic gain control at the ADC can be used as detector, as high power interference lowers the AGC level below a certain threshold (Kaplan and Hegarty (2006)). If the AGC is not already saturated then the gain will be lowered as a consequence of the higher power received at the antenna. This method is appropriate for detection of wideband interference, but the detection of narrowband interfering signals is a more challenging task and cannot be guaranteed.
The same applies to the PSD of the input signal, where certain changes in the spectrum indicate interfering signals. Unusual high power in the monitored frequency spectra presumes the presence of a GNSS jammer since the frequency band is strictly regulated. As a consequence of this regulation the maximum expected power can easily be derived using the number of GNSS signals that are transmitted together with their known power plus thermal noise. Any significant additional power above a certain interference threshold mask (Butsch (1999)) is due to a source of unwanted interference, which can either be unintentional or intentional.
Another possibility to analyze the PSD of the received signal is a statistical one using a large sample T-test. This test checks inconsistencies of the PSDs over time and can be used to detect very low power interferences. Using a large sample T-test is a promising detection algorithm, when no a priori information is available (Pirazzi et al. (2012)).
Using the received baseband samples, the Kurtosis of the signal can be computed. As the received signal without any interference can be modeled as Gaussian distribution, the expected Kurtosis without interference is known. Significant deviations of the Kurtosis computed from the received signal indicate the presence of an interferer (Wendel et al. (2012)). A drawback of this method for interference detection is that no additional information about type and characteristics of the interferer can be derived.
From equation 2.37 follows, that a significantly low C/N$_0$ also indicates occurring interference. Because the values are not constant over time (due to changes in the signal path and atmosphere), a reliable detection algorithm based on C/N$_0$ values must include the comparison of the actual C/N$_0$ with an estimated theoretical one. To detect intentional interferences only, the signals from other satellites and GNSSs must also be included in the theoretical C/N$_0$ estimation following the signal modeling scheme proposed in Wasle et al. (2009) based on the SSC.
The current implementation of the system as described in chapter 3 focuses on using PSD as well as C/N$_0$ and position estimation for interference detection, as these methods promise accurate results. Additionally they are considered to be independent from each other.

3. Concept and implementation

This chapter describes the overall concept of the system and provides details about the development and implementation. Detailed information about the developed software, the implemented detection and classification algorithms as well as the graphical user interface (GUI) is given.

3.1. Overall concept

The developed system for interference detection and classification is embedded in the framework of a software-defined radio developed by TeleConsult Austria GmbH and described in Berglez (2013). Main part of the GAIMS is the GNSS interference monitoring tool (GIMT), which interacts with different parts of the GNSS receiver to manage all detection and classification processes. Figure 3.1 shows the overall concept of the system including the GIMT. The detection module receives its input data from the baseband signal processing as well as the PVT unit and routes it to the different detection algorithms. Each detection algorithm monitors the input data and tries to find an indication for interference. In case of a positive detection of an interferer, the raw data samples from the RF front-end are saved in a data storage module. This data can later be used by the classification module to estimate the parameters of the interferer.
All results are transferred to the GUI and displayed to the user. The GUI is used to manually start and stop the detection and classification modules and change the settings to improve the results.

3.1.1. Real-time vs. postprocessing

The monitoring modules for interference detection are intended to work in real-time together with the SDR. To give useful and timely warnings in the case of interfering signals that could affect the measurement quality, it is important that the whole process of detection works in real-time or at least near real-time. Therefore the detection algorithm triggers a warning as soon as the first module detects an interferer, not waiting for modules with a greater delay as for example the position monitoring. More details on the triggered warnings and alarms with different severities can be found in section 3.2.4.
The classification module is detached from the rest of the GIMT to avoid a delay in the monitoring modules, caused by expensive computations necessary for the classification. Therefore in case of a detected interferer, only raw data samples are stored to a file. This file can later be processed separately to classify the parameters of the detected interferer.

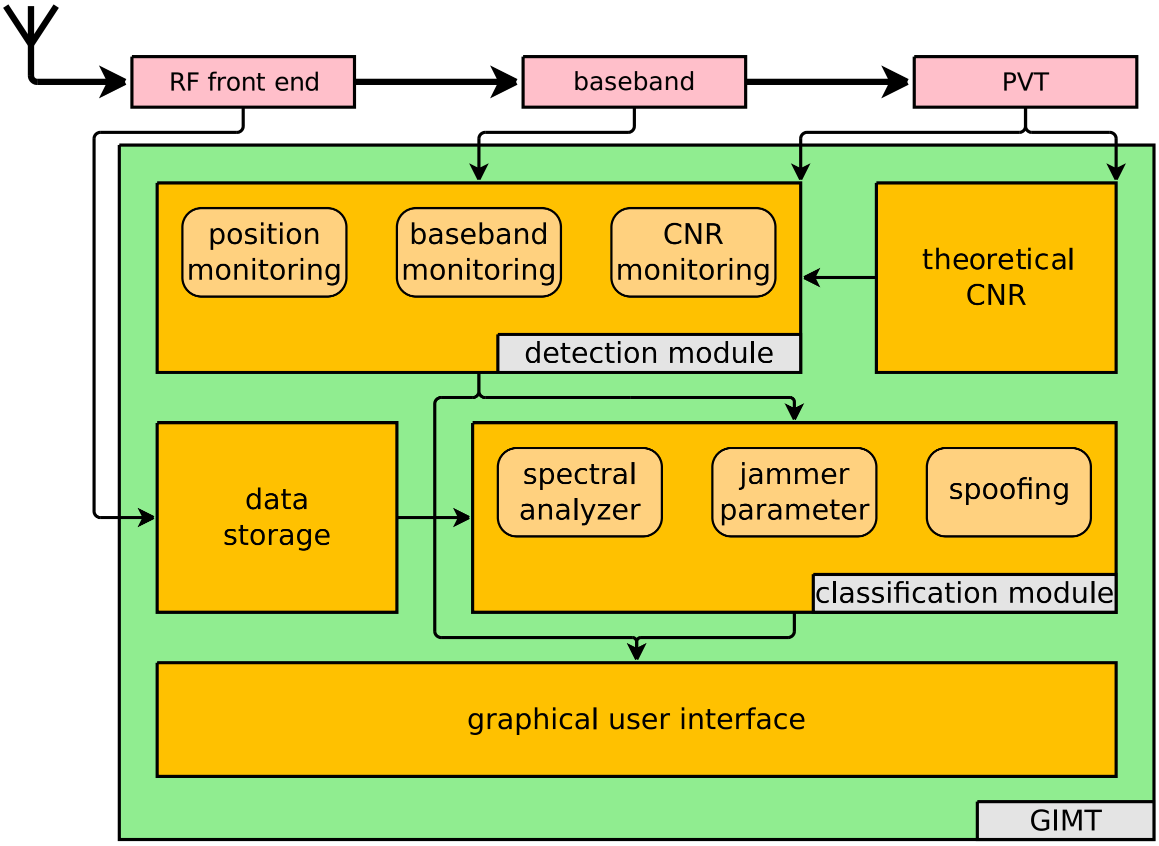


Figure 3.1.: GAIMS system concept - GIMT

The classification module thus is only used in postprocessing. Details about the implemented classification algorithms can be found in section 3.3.
This mechanism ensures that the user has the opportunity to decide, when the classification should start, independently from the real-time processing used to detect interfering signals. Also the classification can be done more than once and tested with different settings to find an optimal estimation for the interference parameters. After a suitable estimation has been found, the user can decide to store the parameters for future use.

3.1.2. Graphical user interface

The basic functionality for the detection process can be accessed through the command line, but the current state outputs are much more user friendly in the developed graphical user interface. Especially the classification tool and the plots that provide important information to the user make a GUI necessary.
The created GUI is divided into two main parts: detection window and postprocessing dialog. These two parts can be used simultaneously and do not interact with each other. The detection window is considered as main window and is opened first when the program starts. Both windows provide a simple interface to start and stop the detection/classification.

Detection window

Figure 3.2 shows the layout of the detection window, consisting of buttons to start and stop the monitoring or open the postprocessing dialog, a tabbed layout for detailed information (e.g. the PSD of the signal in Figure 3.2) and a visualization of the current interferer situation. This is divided into a part for jammer detection and a part for spoofer detection, where the color of the two circles indicates the interferer situation according to an ample principle. A green circle indicates that no interferer has been found, an orange circle indicates a warning and a red circle indicates an alarm. This warning/alarm system is further distinguished for jammer and spoofer independently as can be seen in Figure 3.2.

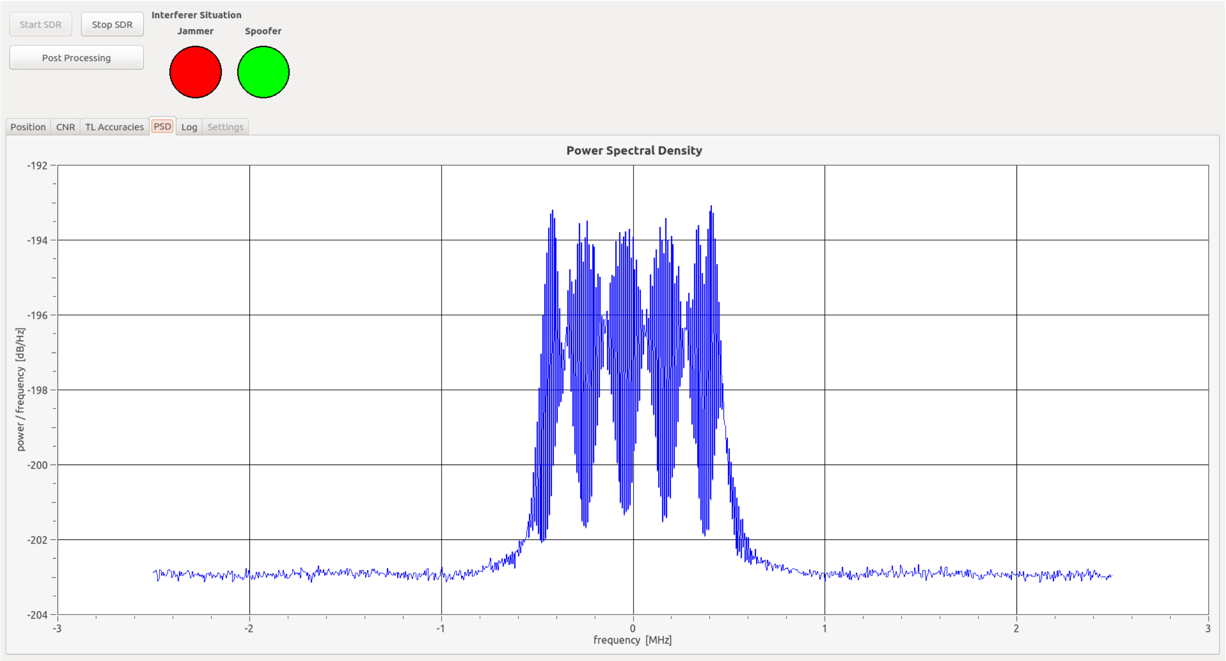
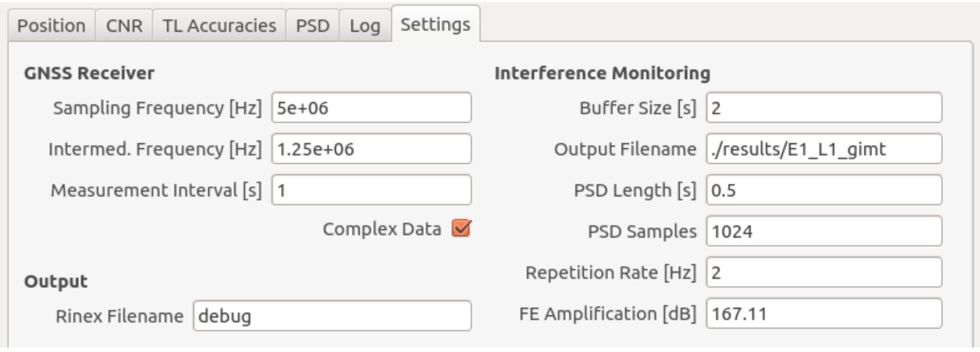


Figure 3.2.: GUI - detection window

The settings tab in the detection window (Figure 3.3) contains basic settings for the GNSS receiver and for the interferer detection. These settings include the parameters of the PSD for the monitoring as well the interface settings for the receiver, including sampling and intermediate frequency and other information.
Each detection algorithm has its own tab in the main window to display important information. Figure 3.4 shows the tab displaying the current C/N$_0$ estimates together with the theoretical values. This time series plot provides the possibility to compare the C/N$_0$ values for the last 60 seconds, where trends can be seen as well as significant drops below the theoretical values, which indicates a jammer like in Figure 3.4.



GNSS Receiver

Sampling Frequency [Hz] 5e+06

Intermed. Frequency [Hz] 1.25e+06

Measurement Interval [s] 1

Complex Data ☑

Output

Rinex Filename debug

Interference Monitoring

Buffer Size [s] 2

Output Filename ./results/E1_L1_gimt

PSD Length [s] 0.5

PSD Samples 1024

Repetition Rate [Hz] 2

FE Amplification [dB] 167.11

Figure 3.3.: GUI - detection settings

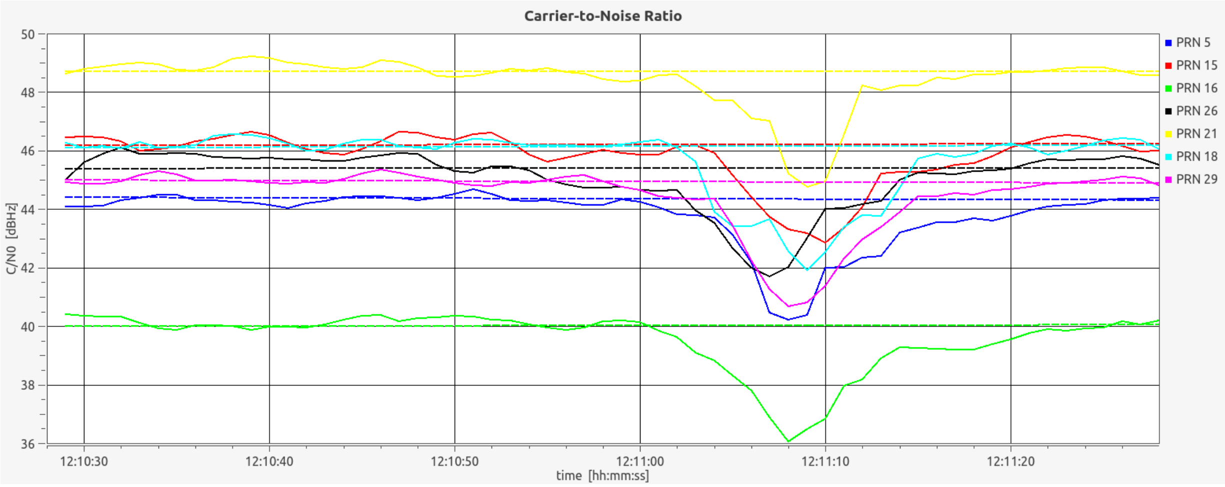


Figure 3.4.: GUI - C/N$_0$ monitoring

Figure 3.5 shows the position output from the PVT solution in relation to the known reference position of the receiver. The position is displayed as time series for all three coordinate axes in a local level reference frame as well as a two-dimensional plot of the horizontal receiver position. Significant variations of the estimated position that can be seen in the figure indicate an interferer.

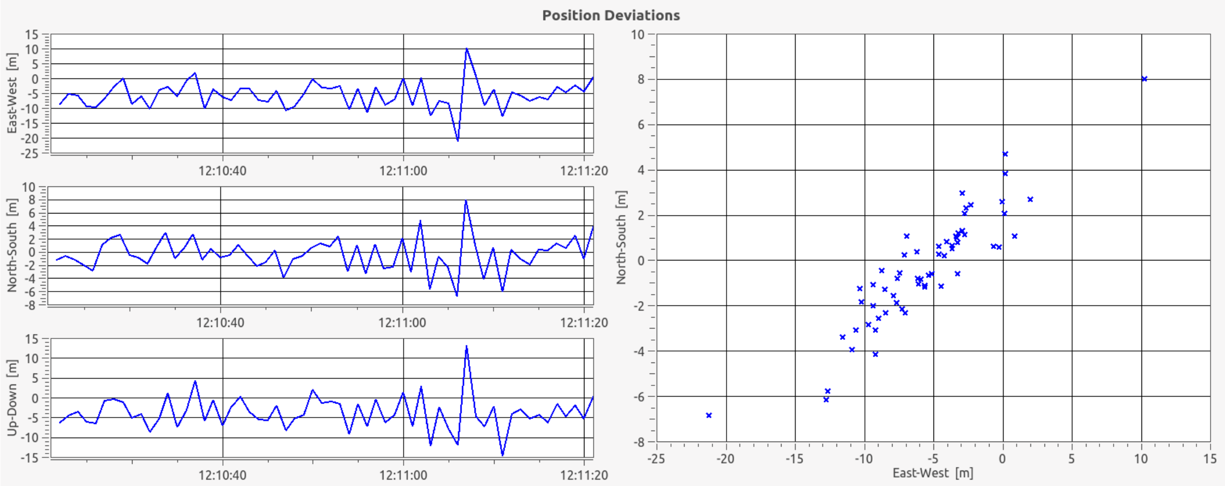
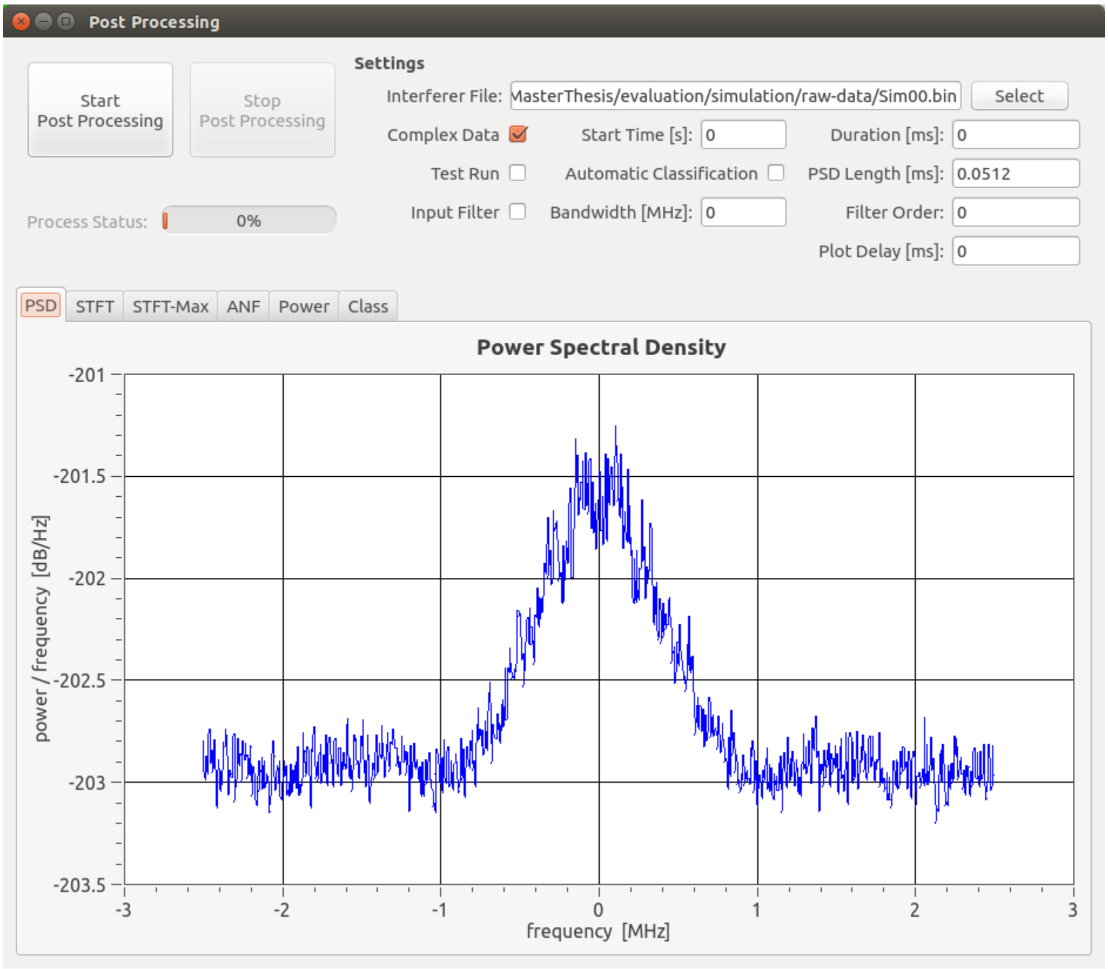


Figure 3.5.: GUI - position monitoring

Postprocessing dialog

Figure 3.6 shows the general layout of the postprocessing dialog. The figure shows that this dialog also has a tabbed layout to display information to the user. The data file for the classification can be selected at the top and some settings can be made that will be explained in section 3.3. A status bar displays the progress of the current task and a plot delay can be set by the user to reduce the update rate of the real-time plot (PSD).



Interferer File: MasterThesis/evaluation/simulation/raw-data/Sim00.bin

Complex Data ☑ Start Time [s]: 0 Duration [ms]: 0

Test Run ☐ Automatic Classification ☐ PSD Length [ms]: 0.0512

Input Filter ☐ Bandwidth [MHz]: 0 Filter Order: 0

Plot Delay [ms]: 0

Process Status: 0%

Figure 3.6.: GUI - postprocessing dialog

Figure 3.7 displays an example for a short time Fourier transform plot. This plot is useful to visually analyze and classify the inspected jammer parameters. The settings for the automatic classification can be chosen based on this plot as well as the progress of interferer power (Figure 3.8) that is shown in the respective tab. The power plot is useful to find the time where the jammer has the highest power, which facilitates the classification process and leads to a more accurate power estimation in the classification.

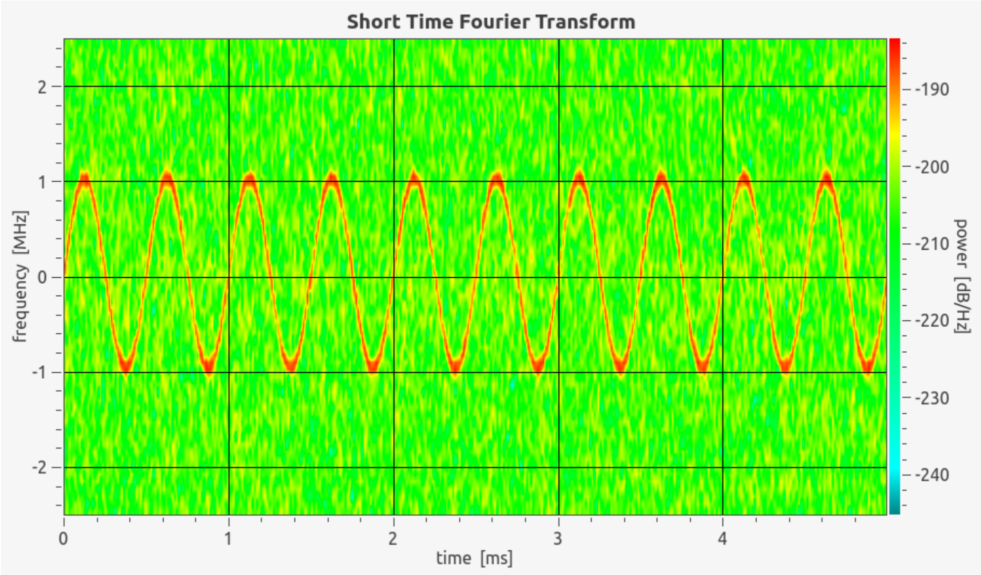


Figure 3.7.: GUI - short time Fourier transform

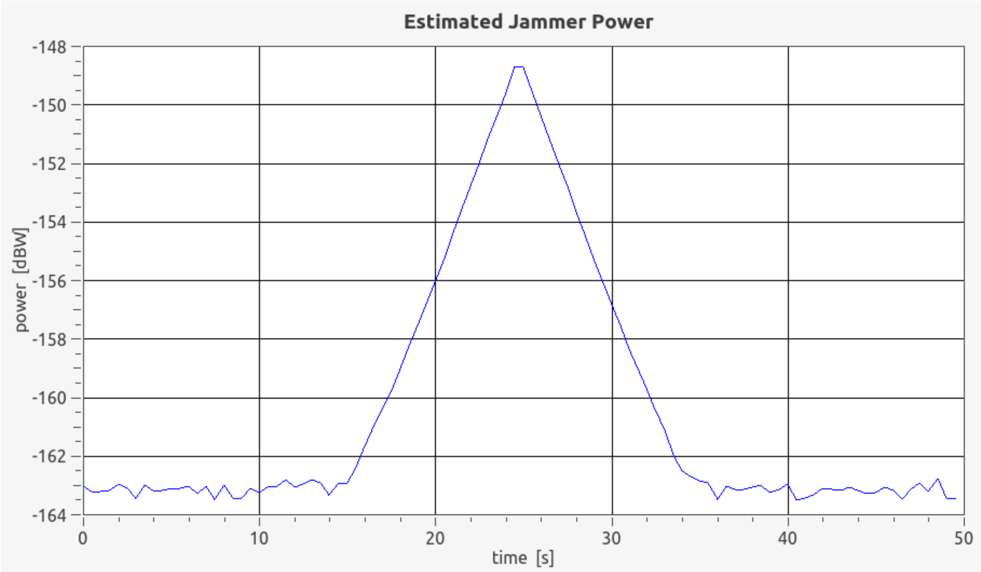
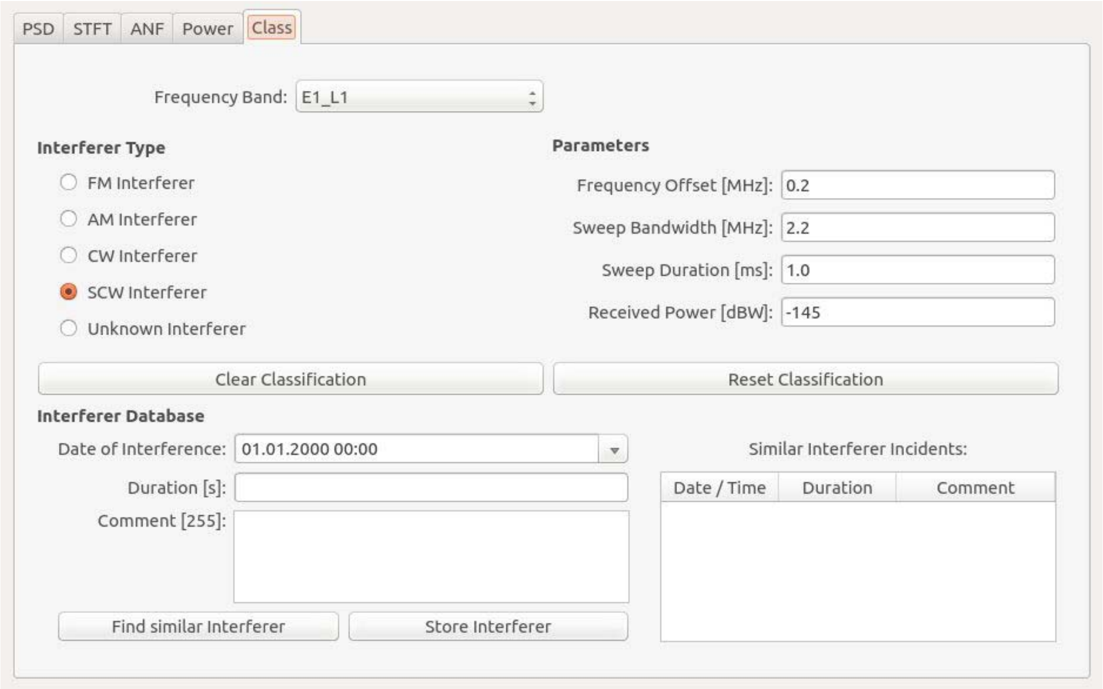


Figure 3.8.: GUI - interferer power

Figure 3.9 shows an example for a classification result as displayed in the post processing dialog. This dialog provides the possibility to override the classified jammer type and manually adjust the estimated parameters if necessary.



Frequency Band: E1_L1

Interferer Type

○ FM Interferer
○ AM Interferer
○ CW Interferer
● SCW Interferer
○ Unknown Interferer

Parameters

Frequency Offset [MHz]: 0.2
Sweep Bandwidth [MHz]: 2.2
Sweep Duration [ms]: 1.0
Received Power [dBW]: -145

Interferer Database

Date of Interference: 01.01.2000 00:00
Duration [s]:
Comment [255]:

Similar Interferer Incidents:

Date / Time	Duration	Comment

Figure 3.9.: GUI - classification result

A connection to the stored jammers is implemented through the interferer database section, which provides functions to search for similar jammers as well as to store the current classification result together with a comment and the current date and time. The list of similar interferer should help the user get an overview of past interferer incidents with similar jammers, which can be useful in finding a regular pattern for these incidents.

3.2. Detection

The following section describes the implementation of the detection module, consisting of different monitoring modules and interacting with a module to compute the theoretical $(C/N_0)_{eff}$. As can be seen in Figure 3.10, each of this monitoring modules (i.e. position, baseband or C/N_0 monitoring) has its own detection algorithm and reports to a common central detection stage, where the final decision on the current interferer state is made. The figure indicates a connection between the position result and the computation of the theoretical $(C/N_0)_{eff}$, although this connection is not necessary in the current implementation of the system, because the receiver has to keep its fixed position. In a future development, this connection will provide the possibility to use the system also for kinematic applications where the a priori position of the receiver is unknown. The current implementation directly uses the known reference position for the estimation of the theoretical effective carrier-to-noise ratio independent from the current PVT solution.

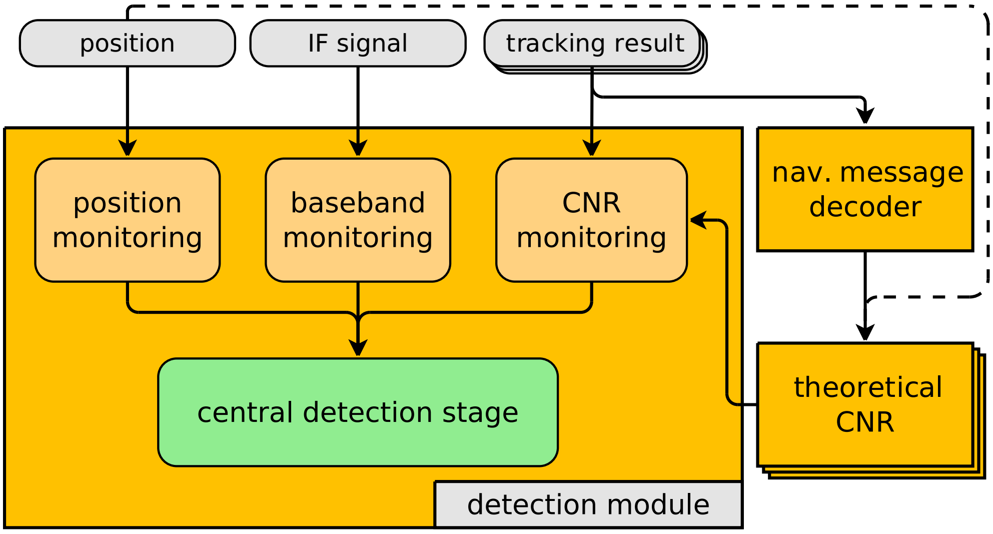


Figure 3.10.: Concept of detection process

The C/N_0 monitoring (including estimation of theoretical $(C/N_0)_{eff}$) as one of the main parts of this thesis is described in detail, while the other modules are only introduced briefly for the sake of completeness, because the final detection depends on the results of all monitoring threads.

3.2.1. C/N_0 monitoring

The C/N_0 monitoring is mainly based on the comparison of a carrier-to-noise ratio estimation by the receiver to the corresponding theoretical one. This section describes the detection algorithm based on the comparison of C/N_0 and theoretical $(C/N_0)_{\text{eff}}$ in detail.

Estimation of actual C/N_0

The estimation of the actual C/N_0 is directly integrated into the baseband processing module of the software-defined radio. The complex correlator output of the tracking is used to compute the C/N_0 estimate according to the power ratio method described in section 2.3.3. After testing all proposed algorithms, this estimation method is implemented because of its high short-time stability and stable reaction to interference as shown in section 2.3.4. The slightly higher computational effort compared to other algorithms is accepted, because a more accurate detection is expected due to lower estimation variations over time.

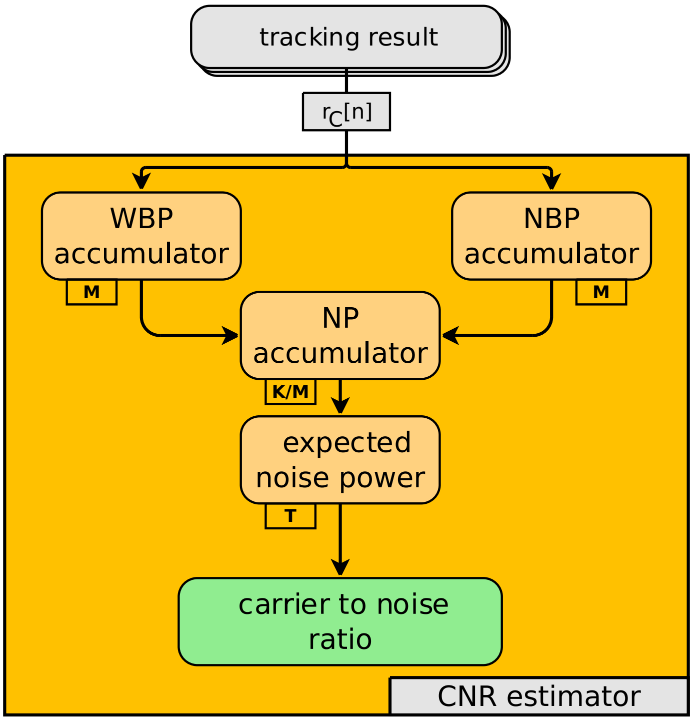


Figure 3.11.: C/N_0 estimation flow chart

Figure 3.11 shows a flow chart of the C/N_0 estimation. The complex correlator output as result of the tracking loops is denoted as $r_C\,[n]$ in this figure and serves as input for the C/N_0 estimation.

The wideband power (WBP) and narrowband power (NBP) accumulators take these input values and sum them according to equations 2.31 and 2.32 over two different bandwidths. The ratio between these bandwidths is defined by the parameter M, which is the number of samples that are summed before passing the values to the noise power (NP) accumulator. Summing over a navigation bit transition as stated in section 2.3.3 would lead to distorted results, which causes the parameter M to be strongly limited by the navigation bit length and the coherent integration time of the tracking loop. The implemented algorithm automatically selects the maximum number of samples M for the summation during its initialization process. For GPS L1 C/A satellite tracking with a navigation bit rate of 50 Hz and a coherent integration time of e.g. 1 ms this leads to a maximum number of 20 samples.

The NP accumulator sums up each K/M noise power values, where K corresponds to the number of correlator output samples during the averaging interval of T. This interval T can be chosen according to the system requirements, where a larger interval leads to a slower detection, but makes it more reliable on the other hand. The result of this accumulation and averaging process is an estimate for the expected noise power value, which can then be transformed into the $\mathrm{C/N_0}$.

In the current implementation, the $\mathrm{C/N_0}$ estimate is output with every measurement result of the receiver, where the measurement interval can be chosen independently from the carrier-to-noise ratio averaging time (generally with a shorter measurement interval than averaging time). This is realized by a moving average algorithm for the estimation of the expected noise power value. While the moving average thread constantly keeps as much samples in memory as needed for the $\mathrm{C/N_0}$ averaging time, the current average result is computed and output at every measurement epoch.

Computation of theoretical $(\mathrm{C/N_0})_{\mathrm{eff}}$

The theoretical values of the effective carrier-to-noise ratio are computed using the GNSS interference analysis tool (GIAT) developed by TeleConsult Austria GmbH and described in Kemetinger et al. (2013). A suitable interface to this software has been developed to transfer the data about the current satellite's and receiver's positions to the GIAT and adjust the settings for the respective antenna gain pattern and processing loss. All updates in the satellite constellation and currently visible and tracked satellites are instantly transferred to the GIAT to ensure receiving the most suitable estimation of theoretical $(\mathrm{C/N_0})_{\mathrm{eff}}$ by means of actual satellite constellation and receiver position.

For every receiver estimated $\mathrm{C/N_0}$ value, the current estimate of the theoretical effective carrier-to-noise ratio is computed based on the equations in section 2.3.2 following Prim et al. (2008). This result is then received from the GIAT and the two values of $\mathrm{C/N_0}$ and $(\mathrm{C/N_0})_{\mathrm{eff}}$ for the current epoch are the input for the detection algorithm.

Detection algorithm

Figure 3.12 shows the detection algorithm based on the carrier-to-noise ratio. C/N_0-based detection in its most obvious form is a threshold-based detection, where the algorithm detects an interfering signal from a jammer as soon as the estimated current C/N_0 drops under a specified threshold value (absolute threshold in Figure 3.12). The reduced tracking quality indicated by a low carrier-to-noise ratio can also have other reasons though. A low satellite elevation combined with a specific antenna gain pattern for example might cause a similar drop in the C/N_0 as a jammer does.

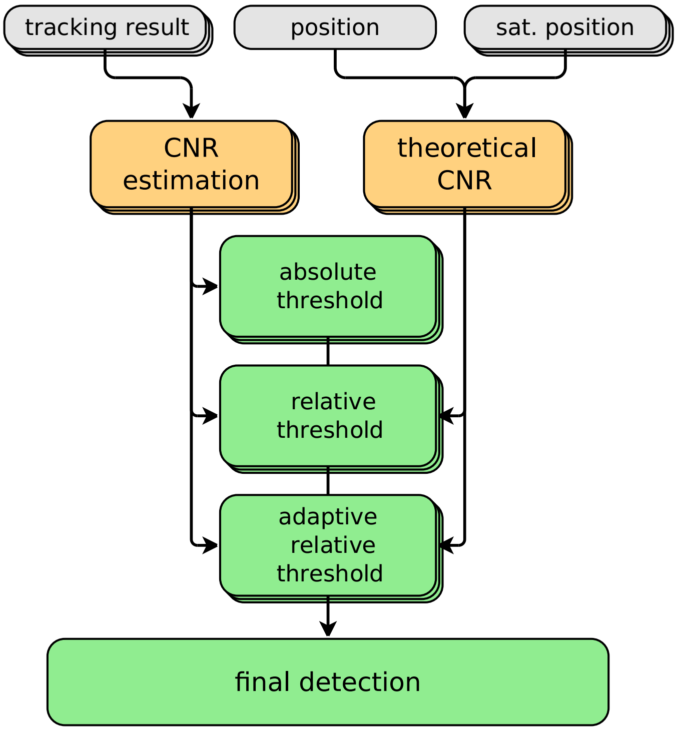


Figure 3.12.: C/N_0 based detection algorithm

Using the theoretical value of the carrier-to-noise ratio, based on the current satellite constellation and user position as well as antenna gain pattern, this algorithm can be enhanced to provide more accurate results. The threshold in this case can be computed by an offset to the theoretical value and is denoted as relative threshold here. This ensures that receiver estimates exceeding a threshold based on the reference $(C/N_0)_{\text{eff}}$ lead to a detected jammer. Low C/N_0 is still accepted if the difference is below the relative threshold. Further refinement of the detection algorithm includes a relative threshold that is computed by the theoretical C/N_0 and the average difference of the last few C/N_0 estimates (adaptive relative threshold). This enables the noise and temporal variations of the carrier-to-noise ratio to be accounted for. Also imperfections in the estimation of the theoretical value can be compensated by this approach.

As Figure 3.12 implies, the current implementation uses a combination of these three detection methods with thresholds chosen to ensure a meaningful coexistence of these detectors. This means that the absolute threshold is chosen rather low to account for satellites where the received signal quality is really bad and at the same time avoiding false detections of low but consistent satellites. The relative threshold on the other hand ensures that unexpectedly low C/N_0 estimates lead to a positive detection where the adaptive relative threshold detects sudden changes in the carrier-to-noise ratio which can indicate an interferer.

Implemented Thresholds: The thresholds in the current implementation are chosen empirically based on the common range of C/N_0 values of GNSS satellite signals. While the absolute threshold is at a value of 35 dBHz and considered to be low, the relative threshold was chosen 2 dBHz below the theoretical value. Therefore the relative threshold will detect an interferer in most cases. To enable an even earlier detection, the adaptive threshold was introduced with a level of three times the standard deviation of the C/N_0 below the theoretical value.

Spoofer detection

In the case of a spoofing attack in contrast to a jammer the C/N_0 value rises above its normal level because the received power of the spoofer, which will be tracked by the receiver just like a satellite, is higher than the power of the received satellite signal. The spoofer power has to be higher to enable an efficient spoofing attack, because otherwise the receiver would still track the real satellite signal. All three detection stages described above are therefore also applied for spoofer detection. The relative thresholds are chosen with the same offset but above the theoretical level and the absolute threshold is at a value of 60 dBHz.

3.2.2. Baseband monitoring

Baseband monitoring is based on the spectral characteristics of the received signal at intermediate frequency. The current PSD is periodically computed and evaluated as well as the noise floor level of the signal. Deviations from the common form of a PSD of the currently monitored signal type or unusually high noise floor levels indicate an interferer. A big advantage of the baseband monitoring is that the processing delay for the detection is much shorter than for C/N_0 or position monitoring. When computing the PSDs of the signal with quite large overlap, the results can be evaluated in shorter intervals (typically down to a minimum of 0.1 seconds depending on the sampling frequency) and a detection is possible without almost any processing delay. C/N_0 or position monitoring on the other hand require a full measurement step to be performed and therefore have a delay as large as the measurement interval, which will often have a magnitude of about one second.

3.2.3. Position monitoring

The position monitoring algorithm uses the known reference position of the receiver to compute the current offset to the PVT solution. Derived from this, the detection is a simple threshold based decision, whether the position offset in all three coordinate directions is above a certain allowed maximum value or not.
This can be used as detection method because the receiver has to stay at a constant and known position during the whole monitoring process. Therefore deviations in the PVT solution that are above the usual noise level are mainly caused by environmental sources. As multipath can easily by excluded by the chosen receiver position and surroundings, remaining significant errors are most likely to be caused by interfering signals. Analog to the other monitoring modules, the position monitoring reports changes in the detected interferer situation to the final detection stage.

3.2.4. Final detection

The final detection as introduced in Figure 3.10 as central detection stage distinguishes between three different states for jammer and spoofer. There can be no detected interferer, an interferer warning and an interferer alarm. Each of them can be detected for jammer as well as spoofer respectively.

No interferer: If none of the monitoring algorithms detect an interferer, there is no warning output and the user can assume that there is no disturbance large enough to lead to a malfunction or deterioration of the system within the specified values.

Interferer warning: An interferer warning is not yet critical, but the first stage of detection. This warning is output if just one monitoring algorithm detects an interferer, and the reference position has no significant deviations. The interferer warning could mean a real detected interferer, but there is also a significant possibility for a false alarm.

Interferer alarm: If multiple monitoring processes detect an interferer, an interferer alarm is output, meaning that there is a high risk of interference. The possibility for a false alarm is very low, because the different monitoring modules work independently from each other and are derived from different physical fundamentals. A detection in the position monitoring module directly leads to an interferer alarm, independent from the results of the other modules.

Spoofer detection

Spoofer detection is a little bit special here in the sense that a distinction between jammer and spoofer is only implemented in the C/N_0 monitoring module (because the baseband processing modules are not significantly affected by a spoofing attack). So in case the C/N_0 module detects a spoofer but the position is still not distorted, a spoofer warning is output and if the position module detects an interferer it will be classified as jammer unless the C/N_0 module detects a spoofer. Positive interferer detection by the position module together with a spoofer detection in the C/N_0 module thus leads to a spoofer alarm. The baseband detection modules though can independently report a jammer warning or alarm at the same time.

3.2.5. Data storage

As long as the receiver is processing data with an active monitoring module a buffer of a predefined length (two seconds in the current implementation) is constantly filled with the incoming raw data samples (received signal). In case the monitoring detects an interferer, the data storage module is called and stores the current contents of the buffer. From that time on the new raw data samples are given directly to the data storage module to be appended to the saved data from the buffer. After the interferer cannot be detected any more, the storage module still keeps further two seconds of data and afterwards stores all this data to a file.

This procedure ensures that the data storage module can store the raw data during the whole interferer event and also some time before and after. Using this data it is possible to reprocess the whole processing chain and also review the detection of the interferer.

Main use for this data storage module is to disconnect the classification from the current monitoring to execute these steps separately. Thus the raw data during the interferer event can be read in for the classification as often as necessary and processed with different parameters.

3.3. Classification

Classification of an interferer and storage of the result is useful to get an overview of the general interference situation at the location of the installed GAIMS system and is a foundation for a future localization of interferer. This section describes the implemented classification algorithm as well as the interaction of the user with the single modules.

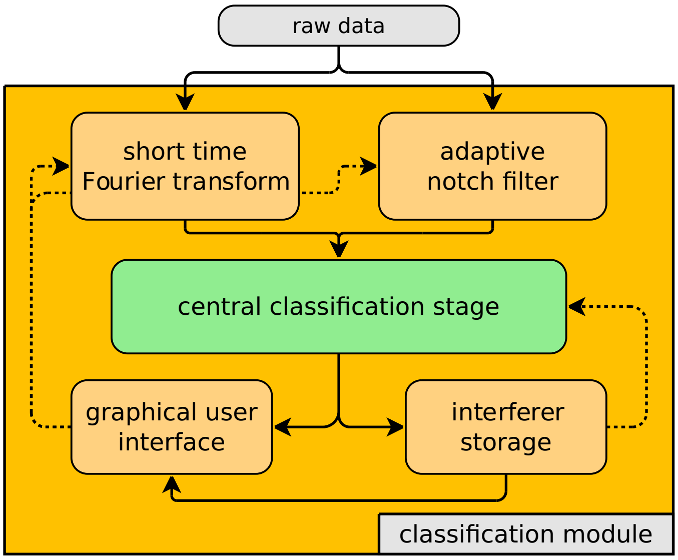
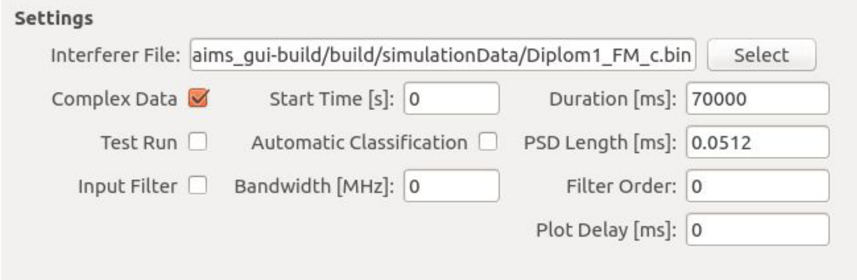


Figure 3.13.: Concept of classification process

As can be seen in Figure 3.13, the current implementation of the classification module is based on two different techniques. The interferer parameters are estimated using a short time Fourier transform (STFT) on one hand and an adaptive notch filter (ANF) on the other hand.

The central classification stage uses the estimated parameters of the ANF as well as the STFT result, where the computation parameters can manually be set using the graphical user interface. The classification result is displayed in the GUI and compared to all stored interferer incidents to find similarities or chronological patterns, which is performed by the interferer storage module.

Classification settings: Figure 3.14 shows the user interface to choose the settings of the classification process. The user can specify the file to read the data and whether the input data is complex. Start time and duration can be defined by the user in the postprocessing case. A preprocessing step (test run button in the GUI) can be selected to search for the time with maximum interferer power and the automatic classification can be enabled or disabled. The PSD length sets the number of samples used to compute one power spectral density for the STFT, which highly influences the classification.



Settings

Interferer File: aims_gui-build/build/simulationData/Diplom1_FM_c.bin

Complex Data ☑ Start Time [s]: 0 Duration [ms]: 70000

Test Run □ Automatic Classification □ PSD Length [ms]: 0.0512

Input Filter □ Bandwidth [MHz]: 0 Filter Order: 0

Plot Delay [ms]: 0

Figure 3.14.: GUI - settings for classification

For some data it might be useful to enable the use of a low-pass filter for preprocessing of the input data, which can be selected in the GUI. This filter removes unused parts of the PSD to improve the estimation of the classification parameters by filtering potentially misleading noise samples.

Estimated parameters: Different parameters of interferer are estimated in the central classification stage. The first decision is whether the interferer is a jammer or spoofer. In the case of a GNSS jammer further parameters can be estimated and different types of jammers are distinguished. Table 3.1 shows an overview of the specific parameters that are estimated for each jammer type. Some general characteristics are computed in each case in addition to the type-specific jammer parameters. These are the frequency offset and received interferer power as well as the duration of the interference incident.

Table 3.1.: Estimated jammer parameters

FM jammer	**AM jammer**	**CW jammer**	**SCW jammer**
frequency offset	frequency offset	frequency offset	frequency offset
mod. frequency	mod. frequency		bandwidth
frequency deviation	modulation index		sweep duration
received power	received power	received power	received power
duration	duration	duration	duration

3.3.1. Computation modules

Two main computation modules are used for the classification of jammers: the short time Fourier transform and an adaptive notch filter.

Short time Fourier transform

The short time Fourier transform generally consists of multiple Fourier transforms over a certain time period. The classification process uses PSDs to build the STFT instead of simple Fourier transforms to correctly estimate the received jamming power. Each PSD

has a specified length that can be chosen by the user. This user-defined length in combination with the data sampling frequency defines the temporal and spectral resolution of the STFT, because the single power spectral densities are computed directly after each other without gaps or overlaps. With this, the temporal change in the power spectrum of the received signal can be visualized and therefore the interferer situation can be analyzed.
The PSD computation in the current implementation is done by Welch's method (Welch (1967)). In this algorithm the input signal is split into several shorter segments with a certain overlap. Each segment is then windowed in time domain using an appropriate filter function (e.g. boxcar or Hann). After windowing, a discrete Fourier transform (DFT) is used to compute the spectrogram of each segment and the segments are averaged over time to reduce the noise.

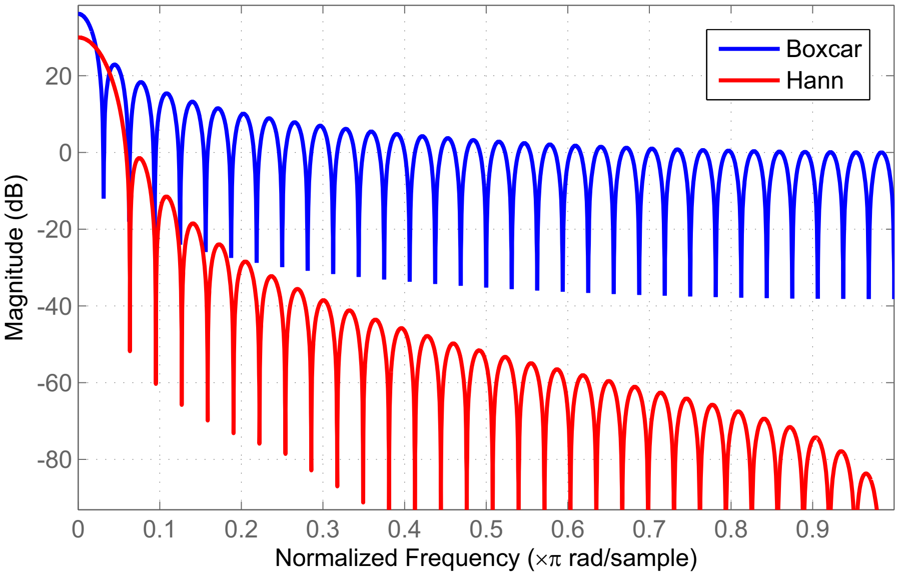


Figure 3.15.: Magnitude response of considered filter functions

Figure 3.15 shows why the Hann window is an appropriate choice for the filter function in the PSD computation. The frequency response has a significantly higher main lobe and smaller side lobes than a simple boxcar (rectangle) filter. The greater width of the main lobe leads to a slightly worse effective frequency resolution, but the impact of noise on the estimation of the jamming power is reduced. This is considered to be more important for the classification as the noise would distract the estimation of the jammer's frequency.
Temporal and spectral resolution of the STFT are inversely proportional, because a higher temporal resolution can only be achieved by choosing shorter PSD lengths which in turn reduces the spectral resolution because less samples can be used for the computation of each PSD. According to the characteristics of the jammer (bandwidth and repetition rate) the user must choose the trade-off between temporal and spectral resolution to enable the best suited parameter estimation.

To estimate the interferer power I it is important to reduce the computed power M from the PSD by the thermal noise floor in each frequency bin. This is done using the relation

$$I = (M - k_B T_0) \cdot f_s / N \ , \tag{3.1}$$

where k_B is the Boltzmann's constant and T_0 denotes the receiver noise temperature in Kelvin. f_s in this equation is the sampling frequency and N the number of samples used to compute each PSD as described in section 2.2.1.

Output to classification algorithm: Output of the STFT module to the classification algorithm is a vector consisting of the frequencies with maximum interferer power for each timestep along with a vector containing these maximum powers as well as the powers of the second largest peaks. Since the size of the frequency bins varies according to the PSD length it can be necessary to sum up more than one frequency bin around the maximum power to avoid an overflow to neighboring and therefore ignored bins. These vectors contain the progress of the estimated interferer frequency and power over time and therefore are the basis for the interferer parameter estimation.

Adaptive notch filter

The adaptive notch filter (ANF) is implemented according to section 2.2.3 and the filter's notch frequency ω_0 is used for the classification and output to the central classification stage. Input to the filter are the raw data samples that have previously been stored by the detection thread. Therefore the resulting sampling for the classification directly corresponds to the raw data sampling frequency. This leads to a substantially higher temporal resolution than in the STFT-based classification.

Nevertheless the so-called "forgetting factor" λ of the adaptation algorithm influences the effective temporal resolution too. Higher values of λ enable faster adaptation of the filter but also increase the noise, which may impair the quality of the estimated parameters.

An important characteristic of the ANF is that the first few estimates of ω_0 are naturally not valid because there is no valid initial value and the algorithm needs some time to adapt to the current interference situation. Therefore the classification algorithm must not use these first samples.

Main drawback of the ANF-based classification beside a possible noise due to bad choice of λ is that there is no possibility to estimate the received power of the interferer. Because of this, the absence of any interferer leads to large variations of ω_0 due to noise only. As soon as an interferer has sufficient power to significantly disturb the incoming signal, the ANF is able to reliably track the interferer frequency.

As the output of the ANF is the filtered signal, where a certain range around the current interferer frequency has been filtered out, it is clear that this output must not be used as input for the STFT-based classification.

Output to classification algorithm: The output of the ANF module to the classification algorithm is a vector containing the estimated notch frequencies ω_0. This vector is an estimate for the progress of the interferer frequency over time and used as basis for the estimation of the interferer parameters.

3.3.2. Work-flow

Classification of GNSS jammers is a task which is typically performed semi-automatic. This means that the estimation of jammer type and parameters is automated but some settings must be set by the user according to the specific jammer in order to achieve an accurate result. Classification therefore is an iterative task in most cases until the best suiting settings for the classification algorithm are found.

The parameters for every implemented type of jammer are estimated in each classification step, which enables the user to easily override and correct a possible wrong estimation of the type. The user is then able to change some estimation settings based on the obtained classification result to find a more suitable solution.

3.3.3. Jammer type distinction

Figure 3.16 shows how the different jammer types are distinguished. Input to the algorithm are the frequency and power vectors of the STFT module. For type distinction, the frequency vector of the largest power peak and the power vector of the second largest power peak are used.

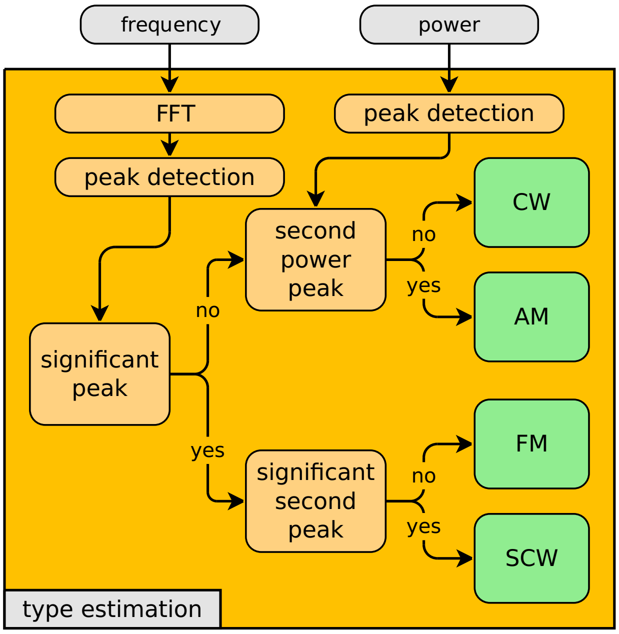


Figure 3.16.: Jammer type estimation

The algorithm starts with computation of a fast Fourier transform of the frequency vector. This spectral response is searched for significant peaks to decide, whether the frequency with maximum power changes over time. In the presence of a GNSS jammer, where the current jammer frequency is always the frequency with highest power, this information can be used to distinguish between AM/CW and FM/SCW jammers.

In the case of significant variations in the frequency vector, indicated by a peak in the spectral analysis, the jammer must be either of FM or SCW type. To further distinguish between these two types the second peak of the spectral analysis is investigated. The sine or cosine modulation wave of the FM jammer can be easily recovered by the spectral analysis and therefore leads to only one significant peak. On the contrary the SCW jammer shows periodic jumps in the frequency behavior, which cannot be estimated with only one sine or cosine wave. This leads to several significant peaks in the spectral analysis. Therefore a significant second peak in the spectral analysis indicates a SCW jammer, where the absence of a second peak indicates a FM jammer.

If no significant peaks at all can be found in the spectral analysis of the frequency vector, the jammer must be of CW or AM type where the jammer frequency stays constant over time. A CW jammer has constant frequency and amplitude and therefore shows only one peak in the PSD of the signal, which is at the jammer frequency and has a height indicating the power of the jammer. An AM jammer on the other hand leads to a peak in the PSD of the signal at its frequency but also a second peak, which comes from the amplitude modulation. This second peak has a distance from the main peak depending on the modulation frequency and its height in relation to the height of the main peak depends on the modulation index.

Figures 3.17 to 3.20 show the short time Fourier transform of all four jammer types, the GAIMS can distinguish. The figures confirm the assumptions made on the signal's frequency response discussed in section 2.5 that are exploited for the type distinction.

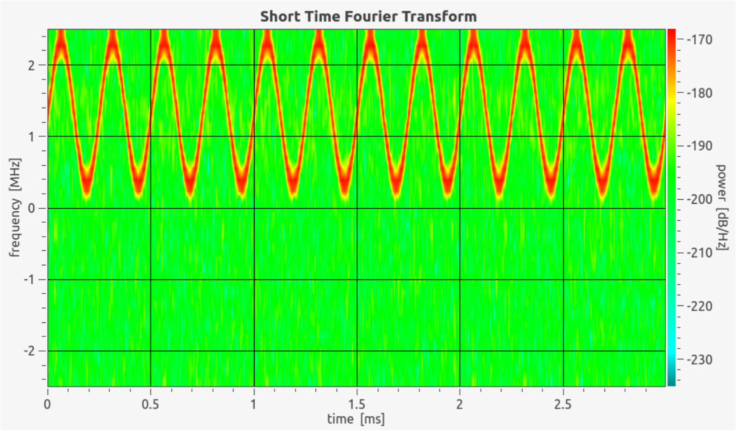


Figure 3.17.: STFT of FM jammer

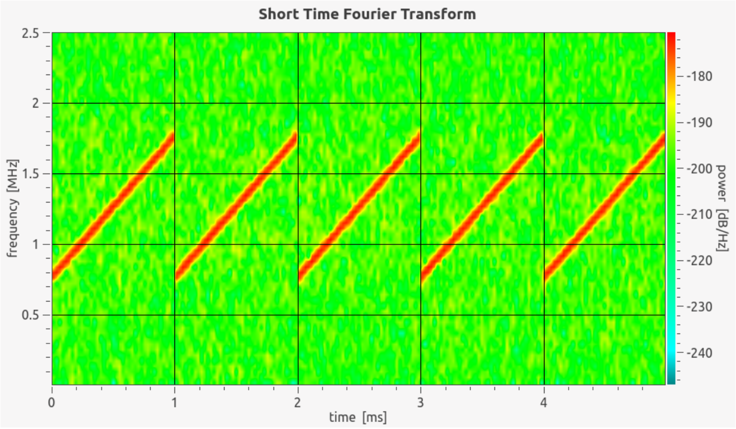


Figure 3.18.: STFT of SCW jammer

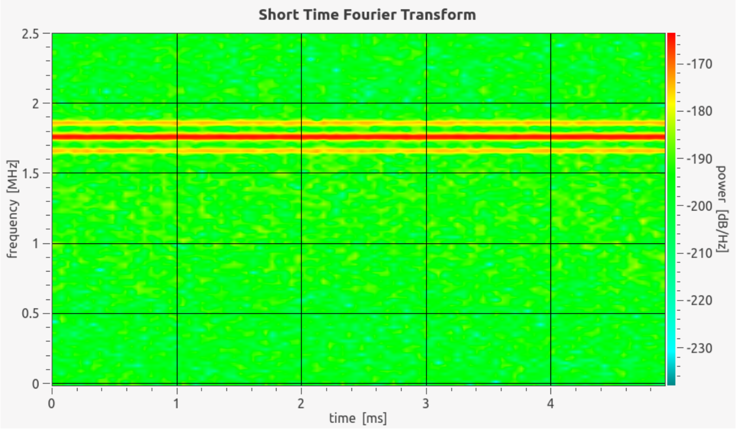


Figure 3.19.: STFT of AM jammer

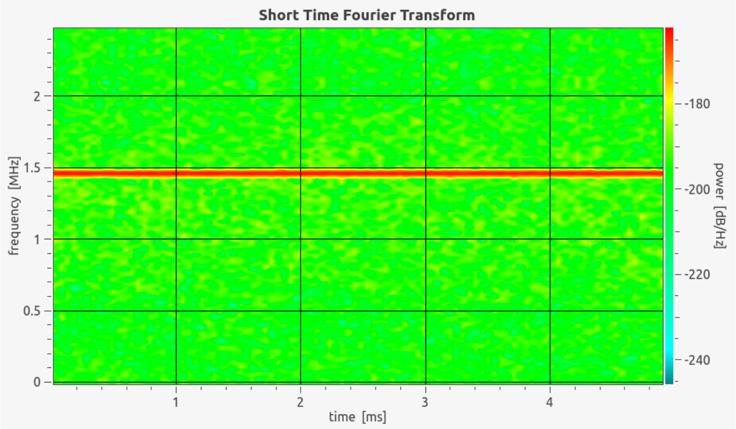


Figure 3.20.: STFT of CW jammer

3.3.4. Parameter estimation

According to Table 3.1, different parameters are estimated for each type of GNSS jammer. The estimation of these parameters is based on the changes of jammer frequency and power over time and can generally be done with the results of both computation modules (STFT and ANF). Parameters requiring the power though can only be estimated using the STFT. Some parameters additionally need the local maxima and minima of the frequency vector to be estimated. For this reason an algorithm searches and stores these peaks in a preprocessing step. This preprocessing peak detection algorithm is based on the fact that the frequency maxima/minima of a jammer are repeated periodically in time. Therefore the FFT of the jammer frequency vector reveals the distance between these peaks, which is used to limit the search space for each local extremum. Starting from the global maximum and minimum of the frequency vector the next local extremum is predicted based on that estimated distance. The global maximum/minimum inside a certain range around this prediction then corresponds to the respective local extremum and is used as starting point for the next prediction.

The following explains the estimation of all jammer parameters in detail. This estimation is based on the frequency vector, the power vector and the local maxima and minima explained above.

Offset frequency: This parameter denotes the offset of the jammer's center frequency to the frequency of the GNSS signal that is being disturbed. When computing the PSD of the input signal from the RF front-end, the zero frequency corresponds to the signal's frequency. For this reason the mean value of the estimated jammer's frequency over time results in the offset frequency.

Offset frequency is estimated for all types of jammers. For jammers with varying frequency over time though the mean value must be computed between a local maximum and minimum as start and end points to avoid a distorting offset due to a leakage effect.

Modulation frequency: Jammers of FM or AM type are modulated with a certain modulation frequency. For a FM jammer this frequency can be estimated using the local maxima and minima of the frequency vector. The distance between each maxima or each minima corresponds to the wavelength of the modulation, for which the modulation frequency is the reciprocal mean distance between the extrema.

For an AM jammer lacking of any frequency maxima and minima the distance between the highest and the second highest peak in the PSD of the input signal indicates the modulation frequency. This frequency thus is estimated as the mean value of this distance over time.

Frequency deviation: FM jammers show a variation in the frequency with a certain modulation frequency which was explained above and a deviation which denotes the offset of the jammer's frequency from the center frequency caused by the modulation. This parameter is estimated by computing the difference of the maxima and minima from the central frequency and averaging them over time.

Modulation index: The modulation index of an AM jammer indicates how much the amplitude of the modulated signal varies from the unmodulated carrier. To estimate this parameter the difference between the values of the highest and second highest peak of the PSD of the input signal is used. The modulation index M is estimated by computing the time average over

$$M = 2/10^{(\Delta A/20)} \, , \tag{3.2}$$

where ΔA denotes the difference between the two peaks in dB.

Bandwidth: Bandwidth of a SCW jammer is similar to the frequency deviation of a FM jammer. The difference between the maximum and minimum frequency of the jammer is denoted as bandwidth. It can be estimated by averaging the difference between each maximum and the subsequent minimum of the frequency vector over time.

Sweep duration: The time for each sweep of the sawtooth function generating the SCW jammer is denoted as sweep duration. It can be estimated by computing the time average over the difference between the positions of two consecutive maxima and minima of the frequency vector.

3.3.5. Interferer storage

The interferer storage module uses an American standard code for information interchange (ASCII) file to store all classification results for later use. Every time an interferer is classified, the corresponding classification results are used to find similar interferer incidents based on the estimated parameters.

Users can add a comment as well as date and time of the interferer incident. Duration, power and all estimated parameters of the classified interferer of the selected type are stored. Each time the program starts all classification results are loaded from the ASCII file and stored in a structure based on the interferer type. This ensures a fast access to the data when needed.

3.4. Implementation in software

The software for the GAIMS project and this thesis has been developed in C++ after testing some modules and algorithms using code snippets in MATLAB. It is based on previously existing C++ modules from TeleConsult Austria GmbH that have been extended and refined during the development. In addition some modules from the BOOST C++ library were used. The graphical user interface has been developed in the Qt framework using the Qwt library for the creation of the plots.

One important aspect during development was a strict separation between functionality and user interface to make sure that command-line usage of the software is also possible. This separation also has the effect of a handy and fast user interface though performing tasks that have a high computational burden, because computations and GUI operations run in different and independent threads.

Main framework for the developed software is the software-defined radio from TeleConsult Austria GmbH in which the interference monitoring and classification modules were integrated together with the GNSS interference analysis tool (GIAT) for the computation of the theoretical $(\mathrm{C}/\mathrm{N}_0)_{\mathrm{eff}}$. This thesis covers the estimation of the actual carrier-to-noise ratio and integration of the theoretical values from the GIAT together with the C/N_0-based detection algorithm as well as all classification modules.

The development of the software - especially the collaboration inside the project team - was managed using the version control system `git`. QtCreator running on a computer powered by Ubuntu Linux was used as development environment. Further information on all used third-party software modules can be found in Appendix A.

4. Evaluation and results

This chapter presents important results and an evaluation of the developed algorithms. The results of the detailed tests of the developed algorithms and software are shown using simulations as well as recorded real-world data from a GNSS front-end. The simulation proves the accuracy and correct implementation of the developed algorithms, while the real-world data tests prove the qualification for an environmental use.

4.1. Test cases

The evaluation of the developed software and implemented algorithms is performed using different test cases for each interferer type based on a simulation of the GNSS signals. Detection and classification are tested independently for each of these test cases. In addition to the simulated data also recorded real-world signals from a GNSS front-end are used to test the detection and classification algorithms under realistic conditions.

4.1.1. Simulation

The performance evaluation of the developed algorithms is performed using a closed-loop simulation, where the parameters to be estimated can directly be set in the simulation. Comparing the estimated values to the simulated ones shows the performance of the algorithms regarding detection time and classification accuracy.

GNSS signals are simulated with and without different types of jammers. The parameters of these jammers are varied as well as the characteristics of the GNSS signal itself (e.g. sampling and intermediate frequency, signal length and GNSS constellation) to test the performance of the detection and classification modules under different conditions. As numerous tests have been performed during the development and evaluation of the software, only the main results are presented and discussed here.

4.1.2. Recorded real-world data

Recorded real-world data are used to test and evaluate the performance of the developed algorithms under realistic conditions. The recorded signals in these cases include the GNSS signals as well as disturbances from other electromagnetic waves in the monitored frequency band and the environment. Environmental influences include shadowing and multipath effects as well as losses caused by the signal propagation through the atmosphere, which cannot be prevented or estimated perfectly.

4.2. Simulated data

The evaluation of the performance of the developed software modules and algorithms is done using an accurate simulation of the received GNSS signals considering the satellite constellation, signal specifications and jammer parameters. The satellite constellations of all considered GNSS has been simulated along with the position of the user and environmental dependencies (e.g. propagation loss due to the atmosphere). The simulations result in digital signals at intermediate frequency (IF), which can directly be processed by the developed software.

4.2.1. Signal generation

The GNSS multisystem performance simulation environment (GIPSIE®) developed by TeleConsult Austria GmbH (2010) is a tool to simulate GNSS signals for a specific constellation. Receiver position and satellite orbits can be chosen for different GNSS and simulated together with other parameters regarding receiver movement and environmental effects using the satellite constellation simulator (SCS). The intermediate frequency signal simulator (IFS) can be used to generate simulated signals out of the SCS output as received from a GNSS front-end at intermediate frequency.

All simulations used for evaluation were generated using the GIPSIE® and use the current GPS constellation as basis. Within the IFS it is possible to simulate different types of GNSS jammers including AM, CW, FM and SCW. As the parameters of the jammers can be arbitrarily selected, the accuracy of the classification algorithm can be assessed.

4.2.2. Simulated data sets

All scenarios were generated for a specified user position of $\phi = 46.9965°$, $\lambda = 15.4462°$, $h = 340.0$ m and time of 12:09:53 on September 8th 2014 using the GIPSIE®-SCS. The scenario was then used for the generation of the simulation files including GNSS jammers using the GIPSIE®-IFS.

All simulated signals presented here were generated with a sampling frequency of 5 MHz and an intermediate frequency of 0 Hz. The simulations include GPS L1 C/A signals as well as the current Galileo in-orbit validation (IOV) satellites (OS-signal on E1 frequency band).

Table 4.1 provides an overview on the different test cases. As the table shows, each simulated signal has the same length of 100 s with a jammer starting after 60 seconds for Sim01 to Sim04 with varying power. The variation of interferer power is set that it increases linear (by means of dB) from the start time (60 seconds) until it reaches its maximum power (75 seconds) and afterwards decreases again until the end time (90 seconds) of the interferer. A simulation with a maximum power peak in the middle of the jamming event corresponds to a real environmental situation where a vehicle equipped with a GNSS jammer passes the antenna.

Table 4.1.: Test cases using simulated data

name	signal length	interferer type	interferer event	interferer power
Sim00	100 s	no	–	–
Sim01	100 s	AM	60 to 90 s	-160 to -135 dBW
Sim02	100 s	CW	60 to 90 s	-160 to -135 dBW
Sim03	100 s	FM	60 to 90 s	-160 to -135 dBW
Sim04	100 s	SCW	60 to 90 s	-160 to -135 dBW

Sim00: This simulation contains no interferer and is intended to test the monitoring algorithm for the probability of false alarms. The parameters for the detection process can be tested and adapted based on the processing results of this simulation only containing the GNSS signals and thermal noise.

Sim01: An amplitude modulation jammer is simulated in this file. Table 4.2 contains the parameters of the simulated AM jammer, where the maximum power stated in the table is reached at a time of 75 seconds. Start and end time of the interferer event can be found in Table 4.1 and are the same for every simulated jammer.

Table 4.2.: Sim01: simulated AM jammer parameters

parameter	value
offset frequency	0.5 MHz
modulation frequency	10 kHz
modulation index	60%
maximum power	−135 dBW
duration	30 s

Sim02: Simulation file Sim02 contains a continuous wave jammer with the same progress of interfering power over time than in simulation Sim01. The parameters of this CW jammer can be found in Table 4.3.

Table 4.3.: Sim02: simulated CW jammer parameters

parameter	value
offset frequency	0 Hz
maximum power	−135 dBW
duration	30 s

A comparison between the classification results of the simulations Sim01 and Sim02 is interesting regarding the performance of the distinction between AM and CW jammers. This distinction is not trivial as both of these jammer types do not vary their frequency over time.

Sim03: This simulation file contains a frequency modulation jammer interfering the GNSS signals. Table 4.4 contains the parameters of this FM jammer.

Table 4.4.: Sim03: simulated FM jammer parameters

parameter	value
offset frequency	0 Hz
modulation frequency	2 kHz
frequency deviation	1 MHz
maximum power	−135 dBW
duration	30 s

Sim04: Simulation Sim04 contains a swept continuous wave jammer, which is particularly interesting regarding the performance of the distinction between FM and SCW jammers. This is because the modulations used for these types of jammers result in a similar frequency response with varying frequency in a certain bandwidth. The parameters of this SCW jammer can be found in Table 4.5.

Table 4.5.: Sim04: simulated SCW jammer parameters

parameter	value
offset frequency	0.5 MHz
sweep duration	0.1 ms
bandwidth	1 MHz
maximum power	−135 dBW
duration	30 s

4.2.3. Performance of detection algorithm

This section presents the detection results for the processed simulations Sim00 to Sim04. It shows how the detection works in presence and absence of GNSS jammer. The detection was performed by the algorithms described in section 3.2, based on GPS C/A-code tracking in the receiver.

Simulation - Sim00

During the processing of the simulated data file Sim00 no interferer was detected at all. None of the implemented detection algorithms (i.e. baseband, position, C/N$_0$) output a jammer or spoofer warning. This result shows that the implemented methods of interferer detection do not produce false alarms when working with simulations considering only the desired GNSS signals as well as a noise component to simulate the environment.

Figure 4.1 shows the carrier-to-noise ratio of the simulated data for a time period of 60 seconds. The dotted lines in the figure show the theoretical C/N$_0$, while the estimated values are indicated by the solid lines. As the estimated values do not differ significantly from the theoretical ones, this figure shows that the C/N$_0$-based detection algorithm lead to no false alarm indicating an interferer. Although the C/N$_0$ time series shows some variations with respect to the theoretical values, these deviations are smaller than the critical thresholds.

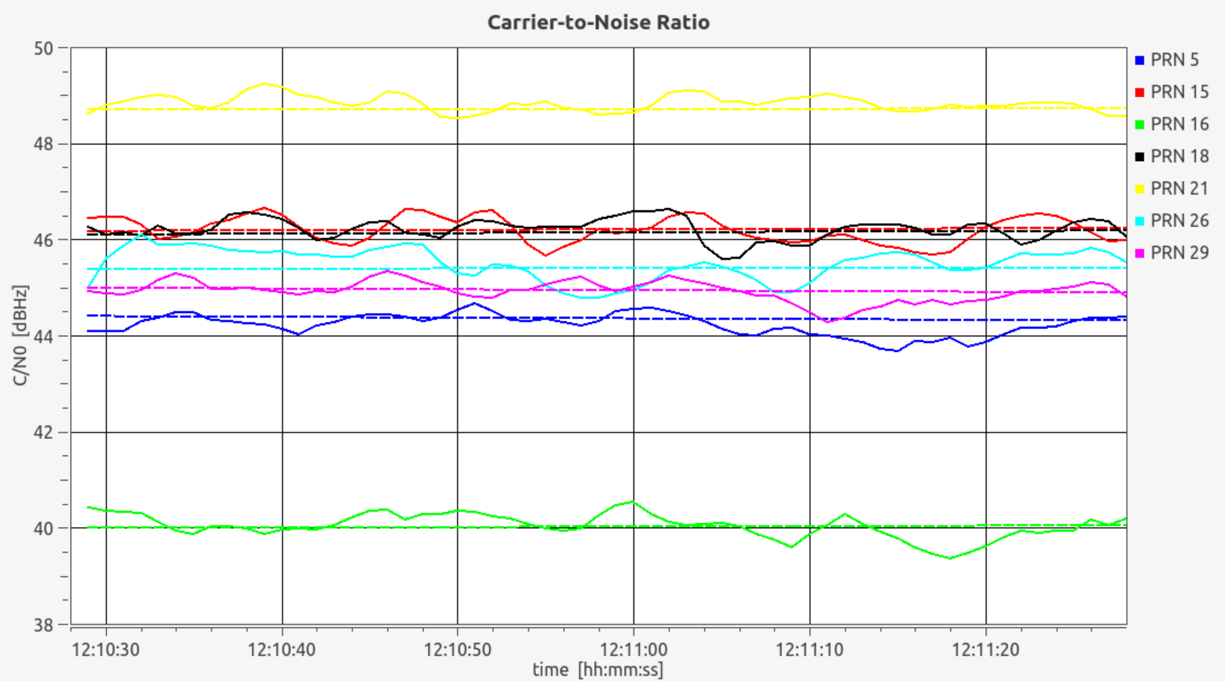


Figure 4.1.: C/N$_0$ time series of Sim00 simulation

The figure indicates that the different carrier-to-noise ratio values for each satellite, due to signal path differences mainly caused by different elevations of the satellite, are considered correctly at the computation of the theoretical values. This shows the correct behavior of the GIAT module because the signal generation in GIPSIE® is totally independent from the C/N$_0$ estimation in the GIAT and the values nevertheless correspond quite well.

Satellite number 16 has a carrier-to-noise ratio that is significantly lower than for the other satellites and which is indicated by the theoretical and estimated values correspondingly. The reason for this low C/N$_0$ is the elevation of the satellite in the simulated constellation, which has a value below 15°. Therefore the path of the signal through the atmosphere is longer, leading to a significantly higher propagation loss. Also the simulated antenna pattern attenuates signals from a lower elevation to reduce the risk of tracking multipath or interferer signals.

Simulation - Sim01

The processing of the simulation file Sim01 revealed the detection of a GNSS jammer for a duration of about 15 seconds. As this file contains the simulation of an AM jammer between a measurement time of 60 and 90 seconds, this detection was expected, although the simulated interferer incident (30 seconds) was longer than its detection.
Figure 4.2 shows a time series of the carrier-to-noise ratio, revealing the reason for this shorter detection. Due to the necessary smoothing in the computation of the C/N_0 and the rather slow increase of the jammer power, the algorithm needs some time before the interferer can be detected.

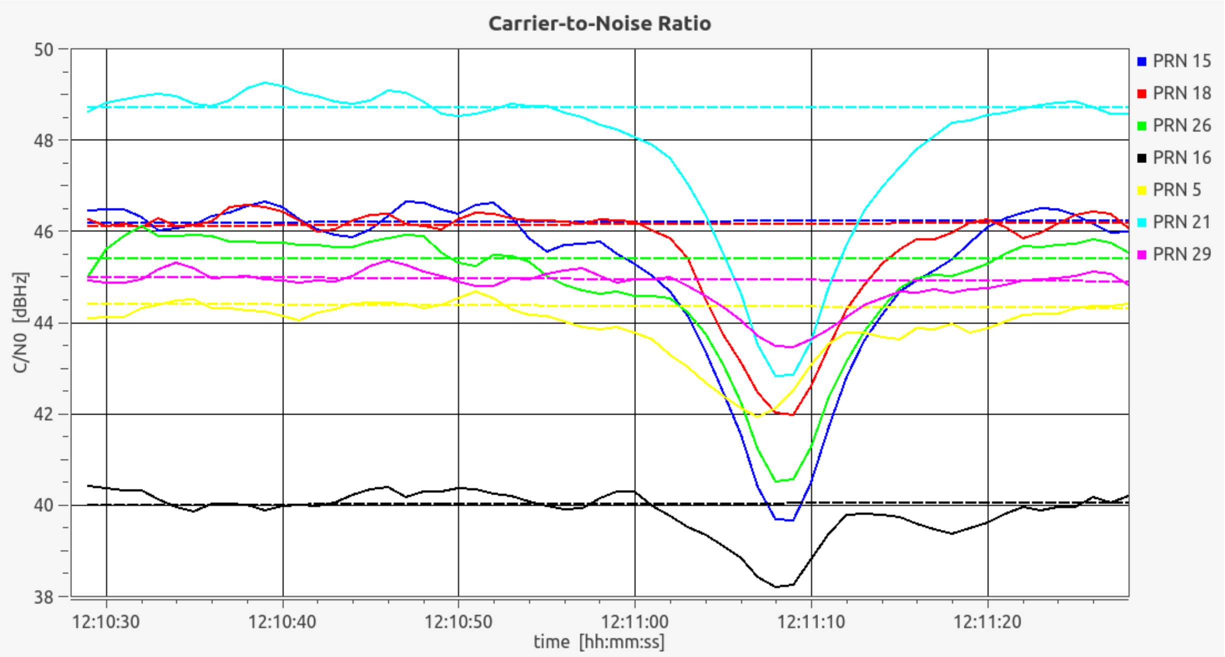


Figure 4.2.: C/N_0 time series of Sim01 simulation

An interferer is only detected when more than a certain percentage of satellites is significantly affected. In this case a threshold of 45% was used, which can be seen in Figure 4.3 and is intended to prevent false detections. In the case of Sim01 all satellites are almost equally affected by the interferer, which cannot be guaranteed in a real environmental situation and also depends on the frequency of the specific interferer. This differences can even be seen in the simulation in Figure 4.2, which shows that the effect of the jammer on the C/N_0 of the GPS satellites 16 and 29 is smaller than on the other satellites.
The C/N_0 based detection, according to Figure 4.3, also allows an approximated estimation of the time with maximum interferer power, which is at the maximum of affected satellites and corresponds to the time with minimum C/N_0 in Figure 4.2. This is estimated as 12:11:08 in this case, which corresponds to the simulation.

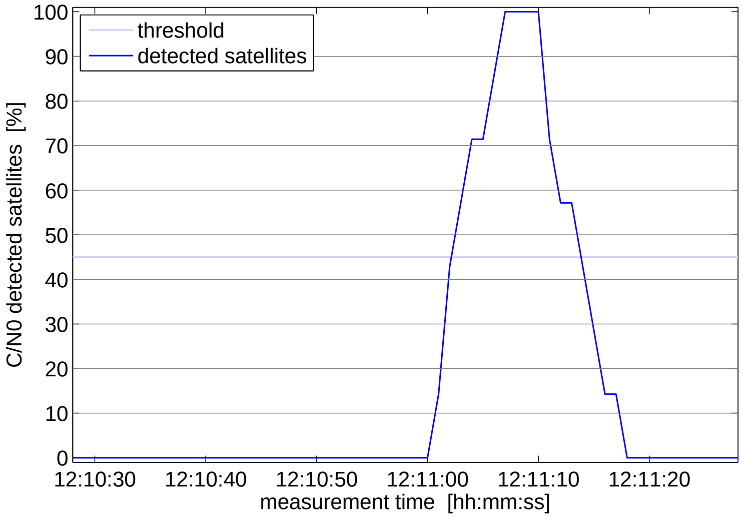


Figure 4.3.: C/N$_0$-based detection for Sim01 simulation

Simulation - Sim02

The simulated file Sim02 contains a CW jammer during a measurement time of 60 to 90 seconds, which transmits directly on the GPS L1 carrier frequency. This jammer has been detected during the processing for a duration of about 20 seconds. The increased detection period compared to Sim01 can be explained by the absence of any offset frequency of the jammer, which increases the effect of the jammer on the C/N$_0$. This increased impact of the jammer leads to a complete loss of tracking of GPS satellite 16, which is the weakest in the current simulation.

A time series of the carrier-to-noise ratio is shown in Figure 4.4, showing the rather large effect that the jammer has. The C/N$_0$ of all tracked satellites except GPS satellite 21 drops significantly as the jammer power rises. The reason for the missing effect on satellite number 21 can be related to the fact that this satellite has the highest nominal power due to its elevation. It is possible that the signal can be tracked without disturbances in this case. The loss of lock of satellite 16 is indicated in the figure by the end of the corresponding lines for the estimated and theoretical values as they cannot be computed correctly tracking the satellite.

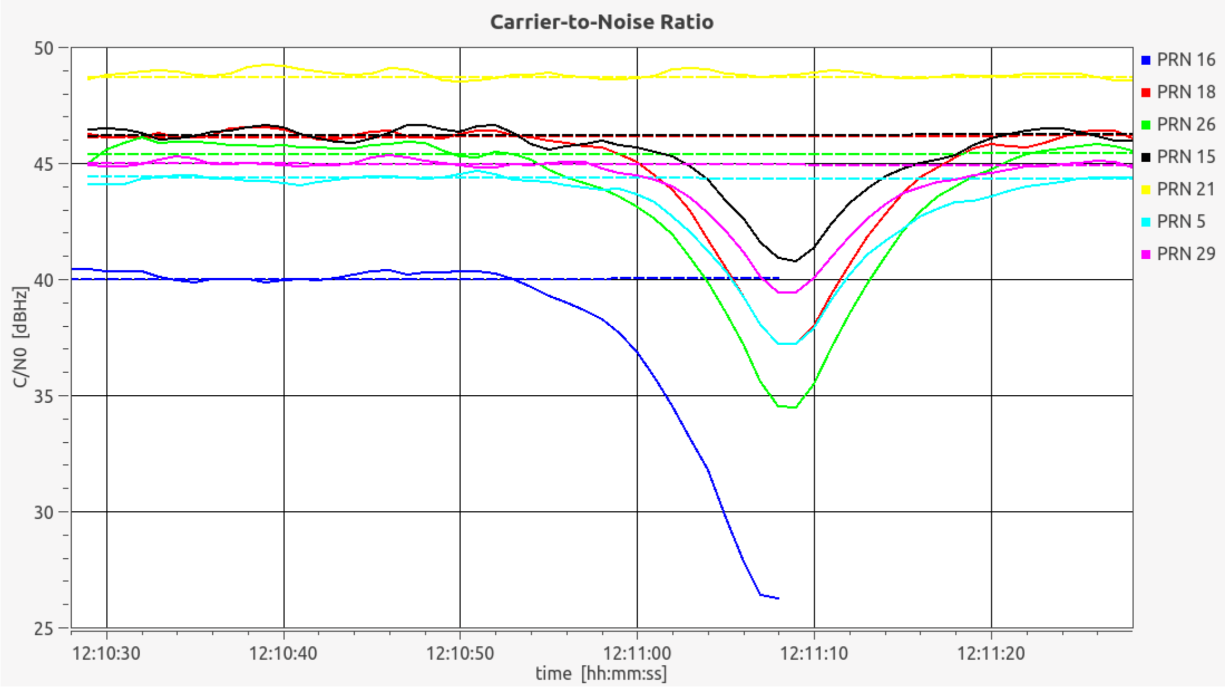


Figure 4.4.: C/N$_0$ time series of Sim02 simulation

Nevertheless the simulated jammer was successfully detected by all implemented algorithms. This example shows that a threshold of 45% of all tracked satellites seems rational because it is high enough to detect corresponding behavior of different satellites but low enough to tolerate single satellites that are not affected by an interferer. Figure 4.5 shows the percentage of satellites for which a jammer was detected based on the C/N$_0$.

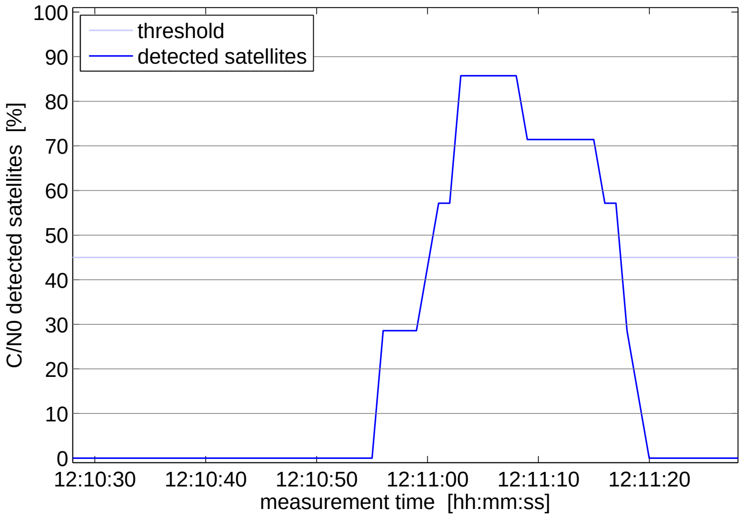


Figure 4.5.: C/N$_0$-based detection for Sim02 simulation

Simulation - Sim03

Sim03 contains a FM jammer between a measurement time of 60 and 90 seconds. As shown in Figure 4.6 the effect of the simulated jammer on the carrier-to-noise ratio is significant. Compared to Sim02 with a CW jammer directly on the carrier frequency, the drop in the C/N_0 is slightly smaller. This can be explained by the signal that the FM jammer emits, which has a varying frequency over time. The frequency in this simulated case varies between -1 and $+1$ MHz, which also leads to larger temporal variations in the impact of the jammer on the C/N_0. A FM jammer on the other hand has the same effect on all satellites in view, showing less differences between the single satellites compared to Sim01 or Sim02 where the jammers have a constant frequency.

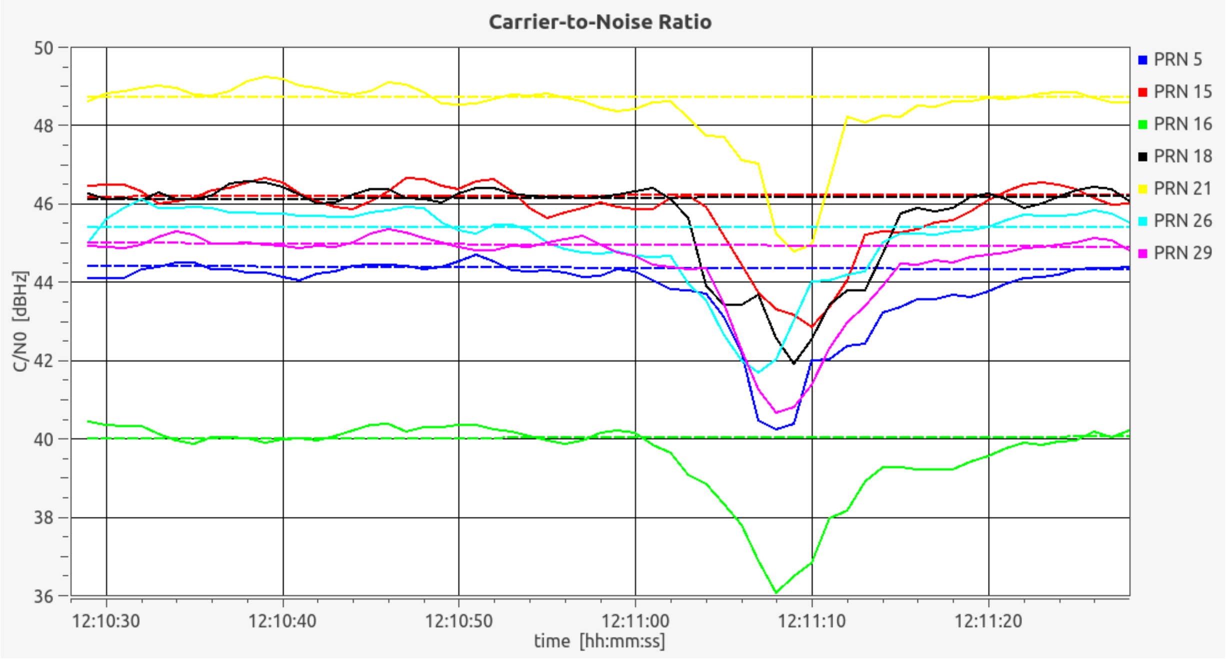


Figure 4.6.: C/N_0 time series of Sim03 simulation

Figure 4.7 shows the percentage of satellites indicating a GNSS jammer compared to the threshold of 45%. The figure shows that the detection time in this simulation is slightly shorter than in the other cases and the jammer can only be confidently detected for a duration of about 10 seconds. This is because of the smaller effect that this type of jammer has on the C/N_0, caused by the variations of the frequency. The results show that the implemented algorithms managed to reliably detect the FM jammer contained in this simulation.

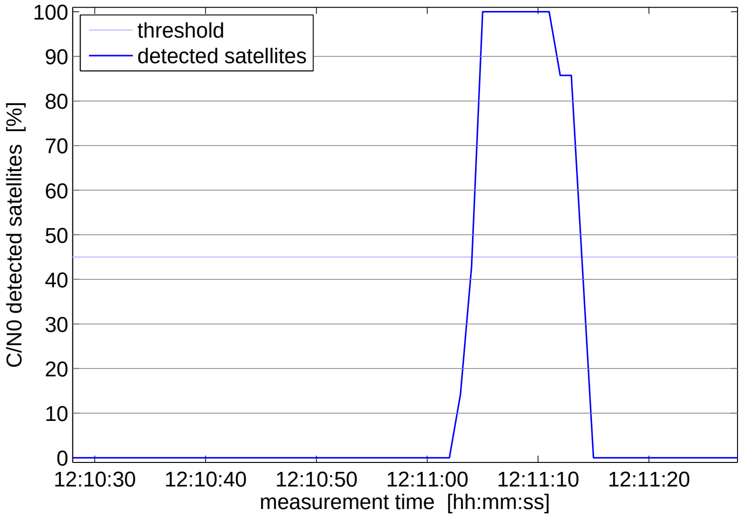


Figure 4.7.: C/N_0-based detection for Sim03 simulation

Simulation - Sim04

The processing of simulation Sim04 reveals a quite similar behavior of the C/N_0 during the jammer event as for Sim03. Figure 4.8 shows the carrier-to-noise ratio during the simulation, where the jammer was clearly detected. The jammer's effect is almost equal on each satellite, but showing significant variations with time due to the changes in the jammer's frequency.

Figure 4.9 shows the percentage of satellites indicating a jammer based on the carrier-to-noise ratio. As can be seen in the figure, a reliable detection is only possible for a duration of about 10 seconds due to the rise and fall of the jammer's impact on the C/N_0, which is typical for a SCW jammer.

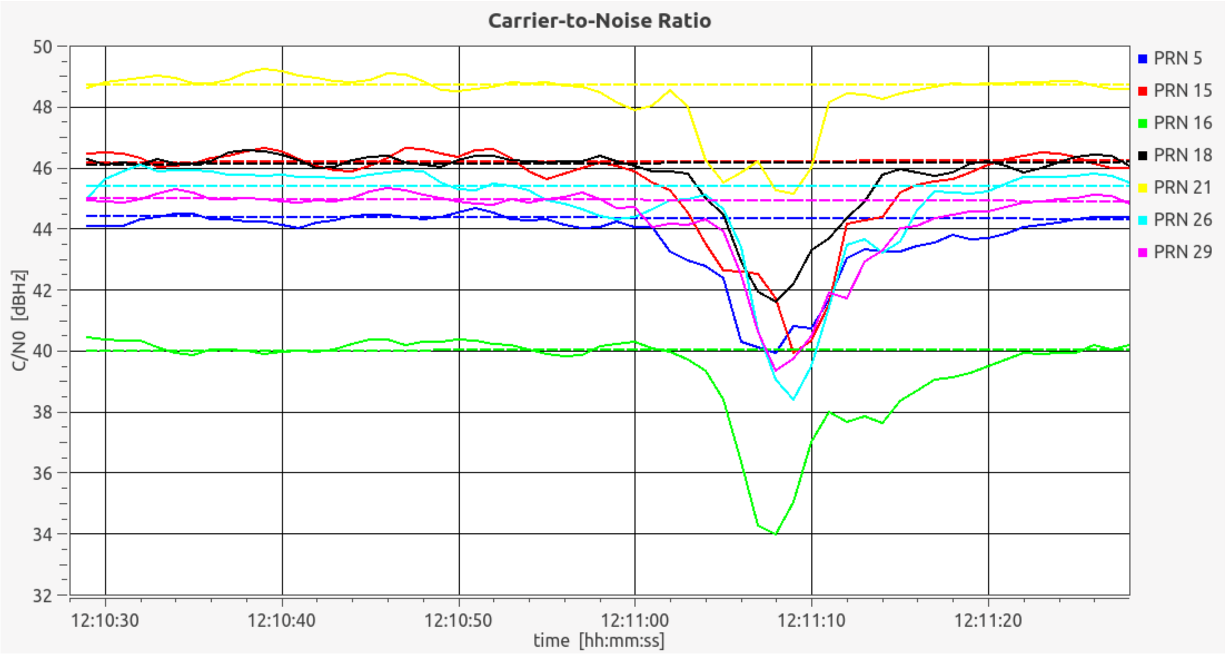


Figure 4.8.: C/N_0 time series of Sim04 simulation

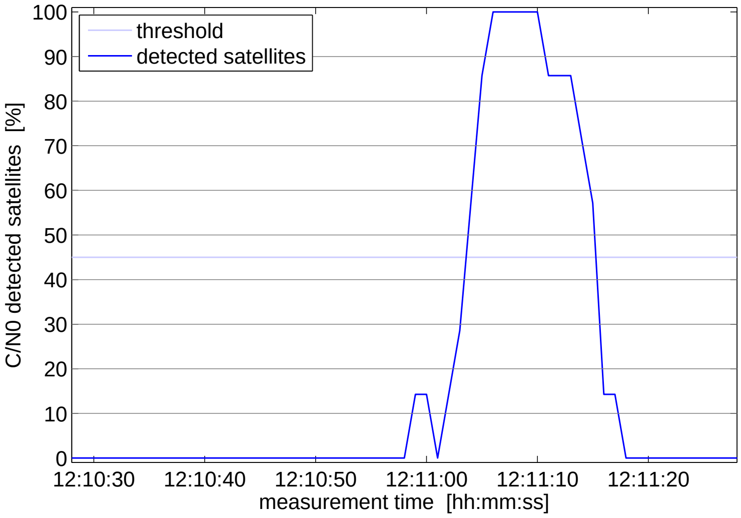


Figure 4.9.: C/N_0-based detection for Sim04 simulation

4.2.4. Performance of classification algorithm

This section shows an evaluation and the results of the classification of the detected jammers in the simulated files. The results of the preprocessing step as well as the automatic classification algorithm results are presented. Refer to section 3.3 for details on the implementation of the classification algorithms.

Simulation - Sim01

The progress of the estimated jammer power based on the PSD of the signal is shown in Figure 4.10. The progress shown in the figure clearly corresponds to the simulated jammer starting with −160 dBW at a measurement time of 60 seconds and a linear rising until it reaches a power of −135 dBW. After the maximum is reached at a measurement time of 75 seconds the power decreases again until the jammer vanishes after 90 seconds measurement time.

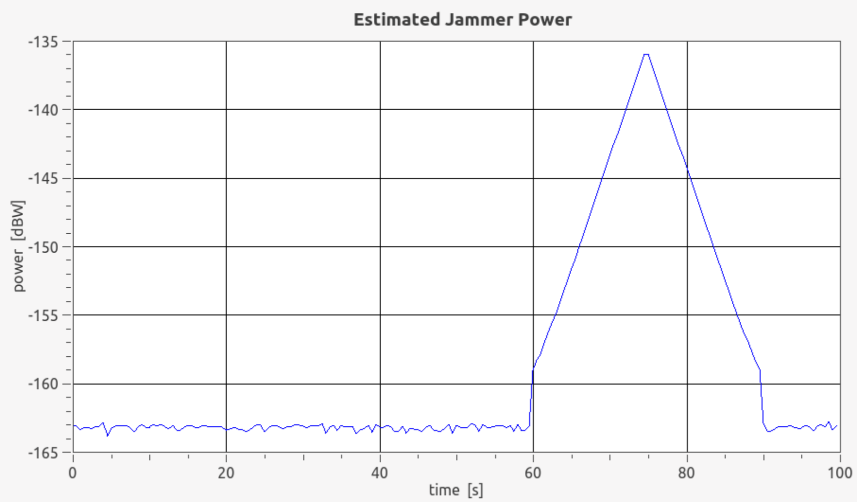


Figure 4.10.: Preprocessing - jammer power of Sim01 simulation

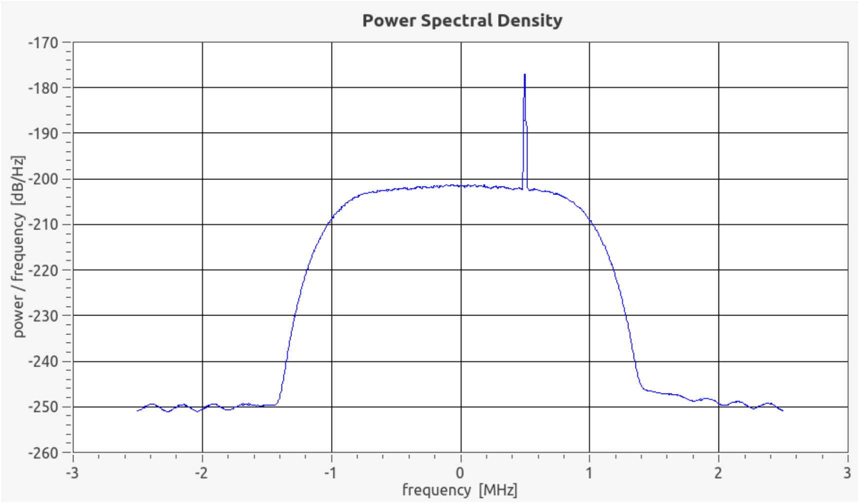


Figure 4.11.: Preprocessing - PSD of Sim01 simulation during jammer event

Figure 4.11 shows a PSD of the signal during the jammer event using the preprocessing PSD settings. With this preprocessing step the time of maximum jammer power can be easily detected and selected as time for the classification. The figure clearly shows the jammer with its frequency offset with respect to the carrier frequency and also shows the effect of the input filter on the signal. The input filter as described in section 3.3 can be used to exclude certain parts of the spectrum, which helps improving the jammer classification.

Table 4.6.: Sim01: classification settings

start time	75 s	PSD length	3.2768 ms
processing time	29.4912 ms		
input filter BW	2 MHz	input filter order	21

The settings used for the classification of the jammer in simulation Sim01 can be found in Table 4.6. As the table shows the classification time is selected as 75 seconds after start of the simulation, which corresponds to the time of maximum jammer power. The PSD length is selected rather large, which can enhance the estimation of power and frequency in the case of a constant jammer frequency which is the case for the simulated AM jammer. The PSD length is changed automatically by the software corresponding to the sampling frequency to match a sample count which is a power of two. This enhances the computational performance of the Welch's algorithm for the PSD computation. The processing time is automatically adapted to match the selected PSD length.

Figure 4.12 shows the computed STFT of the Sim01 simulation during the jammer event. As expected for an AM jammer, the frequency remains constant over time but the STFT shows two side lobes at both sides around the central frequency. The distance between the side lobes and the main lobe corresponds to the modulation frequency of the jammer, which is 10 kHz in this case.

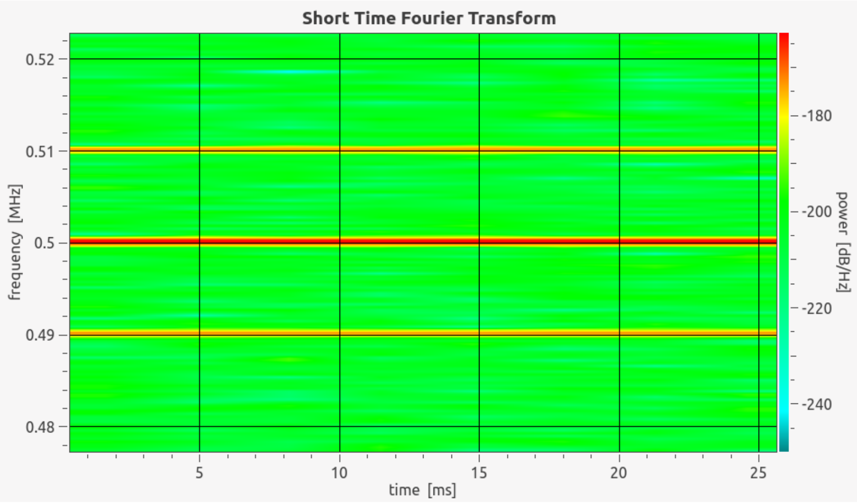


Figure 4.12.: Classification - STFT of Sim01 simulation

The estimated jammer frequency based on the adaptive notch filter is shown in Figure 4.13. The figure shows that the estimation slightly varies with time because of the noise which distracts the adaptation algorithm of the filter, but the mean value of the estimated jammer frequency clearly corresponds to the selected 0.5 MHz in the simulation. The ANF cannot be used to determine modulation frequency or modulation index of an AM jammer as it only estimates the jammer frequency with highest power and therefore cannot resolve the second peak in the Fourier transform that is needed for this estimation.

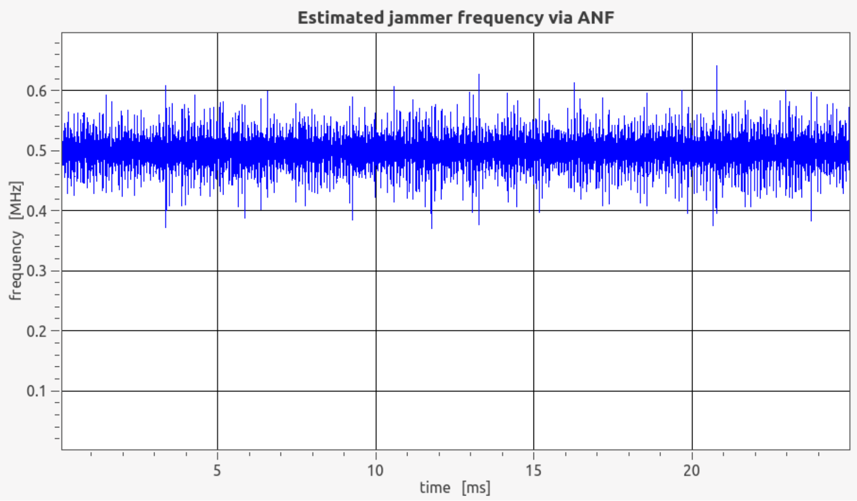


Figure 4.13.: Classification - ANF of Sim01 simulation

Table 4.7 summarizes the jammer parameters that were automatically estimated by the developed software. The table shows that the type of the jammer has been correctly selected as AM and the estimated parameters correspond quite accurate with the simulation settings. The modulation index shows an error of about 10%, which means that this parameter cannot be estimated as accurate as the others. This is due to the resolution of the STFT, but further improvements will be made here in the future. Offset and modulation frequency as well as jammer power are accurately estimated, evaluating the implemented classification algorithms for an AM jammer.

Table 4.7.: Sim01: estimated jammer parameters

parameter	**value**
type	AM
offset frequency	0.500 MHz
modulation frequency	10.070 kHz
modulation index	67%
maximum power	−135.8 dBW

Simulation - Sim02

Simulation Sim02 contains a CW jammer starting after 60 seconds of measurement time with no offset frequency and a maximum power of −135 dBW. Figure 4.14 shows the STFT of the preprocessing for the classification of this jammer. The figure shows how the power of the jammer rises before and falls after its maximum and the frequency stays constant at about 0 Hz. The corresponding PSDs that compose the STFT are visualized in Figure 4.15. The figure clearly shows the effect of the jammer as well as the input filter on the spectrum of the processed data.

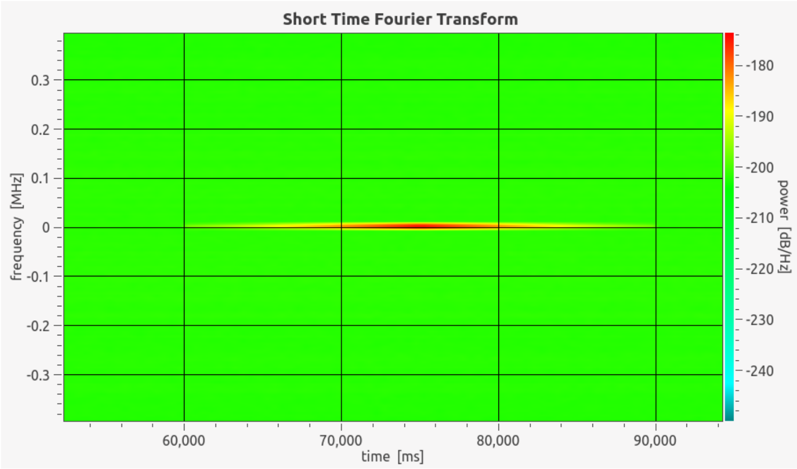


Figure 4.14.: Preprocessing - STFT of Sim02 simulation

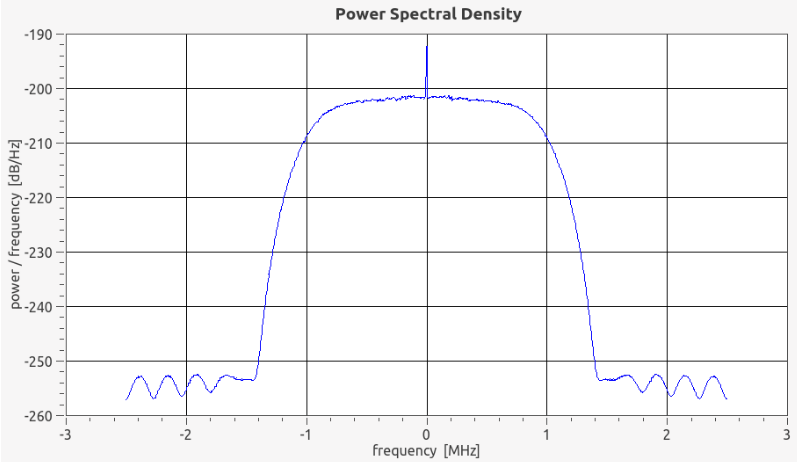


Figure 4.15.: Preprocessing - PSD of Sim02 simulation during jammer event

The settings for the classification of the jammer are summarized in Table 4.8. When classifying a CW jammer like in Sim02 a rather large PSD length is an advantage. The longer the length of each power spectral density is, the better is the spectral resolution of the STFT. This though worsens the temporal resolution, but as the frequency of the jammer is constant the temporal resolution is not important for the classification. The input filter removes unwanted parts of the signal and the start time is set to 75 seconds, where the jammer has its maximum power. If the jammer has a constant frequency over time and is located directly on or near the GNSS carrier frequency, the bandwidth of the input filter can be set even smaller to filter more noise surrounding the desired signal parts without affecting the jammer itself. In this case, the filter settings do not significantly change the estimation quality because - apart from the jammer - no significant power above the noise level can be found in the spectrum.

Table 4.8.: Sim02: classification settings

start time	75 s	PSD length	1.6384 ms
processing time	29.4912 ms		
input filter BW	2 MHz	input filter order	21

Figure 4.16 shows a detailed view of the STFT computed for the classification of the GNSS jammer. The figure clearly shows that the frequency of the jammer as well as its power are constant over time. The jammer's frequency is about 0 Hz, which is also confirmed by the estimation from the adaptive notch filter.

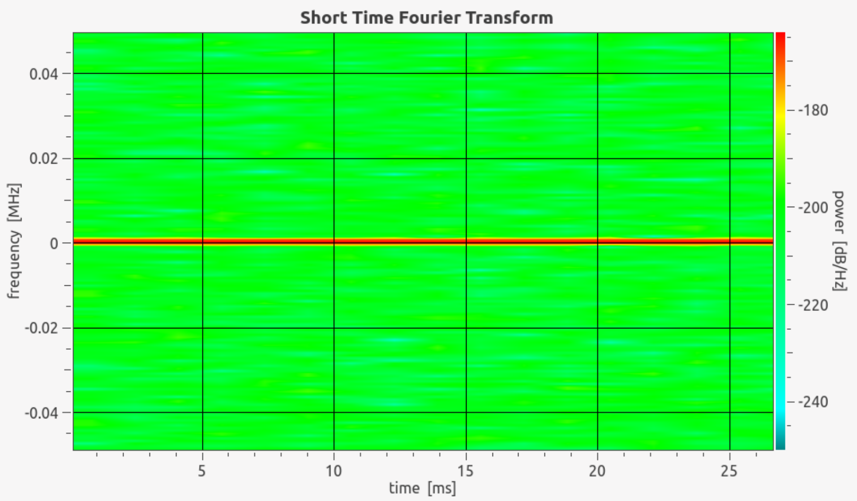


Figure 4.16.: Classification - STFT of Sim02 simulation

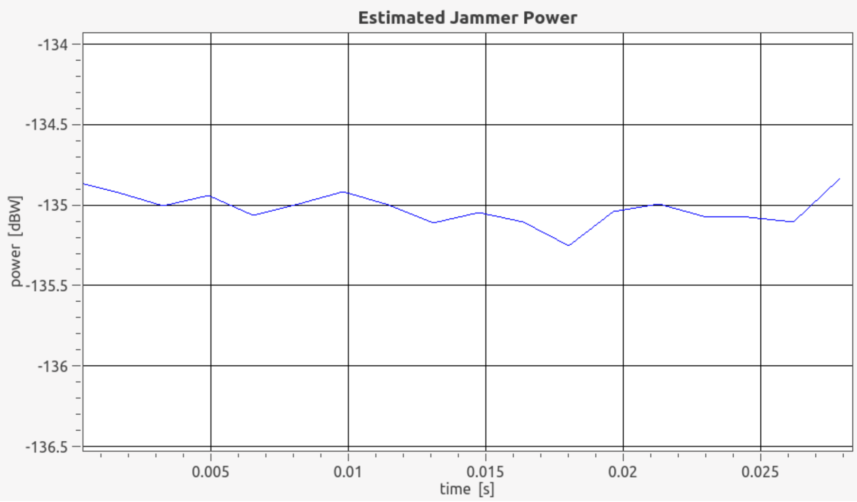


Figure 4.17.: Classification - jammer power of Sim02 simulation

A detailed view of the estimated power of the jammer can be found in Figure 4.17, showing that the power of the jammer has no significant short-time variations. This is independent from the length of the PSDs and typical for a CW jammer.
Table 4.9 summarizes the estimation of the jammer's parameters and shows that the automatic estimation of the type was correct. Also jamming power and offset frequency are estimated acceptably, which shows the functioning of the algorithms for classifying a CW jammer.

Table 4.9.: Sim02: estimated jammer parameters

parameter	**value**
type	CW
offset frequency	0.000 MHz
maximum power	−135.0 dBW

Simulation - Sim03

Simulation Sim03 contains the signals of a FM jammer starting at a measurement time of 60 seconds and lasting until 90 seconds. Figure 4.18 shows the STFT of a preprocessing step used to estimate the time of maximum interferer power. The figure shows the impact of the input filter on the STFT, filtering out the lower and upper parts of the spectrum. Also the jammer can be clearly recognized along with the typical spectral structure of a FM jammer, indicating the wide frequency range in which it operates.

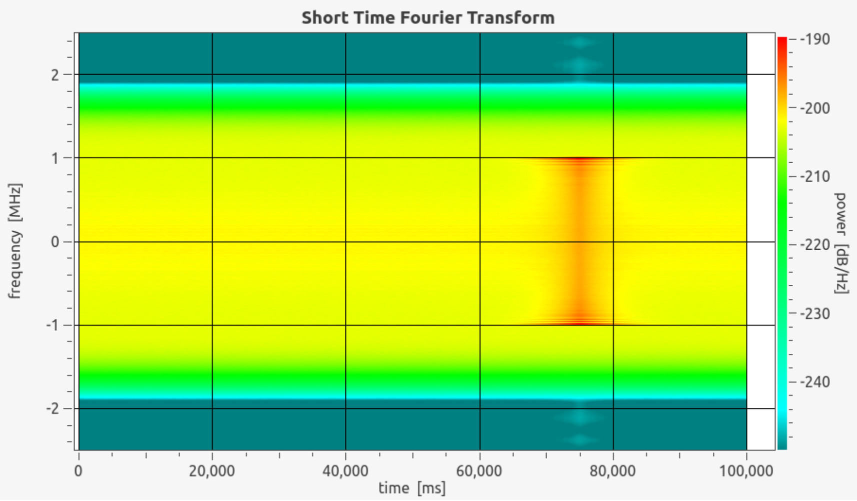


Figure 4.18.: Preprocessing - STFT of Sim03 simulation

This is even more clearly visible in Figure 4.19 showing a single PSD of the signal during the jammer event. The figure shows that the maximum jammer power appears to be around ±1 MHz, which corresponds to the simulated frequency deviation of the jammer.

This is the expected behavior as the jammer varies its frequency way faster than the STFT can resolve with the given settings for the preprocessing.

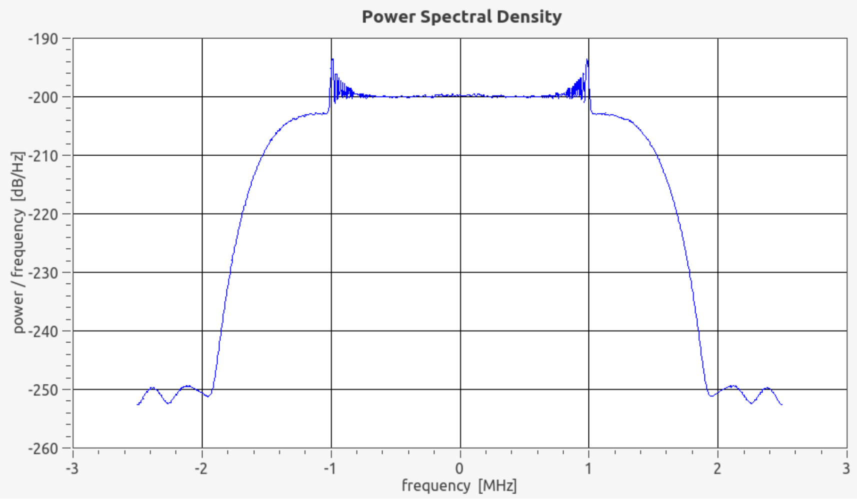


Figure 4.19.: Preprocessing - PSD of Sim03 simulation during jammer event

To classify the parameters of a FM jammer it is important to use shorter PSD lengths, which can be seen in Table 4.10, showing the selected settings for the classification of this jammer. The length of each PSD must be short enough to recover the temporal behavior of the jammer. The chosen PSD length guarantees that the simulated jammer with a modulation frequency of 2 kHz can be estimated correctly.

Table 4.10.: Sim03: classification settings

start time	75 s	PSD length	0.0128 ms
processing time	9.984 ms		
input filter BW	3 MHz	input filter order	21

Figure 4.20 shows the detailed STFT of the signal, which is used to classify the detected jammer. The figure shows the variations of the jammer's frequency with time, showing the typical sinusoidal wave that is determined by the modulation parameters. The main drawback of the STFT-based classification is the trade-off between the spectral and temporal resolution, which can also be recognized in the figure. A high spectral resolution is important for an accurate estimation of the jammer's frequency but can - according to the signal's sampling frequency - only be achieved with rather large PSD lengths. Jammers with a high modulation frequency on the other hand require a high temporal resolution as well, which can only be achieved by using short PSDs. Therefore the classification of a FM jammer is an iterative process to find the optimal settings.

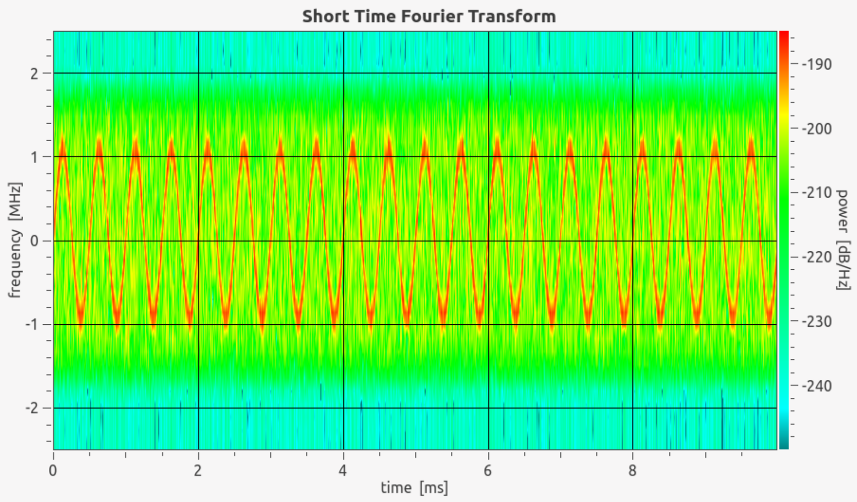


Figure 4.20.: Classification - STFT of Sim03 simulation

The frequency estimation of the jammer, based on the ANF, can be seen in Figure 4.21. This figure shows that the adaptive notch filter is able to accurately estimate and follow the jammer's frequency over time. Frequency deviation as well as modulation frequency can easily be determined in the output of the ANF in this case. The estimation accuracy of the ANF depends on the respective parameters of the filter. Most important setting for the adaptation algorithm of this filter is the so-called "forgetting factor", which determines how fast the filter can adapt to changes in the frequency of the signal. In this case the forgetting factor λ was chosen to be 0.95.

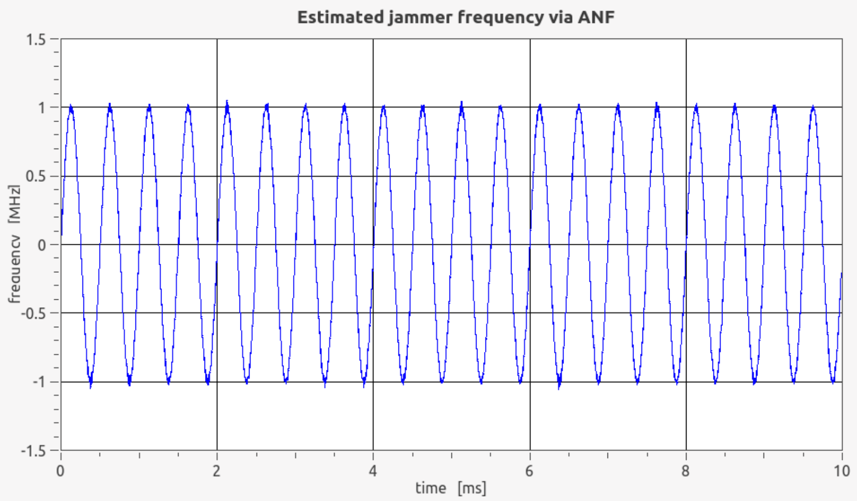


Figure 4.21.: Classification - ANF of Sim03 simulation

Table 4.11 summarizes the results of the classification for this simulation file. The table shows that all parameters as well as the type of interferer have been estimated correctly.

The estimated offset frequency, which has not been simulated, is due to the relatively low spectral resolution of the STFT, which cannot be avoided in this case.

Table 4.11.: Sim03: estimated jammer parameters

parameter	value
type	FM
offset frequency	0.010 MHz
modulation frequency	1.998 kHz
frequency deviation	1.006 MHz
maximum power	−135.0 dBW

Simulation - Sim04

Figure 4.22 shows the STFT of the preprocessing step for simulation Sim04 containing a SCW jammer between 60 and 90 seconds. The STFT looks quite similar to the preprocessed STFT of the FM jammer analyzed previously. The reason for this is that the SCW jammer shows similar frequency variations over time and the sweep duration is shorter than the PSDs in the preprocessing step can resolve.

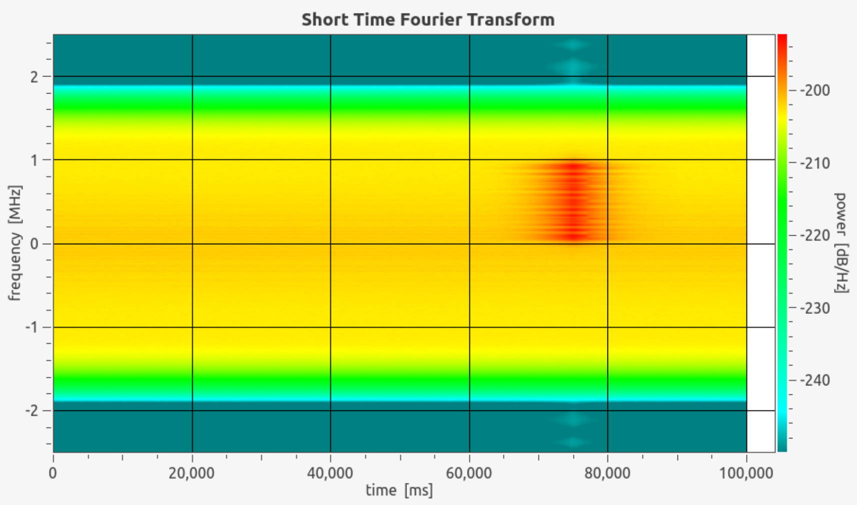


Figure 4.22.: Preprocessing - STFT of Sim04 simulation

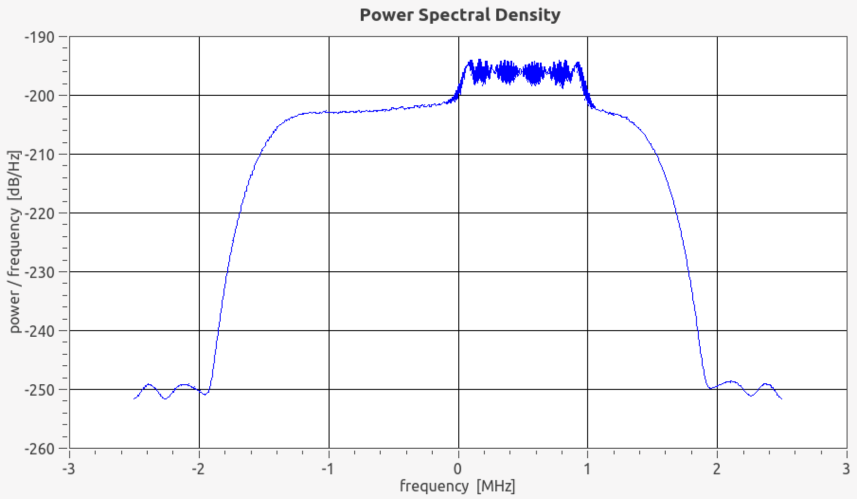


Figure 4.23.: Preprocessing - PSD of Sim04 simulation during jammer event

A single PSD during the jammer event can be seen in Figure 4.23. This shows the frequency offset of this jammer, which has been simulated, but it cannot be used to make further classifications since no temporal variations of the jammer's frequency can be seen. In contrast to the FM jammer the power seems to be equally distributed over the jammed frequencies, instead of being concentrated in the outer ranges. This makes sense when considering the progress of a SCW compared to a FM jammer. Using a SCW jammer the frequency changes linear in its bandwidth and when it reaches the border of the chosen bandwidth it continues on the other side of the spectrum. The FM jammer in contrast uses a frequency modulation by a sinusoidal wave, which leads to a stronger jamming of the upper and lower frequency ranges.
The classification settings for the simulated SCW jammer can be found in Table 4.12 and correspond to the settings chosen for the classification of the FM jammer. Important for the correct classification of a SCW jammer is a PSD length short enough to account for frequency changes of the jammer but long enough to get the best possible spectral resolution. Figure 4.24 shows the STFT of the simulated SCW jammer. The figure shows the offset frequency, sweep duration and bandwidth of the simulated jammer. The spectral resolution is rather low, due to the relatively short sweep duration of 0.1 ms, limiting the maximum number of samples that can be used for one PSD.

Table 4.12.: Sim04: classification settings

start time	75 s	PSD length	0.0064 ms
processing time	9.9968 ms		
input filter BW	3 MHz	input filter order	21

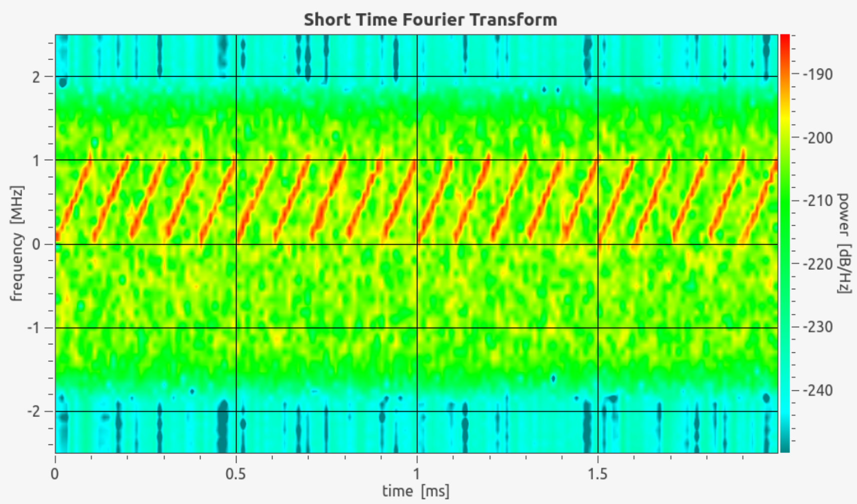


Figure 4.24.: Classification - STFT of Sim04 simulation

The output of the adaptive notch filter for this type of jammer is quite interesting. It is shown in Figure 4.25 and reveals that the adaptation algorithm of this filter has some problems with a correct estimation of the frequency jumps of a SCW jammer. The impact of this problem can be reduced by setting an appropriate value for the forgetting factor λ. But it cannot be fully avoided as it is inherent in the concept of the adaptation algorithm. The figure shows that the ANF-based estimation accuracy for the parameters of a SCW jammer must be rather low in relation to the STFT-based estimation. Depending on the possible spectral resolution problem using the STFT for estimation though, the ANF can be useful for classification of a GNSS jammer.

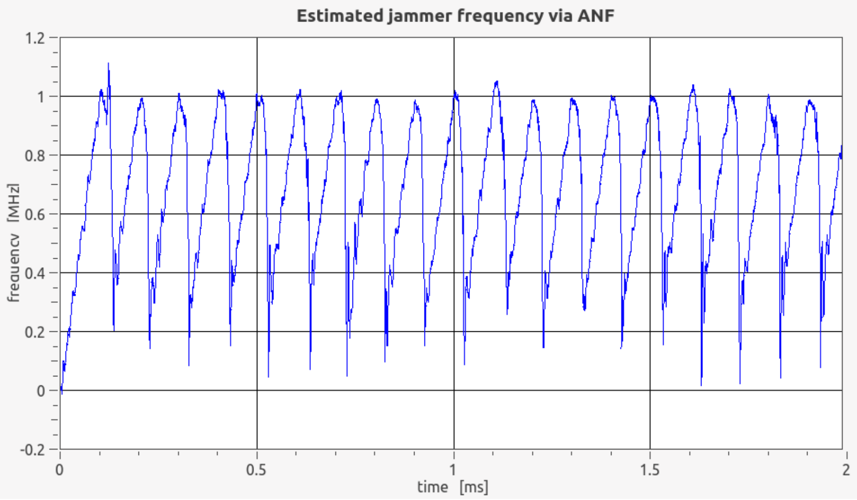


Figure 4.25.: Classification - ANF of Sim04 simulation

The estimated parameters of the SCW jammer in this simulation can be found in Table 4.13. The table shows that the estimation of power and sweep duration is as accurate as for the other types of jammers. But the frequency-related parameters like offset frequency and bandwidth suffer from the problems described above. Although the distinction of the type of jammer shows reliable results, this evaluation shows that the estimation of the parameters for a SCW jammer is a more challenging task than for the other types of jammers.

Table 4.13.: Sim04: estimated jammer parameters

parameter	**value**
type	SCW
offset frequency	0.595 MHz
sweep duration	0.100 ms
bandwidth	0.911 MHz
maximum power	−135.0 dBW

The analog generation of the jamming signal following a swept continuous wave in such a jammer on the other hand suffers from the same problems that the recovery of this signal does and thus the temporal changes of the frequency of a SCW jammer cannot be as accurate in a real environmental situation than it is possible in this simulation.

4.3. Recorded real-world data

This section presents the main results of the processing of the recorded real-world data. The data have been recorded during a measurement campaign using a GNSS antenna and RF front-end. Detection and classification modules have been tested in postprocessing to evaluate the algorithms under realistic conditions.

4.3.1. Measurement campaign

During the development of this thesis a measurement campaign next to highways in the surrounding area of the airport Graz Thalerhof was performed on August 8th 2014. This measurement campaign included five different locations near the highways A2 and A9, which are shown in Figure 4.26, where a GNSS antenna and RF front-end were used to record GNSS signals. Using the recorded data samples, the detection algorithm is evaluated and tested under realistic conditions.

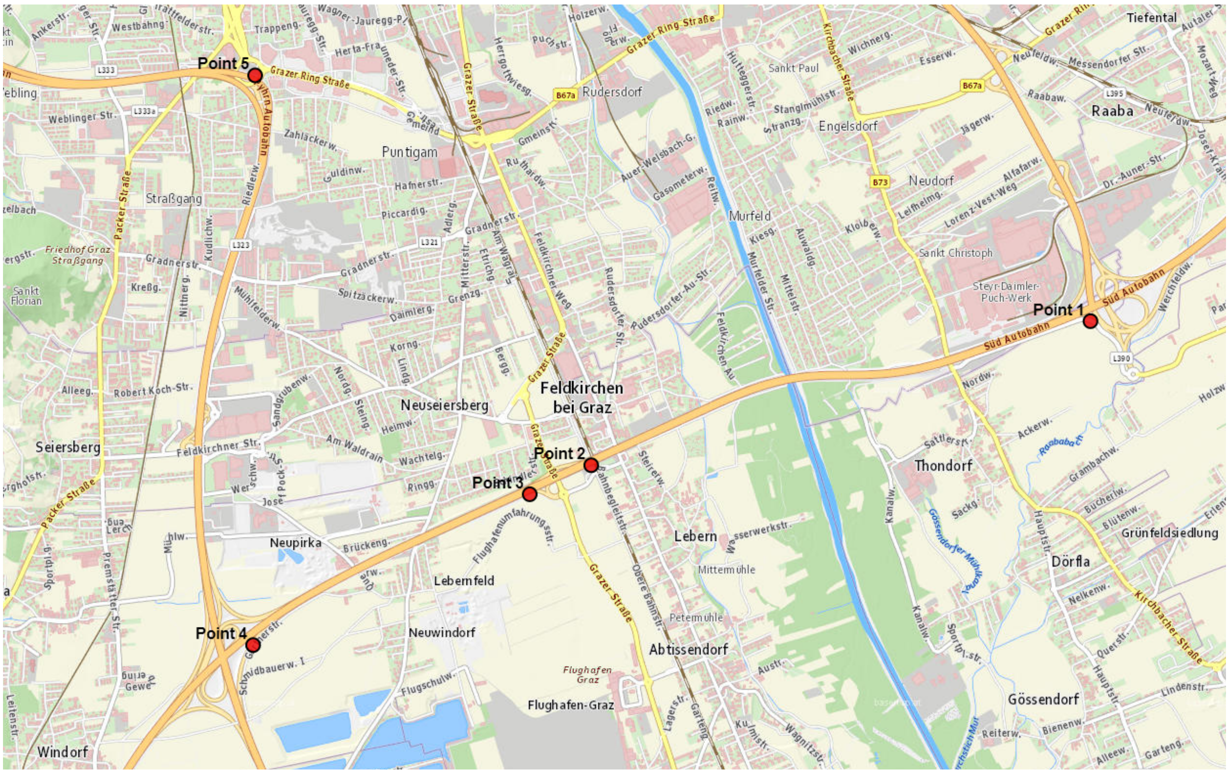


Figure 4.26.: Overview of measurement points (basemap.at)

The coordinates of the selected points were measured before by the Institute of Navigation at Graz University of Technology with high accuracy. The obtained coordinates are used as a reference for the position monitoring algorithm. Using the estimated position from the PVT in combination with the previously computed reference, the impact of GNSS

jammers on the position solution can be analyzed including environmental disturbances as multipath or shadowing.
The test measurements were made at the five selected locations for a duration of 45 minutes each, seperated into segments of 15 minutes. Each segment containing 15 minutes of GNSS signals is stored in a separate file as raw data samples. The segmentation into rather short segments of data recording has practical reasons considering memory and data processing which is more convenient with smaller files.
The recording was done by a computer onto an universal serial bus (USB) 3.0 powered hard drive. The computer was connected to a GNSS front-end developed by Fraunhofer (2010) also via USB 3.0. This front-end provided the data samples in complex numbers with a sampling rate of 40 MHz at an intermediate frequency of 0 Hz. This leads to large file sizes even for segments of 15 minutes. Using complex numbers leads to a memory consumption of two bytes per sample, which leads to a file size of

$$M = 2 \cdot f_s \cdot t \; . \tag{4.1}$$

Considering the sampling rate f_s of 40 MHz and a signal length t of 900 seconds, the size of each file is approximately 72 Gigabyte. Thus about one Terabyte of data were recorded during this measurement campaign.

4.3.2. Recorded data sets

Two different test cases using the recorded data from the GNSS front-end are analysed in detail in this thesis. Both of them contain 900 seconds of GNSS signals including varying noise levels as well as environmental disturbances like multipath or signal propagation losses due to the atmosphere.
The first real-world data set Rec00 contains the recorded signal during the second measurement segment at point 3 and the second data set Rec01 contains the signal of the third measurement at point 2. These data sets are interesting because of the satellite constellation and environmental obstructions. The files are used to evaluate the detection process under environmental conditions in general and test the C/N$_0$-based detection algorithm in detail.

Data set Rec00

Figure 4.27 shows a more detailed map of the measurement point 3, where the data of the file Rec00 was recorded. The measurement point was located directly beside and slightly higher than the highway.
Figure 4.28 shows a skyplot for measurement point 3 containing all visible GPS satellites for the time of measurement. This plot shows a low elevation of satellite number 14, which will be of importance for the detection algorithm.

Despite the low elevation of satellite 14, the constellation is quite good and shows equally distributed satellites. No significant environmental obstructions can be found in the surroundings of the measurement point.

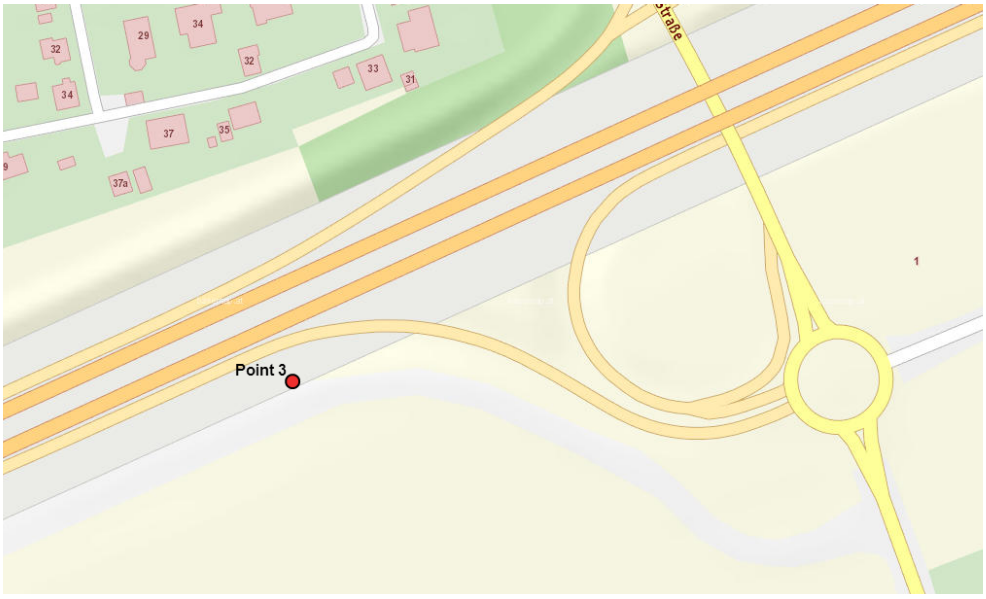


Figure 4.27.: Measurement point 3 - Rec00 data file (basemap.at)

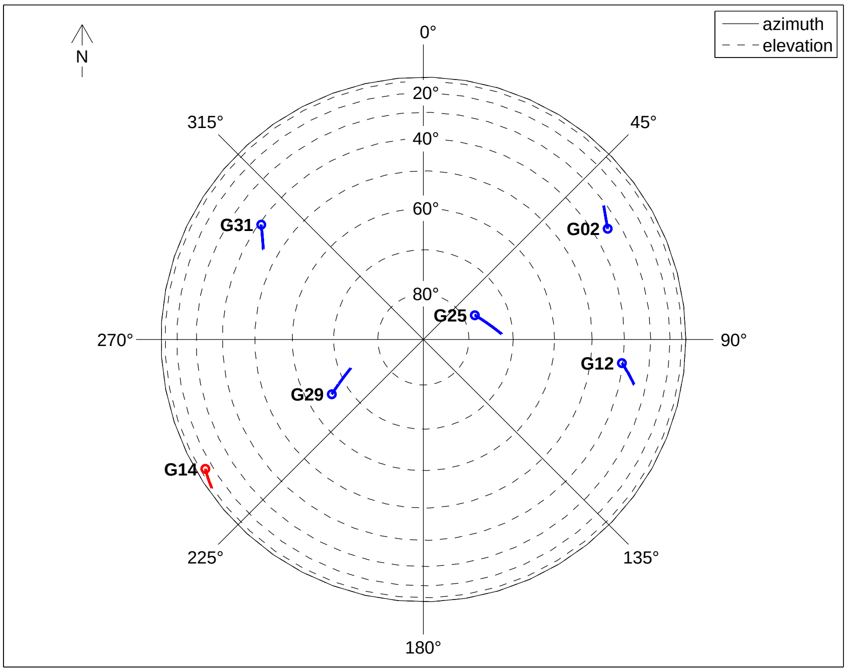


Figure 4.28.: Rec00 - skyplot during measurements

Data set Rec01

The data file Rec01 contains the recorded raw data samples during one measurement at point 2. The surroundings of the point 2 are shown in Figure 4.29. As the figure shows, the measurement point was located directly beside the highway and a railroad, where the small road in the map on which the point is located is a cycling route which crosses the highway using a small bridge. The GNSS antenna was located directly on one side of this crossing, providing small obstructions in the direction of the highway.

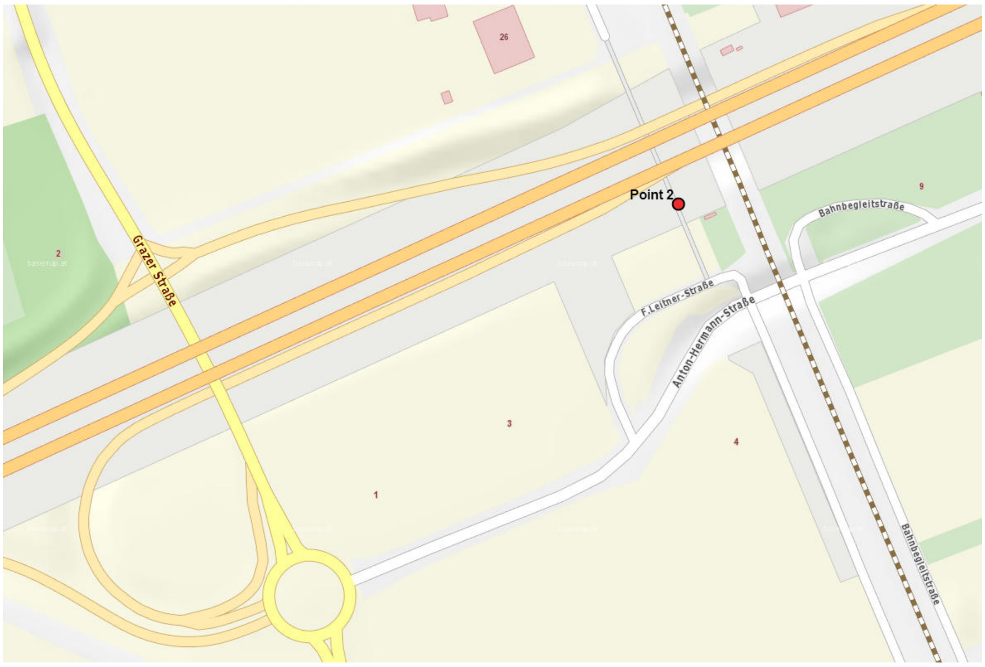


Figure 4.29.: Measurement point 2 - Rec01 data file (basemap.at)

Figure 4.30 shows a skyplot of the visible satellites at measurement point 2. The figure shows a good constellation of seven visible GPS satellites at elevations above 20° that are equally distributed over the horizon. Nevertheless, some obstructions due to vegetation as well as the pillars of the bridge near the antenna disturb the GNSS signals.

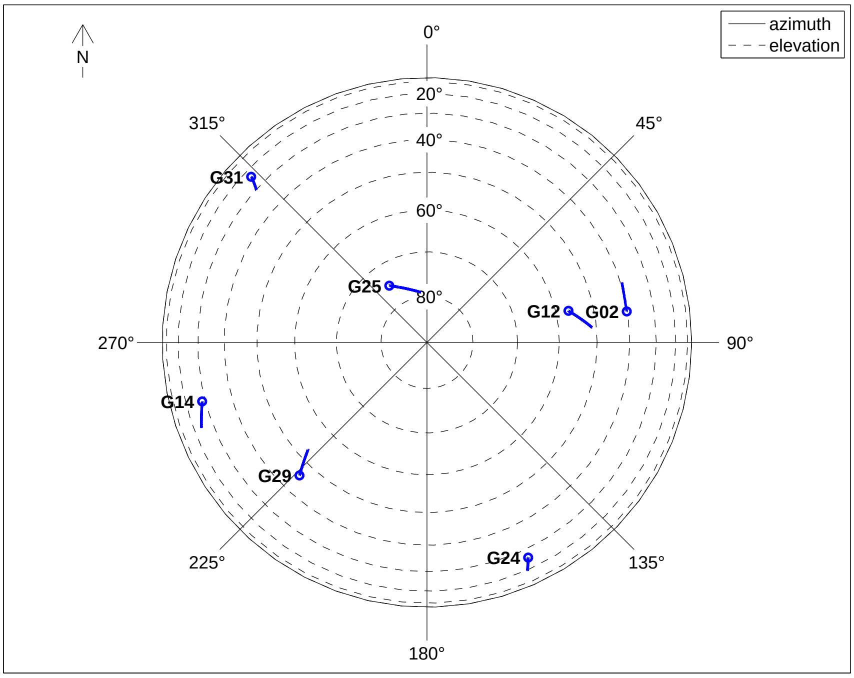


Figure 4.30.: Rec01 - skyplot during measurements

4.3.3. Analysis of data set Rec00

This section presents the processing results of the data set Rec00. It shows the results of the detection algorithm, focusing on the C/N_0-based detection.

Detection algorithm

Figure 4.31 shows a PSD of the recorded signal from the GNSS front-end. The appearance of the frequency spectrum is determined by the input filter that is used in the front-end, which is a low-pass filter with rather low order leading to power variations in the considered frequency range. This filter enhances the tracking quality by filtering out unwanted parts of the signal.

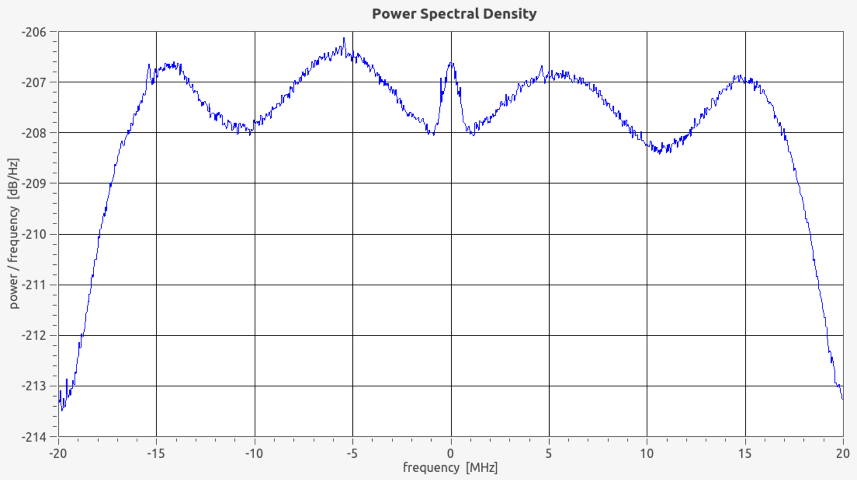


Figure 4.31.: PSD of Rec00 data set

A time series of the estimated C/N_0 over the measurement period of 900 seconds can be found in Figure 4.32. This figure shows that the carrier-to-noise ratio of most of the tracked satellites corresponds quite accurate to the theoretical $(C/N_0)_{\text{eff}}$. The largest difference can be seen for satellite number 14. This difference can be explained by the low elevation of this satellite as shown in Figure 4.28. According to this, the estimated as well as theoretical values decrease quite fast over time. Because of this, the rather large variations for this satellite compared to the others in combination with the low C/N_0 value indicate that tracking of this satellite will most likely be lost within the next minutes.

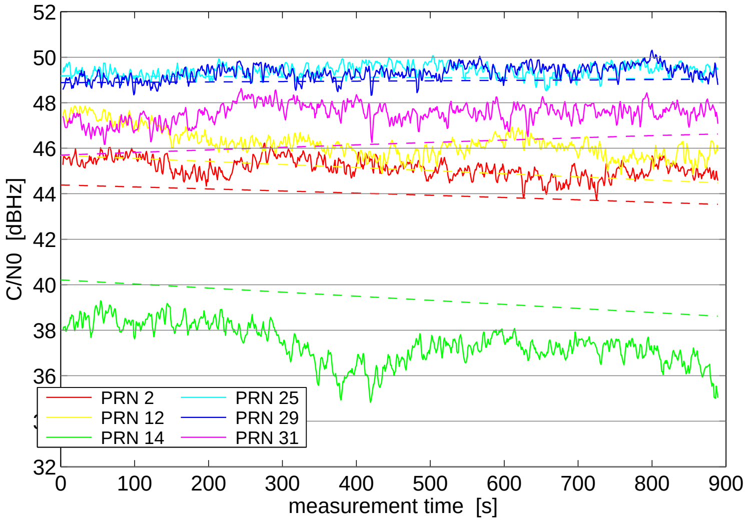


Figure 4.32.: C/N_0 of Rec00 data set

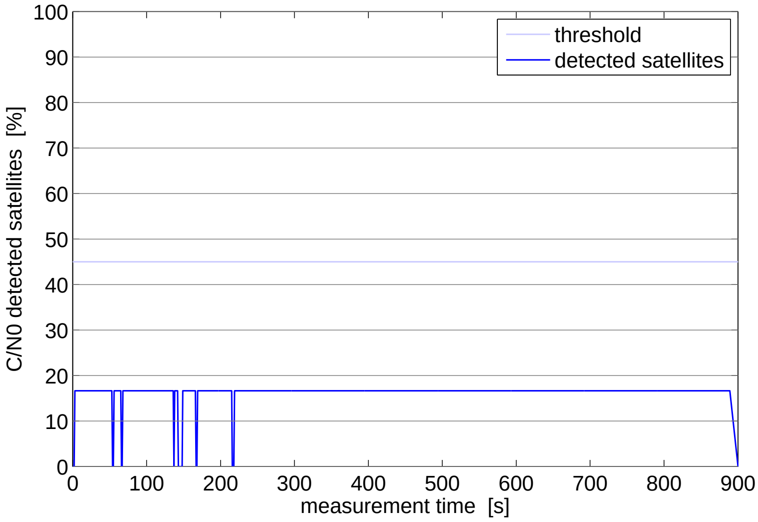


Figure 4.33.: C/N_0-based detection of Rec00 data set

Figure 4.33 shows the percentage of satellites indicating a GNSS jammer for the recorded data set Rec00. The figure shows that the threshold-based detection indicates an interferer for satellite number 14 for almost the whole measurement time. As the C/N_0 of the other satellites corresponds to the theoretical values, no interferer warning is shown for this data set. This shows that the detection algorithm also works in real environmental situations like in the present case, where the signal of one satellite can only be tracked with low accuracy. Also none of the other implemented detection modules lead to an interferer warning or alarm during this analysis.

4.3.4. Analysis of data set Rec01

In this section, the test of the detection and classification algorithm using the data set Rec01 is shown. The results presented here focus on the comparison of the C/N$_0$-based detection to the other implemented methods (i.e. baseband and position monitoring).

Detection algorithm

Figure 4.34 shows the power spectral density of the recorded signal, where an unexpected peak can be seen. This peak shows a higher power than expected in the investigated frequency range, which indicates the presence of a GNSS jammer. As can be seen in the figure, the power of the jammer is significantly higher than the noise level and the frequency is almost directly on the GPS L1 carrier. These two facts facilitate a positive detection of the jammer as its impact on the measurement results is increased.

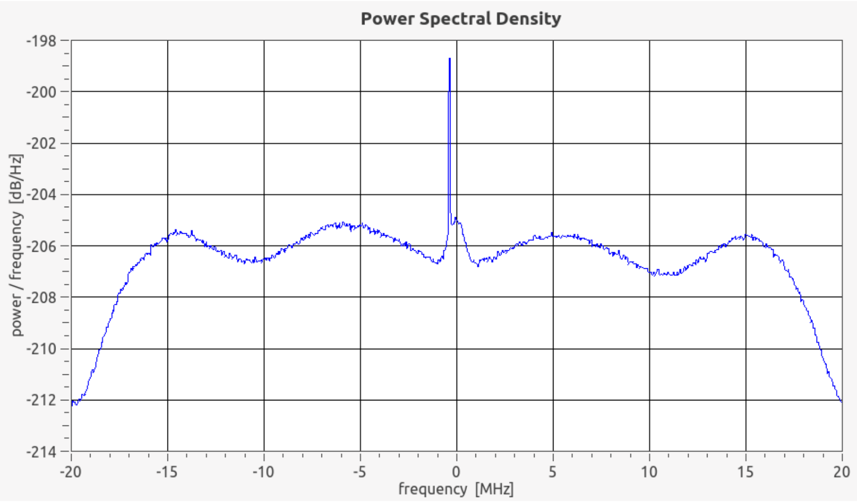


Figure 4.34.: PSD of Rec01 during jammer event

Figure 4.35 shows the progress of the estimated and theoretical C/N$_0$ over the whole measurement time of 900 seconds. Due to environmental reasons, the correspondence between estimated and theoretical values is not as high as in the first processed file Rec00, but still shows that the developed software can estimate these values. As the measurement point 2 was located on the side of a bridge crossing the highway, the pillars of this bridge as well as vegetation surrounding the antenna shadowed the GNSS signals, leading to larger variations in the tracking accuracy. At a measurement time of about 510 to 520 seconds a sudden drop in the C/N$_0$ for a short time period can be seen, which presumes the presence of a GNSS jammer.

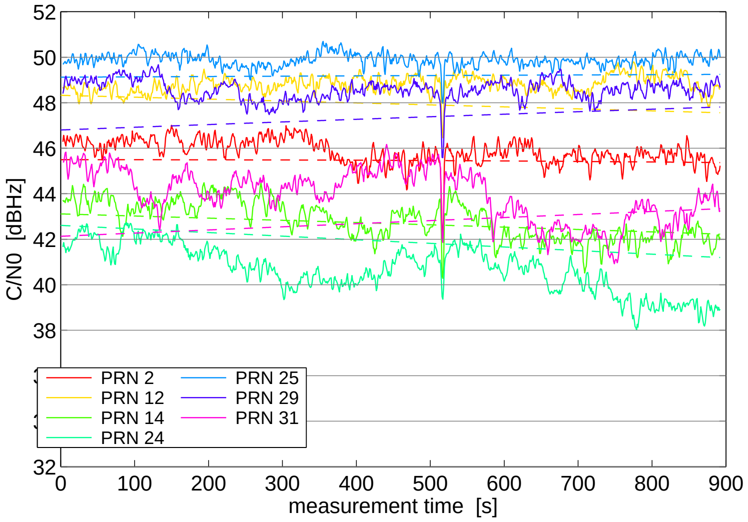


Figure 4.35.: C/N$_0$ of Rec01 data set

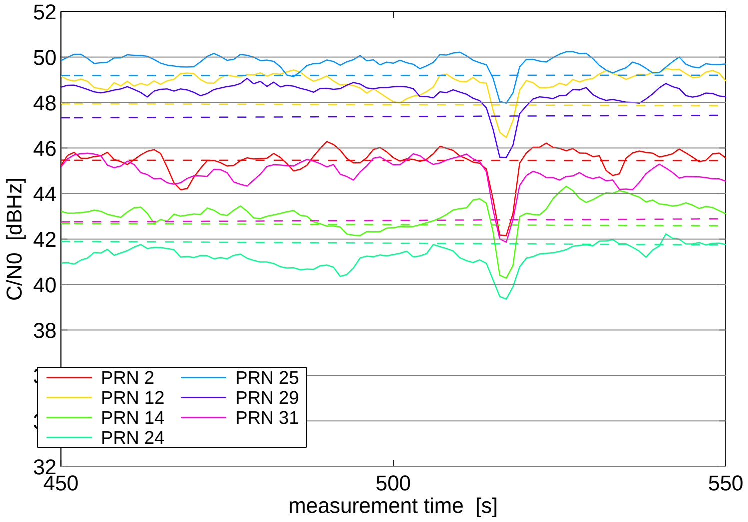


Figure 4.36.: C/N$_0$ of Rec01 during jammer event

This positive jammer detection can be confirmed by Figure 4.36, showing a more detailed view of the C/N$_0$ during the respective time period. The figure clearly shows that the C/N$_0$ of all tracked satellites is affected in a similar way for the the same amount of time, which is a certain indication for the presence of a GNSS jammer. The drop in the C/N$_0$ is definitely of a significant magnitude and leads to a detection based on the specified thresholds.

The detection based on the implemented C/N_0 module is also confirmed in Figure 4.37, which shows the percentage of satellites indicating a GNSS jammer. The figure shows that a definite detection only occurs during the inspected time discussed above at about 520 seconds measurement time and the number of indicating satellites is otherwise always below the threshold of 45%. After a measurement time of 820 seconds, the implemented C/N_0-based algorithm almost detected another GNSS jammer. This is explained in Figure 4.35, showing that short-time variations of the C/N_0 of satellite 31 and the ongoing loss of tracking of satellite number 24 coincide for this time, for which the threshold of 45% is almost reached. But since the C/N_0 of the other satellites does not show a corresponding behavior, no jammer is detected for this time. Analyzing the C/N_0 for the jammer detection at 520 seconds and the nearly detection at 820 seconds shows a clear difference and confirms that the C/N_0-based algorithm only detects one jammer in this data set.

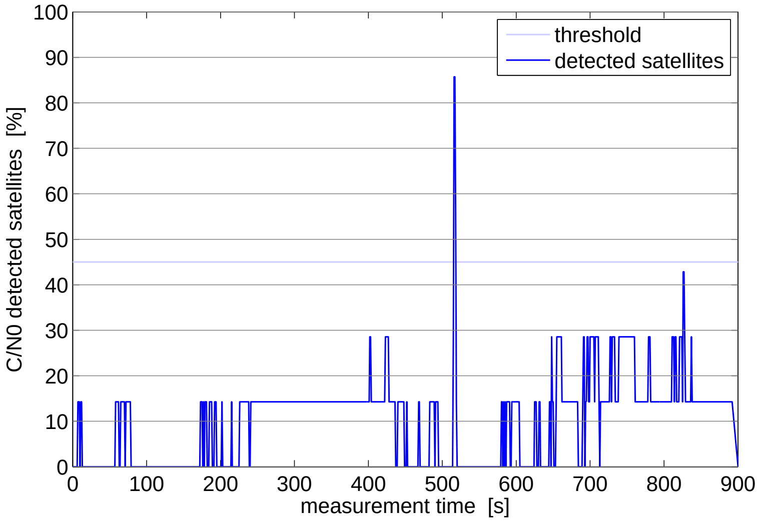


Figure 4.37.: C/N_0-based detection of Rec01 data set

Figure 4.38 confirms that the processing of this measurement including all detection algorithms only detects an interferer at a measurement time of about 520 seconds. In this case the C/N_0 as well as the baseband monitoring indicate an interferer, which leads to a clear jammer alarm. Thus a definite detection of a real GNSS jammer in the vicinity of the antenna was achieved.

As this jammer detection is the first documented and recorded incident of intentional GNSS interference in Austria, the GAIMS project team issued a press release, TeleConsult Austria GmbH (2014), to inform the public about this issue.

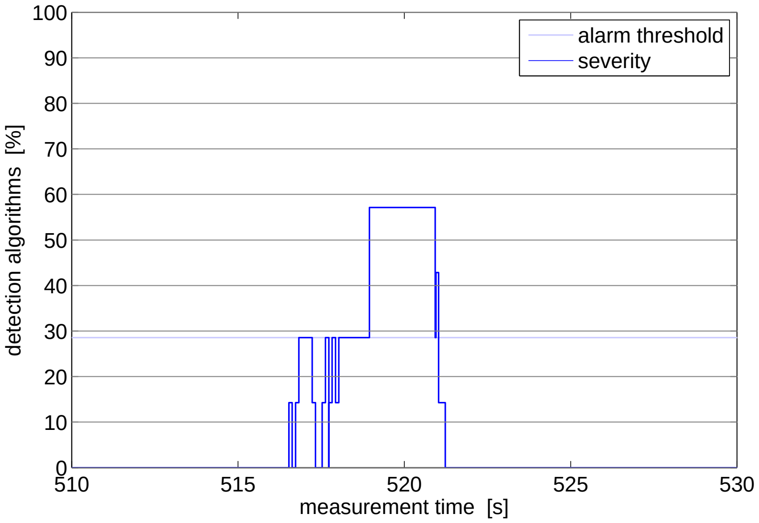


Figure 4.38.: Severity of Rec01 during jammer event

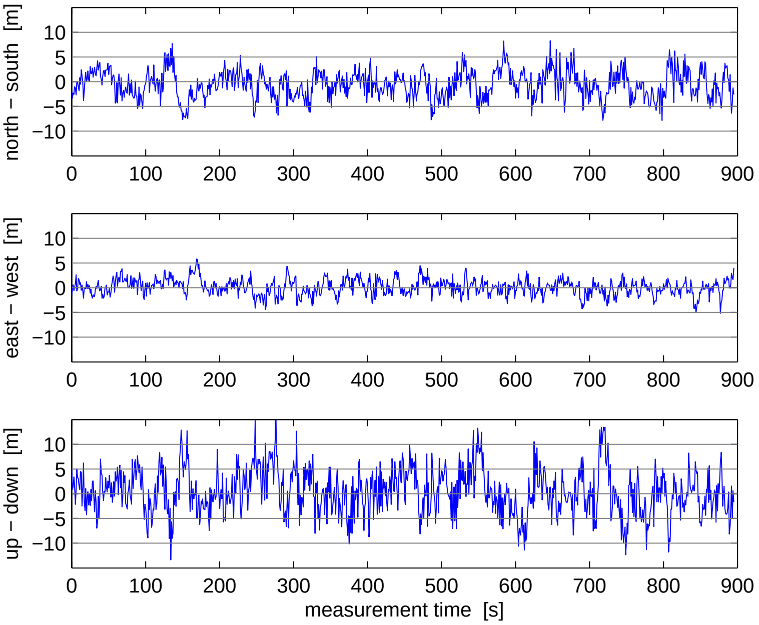


Figure 4.39.: Position differences of Rec01 data set

A time series of the differences between estimated and reference position during the measurements of data set Rec01 is shown in Figure 4.39. The position differences in the figure are related to a local-level reference frame with its center at the measured reference position. As can be seen, the height of the measurement point can be determined worse than the horizontal position, but the measurement errors remain below 15 meters, which is as expected for GPS C/A-code measurements in the case of using a sampled signal in the software-defined radio (Berglez (2013)). The differences of the computed coordinates are equally distributed in their sign, showing no constant offset which would reveal a systematic error during the measurement.

No impact of the detected interferer on the estimated position can be seen in this case. This is partly due to the fact that the measurements using C/A-code only are not very accurate. When using phase measurements or timing applications for example, the tracking errors caused by the detected jammer would be of significant magnitude.

Figure 4.40 shows the estimated horizontal position with respect to the reference. The measurements are equally distributed around the reference, which means that the mean value is not distorted in this case. No significant outliers of unexpected magnitude can be seen in the figure, which confirms that the detected jammer had no significant effect on the estimated position in this case, using GPS C/A-code measurements.

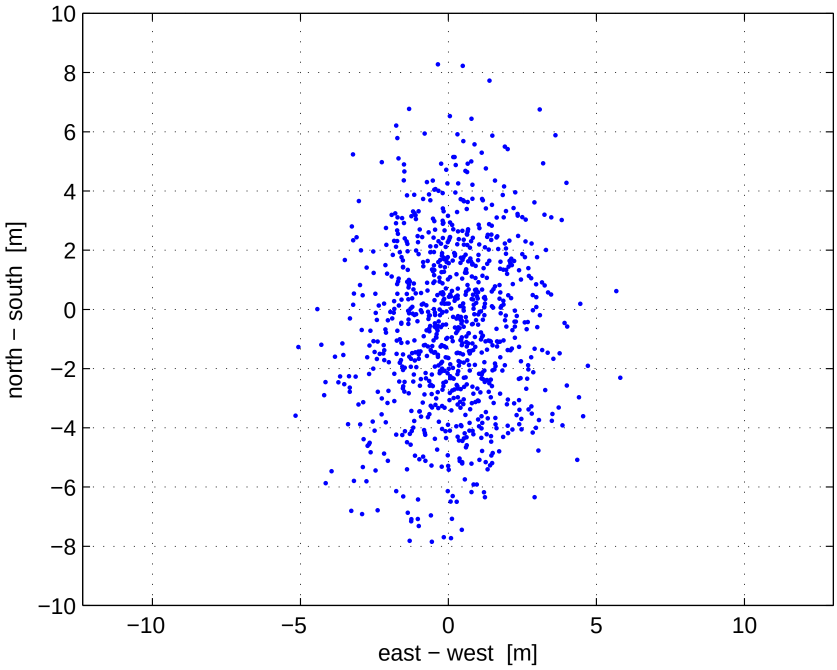


Figure 4.40.: Horizontal position of Rec01 data set

Further evaluation of the detected jammer using postprocessing methods will include an analysis of the impact that the jammer has on the residual phase error. For applications with high accuracy, this error is of importance and the impact of GNSS jammers on the estimation of phase as well as accurate timing is to be investigated.

Classification algorithm

This section shows the evaluation and results of the classification algorithm for the detected jammer in the recorded data from the GNSS front-end. Figure 4.41 shows the temporal variations of the estimated jammer power during the detected jammer incident. The figure shows that the power rises and drops quite fast at beginning and end of the incident. This can be due to a high velocity, which leads to the conclusion that the detected jammer was presumably operated in a passing car or truck on the highway. The short-time variations in the received power moreover indicate some environmental obstructions, which can be explained by the foundation of the bridge crossing over the highway on which the antenna was mounted.

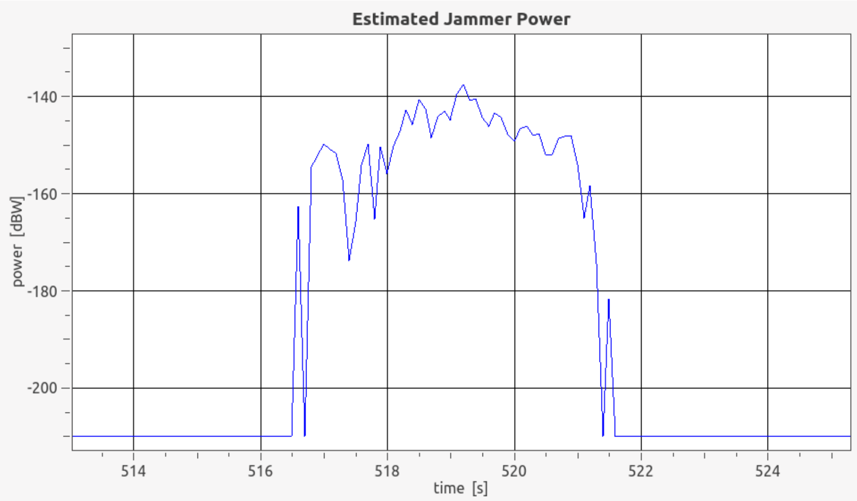


Figure 4.41.: Preprocessing - jammer power of Rec01 data set

Table 4.14 shows the chosen settings for the classification of the detected jammer. Due to the input filter implemented in the used front-end, no input filter was chosen here for the processing. The setting of the PSD length was chosen based on some tests of the classification based on a visual analysis of the resulting STFT. The processing time was set to be longer compared to the simulation files to account for larger deviations caused by additional environmental obstructions and other unmodeled effects (e.g. shadowing, multipath, atmospheric loss).

Table 4.14.: Rec01: classification settings

start time	519.18 s	PSD length	0.0512 ms
processing time	78.6432 ms		
input filter BW	–	input filter order	–

Figure 4.42 shows the computed STFT of the signal during the jammer event. The figure indicates that the detected jammer is of CW type, having a small offset frequency with respect to the GPS L1 carrier. This corresponds to the previous assumptions based on Figure 4.34. The power of the jammer is quite constant over the processing time, showing only two short periods with a slight decrease of power. As the STFT-based classification is based on the estimated jammer frequency, these estimations are shown in Figure 4.43. The figure shows that the frequency is constant over time except for a single outlier. This can be due to a noise sample distracting the algorithm, leading to a difference of about 20 kHz. A single outlier of the frequency estimation though does not significantly affect the classification algorithm and can therefore be tolerated.

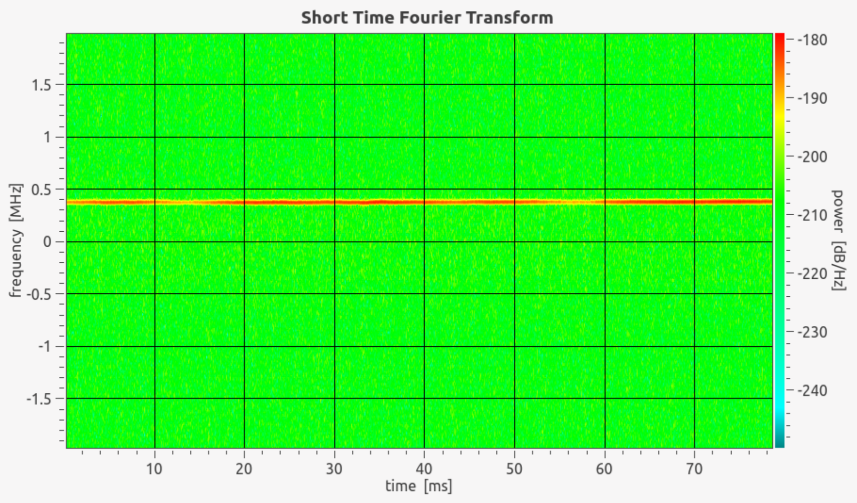


Figure 4.42.: STFT of Rec01 data set during jammer event

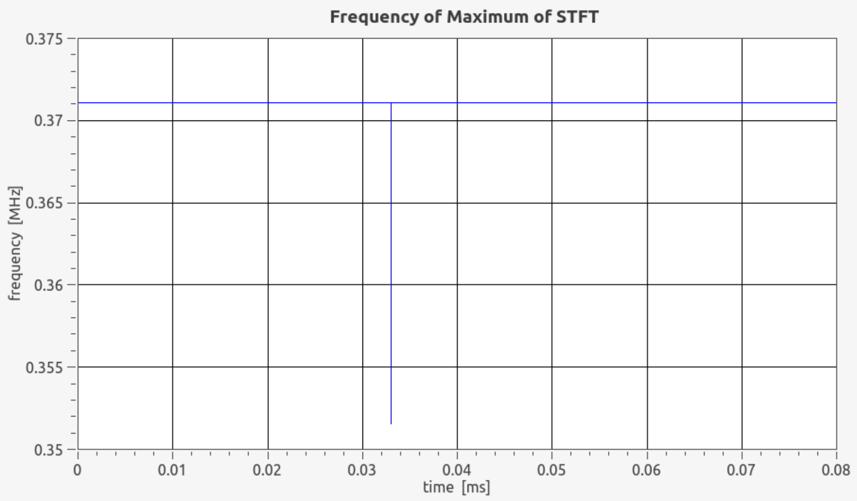


Figure 4.43.: STFT maximum frequency of Rec01 data set during jammer event

The ANF-based estimation of the jammer's frequency over time can be found in Figure 4.44, which shows that the noise in the estimation rises as the jammer power decreases. This can be seen in Figure 4.42, where the color indicates the power of the jammer. The average jammer frequency over time though stays constant for the whole processing time of about 80 ms. This leads to an undistorted estimation of the jammer frequency based on the adaptive notch filter.

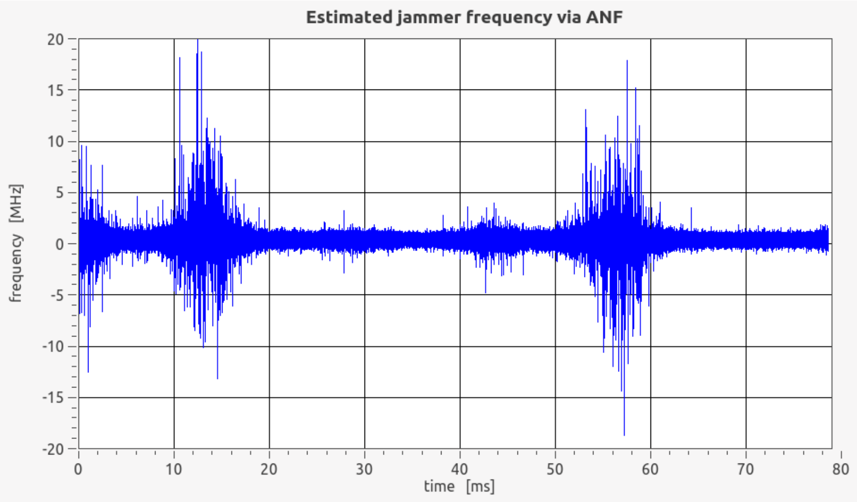


Figure 4.44.: ANF of Rec01 data set during jammer event

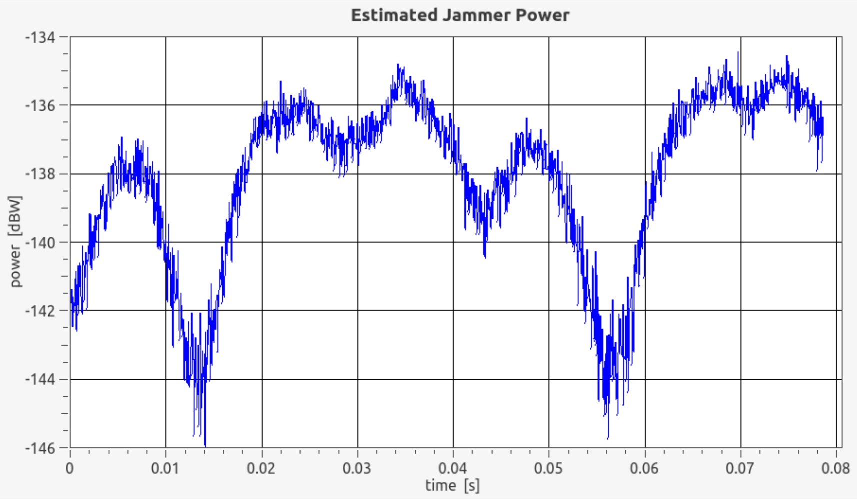


Figure 4.45.: Jammer power of Rec01 data set during jammer event

Figure 4.45 shows the temporal variations of the estimated jammer power during the time of processing. The figure shows the two detected periods of lower power (compare to Figure 4.42 and 4.44) and reveals a maximum received power of about −135 dBW for the detected GNSS jammer.

The final classification result for the detected jammer in the recorded data can be found in Table 4.15. The table shows that the classification algorithm estimates the jammer as of CW type, which can be confirmed based on the figures above. The estimation of the received jammer power reaches a value of −137.5 dBW which has a significant magnitude and is able to harmfully deteriorate the GNSS measurement quality.

The jammer's offset frequency compared to the GPS L1 carrier is quite low with a value of 380 kHz. This confirms the assumption that the detected interferer incident was an intentional one. The gathered information on the jammer discussed above leads to the profound assumption that the detected jammer was a so-called personal privacy device (PPD). The variations of power and frequency over time support this assumption.

Table 4.15.: Rec01: estimated jammer parameters

parameter	**value**
type	CW
offset frequency	0.380 MHz
maximum power	−137.5 dBW

5. Conclusions and outlook

The main goal of this thesis was the development of a reliable software module to detect and classify GNSS interferer, which can provide measurement results with a high level of integrity. A combination of different algorithms is used to make the detection as reliable as possible.
The ongoing gain of importance of GNSS for all kinds of applications including safety-critical applications as for example aircraft approach and landing affirms the need for reliable results of high integrity. Also the fact that timing applications that need a highly accurate synchronization are often based on GNSS shows the importance of these systems nowadays. As global navigation satellite systems thus provide global timing standards with high accuracy around the globe, some threats to the systems and signals including interference have to be rethought. The motivation to disturb GNSSs rises inevitably as the importance of the systems grows. As the topic of this thesis is of importance within the current discussions and developments regarding GNSS, the outcome of this thesis is scheduled for a scientific presentation at the AHORN 2014[1] conference held in Graz from 20th to 21st of November 2014.

Chapter 1 contains an introduction to the topic of GNSS interference. Problems caused by interfering signals are discussed and different state-of-the-art detection algorithms are shown. The chapter is concluded with an introduction to the GAIMS project and the contributions of this thesis to the project.
In the second part of this thesis, the theoretical background is discussed, considering the signal characteristics of GNSS and GNSS jammers and spoofers as well as the impact of interference on different measurements. Current state-of-the-art detection algorithms are discussed and evaluated.
Chapter 3 describes the implementation and necessary adaptations of some of the discussed algorithms. This thesis mainly covers the implementation of the C/N_0-based detection algorithm as well as all implemented classification algorithms, while monitoring the baseband characteristics and estimated position was also part of the GAIMS project.

[1] AHORN 2014 - der Alpenraum und seine Herausforderungen im Bereich Orientierung, Navigation und Informationsaustasuch; organized by the Austrian Institute of Navigation - Graz University of Technology, 20th and 21st of November 2014 - www.ovn.tu-graz.ac.at/ahorn2014.htm

The developed software has been tested and evaluated using simulations as well as recorded data in chapter 4. Within this evaluation process it was possible to detect the first documented incident of intentional interference of GNSS signals in Austria. For general information on GNSS interference and jamming in Austria a press release, TeleConsult Austria GmbH (2014), was issued on this topic, summarizing the work that has been done during the GAIMS project and this thesis.

The evaluation of the system in chapter 4 shows that the implemented detection and classification algorithms work as expected. Every simulated jammer was successfully detected and could accurately be classified. The estimated parameters of the jammers matched the simulated ones in every case within a tolerable deviation. It was even possible to detect a real operated jammer on a highway near Graz airport.

The processing of the detected jammer showed that the developed classification module indeed is a useful tool to gain knowledge about operated interferer by classifying their type and parameters. The implemented algorithms are suitable methods to reliably fulfill this task when operated by a user with basic knowledge of the signal structure of possible interferer types.

A critical evaluation criteria beside the positive detection of an interferer is the avoidance of false alarms, which should be as accurate as possible. The simulations as well as the recorded data from a GNSS front-end show that this was successfully considered, as the processing revealed no false alarms at all during the evaluation of the system. Considering high environmental noise and other unmodeled factors though it sure is possible that one of the implemented methods can indicate a false alarm. In this case the concurrent use of more than one detection algorithms ensures that instead of an alarm only a warning is output that indicates that an interferer might be present, but the results are not unambiguous.

Computational efficiency is a drawback of the developed system at the moment, as real-time processing of all tasks required for the monitoring cannot be guaranteed for all computers and front-end settings. Higher sampling frequencies severely increase the computational burden, but as a high sampling frequency has some advantages considering the signal reconstruction and classification of jammers, the computational efficiency of the software-defined radio will be a main task in further developments.

An interesting part during the development of this thesis was the consideration of the new upcoming Galileo signals as they are generally more resistant to interference. The Galileo public regulated service (PRS) and the commercial service (CS) are designed to be particularly resistant to disturbances from other signals. This is achieved by the different structure of these signals and also supported by the fact that they are transmitted in E6 frequency band. Beside the PRS and CS also the Galileo open service (OS) signals with their CBOC modulation are more resistant to interference than the GPS C/A signal currently is. This will also be part of further investigations as the number of available Galileo satellites will be increased in the near future.

As stated above, improvements on the computational efficiency will be an important task in the further development of the system. The task with the highest computational burden within the SDR clearly is the process of continually tracking the satellites. As this task is already implemented with parallel computational threads using all cores of the processor, further improvements will concentrate on implementing the tracking process directly on the graphics processing unit (GPU) of the computer or on using a field programmable gate array (FPGA), which can more efficiently perform the required correlation.

The ability to use the developed system for kinematic applications is also a consideration for further developments as already mentioned in section 3.1 of this thesis. This can be done by connecting the PVT solution to the GIAT. In addition to this, the influences of the movement on the frequency spectrum as well as the other detection methods have to be investigated. Also environmental multipath can become a relevant factor in kinematic applications, since the presence of multipath signals cannot be reduced for a moving GNSS antenna.

Further developments to enhance the pratical benefit of the developed system include the implementation of an algorithm to estimate the position of the detected interferer. For this task, more than one monitoring stations have to be used simultaneously and then the received jammer power as well as characteristics in the temporal changes of this power can for example be used to estimate the position. This development requires further investigations on the signal characteristics of GNSS jammers as well as some practical considerations regarding the simultaneous use of multiple monitoring stations that are synchronized with each other.

Beside the planned enhancements of the GAIMS discussed above, an intensive measurement campaign including a further evaluation of the practical use of the system is planned. This evaluation will include a permanent installation of the GAIMS in the vicinity of an airport and will be used to gain more knowledge on operated GNSS jammers and their signal characteristics.

Further tests of the system will reveal the long-term stability of the monitoring algorithms as well as the practicability for the user. The system will be installed at an airport and also used to test the upcoming Galileo signals regarding their higher stability with respect to disturbances from interfering signals. This can be achieved by comparing different results of the monitoring algorithms for GPS and Galileo. The additional number of signals is also expected to increase the accuracy and stability of detection and classification.

Apart from the use of the developed system and algorithms at an airport for GNSS-based approach and landing, the GAIMS provides benefits to a wide range of other safety-critical applications. Possibilities for further use of the developed system include for example power supply companies or telecommunications provider monitoring their networks as well as railway companies that track the current position of their trains to automatically adjust the switches and gates for traffic control. Monitoring of highways is interesting for road tolls as well as insurance companies. As the developed system is useful for numerous applications, the rising number of users and incidents of intentional interference promise a bright future for the GAIMS.

List of Figures

List of Tables

References

Allen JB (1977): Short term spectral analysis, synthesis, and modification by discrete Fourier transform. IEEE Transactions on Acoustics, Speech and Signal Processing, 25(3): 235–238.

Balaei AT, Dempster AG (2009): A statistical inference technique for GPS interference detection. IEEE Transactions on Aerospace and Electronic Systems, 45(4): 1499–1511.

Balaei AT, Dempster AG, Barnes J (2006): A novel approach in detection and characterization of CW interference of GPS signal using receiver estimation of C/N0. In: Proceedings of the Position, Location and Navigation Symposium IEEE/ION 2006, San Diego, California, April 25–27: 1120–1126.

Beaulieu NC, Toms AS, Pauluzzi DR (2000): Comparison of four SNR estimators for QPSK modulations. IEEE Communications Letters, 4(2): 43–45.

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

Betz JW, Kolodziejski KR (2009): Generalized theory of code tracking with an early-late discriminator part I: lower bound and coherent processing. IEEE Transactions on Aerospace and Electronic Systems, 45(4): 1538–1556.

Butsch F (1999): A concept for GNSS interfence monitoring. In: Proceedings of the 12th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS 1999), Nashville, Tennessee, September 14-17: 125–136.

Dierendonck AJ (1996): GPS receivers. In: Parkinson BW, Spilker JJ (eds.): Global Positioning System: theory and applications. American Institute of Aeronautics and Astronautics, Washington DC, vol. 1: 329–407.

Falletti E, Pini M, Presti LL (2011): Low complexity carrier-to-noise ratio estimators for GNSS digital receivers. IEEE Transactions on Aerospace and Electronic Systems, 47(1): 420–437.

Fraunhofer (2010): Fraunhofer IIS multiband GNSS frontend manual. Power Efficient Systems Department at Fraunhofer Institute for Integrated Circuits, Nuremberg, Germany.

Hofmann-Wellenhof B, Legat K, Wieser M (2003): Navigation. Springer, Wien, New York.

Hofmann-Wellenhof B, Lichtenegger H, Collins J (2001): Global Positioning System: theory and practice, 5th edition. Springer, Wien, New York.

Hofmann-Wellenhof B, Lichtenegger H, Wasle E (2007): GNSS–global navigation satellite systems: GPS, GLONASS, Galileo, and more. Springer, Wien, New York.

Isoz O, Akos D, Lindgren T, Sun CC, Jan SS (2011): Assessment of GPS L1/Galileo E1 interference monitoring system for the airport environment. 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: 1920–1930.

Johnston KD (1999): A comparison of CW and swept CW effects on a C/A code GPS receiver. In: Proceedings of the 12th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS 1999), Nashville, Tennessee, September 14-17: 149–158.

Kaplan E, Hegarty C (Eds.) (2006): Understanding GPS: Principles and Applications, 2nd edition. Artech House, Norwood.

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

Krumvieda K, Madhani P, Cloman C, Olson E, Thomas J, Axelrad P, Kober W (2001): A complete IF software GPS receiver: A tutorial about the details. In: Proceedings of the 14th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2001), Salt Lake City, Utah, September 11-14: 789–829.

Mitch R, Dougherty R, Psiaki M, Powell S, O'Hanlon B, Bhatti J, Humphreys T (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.

Oppenheim AV, Schafer RW, Buck JR (1999): Discrete-time signal processing, 3rd edition. Prentice Hall, London.

Petovello M, Badke B, Chanthalansy L, Noureldin A (2009): Carrier-to-Noise Density and AI for INS/GPS Integration. Inside GNSS, 4(5): 20–23.

Petovello M, Joseph A (2010): Measuring GNSS Signal Strength. Inside GNSS, 5(8): 20–25.

Pini M, Falletti E, Fantino M (2008): Performance evaluation of C/N0 estimators using a real time GNSS software receiver. In: Proceedings of the IEEE 10th International Symposium on Spread Spectrum Techniques and Applications, Bologna, Italiy, August 25-28: 28–31.

Pirazzi G, Cucchi L, Marigi D, Dionisio C (2012): A GNSS integrity monitoring station with Software Defined Radio and low cost receivers. In: Proceedings of the IEEE First AESS European Conference on Satellite Telecommunications (ESTEL), Rome, Italy, October 2-5: 1–6.

Prim DF, Schoenhuber M, Koudelka O (2008): Determination of the spectral separation between signals and its effect on the GNSS receiver performance: A more pragmatic approach. In: Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, Georgia, September 16-19: 2669–2676.

Regalia PA (1991): An improved lattice-based adaptive IIR notch filter. IEEE Transactions on Signal Processing, 39(9): 2124–2128.

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

Scott L (2011): J911: The case for fast jammer detection and location using crowdsourcing approaches. 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: 1931–1940.

Sharawi MS, Akos DM, Aloi DN (2007): GPS C/N0 estimation in the presence of interference and limited quantization levels. IEEE Transactions on Aerospace and Electronic Systems, 43(1): 227–238.

Spilker JJ (1996): GPS signal structure and theoretical performance. In: Parkinson BW, Spilker JJ (eds.): Global Positioning System: theory and applications. American Institute of Aeronautics and Astronautics, Washington DC, vol. 1: 57–120.

TeleConsult Austria GmbH (2010): GNSS multisystem performance simulation environment Manual. Version 1.1. Graz, Austria.

TeleConsult Austria GmbH (2013): GNSS Airport Interference Monitoring System - Austrian Space Applications Programme, 9th call for proposals.

TeleConsult Austria GmbH (2014): TeleConsult Austria detektiert GPS-Störsignal in Graz, September 23rd. PresseBox, More information can be found on:
http://www.pressebox.de/pressemitteilung/teleorbit-gmbh/TeleConsult-Austria-detektiert-GPS-Stoersignal-in-Graz/boxid/703455.

Turner D, Lazar S, Raghavan S, Maine K, Clark J, Winn B, Holmes J (2002): GPS and Galileo - compatibility or interoperability? A hierarchical assessment of time, geodesy, and signal structure options for civil GNSS services. In: Proceedings of the European Navigation Conference 2002, Kopenhagen, Denmark, May 27-30.

Volpe J (2001): Vulnerability assessment of the transportation infrastructure relying on the global positioning system.

Walker JS (1996): Fast fourier transforms, 2nd edition. CRC press, Boca Raton, New York, London, Tokyo.

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: 55–65.

Welch PD (1967): The use of fast Fourier transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms. IEEE Transactions on Audio and Electroacoustics, 15(2): 70–73.

Wendel J, Kurzhals C, Houdek M, Samson J (2012): An interference monitoring system for GNSS reference stations. In: Proceedings of the 15th International Symposium on Antenna Technology and Applied Electromagnetics (ANTEM), Toulouse, France, June 25-28: 1–5.

Yang JH, Kang CH, Kim SY, Park CG (2012): Intentional GNSS interference detection and characterization algorithm using AGC and adaptive IIR notch filter. International Journal of Aeronautical and Space Sciences, 13(4): 491–498.

A. Third-party software

Some third-party software products have been used during the development of this thesis. This section contains a list of these software products together with some license and copyright information.

- **GCC C++ compiler**
  Standard C++ compiler for Ubuntu Linux, used in version 4.8, GNU general public license. Can be downloaded from: gcc.gnu.org

- **Cmake**
  Cross-platform build tool for C++ , used in version 3.0.2, BSD 3-clause license. Can be downloaded from: www.cmake.org

- **Qt framework**
  Cross-platform application and user interface framework for C++ including QtCreator software, used in version 5.3.2, GNU general public license v3 license. Can be downloaded from: qt-project.org

- **Qwt library**
  Library addition to Qt containing GUI elements mainly useful for technical applications, used in version 6.1.1, GNU lesser general public license. Can be downloaded from: qwt.sourceforge.net

- **Boost library**
  Portable C++ source library for a wide range of applications, used in version 1.56.0, Boost software license - free to use and distribute. Can be downloaded from: www.boost.org

- **Matlab**
  Language of technical computing and visualization, used in version 2013a, Mathworks proprietary license. More information on: www.mathworks.com/matlab

- **git**
  Distributed version control system, used in version 2.1.2, GNU general public license v2. Can be downloaded from: www.git-scm.com

- **Dia Diagram Editor**
  Cross-platform software for creating diagrams and flow charts, used in version 19.094, GNU general public license v2. Can be downloaded from: www.dia-installer.de

- **TEXStudio**
  Integrated writing environment for creating LATEX documents, used in version 2.8.4, GNU general public license v2. Can be downloaded from: texstudio.sourceforge.net

- **TEX Live**
  Cross-platform TEX compiler including LATEX and BIBTEX packages, used in version 2014, Latex project public license. Can be downloaded from: www.tug.org/texlive