Patrick Dumitraschkewitz, BSc.

GNSS snapshot techniques for quality of service monitoring

Master's Thesis

to achieve the university degree of

Diplom-Ingenieur

Master's degree programme: Geomatics Science

submitted to

Graz University of Technology

Supervisor

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

Co-supervisor

Dipl.-Ing. Dr.techn. Philipp Berglez

Institute of Geodesy

Graz, January 2020

Affidavit

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

Date	Signature

Eidesstattliche Erklärung

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

Datum	Unterschrift

Abstract

The use of global navigation satellite systems (GNSS) and the associated permanent availability of position as well as precise time measurements become more and more a matter of course in many areas of everyday life. The information from GNSS satellites is used in many applications like civil engineering, energy industry, agriculture, civil protection, telecommunication, banking, transport, surveying and many others. Studies show that the main GNSS markets are road applications and location-based services (LBS). The number of GNSS users is constantly increasing and forecasts show that there will be one device per human in the next few years. Due to the increasing number of applications and users, it becomes more important to consider not only the opportunities, but also the weaknesses and risks of a satellite-based position determination. Currently, many users are unaware of potential GNSS threats and their impacts. In recent years, GNSS applications have become the target of intentional interference attacks. Studies show that interference can cause both considerable economic and material damage, as interference signals can significantly influence the operation of GNSS receivers. In general, the impact of interference can lead to degraded position and timing accuracies or to a total failure of the positioning.

Successful mitigation techniques require a successful and reliable detection and classification of GNSS interference in advance. Classical approaches perform a continuous quality of service monitoring within the GNSS signal bands. Since the processing requirements and the amount of data to be processed are considered to be very high, a continuous monitoring is not suitable for all, especially low-cost, GNSS applications.

A GNSS positioning technique which uses only a limited amount of data (i.e. signal length) is called GNSS snapshot processing. This technique is used in GNSS receivers if only a limited amount of energy is available for computing the position solution, reducing the necessary computing power to a minimum. The receiver records only a few milliseconds of digitized GNSS signals and processes these signals in order to obtain a position, velocity and time (PVT) solution. Since no decoding of the navigation data takes place, the receiver needs to estimate the time of signal transmission on its own. This reduces the accuracy of the position solution down to several tens of meters. However, this accuracy is sufficient for tracking and tracing

applications which have less stringent accuracy requirements.
Within this thesis GNSS snapshot techniques are investigated in more detail. Their potential regarding interference detection, using very short signal snapshots, is investigated.
The algorithms are implemented and tested with respect to their accuracy and precision with very short snapshot lengths and varying sampling frequencies. This is done to determine the minimum amount of required snapshot length and sampling frequency to successfully detect interference while maintaining a precise and accurate position solution. The time free Doppler and pseudorange positioning is investigated in more detail with simulated and recorded real-world data. Several detection methods have been implemented and those exploiting snapshot techniques are elaborated in more detail. The algorithms have been tested and analysed using simulated signals containing intentional interference such as different jamming events and spoofing attacks. These algorithms are then tested on real-world data without intentional interference to investigate their false alarm rates. The results are analysed and discussed and a conclusion is provided including an outlook on future improvements and possible further implementations.

Zusammenfassung

Der Einsatz globaler Navigationssatellitensysteme (GNSS) und die damit verbundene ständige Verfügbarkeit von Positions- und präzisen Zeitmessungen wird in vielen Anwendungen des täglichen Lebens immer mehr zur Selbstverständlichkeit. Die Informationen von GNSS-Satelliten werden in vielen Bereichen wie dem Bauingenieurswesen, der Energiewirtschaft, der Landwirtschaft, dem Katastrophenschutz, der Telekommunikation, dem Finanzsektor, dem Transportwesen, dem Vermessungswesen und in vielen weiteren verwendet. Studien zeigen, dass die wichtigsten GNSS-Märkte Verkehrsanwendungen und standortbezogene Dienste sind. Die Anzahl der GNSS-Nutzer nimmt ständig zu und Prognosen zeigen, dass es in den nächsten Jahren pro Person ein Gerät geben wird. Aufgrund der zunehmenden Anzahl von Anwendungen und Nutzern wird es immer wichtiger, nicht nur die Chancen, sondern auch die Schwächen und Risiken einer satellitengestützten Positionsbestimmung zu berücksichtigen. Derzeit sind sich viele Nutzer der potenziellen GNSS-Bedrohungen und ihrer Auswirkungen nicht bewusst. In den letzten Jahren sind GNSS-Anwendungen zum Ziel von absichtlichen Interferenzangriffen geworden. Studien zeigen, dass Störungen sowohl erhebliche wirtschaftliche als auch materielle Schäden verursachen können, da Störsignale den Betrieb des GNSS-Empfängers erheblich beeinflussen können. Im Allgemeinen können die Auswirkungen von Störungen zu verminderten Positions- und Zeitgenauigkeiten oder zu einem Totalausfall der Positionierung führen.
Erfolgreiche Mitigationstechniken erfordern eine erfolgreiche und zuverlässige Erkennung und Klassifizierung von GNSS-Interferenzen im Vorhinein. Klassische Ansätze verwenden ein kontinuierliches Monitoring innerhalb der GNSS-Signalbänder. Da der Prozessierungsaufwand und die zu verarbeitenden Datenmengen als sehr hoch angesehen werden, ist eine kontinuierliche Überwachung nicht für alle und insbesondere nicht für kostengünstige GNSS-Anwendungen geeignet.
Eine GNSS-Positionierungstechnik, die nur eine begrenzte Datenmenge (z.B. die Signallänge) verwendet, wird als GNSS-Snapshot-Prozessierung bezeichnet. Diese Technik wird in GNSS-Empfängern eingesetzt, wenn nur begrenzt Energie für die Berechnung der Positionslösung zur Verfügung steht. Dadurch wird die erforderliche Rechenleistung auf ein Minimum reduziert. Der Empfänger erfasst nur wenige Millisekunden der digitalisierten GNSS-Signale und verarbeitet diese, um eine

Lösung für Position, Geschwindigkeit und Zeit zu erhalten. Da keine Dekodierung der Navigationsnachricht stattfindet, muss der Empfänger den Zeitpunkt der Signalübertragung selbst schätzen. Dies reduziert die Genauigkeit der Positionslösung auf mehrere Dutzend Meter. Diese Genauigkeit ist jedoch ausreichend für Tracking- und Tracing-Anwendungen, die weniger strenge Anforderungen haben. Im Rahmen dieser Arbeit wurden die GNSS-Snapshot-Technik näher untersucht. Das Potenzial der Interferenzerkennung mit sehr kurzen Signalstücken wurde untersucht, implementiert und getestet.
Diese Algorithmen wurden hinsichtlich ihrer Genauigkeit und Präzision mit unterschiedlichen Abtastfrequenzen und Signallängen verglichen. Daraus wurde die geringste mögliche Abtastfrequenz und Signallänge ermittelt, mit der die Interferenzsignale erfolgreich detektiert wurden, unter Aufrechterhaltung einer genauen und präzisen Positionslösung. Die zeitfreie Doppler- und Pseudorange- Positionsmethoden wurden mittels simulierten und echten aufgezeichneten Daten untersucht. Verschiedene Detektionsmethoden für Interferenzen wurden implementiert und jene, die auf Snapshot-Techniken basieren, wurden im Detail analysiert und diskutiert. Als Interferenzsignale wurden verschiedene Jamming- und Spoofingsignale simuliert und das Verhalten der Detektoren untersucht und analysiert. Im Anschluss wurden die Detektoren auf echte aufgezeichnete Daten angewandt, um ihr Verhalten ohne Interferenzsignale zu untersuchen. Die Resultate werden im Detail diskutiert und eine Schlussfolgerung daraus gezogen. Weiters wird ein Ausblick auf zukünftige Themen in diesem Bereich gegeben.

Contents

Acknowlegdements

There are many people which deserve my gratitude in supporting me throughout my studies and this thesis. Foremost I would like to mention my supervisor Univ.-Prof. Dipl.-Ing. Dr.techn. Dr.h.c.mult. Bernhard Hofmann-Wellenhof who arranged for me to work at TeleConsult Austria (now OHB Digital Solutions) where I was able to expand and use my knowledge within the company.
Furthermore my gratitude goes to my co-supervisor Dipl.-Ing. Dr.techn. Philipp Berglez and my co-worker Dipl.-Ing. Bakk.techn. Sascha Bartl who supported me throughout this thesis. I really appreciate all their input in the form of discussions, advices and revisions of my thesis.
Further I want to mention my other colleagues at OHB Digital Solutions who also helped me in various ways in regards to this thesis and other GNSS related topics. Working at OHB Digital Solutions with colleagues witch have an amazing expertise in GNSS has always been a motivation and inspiration.
Furthermore I want to thank my family for supporting me throughout my studies. Without them I probably would have flunked out of school. I also want to mention my brother Dipl.-Ing. Dr.mont. Phillip Dumitraschkewitz who has been an inspiration for me as well as a great help throughout my studies.

Abbreviations

A/D	analogue-to-digital
AGC	automatic gain control
AM	amplitude modulated
ARNS	aeronautical radio navigation services
ASAP	Austrian space application programme
AWGN	additive white Gaussian noise
BMVIT	Bundesministerium für Verkehr, Innovation und Technologie (Federal Ministry of Transport, Innovation and Technology)
BOC	binary offset carrier
BPSK	binary phase shift keying
C/A	coarse/acquisition
C/N_0	carrier-to-noise-power-density ratio
CDF	cumulative density function
CDMA	code division multiple access
CPNR	correlation peak-to-noise floor ratio
CW	continuous wave
DLL	delay locked loop
DOP	dilution of precision
ESA	European space agency
FDMA	frequency division multiple access
FFG	Österreichische Forschungsförderungsgesellschaft (Austrian Research Promotion Agency)
FLL	frequency locked loop
FM	frequency modulated
GDOP	geometric dilution of precision
GIPSIE®	GNSS multisystem performance simulation environment
GLONASS	global'naya navigatsionnaya sputnikovaya sistema (global navigation satellite system)
GNSS	global navigation satellite system
GPS	global positioning system
GPST	GPS time

GRISMO	GNSS risk and service monitoring
HDOP	horizontal dilution of precision
ICD	interface control documents
IF	intermediate frequency
IOC	Initial operational capability
LBS	Location-based services
LSA	least squares adjustment
MBOC	multiplexed binary offset carrier
NAVIC	navigation with Indian constellation
NCO	numerically controlled oscillator
OFB	Oberste Fernmeldebehörde (Supreme Telecommunication Authority)
PDOP	position dilution of precision
PLL	phase locked loop
PRN	pseudorandom noise
PSD	power spectral density
PVT	position, velocity and time
QZSS	quasi-zenith satellite system
RF	radio frequency
RFFE	radio frequency front-end
RINEX	receiver independent exchange format
SAM	slope asymmetry metric
SBAS	satellite based augmentation system
SCW	swept continuous wave
SDR	software-defined radio
SIS	signal in space
SNR	signal-to-noise ratio
SOL	speed of light
STFT	short-time-Fourier-transformation
TOW	time of week
UERE	user equivalent range error
US	United States
VDOP	vertical dilution of precision

1 Introduction

Within the last decade global navigation systems (GNSS) have become more and more important for positioning and timing. GNSS are not only used in the field of transportation but in a wide spectrum of fields and industries such as civil engineering, energy industry, agriculture, banking, civil protection, telecommunication, surveying and many other. GNSS have become a critical part of everyday live and according to European Global Navigation Satellite Systems Agency (2017) it will increasingly do so in the future with a forecast predicting at least one GNSS device per person within the next few years. GNSS has been proven to be an economic factor and estimations presume that GPS alone has roughly generated $1.4 trillion in economic benefits since in use. A GPS outage could amount to a loss up to $1 billion per day (O'Connor et al. 2019). These economic numbers underline the importance of GNSS and special precaution must be undertaken to guarantee the continuous service availability. This is critical since GNSS has been found to be more and more under attack by means of intentional interference as shown by several incidents in the past years. Thus there is a need for GNSS quality of service monitoring which is usually done as continuous signal monitoring. The required processing and amount of data required made it unviable in low power GNSS devices. With the use of the five state positioning algorithm proposed by Hartnett et al. (1995), also refereed to as snapshot positioning a new possible way of separating data recording and signal processing gave way to new possible quality of service techniques. The recorded data, being short records of the continuous signals, also denoted as snapshots can be processed offline from the receiver and thus decreasing the workload of the GNSS device. This separation provides the possibility of GNSS monitoring for low power GNSS devices. This thesis deals with quality of service monitoring using GNSS snapshot techniques. Different snapshot techniques as well as interference detection methods using short signal samples are investigated and discussed.

1.1 Motivation

GNSS interference has been associated for a long time with applications in the field of military such as the spoofing attacks in the Black Sea and Syria both conducted by Russia (C4ADS 2019) or the GPS jamming attacks conducted by North Korea (Jiwon Seo 2017). But GNSS interference has become more than just a military strategy, it has become an everyday occurrence. A famous incident of civilian interference was in 2010 at Newark Liberty International Airport where a truck driver was caught and arrested for the usage of GPS jammers on the near highway. These jammers which can be plugged directly into the cigarette lighters lead to outages and unreliable results of the installed ground-based augmentation system (Scott 2011). Even in Austria near the airport in Graz several jamming incidents were detected (Berglez 2017). These incidences show that GNSS monitoring is necessary in order to validate the quality of GNSS service. Quality of service monitoring is usually done by means of continuous monitoring of the signal, the tracking results and the position, velocity and time results. Snapshot techniques could decrease this computational burden since these techniques only use a small part of the continuous signal. The digitized signal can be processed directly after the recording or the signal could be processed outsourced to a cloud server (Dierendonck et al. 2018). This independence of recording and processing provides the possibility of quality of service monitoring which can be used even in low power required GNSS devices. In this thesis the frequency band L1/E1, which is the most used frequency band in GNSS (i.e. GPS, Galileo and BeiDou) according to European Global Navigation Satellite Systems Agency (2018) and comprises three different GNSS with their respective signals (i.e. GPS L1 C/A, Galileo E1B and E1C, BeiDou $B1C_d$ and $B1C_p$), is investigated.

1.2 State-of-the-art

Interference detection can be conducted at different receiver stages of a GNSS receiver and according to Borio et al. (2016) can be categorized into: Hardware indicators, digital samples and post-correlation outputs as shown in Figure 1.1.

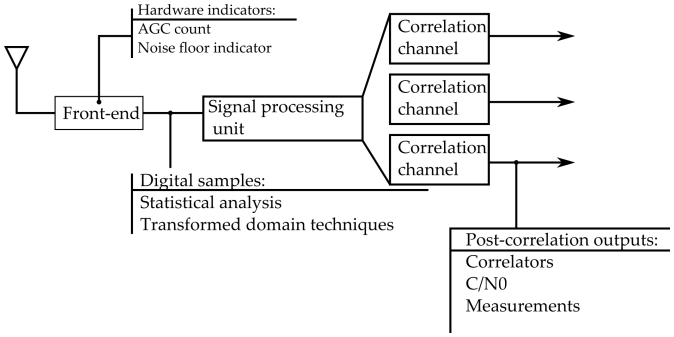

Figure 1.1: Detection using measurements from different receiver stages (c.f. Borio et al. 2016)

A possible detection method using a hardware indicator is the usage of the automatic gain control (AGC) and was used by Isoz et al. (2011) near the Kaohsiung International Airport in Taiwan to detect interference events successfully. According to Borio et al. (2016) the digital samples can be used in periodogram methods or statistical methods. Statistical methods exploit the statistical properties of the digital signal which follows an approximated Gaussian distribution. Another method proposed by Motella and Presti (2014) uses a Chi-square test to detect interferences within the signal. Post-correlation techniques for interference detection use the carrier-to-noise-power-density ratio ($^{C}/_{N_0}$) and statistical methods for detecting interference as proposed by Calcagno et al. (2010). This is possible since the $^{C}/_{N_0}$ shows a predictable behaviour for different interference incidents. Each detection method has its advantages and drawbacks such as the hardware indicators requiring no additional signal processing which result in the possible fastest available detection result in comparison to the others. On the other hand digital sample and post-correlation methods require longer signal lengths but can detect interferences more sophisticated in comparison to hardware methods. A combination of different detection methods in each stage of the receiver is a must have for a reliable and fast interference detection in traditional receivers.
The proposed five state positioning model equation by Hartnett et al. (1995) provide the possibility of computing position solution without time dependence and created new possible receiver design concepts without the usage of tracking loops. These new receiver designs also denoted as snapshot receivers provides

the possibility of separating the signal recording from the signal processing by transmitting the signal to a central processing unit or cloud server (Lucas-Sabola et al. 2016). The processing of the snapshots is limited by their snapshot length but also enables new possibilities such as the code-Doppler domain for quality of service monitoring. One such technique proposed by Lopez-Salcedo et al. (2009) exploits the code-Doppler domain of the visible satellites by using the slopes of the correlation peaks in combination of a correlation of all peaks to determine multipath in harsh environment. Current research on snapshot quality of service monitoring is to establish monitoring techniques which can work independently from the recording device. A method proposed by Merwe et al. (2019) is the usage of a multi-antenna snapshot receiver to detect spoofing. This proposed technique has been shown to work without array calibration or additional information. This thesis intends to provide additional possible quality of service monitoring techniques using snapshot data.

1.3 Thesis outline

Chapter 1 states the reason and motivation for this thesis and provides an overview of state-of-the-art work in the field of interference detection. It highlights the innovative elements and detailed work of this thesis.
In Chapter 2 the basics of GNSS positioning, signal structure and receiver considerations for traditional and snapshot receivers are elaborated.
Chapter 3 gives an overview of snapshot positioning techniques and describes their advantages and limitations.
Chapter 4 briefly describes the acquisition process for GNSS signals and the refinement of the measurements for snapshot receivers.
Chapter 5 presents the different types of interferences and elaborates their characteristics and behaviours followed by a description of spoofing.
In Chapter 6 the quality of service monitoring techniques for snapshots receivers are elaborated and discussed. Especially the use of the STFT for jammers and the peak monitoring technique are described in more detail.
Chapter 7 discusses different signal properties considerations and their influence on the signal quality, data usage and impact on the frequency and time domain of the spectrogram. The software design for the snapshot SDR used for the analysis is presented.
Chapter 8 shows the analysis of the results using the developed SDR. Different data sets are used to evaluate the performance of the snapshot positioning and monitoring techniques.

Chapter 9 concludes the results and provides ideas for future possible implementations.

1.4 Related work

This thesis contributes to the research project "GNSS Risk and Service Monitoring (GRISMO)" from OHB Digital Solutions GmbH (former TeleConsult Austria GmbH). Risk management is used in many areas of our daily lives to avoid, reduce or share risks. Risk management strategies exist for almost every aspect of our lives, but none for GNSS data. Comprehensive risk management not only requires monitoring of GNSS signals, but also identifying and analysing different threat scenarios before deploying the application, applying risk minimization strategies, and monitoring the success of these strategies. Previous monitoring concepts are based on static reference stations to perform a quality assessment and are thus locally bound on the one hand and tailored to professional users on the other hand and therefore neglect the underlying GNSS application. GRISMO provides a sound risk assessment based on actual user requirements, specific threat scenarios, and the technical data provision capabilities of the users. The assessment of the effects on the quality of service takes into account different mitigation strategies and different GNSS services. The online quality and service monitoring tool GRISMO will carry out a risk analysis based on the respective GNSS application and the threat scenario to determine the probability of occurrence as well as the effects on the receiver, the application and the user. Building on this, suitable GNSS services and mitigation strategies are proposed for the specific application. The objective of GRISMO is to enable Austrian stakeholders to assess their GNSS related risks and to better handle them based on an online quality and service monitoring tool. GRISMO allows GNSS users to determine whether GNSS signals received meet their requirements and if there are imminent jamming, spoofing or meaconing threats. This thesis contributes by algorithms, detailed analyses, requirements and limitations for snapshot techniques as an online quality and service monitoring tool. It provides insights how snapshot techniques can be exploited for future quality assessments while providing an accurate and precise position. The project is managed by the Austrian Research Promotion Agency (FFG) and received funding from the Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program line Austrian Space Application Programme (ASAP). The project is led by OHB Digital Solutions, together with its partner Brimatech Services GmbH and the Austrian Ministry of defence. The project was successfully completed in December 2019.

2 Global Navigation Satellite Systems

Satellite navigation systems are designed for positioning, navigation and timing, on land, sea or air using signals from satellites in space. Global navigation satellite system (GNSS) provide global coverage like the United States (US) global positioning system (GPS), the Russian global'naya navigatsionnaya sputnikovaya sistema (GLONASS), the European Galileo system and the Chinese BeiDou system. GPS and GLONASS were designed during the cold war for military applications and became available for civilian applications later. Both systems are maintained by their respective government. The Chinese and European systems originated from the necessity of independence from GPS and GLONASS. GNSS are available at any time, at any location (Hofmann-Wellenhof et al. 2008).
In addition to the global systems several countries developed regional satellite navigation systems such as the Japanese quasi-zenith satellite system (QZSS) or the navigation with Indian constellation system (NAVIC). GNSS and regional systems are further enhanced by satellite-based augmentation systems (SBAS). SBAS consists of geostationary satellites which support other satellite navigation systems (e.g. GPS) in terms of accuracy, integrity and availability. SBAS accomplishes this by transmitting additional information and correction data which can be used to improve GPS. The basic principle, the signal structures and receiver design considerations for GNSS are explained in the following sections.

2.1 Basics

The basic principle of satellite-based positioning is based on trilateration of ranges ρ_r^s between the satellite s and a receiver r. The range

$$\rho_r^s = c \cdot \Delta t_r^s = c \cdot (t_r - t^s) \tag{2.1}$$

is computed by using the time difference Δt_r^s between the received time t_r and the satellite transmission time t^s multiplied by the speed of light (SOL) c. Using

these ranges together with the known position of the satellites, a position can be determined using the navigation model

$$\rho_r^s(t) = ||\boldsymbol{\rho^s}(t) - \boldsymbol{\rho_r}(t)||. \tag{2.2}$$

Geometrically the model is shown in Figure 2.1, where $\boldsymbol{\rho}^s(t) = [x^s(t), y^s(t), z^s(t)]^T$ is the position vector from the geocenter to the satellite and $\boldsymbol{\rho}_r(t) = [x_r(t), y_r(t), z_r(t)]^T$ is the position vector from the geocenter to the receiver.

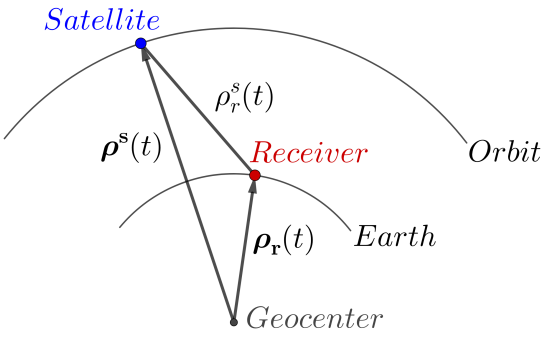

Figure 2.1: Principle of satellite-based positioning (c.f. Hofmann-Wellenhof et al. 2008)

Satellite-based positioning relies on the satellite and receiver clock to derive the signal runtime. Due to unsynchronized clocks the measured distance is not the geometric distance $\rho_r^s(t)$, but a so-called pseudorange

$$R_r^s(t) = \rho_r^s(t) + \Delta\delta_r^s(t), \tag{2.3}$$

where $\Delta\delta_r^s(t) = (\delta_r(t) - \delta^s(t))$ is the combined clock error of the satellite clock error $\delta^s(t)$ and the receiver clock error $\delta_r(t)$. Inserting the geometric range from Equation 2.2 into Equation 2.3 leads to the navigation model for pseudoranges according to Hofmann-Wellenhof et al. (2003)

$$R_r^s(t) = ||\boldsymbol{\rho^s}(t) - \boldsymbol{\rho_r}(t)|| + \Delta\delta_r^s(t), \tag{2.4}$$

with the receiver position vector $\boldsymbol{\rho_r}(t) = [x_r(t), y_r(t), z_r(t)]^T$ and the clock error $\Delta\delta_r^s(t)$ being the unknown parameters in the model. To solve for the four unknowns at least four observations are necessary. More regarding the positioning techniques can be found in Chapter 3.

2.2 Signal structures

Typically a GNSS signal is composed of a carrier wave, a data message and a ranging code as shown in Figure 2.2.

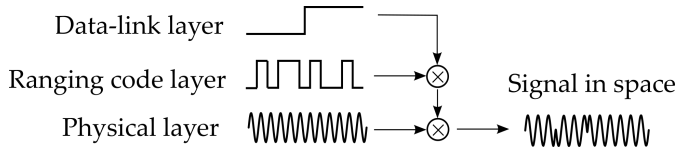

Figure 2.2: Composition of the navigation satellite signal (c.f. Hofmann-Wellenhof et al. 2008)

The carrier wave, also called physical layer, is a sinusoidal wave created by an onboard oscillator at a certain centre frequency f_c. GNSS signals reside within the L-band, which ranges from 1 to 2 GHz. The L-band was chosen due to the capability of passing the atmosphere. Table 2.1 shows the centre frequencies for different GNSS. The values were taken from the respective interface control documents (ICD) from United States Department of Defense (2019), European Global Navigation Satellite Systems Agency (2016), China Satellite Navigation Office (2017) and Russian Space Systems (2016). The carrier wave is modulated by a bit sequence, called the navigation message and a ranging code. The navigation message contains information about satellite ephemeris, health status and other parameters.
The ranging codes are generated as pseudorandom noise (PRN) codes, which are a deterministic sequences with noise like properties. In all GNSS except GLONASS L1, L2 these ranging codes are used to distinguish individual satellites within the signal. This principle is called code division multiple access (CDMA). CDMA assigns each satellite an individual PRN code and distinguishes them by exploiting the crosscorrelation properties of the code sequences. The crosscorrelation function for two signals $s_1(t)$ and $s_2(t)$ is defined as

$$R(\tau) = (s_1(t) \star s_2(t))(\tau) = \int_{-\infty}^{\infty} s_1(t) s_2(t+\tau) dt, \tag{2.5}$$

where the operator $\star$ denotes the crosscorrelation operation and the parameter τ defines the time shift between between the two signals. The crosscorrelation is a measure of similarity between the two signals. If the crosscorrelation is done with a replica of the original signal the crosscorrelation becomes the autocorrelation. The autocorrelation of a replica PRN code with a shifted version of the same PRN code is shown in Figure 2.3.

Table 2.1: GNSS centre frequencies

GNSS	Link	Frequency [MHz]
GPS	L1	1575.420
	L2	1227.600
	L3	1176.450
GLONASS	G1	1600.990
	G2	1248.060
	G3	1202.025
Galileo	E1	1575.420
	E5a	1176.450
	E5b	1207.140
	E5	1191.795
	E6	1278.750
BeiDou	B1	1561.100
	B2	1207.140
	B3	1268.520
	B1C	1575.420
	B2a	1176.450

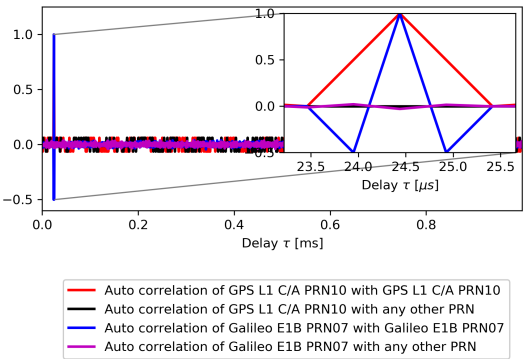

Figure 2.3: Autocorrelation of GPS L1 C/A PRN10 with the same PRN (red), GPS L1 C/A PRN10 with any other PRN (black), Galileo E1B PRN07 with PRN07 (blue) and Galileo E1B with any other PRN (magenta)

If both signals are identical, a significant correlation peak is visible with a certain delay. If this is not the case the correlation shows only noise like behaviour and insignificant small correlation values. Other methods to distinguish individual satellites such as frequency division multiple access (FDMA) used by GLONSASS are explained in detail in Kaplan and Hegarty (2006).

The navigation data and ranging codes are phase modulated onto the carrier. The two main modulation types used in GNSS are the binary phase shift keying (BPSK) and the binary offset carrier (BOC) techniques. BPSK as shown in Figure 2.4 applies a phase shift of π to the carrier wave whenever the bit state of the data or PRN code changes.

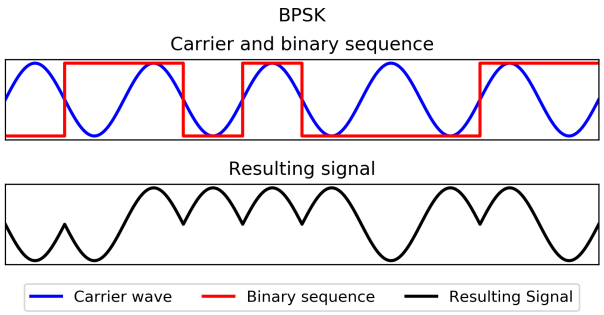

Figure 2.4: Principle of BPSK modulation, Carrier (blue) and binary sequence (red) before modulation (top) and the resulting signal (bottom)

BOC on the other hand uses an additional binary sequence, called sub-carrier, to be modulated onto the PRN code as shown in Figure 2.5. According to Borre et al. (2007) BOC modulation is defined by two parameters, the sub-carrier frequency f_s and the spreading code rate f_c. The notation $\texttt{BOC}(n, m)$ describes the sub-carrier frequency $f_s = m \cdot f_0$ and the code rate $f_c = n \cdot f_0$ with $f_0 = 1.023$ MHz.

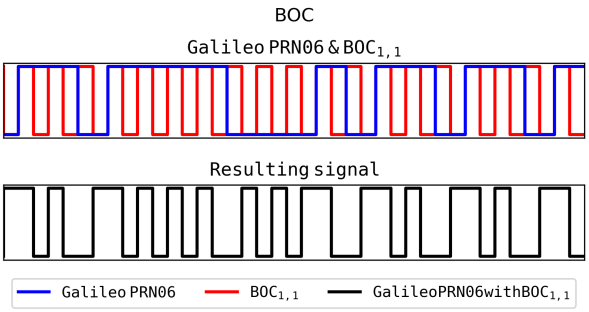

Figure 2.5: Principle of BOC modulation. Unmodulated Galileo PRN06 (blue) and BOC(1,1) (red) in the top and the resulting signal in the bottom

The impact of the different modulation types on the autocorrelation functions is shown in Figure 2.3. The additional usage of a sub-carrier results in multiple correlation peaks. These additional correlation peaks must be taken into account

during the signal processing. Furthermore, the BOC modulation impacts the power spectral density (PSD). The PSD describes the distribution of the signal power with respect to its frequency and can be computed according to Borre et al. (2007) by the Fourier transformation of the crosscorrelation function from Equation 2.5 in the form of

$$S(f) = \int_{-\infty}^{\infty} R(\tau) \cdot e^{-2\pi i f \tau} d\tau. \tag{2.6}$$

Figure 2.6 shows the PSD of a BOC and a BPSK modulated signal.

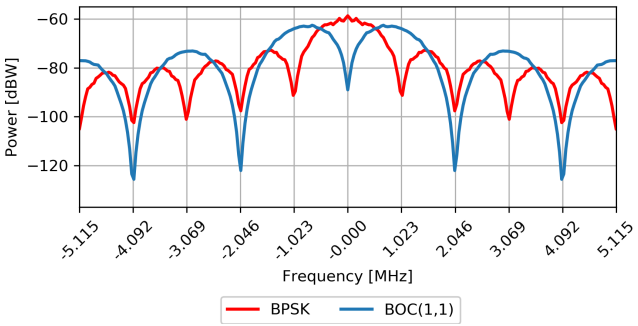

Figure 2.6: PSD comparison of BOC(1,1) (blue) and BPSK (red)

While the BPSK modulated signal shows its strongest power at the centre frequency, a BOC modulation spreads the main power around the centre frequency, by equal distance with significant low power at the centre frequency itself. The advantage of this is a higher robustness against interference. An interferer would require a higher bandwidth to cover the two side lobes. Furthermore, the BOC modulation is used to decrease interference between different GNSS. For example Galileo and GPS use the L1 centre frequency for the signals GPS L1 C/A and Galileo E1B/E1C. GPS L1 C/A uses a BPSK modulation while Galileo E1B/E1C use a MBOC(6,1,1⁄11) modulation. As shown in Figure 2.6 this leads to the Galileo signals being spread around the centre frequency where the GPS L1 C/A BPSK main lobe resides.
Several BOC can be combined and modulated onto one signal, which is known as multiplexed binary offset carrier (MBOC). Using this method the power of side lobes can be further increased. The Galileo E1B/E1C signals are further enhanced with this method by a combining a $\texttt{BOC}(1,1)$ and a $\texttt{BOC}(6,1)$ to a $\texttt{MBOC}(6,1,1/11)$ by

$$|S(f)|^2 = \frac{10}{11}|S_{\texttt{BOC}(1,1)}|^2 + \frac{1}{11}|S_{\texttt{BOC}(6,1)}|^2. \tag{2.7}$$

The result of this $\texttt{MBOC}(6,1,1/11)$ are increased side lopes around ± 6 MHz and details regarding this topic can be found in Berglez (2013).

Several GNSS use the same centre frequency for different signals. Combining two signals on a common carrier is accomplished in GNSS by multiplexing them in-phase I and quadrature-phase Q by

$$s(t) = \sqrt{2P_I}D_I(t)C_I(t)cos(2\pi f_c t) - \sqrt{2P_Q}D_Q(t)C_Q(t)sin(2\pi f_c t), \qquad (2.8)$$

where P denotes the signal power, D is the data message, C is the ranging code and f_c is the centre frequency. The multiplexing is used by all GNSS such as the L1 combinations for GPS combining the C/A and P code, Galileo combining the E1B and E1C code and BeiDou combining the $B1C_d$ and $B1C_p$ code. The Galileo E1C and BeiDou $B1C_p$ signals are so-called pilot signals, which means that no data message is modulated onto them. The advantage of pilot signals are theoretical infinite integration times during the tracking of satellites which increases the tracking performances for weaker signals. A more refined signal plan of the GNSS can be found in Ávila-Rodríguez (2008) and respective signal in space (SIS) documents.

2.3 Receiver design considerations

A typical GNSS receiver consists of three main components as shown in Figure 2.7: the radio frequency front-end (RFFE), the digital signal processor and the navigation processor.

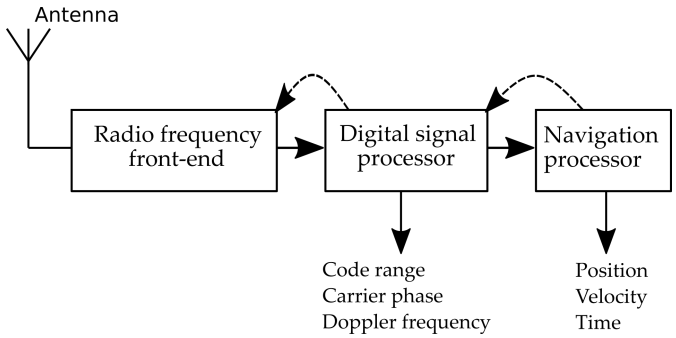

Figure 2.7: GNSS receiver components (c.f. Hofmann-Wellenhof et al. 2008)

According to Borre et al. (2007) the first component within the RFFE is a bandpass filter followed by an amplifier which increases the incoming signals magnitude. The goal of amplification is to increase the signal to a constant power level. Afterwards the signal is mixed with a frequency generated by a local oscillator to convert the

GNSS centre frequency to a lower intermediate frequency (IF). An analogue-to-digital (A/D) converter converts the signal, for further processing in the digital signal processor. The digital signal processor consists of the acquisition and the tracking stages as shown in Figure 2.8.

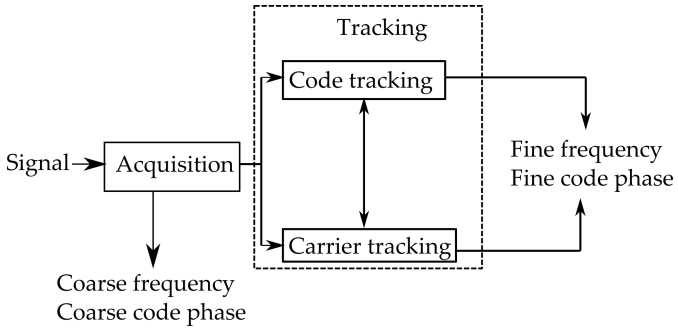

Figure 2.8: Signal processor unit (c.f. Borre et al. 2007)

If the receiver is activated it has no knowledge of available satellites, their Doppler frequencies or their code phases. Thus the acquisition has to perform a search for all satellite signals and estimates coarse values for frequency and code phase. For an acquired satellite a tracking channel using the coarse values is initialized. As long as the tracking channel for a respective satellite is active no further acquisition has to be done.
The purpose of tracking is to refine the rough estimates, to keep track of the signal and to keep an aligned replica of the signal. For this purpose a control system, based on tracking loops, as shown in Figure 2.9, is used.

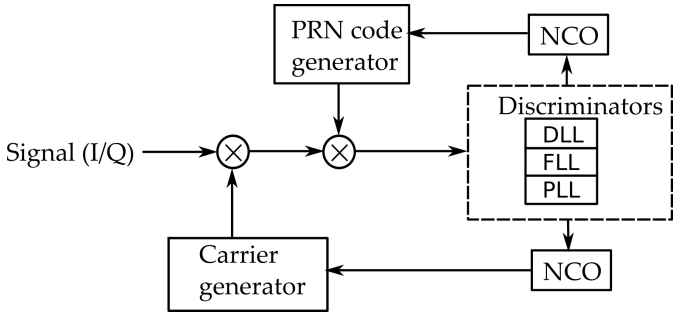

Figure 2.9: Tracking loop (c.f. Borre et al. 2007)

The tracking channel generates a carrier replica wave with the respective estimated Doppler frequency from the acquisition stage. This carrier wave is then mixed with

the incoming signal to wipe off the carrier wave from the incoming signal. The approximate code phase is used by the receiver to initialize several replicas of the satellite PRN code. These replicas are then correlated with the carrier wiped off signal by the discrete crosscorrelation function

$$R(\tau) = (s_1(n) \star s_2(n))[\tau] = \sum_{n=-\infty}^{\infty} s_1[n]s_2[n+\tau]. \tag{2.9}$$

Usually three local replica codes are generated: an early, a late and a prompt code. The principle of adjusting the aligned replica with three replica codes and their correlation values is shown in Figure 2.10.

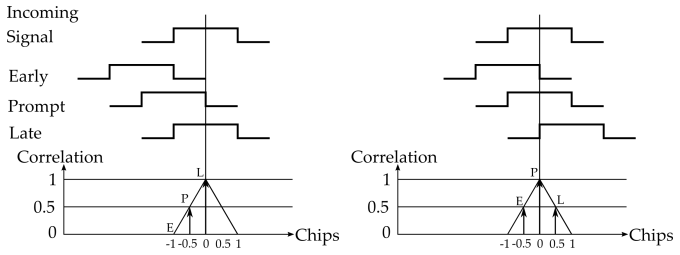

Figure 2.10: Early, late, prompt code correlation principle (c.f. Borre et al. 2007)

Within the left example of Figure 2.10 the late replica shows the highest correlation value which indicates that the code phase needs to be adjusted. Therefore, the code phase must be decreased to properly align the replicas. This results in the correlation values on the right part of the figure. The resulting correlation values are evaluated within the discriminator function and applied to the local carrier and replicas by a numerically controlled oscillator (NCO). The code is tracked by the delay locked loop (DLL), while the carrier is tracked either by a frequency locked loop (FLL) or a phase locked loop (PLL). Within the next iteration of the tracking loops are then correlated with the adjusted local replicas of carrier and codes. More information regarding the tracking can be found in Borre et al. (2007) or Kaplan and Hegarty (2006). The tracking results consisting of an aligned local replica and carrier, are further processed in the navigation processor.
The navigation processor is responsible for decoding the navigation message, converting the tracking results into measurements and computing a PVT solution. At this point the refined code phase, as a result from the tracking, corresponds to a value within one code period and is not the measured pseudorange. According to Borre et al. (2007) the initial set of pseudoranges is found by decoding the navigation message, which contains a time stamp by the satellite. This time stamp is called time of week (TOW). The satellite which has its TOW decoded first by

the receiver, is used to create the initial set of pseudoranges by adding a value between 65 and 83 ms, which is the range of signal runtime from satellite to earth as shown in Figure 2.11. The other pseudoranges are computed with respect to this tracking channel.

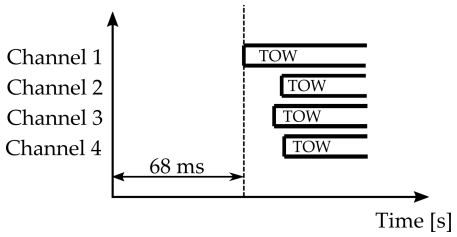

Figure 2.11: Pseudorange computation (c.f. Borre et al. 2007)

After the first PVT solution, the pseudoranges are corrected by the clock error to compensate the initial rough estimate.

2.4 Snapshot receiver design considerations

A snapshot receiver in contrast to a traditional receiver, as explained in Section 2.3, processes only short portion of the signal also called snapshot. This snapshot as shown in Figure 2.12 are short piecewise recordings of the continuous signal with time gaps between each snapshot recording.

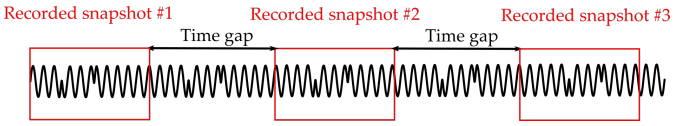

Figure 2.12: Principle of snapshot recordings

These snapshot recordings can vary from a few milliseconds up to several hundreds of milliseconds in length and a receiver processing these snapshots has to take the time gap between the recordings into account. This can be achieved by different means. Typically snapshot receivers accomplish this in three different approaches according to Fernandez-Hernandez (2015):

Open-loop: For each snapshot an acquisition is computed followed by a fine measurement estimation. Each snapshot is independently processed from the

previous ones. The time gap between snapshots has no influence on the result and can be chosen as needed.

Closed-loop: The first time a snapshot signal arrives an acquisition is computed and for each available satellite a tracking channel is initialized. Each arriving snapshot is processed through the tracking loops as if it was a traditional receiver. The time gap is overcome by the tracking loops by making the tracking loops more sensitive to higher dynamics which in exchange makes them more noisy resulting in less accurate measurements in comparison to continuous tracking channels. This architecture requires longer snapshots than the open-loop architecture to converge the tracking loops to a reasonable refinement and the time gap cannot be too long. Otherwise the loops will not converge.

Semi open-loop: The fine measurements are refined by interpolation or Kalman filtering and therefore previous epochs influence the next measurements according to the selected interpolation or filter. The snapshot length and time gap do not influence this architecture significantly if the interpolation or Kalman filtering parameters are chosen correctly.

In this thesis an open-loop architecture has been chosen to be implemented within a software-defined receiver (SDR) which has several advantages and disadvantages. A great advantage is that signal processing and position estimation can be performed long after the signal capture and thus providing the possibility of outsourcing these processes onto another device lowering the processing power for personal devices (Dierendonck et al. 2018). The disadvantages are less accurate and precise measurements and PVT results in comparison to traditional receivers. Furthermore, it is not possible to decode the navigation message requiring external information of the satellite ephemeris.
The method for snapshot positioning can be described by three steps: an acquisition step, a fine acquisition step and a snapshot positioning process as shown in Figure 2.13.

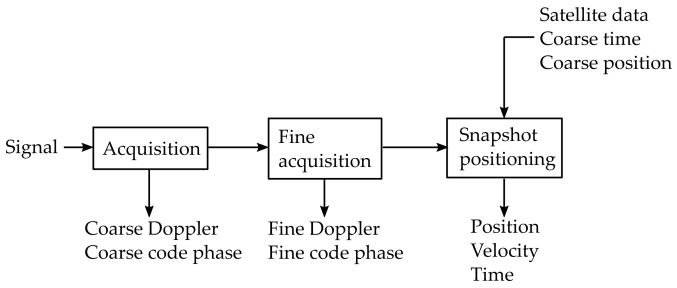

Figure 2.13: Open-loop architecture

The acquisition works analogue to common receivers described in Chapter 4. For very short signal lengths of a few ms the common way of converging the tracking loops for refinement of measurements become inapplicable and thus a different approach has to be selected (Dierendonck et al. 2018). This is done in the fine acquisition step in which the approximated values are refined by interpolation, estimation or other approaches resulting in fine measurements for code phase and Doppler frequency. The fine measurements are then used in a snapshot positioning process. Since no tracking loops are available the navigation data cannot be decoded. Hence a snapshot receiver requires external satellite data and a different approach for computing the pseudoranges. A snapshot receiver creates full pseudoranges $R_r^s(t)$ according to Diggelen (2009) by

$$R_r^s(t) = (N(t) + \delta N(t))/1000 \cdot c, \tag{2.10}$$

where $N(t)$ is the full amount of ms signal runtime from a satellite to the receiver, also known as the millisecond ambiguity and δN is the fractural millisecond part measured within the snapshot receiver. The receiver requires an estimated current time, denoted as coarse time and an estimated receiver position, denoted as coarse position to solve the millisecond ambiguity correctly. Solving the millisecond ambiguity, limitations and considerations are further discussed in Chapter 3.

3 Snapshot positioning models

Snapshot receivers use a coarse time which can differ by several seconds, minutes, hours or even days to the transmission time of the signal. This time offset, if too large makes common satellite-based positioning impossible and thus requires a different approach. Such approaches which can close the time gap between coarse and transmission time of the signal are denoted as time-free positioning models. This chapter describes the least squares adjustment for solving the time-dependent and their derived time-free counterparts.

3.1 Least squares adjustment

A set of equations can be written in matrix form

$$\mathbf{l}_{n\times 1} = \mathbf{A}_{n\times m} \cdot \mathbf{x}_{m\times 1}, \tag{3.1}$$

where $\mathbf{l}$ denotes to the observation vector, $\mathbf{x}$ represents the parameter vector and $\mathbf{A}$ is the design matrix. The subscripts n and m denote the number of observation and parameters. If n>m the equation system is considered to be overdetermined. The design matrix in case of a linear observation model

$$l_i = a_{i1}x_1 + a_{i2}x_2 \dots a_{im}x_m, \tag{3.2}$$

consists of the coefficients $a_{i1} \dots a_{im}$ in the following form

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{bmatrix}. \tag{3.3}$$

To solve an overdetermined system a possible way of obtaining a solution is by solving the least squares problem according to Higham (2002)

$$||\mathbf{A} \cdot \mathbf{x} - \mathbf{l}||_2 \stackrel{!}{=} \mathtt{min}, \tag{3.4}$$

whereas $||.||_2$ denotes the Euclidean norm. The solution of this problem according to Niemeier (2008) is given by

$$\hat{\mathbf{x}} = \mathbf{N}^{-1} \cdot \mathbf{n}, \tag{3.5}$$

$$\mathbf{N} = \mathbf{A}^T \mathbf{A}, \tag{3.6}$$

$$\mathbf{n} = \mathbf{A}^T \mathbf{l}. \tag{3.7}$$

In case the observation model is non-linear a linearisation is required. This can be done by expanding the functional model with a Taylor series

$$f(x) = \sum_{n=0}^{\infty} \frac{f^n(x_0)}{n!} \cdot (x - x_0)^n, \tag{3.8}$$

where $f^n(x_0)$ is the n-th derivative of the functional model and x_0 being the evaluation point. In LSA the Taylor series expansion is truncated after the linear part ($n = 1$) and the design matrix $\mathbf{A}$ becomes a Jacobian matrix. It consists of the models partial derivatives by the model parameters in the form of

$$\mathbf{A} = \frac{\partial f_i}{\partial dx_j} = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \frac{\partial f_m}{\partial x_2} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix}. \tag{3.9}$$

Due to this linear approximation of the observation model Equation 3.1 becomes

$$\mathbf{l}_{n\times 1} = \hat{\mathbf{l}}_{n\times 1} + \mathbf{A}_{n\times m} \cdot \Delta\mathbf{x}_{m\times 1}, \tag{3.10}$$

$$\Delta\mathbf{l}_{n\times 1} = \mathbf{A}_{n\times m} \cdot \Delta\mathbf{x}_{m\times 1}, \tag{3.11}$$

where $\hat{\mathbf{l}}$ is the estimated observation vector. The solution can be computed by

$$\boldsymbol{\Delta}\hat{\mathbf{x}} = \mathbf{N}^{-1} \cdot \mathbf{n}, \tag{3.12}$$

$$\mathbf{N} = \mathbf{A}^T \mathbf{A}, \tag{3.13}$$

$$\mathbf{n} = \mathbf{A}^T \boldsymbol{\Delta}\mathbf{l}. \tag{3.14}$$

The computation starts with an initial $\mathbf{x_0}$, computes the estimated observation vector $\hat{\mathbf{l}}$, solves for $\Delta\hat{\mathbf{x}}$ and applies the results for the next iteration in form of

$$\hat{\mathbf{x}} = \mathbf{x_0} + \Delta\hat{\mathbf{x}}. \tag{3.15}$$

This is done until the residuals no longer change by significant values.
The quality of a solution is given by the and covariance matrix

$$\boldsymbol{\Sigma}(\hat{\mathbf{x}}) = \sigma^2(\mathbf{N}^{-1}) = \sigma^2(\mathbf{Q_x}), \tag{3.16}$$

where σ describes the variance of unit weight and is computed by

$$\sigma = \frac{\mathbf{e}^T\mathbf{e}}{n-m}, \tag{3.17}$$

using the residuals vector

$$\mathbf{e} = \mathbf{A}\mathbf{x} - \mathbf{l}. \tag{3.18}$$

3.2 Pseudorange observation model

The pseudorange obervation model in Equation 2.4 can be further expanded by introducing atmospheric delays in the form of

$$R_r^s(t) = \rho_r^s(t) + (\delta_r(t) - \delta^s(t)) + \Delta\texttt{iono}_r^s(t) + \Delta\texttt{tropo}_r^s(t) + \epsilon(t). \tag{3.19}$$

The position model has the receiver position and receiver clock error as unknown parameters. The satellite positions can be computed by the ephemeris which are transmitted as described in Chapter 2. The satellite clock error, ionospheric and tropospheric delays are systematic biases which can be modelled. The satellite clock error parameters are transmitted along with the ephemeris on the navigation message. For the ionospheric and tropospheric delay typical models are the Nequick and Klobuchar ionospheric models and for the tropospheric delay typical models are the Hopfield or Saastamoinen models. These models are described in Hofmann-Wellenhof et al. (2008). In this thesis the Klobuchar model and the tropospheric model developed by Collins (1999) were implemented. A detailed implementation algorithm of this tropospheric model can be found in Subirana et al. (2013).
The position quality is influenced by the measurement error of the pseudoranges and the geometry of visible satellites with respect to the receiver. A measure of this geometry is the so-called dilution of precision (DOP) which can be calculated by using Equation 3.16 with $\sigma = 1$, resulting in the cofactor matrix according to Hofmann-Wellenhof et al. (2008) and reads

$$\mathbf{Q_x} = \begin{bmatrix} q_{xx} & q_{xy} & q_{xz} & q_{xt} \\ q_{xy} & q_{yy} & q_{yz} & q_{yt} \\ q_{xz} & q_{yz} & q_{zz} & q_{zt} \\ q_{xt} & q_{yt} & q_{zt} & q_{tt} \end{bmatrix}. \tag{3.20}$$

The DOP can be calculated by using the diagonal elements of $\mathbf{Q_x}$. Different definitions for the DOP exist, such as the

$$\texttt{geometric dilution of precision (GDOP)} = \sqrt{q_{xx} + q_{yy} + q_{zz} + q_{tt}} \tag{3.21}$$

and the

$$\texttt{position dilution of precision (PDOP)} = \sqrt{q_{xx} + q_{yy} + q_{zz}}. \tag{3.22}$$

The cofactor matrix $\mathbf{Q_x}$ can be further transformed into a local-level frame thus providing horizontal and vertical dilution of precision (HDOP and VDOP respectively). Generally speaking a positioning solution with a $\texttt{PDOP} < 3$ and a $\texttt{HDOP} < 2$ are considered to represent a good satellite geometry. Using the DOP in combination with the user equivalent range error (UERE), one can estimate the possible precision of the position solution. The UERE is an estimation of the pseudorange bias and according to Hofmann-Wellenhof et al. (2001) given by

$$\sigma_{UERE} = \sqrt{\sigma_{sc}^2 + \sigma_{eph}^2 + \sigma_{iono}^2 + \sigma_{trop}^2 + \sigma_{mp}^2 + \sigma_{rc}^2 + \sigma_{noise}^2}, \tag{3.23}$$

where σ_{sc} is the satellite clock uncertainty, σ_{eph} is the ephemerides uncertainty, σ_{iono} and σ_{trop} are the atmospheric uncertainties, σ_{mp} is the multipath error, σ_{rc} is the receiver clock error and σ_{noise} represents white noise. According to Hofmann-Wellenhof et al. (2008) the UERE has an average value of 5.3 m. Using this UERE and multiplying it with the respective DOP or using Equation 3.16 one can derive an estimated position accuracy.
This observation model is usually used in common receivers where the available satellites are continuously tracked. The maximum allowed time offset for computing a position with this observation model is according to Diggelen (2009) around 10 ms. According to Diggelen (2009) the satellites have range changes at rates up to ± 800 m⁄s and one second error would result in several hundreds meters error for the computed satellite positions. A time accuracy of 10 ms or better would then have an error of around 8 m or less. Higher time offsets require a different approach of computing precise position results.

3.3 Doppler observation model

The Doppler effect describes the change of frequency due to a relative motion between the transmitter and the receiver. The frequency change $\Delta f(t)$ is proportional to the radial velocity $\dot{\rho}_r^s(t)$ between the transmitter s and the receiver r and can be written as

$$\Delta f(t) = -\frac{\dot{\rho}_r^s(t)}{c} \cdot f_s, \tag{3.24}$$

where f_s is the emitted signal frequency. Figure 3.1 illustrates the Doppler effect for a receiver and a satellite with their respective velocity vectors $\dot{\boldsymbol{\rho}}_r(t) =$

$[\dot{x}_r(t), \dot{y}_r(t), \dot{z}_r(t)]^T$ and $\dot{\boldsymbol{\rho}}^s(t) = [\dot{x}^s(t), \dot{y}^s(t), \dot{z}^s(t)]^T$. The observed radial velocity $\dot{\rho}_r^s(t)$ is formed by a projection of the relative velocity vector $\Delta\dot{\boldsymbol{\rho}}_r^s(t)$ onto the line of sight (LOS) vector between the receiver and a satellite in form of

$$\dot{\rho}_r^s(t) =< \frac{\boldsymbol{\rho}_r^s}{\rho_r^s}, \Delta\dot{\boldsymbol{\rho}}_r^s(t) >, \tag{3.25}$$

where $< ., . >$ denotes the scalar product. Rewriting Equation 3.24 to

$$-\Delta f(t) \cdot \frac{c}{f_s} = \dot{\rho}(t) \tag{3.26}$$

and inserting into Equation 3.25 leads to the position model for Doppler observations in the form of

$$-\Delta f(t) \cdot \frac{c}{f_s} =< \frac{\boldsymbol{\rho}_r^s}{\rho_r^s}, \Delta\dot{\boldsymbol{\rho}}_r^s(t) > . \tag{3.27}$$

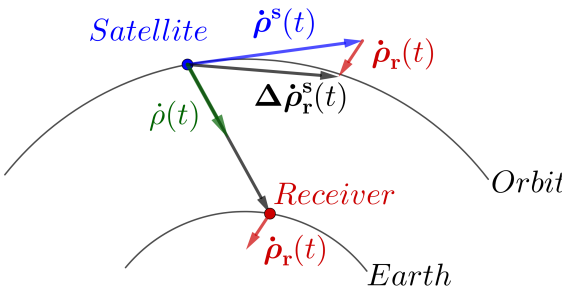

Figure 3.1: Geometrical interpretation of the Doppler

This model assumes no time dependent clock errors which is not the case for GNSS as described in Chapter 2. Applying the time derivative to the basic satellite-based position model results in

$$\dot{R}_r^s(t) = \dot{\rho}_r^s(t) + \Delta\dot{\delta}_r^s(t). \tag{3.28}$$

The observed radial velocity, denoted as range rates $\dot{R}_r^s(t)$, is not influenced by the combined clock error $\Delta\delta_r^s(t)$ as the pseudoranges but by the combined clock drift $\Delta\dot{\delta}_r^s(t)$. Inserting Equation 3.25 into Equation 3.28 leads to the Doppler observation model used in GNSS in the form of

$$\dot{R}_r^s(t) =< \frac{\boldsymbol{\rho}_r^s}{\rho_r^s}, \Delta\dot{\boldsymbol{\rho}}_r^s(t) > +\Delta\dot{\delta}_r^s(t). \tag{3.29}$$

This model is often used to compute an initial position for the receiver. Snapshot receivers can use this positioning model with some limitations and constraints. According to Hill (2001) one Hz measurement error within the Doppler observations will result in a position error of around one km. Assuming Doppler measurements without any errors the position solution is depending on the receiver time for deriving the satellite positions and velocities. According to Diggelen (2009) the maximum observed Doppler rate of GNSS is approximately 0.8 $^{\text{Hz}}/_{\text{s}}$ and thus several seconds offset can be neglected, if the accuracy of the position is not of importance. Figure 3.2 shows the influence of the time offset on the position solution.

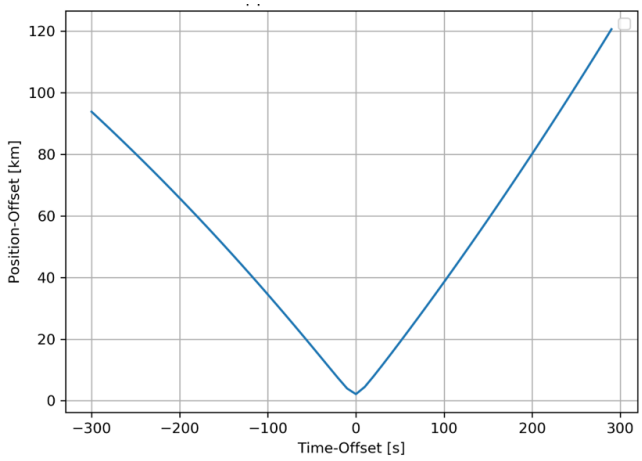

Figure 3.2: A-priori time offset influence on the position solution

Note that, time offsets of several hours or days require a different approach.

3.4 Time free pseudorange observation model

The time free pseudorange observation model provides the possibility of computing a position with several seconds offset to the exact signal transmission time. One element of the observation vector $\mathbf{\Delta l}$ (c.f. Equation 3.11) for the pseudorange model can be written as

$$\Delta l_r^s = R_r^s(t) - \hat{R}_r^s(t), \tag{3.30}$$

where $\hat{R}_r^s(t)$ is the estimated pseudorange. An error in time influences the position of the satellites and their respective clocks will be modelled incorrect, resulting in an erroneous estimated pseudorange. Hartnett et al. (1995) suggested that an error in transmission time is accounted for in the range rates $\dot{R}_r^s(t)$ and Diggelen (2009)

proves mathematically how the range rates influence the individual estimated pseudorange for an estimated time. The difference between the exact time t and the coarse time $\hat{t}$ can be written as

$$t = \hat{t} + \delta_t, \tag{3.31}$$

where δ_t describes the offset between the coarse time and the exact time. The differences in estimated pseudoranges between t and $\hat{t}$ can be written as

$$\hat{R}_r^s(\hat{t}) - \hat{R}_r^s(t) = \hat{R}_r^s(\hat{t}) - \hat{R}_r^s(\hat{t} + \delta_t), \tag{3.32}$$

which can be expressed as range rates $\dot{R}_r^s(t)$ in the form of

$$\hat{R}_r^s(\hat{t}) - \hat{R}_r^s(\hat{t} + \delta_t) = -\dot{R}_r^s(t) \cdot \delta_t. \tag{3.33}$$

Expanding the pseudorange observation model from Equation 3.19 with Equation 3.33 leads to

$$R_r^s(t) + \delta^s(t) = \rho_r^s(t) + \delta_r(t) - \dot{R}_s^r(t) \cdot \delta_t + \epsilon(t), \tag{3.34}$$

adding an additional unknown δ_t denoted as a time update to the parameter vector. For snapshot receivers, which can have and offset of several seconds, this model can be used to compute accurate positions. As described in Section 2.4 only the fractural millisecond part of the pseudorange is measured and the full pseudorange needs to be constructed according to Equation 2.10. The milliseconds ambiguities $N_r^s(t)$ can be estimated using a coarse time by

$$N_r^s(\hat{t}) = \texttt{round}(\frac{\hat{R}_r^s(\hat{t})}{c} \cdot 1000 - \delta N_r^s(\hat{t})). \tag{3.35}$$

The clock errors and other influences can lead to a wrong estimate of this integer ambiguities. One way to overcome this issue is to solve the milliseconds ambiguity of the satellite closest to the zenith and then compute the other ambiguities with respect to this satellites as explained in Diggelen (2009).
Another approach found by Othieno (2012) computes the ambiguities for each satellite individually and estimates the pseudoranges according to Equation 3.34. The millisecond rollover is corrected within the observation vector $\mathbf{\Delta l}$. If the absolute difference between the absolute minimum of $\mathbf{\Delta l}$ and an individual observation Δl_r^s is larger than half the distance travelled by the speed of light in one millisecond, then a roll over occurred and must be adjusted by one millisecond as shown in Algorithm 1.

Algorithm 1: Rollover correction

Input: $\mathbf{\Delta l}$
Output: Rollover corrected $\mathbf{\Delta l}$

$\texttt{min}_{\mathbf{\Delta l}} \leftarrow \min(\mathbf{\Delta l})$
$\texttt{SOL}_{1ms} \leftarrow \texttt{SOL} \cdot 0.001$
for Δl_i *in* $\mathbf{\Delta l}$ **do**
  if $min_{\mathbf{\Delta l}}$ - $\Delta l_i > \frac{\texttt{SOL}_{1ms}}{2}$ **then**
    $\Delta l_i \leftarrow \Delta l_i - \texttt{SOL}_{1ms}$
  else if $min_{\mathbf{\Delta l}}$- $\Delta l_i < \frac{\texttt{SOL}_{1ms}}{2}$ **then**
    $\Delta l_i \leftarrow \Delta l_i + \texttt{SOL}_{1ms}$
end

Following the rollover correction the LSA can be computed as described in Section 3.1. Furthermore, to assure that the LSA converges correctly an estimated receiver position within half the distance travelled by the speed of light in one millisecond (around 150 km) to the true receiver position and a maximum time deviation of 2 minutes is necessary (Diggelen (2009)). The additional unknown furthermore influences the accuracy and precision of the position. The cofactor matrix from Equation 3.20 changes to

$$\mathbf{Q_x} = \begin{bmatrix} q_{xx} & q_{xy} & q_{xz} & q_{xt} & q_{x\delta_t} \\ q_{xy} & q_{yy} & q_{yz} & q_{yt} & q_{x\delta_t} \\ q_{xz} & q_{yz} & q_{zz} & q_{zt} & q_{x\delta_t} \\ q_{xt} & q_{yt} & q_{zt} & q_{tt} & q_{x\delta_t} \end{bmatrix}, \tag{3.36}$$

which has an impact on the DOP values. Diggelen (2009) tested several scenarios with different satellite constellations and came to the conclusion that, if using only a few satellites, the difference between the time free DOP and the normal DOP can be very large depending on the constellation. On the other hand the difference becomes negligible the more satellites are available. Figure 3.3 shows a 24 hour PDOP comparison between the four parameter and five parameter positioning model for GPS and Galileo. Both GNSS show significant differences in PDOP if the number of satellites decreases to 6 or 7 satellites. Therefore, it is advised to combine several GNSS to increase the number of satellites which makes the difference in PDOP insignificant.

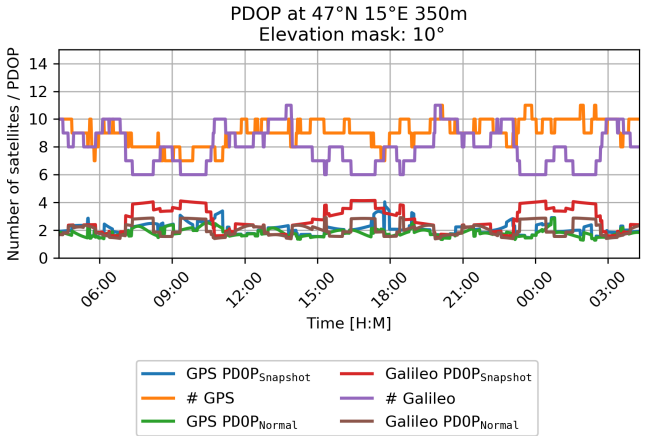

Figure 3.3: PDOP comparison between four and five unknown parameter positioning model for GPS and Galileo nominal orbits over 24 hours

3.5 Time free Doppler observation model

Analogue to Section 3.4 a time free positioning can be formed using Doppler observations by introducing a fifth parameter which corresponds to a time update. Since the positioning with Doppler observation is also the first time derivative of the pseudorange observation model as described in Equation 3.28 the same principle can be applied here. The resulting Doppler observation model as a time derivative of the time free positioning from Equation 3.34 can be written according to Fernandez-Hernandez (2015) as follows

$$\dot{R}_r^s(t) + \Delta\dot{\delta}^s(t) =< \frac{\boldsymbol{\rho}_r^s}{\rho_r^s}, \Delta\dot{\boldsymbol{\rho}}_r^s(t) > + \Delta\dot{\delta}_r(t) + \ddot{R}_r^s(t) \cdot \delta_t, \tag{3.37}$$

where $\ddot{R}_r^s(t)$ is the change in range rate and δ_t is the time update. According to Fernandez-Hernandez (2015) the time free Doppler observation model converges to a correct position if the coarse time is within ± 3 hours. The initial position can be selected without any constraints. Fernandez-Hernandez (2015) suggests computing a position solution over a time interval and comparing the residuals with a threshold.
In this thesis it has been found reasonable to compute for each hour within a time range, a PVT solution and select the result with the lowest residuals which also passes a global model test as described in Chapter 6. Using only one GNSS the time range is limited by the orbit repetition time. Combining several GNSS can further increase the time span to several days or weeks.

4 Signal acquisition

The goal of signal acquisition is the determination of available satellites within the signal and estimating coarse values of Doppler and code phase. As mentioned in Chapter 2 all GNSS except GLONASS L1/L2 use the CDMA principle. Each satellite has an individual PRN code assigned and these PRN codes can be distinguished by using their correlation properties. The PRN codes are designed in a way that they only show significant correlation with the same PRN code and only noise like behaviour for correlation results with a different PRN as shown in Figure 2.3. The correlation also provides the time delay between the two correlated signals. This time delay is also denoted as the code phase and based on it the signal runtime can be derived. Before the correlation can be performed the Doppler effect has to be taken into account. Due to the relative motion between the satellite and the receiver, the transmitted signal is shifted in the frequency with respect to the centre frequency. GNSS satellites can reach velocities with respect to a static receiver up to $\pm$ 900 $^{m}/_{s}$ which results in a Doppler shift of up to $\pm$ 4.5 kHz with respect to the centre frequency. Additional movements by the receiver can increase this Doppler shift even further by several hundred Hz. A receiver therefore has to find available satellites in a range of $\pm$ 5 kHz around the centre frequency for all possible time delays. This is also denoted as the code-Doppler search space. This chapter explains different acquisition techniques as well as fine acquisition techniques for refinement of the Doppler and code phase.

4.1 Acquisition techniques

The result of the acquisition are coarse values for the Doppler shift and code phase. These values can be any frequency and code phase combination which lead to immense computational expenses. As noted before, due to the Doppler effect the signal can vary up to $\pm$ 5 kHz and acquisition algorithms require to find the code phase within these frequency range. Since checking every possible frequency would lead to an immense computational burden the Doppler range is split into a sequence ranging from $\pm$ 5 kHz with a certain step size. The step size is chosen

as the minimum required Doppler step size, and is also denoted as the Doppler bin size. The minimum required bin size of the Doppler shift is depending on the length of the primary code and can be computed by

$$\Delta f = \frac{f_s}{N_s}, \tag{4.1}$$

where f_s is the sampling frequency and N_s is the length of the signal in samples. This minimum required bin size also impacts the accuracy of the coarse Doppler. Increasing the frequency bin size has an influence on the computational burden of the acquisition. Table 4.1 shows the properties and possible code-Doppler combinations for the minimum required frequency bin sizes for selected GNSS signals using a sampling frequency of 10.23 MHz.

Table 4.1: Search space properties for a signal with a sampling frequency of 10.23 MHz and a Doppler range of ± 5 kHz

	GPS L1 C/A	Galileo E1B/E1C	BeiDou $B1C_d/B1C_p$
Length [ms]	1.0	4.0	10.0
Possible code phases	10230	40920	102300
Doppler bins	11	41	101
Doppler bin size $\Delta f[Hz]$	1000	250	100
Possible combinations	112530	1677720	10332300

In the following the main acquisition techniques for serial and parallel acquisition will be elaborated.

4.1.1 Serial search

According to Borre et al. (2007) the serial search algorithm is based on the multiplication of locally generated PRN code sequences and locally generated carrier signals as shown in Figure 4.1. The incoming signal is multiplied with a local generated PRN code with a certain delay and a locally generated carrier signal which generates the in phase signal I and the 90° phase-shifted in quadrature signal Q. These signals are integrated over their primary code length, squared and finally summed together. If the resulting sum exceeds a certain threshold a satellite signal has been found. If the result does not exceed the threshold the process is repeated again with a different PRN code phase and Doppler. This method has to be repeated for all possible code-Doppler combinations making it inefficient due to the large computational burden.

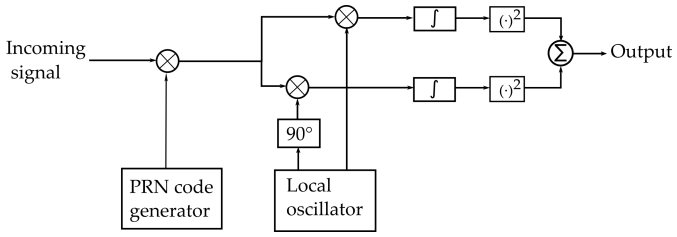

Figure 4.1: Serial search algorithm (c.f. Borre et al. 2007)

4.1.2 Parallel frequency space search

The parallel frequency space search eliminates the need for searching all frequency bins by exploiting the transformation of the signal from the time domain into the frequency domain. This transformation is accomplished by applying the Fourier transformation

$$\mathcal{F}\{s(t)\} = S(f) = \int_{-\infty}^{\infty} s(t) \cdot e^{-2\pi fit} dt. \tag{4.2}$$

The Fourier transformation $\mathcal{F}\{s(t)\}$ describes an operator which transform a signal into its frequency components. According to Borre et al. (2007) the incoming signal is multiplied by a locally generated PRN code sequence, transformed into the frequency domain and squared as shown in Figure 4.2.

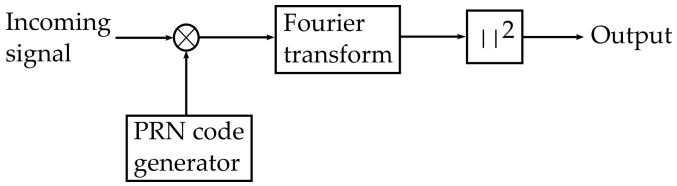

Figure 4.2: Parallel frequency search space algorithm (c.f. Borre et al. 2007)

If the local generated PRN code sequence is perfectly aligned the PRN code will be wiped off and the navigation data and carrier wave will remain. If this signal is transformed into the frequency domain it will show a significant peak at the Doppler frequency and if the PRN code is not aligned correctly only noise will be visible as shown in Figure 4.3. Furthermore, if a navigation bit transition occurs within the signal the expected peak in the frequency domain will be split similar to a BOC modulation which needs to be taken into account (Leclère et al. 2013). While this algorithm is significantly faster than the serial search algorithm the computational burden is still high, especially for high sampling frequencies.

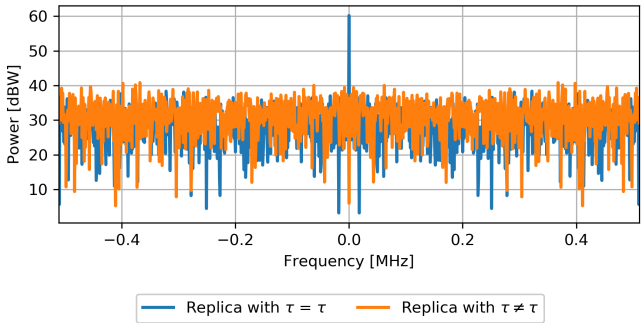

Figure 4.3: Result of parallel frequency space search

4.1.3 Parallel code phase search

The parallel code phase search eliminates the necessity for generating a replica code for every code phase by exploiting the properties of the crosscorrelation function. Comparing the convolution

$$(s_1(t) * s_2(t))(\tau) = \int_{-\infty}^{\infty} s_1(t)s_2(t-\tau)dt, \tag{4.3}$$

with the crosscorrelation from Equation 2.6 the following relation can be established

$$s_1(t) \star s_2(t)) = s_1^*(-t) * s_2(t) = s_1^*(t) * s_2(-t), \tag{4.4}$$

where s_1^* is the complex conjugate of s_1. The only difference between the convolution and the crosscorrelation is the time reversal and conjugation of one of the respective input signals. According to the convolution theorem, the Fourier transformation can be used for computing the convolution by

$$s_1(t) * s_2(t) = \mathcal{F}^{-1}\{\mathcal{F}\{s_1(t)\} \odot \mathcal{F}\{s_2(t)\}\}. \tag{4.5}$$

Using the relation from Equation 4.4 and inserting it into Equation 4.5 leads to the crosscorrelation computation using the Fourier transformation in the form of

$$s_1(t) \star s_2(t) = \mathcal{F}^{-1}\{\mathcal{F}\{s_1(t)\} \odot \mathcal{F}^*\{s_2(t)\}\}. \tag{4.6}$$

According to Borre et al. (2007) this is a fast method for acquisition which can be used as shown in Figure 4.5. The incoming signal is multiplied with a local created carrier to wipe off the carrier wave from the signal. Afterwards the Fourier transformation is performed. The result is then multiplied with the local PRN code sequence which has been Fourier transformed and complex conjugated.

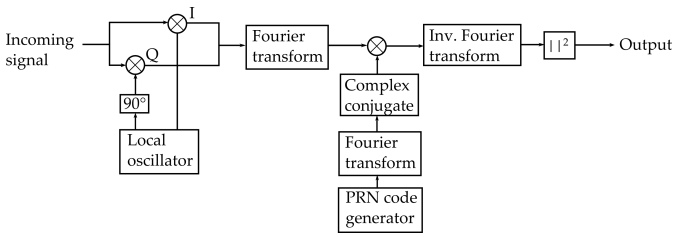

Figure 4.4: Parallel code phase algorithm (c.f. Borre et al. 2007)

The result is then inverse Fourier transformed resulting in a correlation result for all code phases for the given local carrier wave. At last this result is squared and the maximum is compared to a threshold to decide whether the satellite signal is present or not. If no significant correlation peak is found the process is repeated with a different local carrier wave. These local carrier waves are created according to the required minimum Doppler bins. The local PRN sequence is only required to be created, Fourier transformed and complex conjugated once saving additional computations. Figure 4.5 shows the result search space of the parallel code phase search for a visible and a non visible GPS satellite.

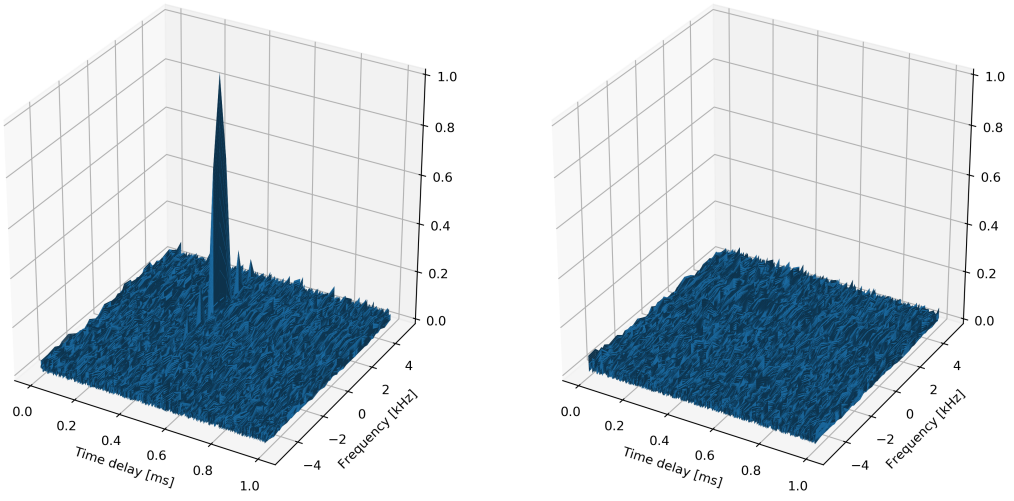

Figure 4.5: Result in the search space of the parallel code phase search algorithm for a visible GPS L1 C/A satellite (left) and a non available satellite (right)

4.2 Refinement methods

The obtained acquisition results are only coarse values for the Doppler and the code phase and need to be refined. The coarse Doppler can have several 100 Hz error after the acquisition. According to Hill (2001) 1 Hz error in the frequency estimation leads to 1 km error in the position solution with Doppler based positioning methods. To initialise a snapshot receiver it is necessary to have an initial position estimate within ± 150 km to the true receiver position according to Diggelen (2009) to have a position solution. The accuracy for pseudorange based methods on the other hand is depending on the possible code phase resolution. After the acquisition the code phase has a sample accuracy and using this would lead to pseudorange errors up to ±150 m depending on the sampling frequency as shown in Figure 4.6. Increasing the sampling frequency increases the pseudorange accuracy after the acquisition in exchange of computational burden. It is shown that at a certain point the accuracy profit from increasing the sampling frequency is not justified for the resulting computational burden.

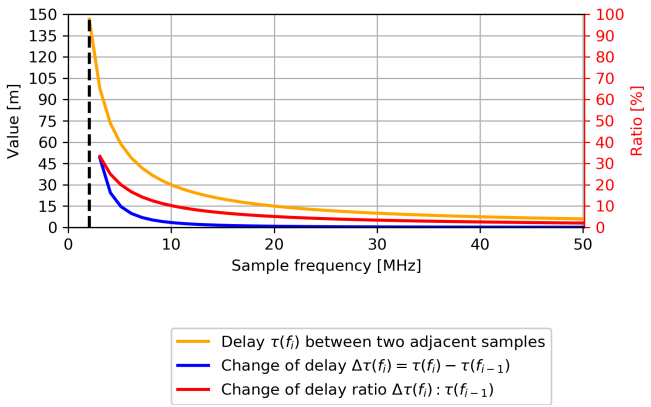

Figure 4.6: Delay between two adjacent samples and accuracy profit of increasing sampling frequency

4.2.1 Fine Doppler estimation

A fine frequency estimation can be done by means of averaging, interpolation or phase relation. The averaging method uses several epochs of code phase observations

and computes the range rates by

$$\hat{\dot{R}}_r^s(t) = \frac{R_r^s(t) - R_r^s(t-1)}{\Delta t}, \tag{4.7}$$

where $\hat{\dot{R}}_r^s(t)$ is the estimated range rate for the epoch t. Since the code measurements are quite noisy and the Doppler change rate is 0.8 $\frac{\text{Hz}}{\text{s}}$ according to Diggelen (2009) several previous estimated range rates can be weighted averaged to an estimated average range rate $\bar{\hat{\dot{R}}}_r^s(t)$ by

$$\bar{\hat{\dot{R}}}_r^s(t) = \frac{\sum_{i=t-x}^{t} P_i \cdot \hat{\dot{R}}_r^s(i)}{\sum_{i=t-x}^{t} P_i}, \tag{4.8}$$

where P_i is the weighting factor of the individual epoch and x the number of epochs considered from the past. Choosing $P_i = 1$ leads to the standard averaging method.
The interpolation method interpolates the samples around the maximum peak of a PSD from a code wiped off signal using a polynomial of 2nd degree, $\texttt{sinc}(x)$ or other functions to estimate the frequency.
The phase relation method uses a code wiped off signal. According to Yang et al. (2011) and Zhi-Feng et al. (2013) a phase angle can be computed for the signal by

$$\Phi_j = \arctan \frac{\Im(X_j)}{\Re(X_j)}. \tag{4.9}$$

Using a phase angle Φ_k, with a short time delay to Φ_j, the two phase angles can be used to compute the fine frequency by

$$f = \frac{\Phi_k - \Phi_j}{2\pi(n-m)}, \Phi_k - \Phi_j < 2\pi. \tag{4.10}$$

This is the fastest of the given methods but requires several ms of snapshot signals. According to literature at least 5 ms of signal should be used to estimate a fine frequency by the phase relation.

4.2.2 Fine code phase estimation

The fine estimation of the code phase uses different interpolation techniques to estimate the correlation peak and gaining sub sample accuracy.
The peak estimation by line intersection uses the full correlation peak and estimates a line for the left flank and the right flank. These lines are then intersected and

the intersection point represents the maximum correlation peak. This method is simple but requires a high sampling frequency to estimate the flanks of correlation peaks accurately.
The next method uses a 2nd degree polynomial for interpolation: Using the maximum of the correlation result and certain amount of samples around it, this method estimates a best fitting polynomial of 2nd degree into these samples. This method is especially useful for signal snapshot with low sampling frequency. Furthermore, according to Tsui (2005), this method approximates the correlation peak most realistic in natural environment.
Advanced interpolation methods use different row expansions and functions to interpolate the correlation peak. Zheng et al. (2010) uses a Taylor approximation to fine estimate the peak for very low bandwidths in the range of 2 to 4 MHz.
In this thesis the interpolation by polynomial of 2nd degree has been chosen for the fine estimation of the code phase since it is suitable for low and high sampling frequencies. Figure 4.7 shows the line intersection method and interpolation method for a correlation peak and their estimated maximum peaks. The used sampling frequency was 20.25 MHz and it can be observed that the difference are marginal between the two methods. Since the interpolation method works for lower sample frequencies as well it is considered more advantageous.

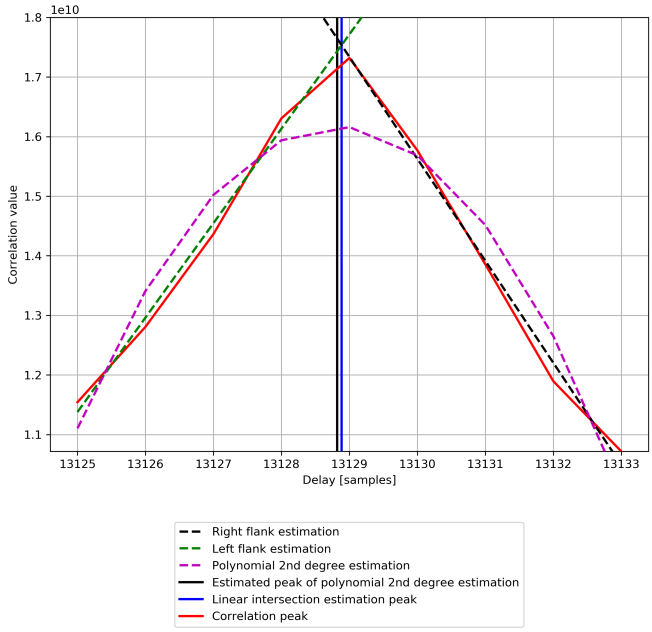

Figure 4.7: Correlation peak estimation with line intersection method and interpolation by polynomial of 2nd degree with 20.25 MHz sampling frequency

5 Interference

GNSS signals are received on the earth's surface with a power below -157 dBW. According to Borre et al. (2007) this is below the thermal noise of -140 dBW. This makes the signal quite vulnerable to interferences from different sources. Radio frequency signals from any undesired source that are received by a GNSS receiver are considered to be interference (Kaplan and Hegarty 2006). Interference can lead to a degraded position solution or even to a denial of service. According to Kaplan and Hegarty (2006) interference can be categorized into intentional and unintentional interference. Unintentional interference is due to the environment such as natural sources, other satellite signals and other external signals. Even though different GNSS apply different code structures and modulations to not interfere with each other such as GPS L1 C/A and Galileo E1B, a remaining impact cannot be avoided completely. This is denoted as inter-system interference. Furthermore, within one GNSS the PRN codes are not completely orthogonal resulting in interference between satellites of the same GNSS denoted as intra-system interference. Signals from non-GNSS systems such as aeronautical radio navigation services (ARNS) influencing GNSS are denoted as external interference. Other unintentional interferences are due to natural sources such as ionospheric scintillation or solar burst.
On the other hand intentional interference has the objective of degrading the navigation solutions intentionally, the denial of service or misguide the receiver. This is also referred to as jamming, meaconing and spoofing. Due to the low received power of GNSS signals it is easy to overpower the signal with another radio frequency signal. Thus, the GNSS signals gets drowned, which leads to degraded navigation solutions or a complete denial of service and is denoted as jamming. According to Kaplan and Hegarty (2006) the intent of misguiding a receiver in its position through broadcast of fake GNSS signals is denoted as spoofing. Meaconing is another form of spoofing where the received authentic signals are rebroadcast time delayed to degrade the position solution.

5.1 Jamming

Jamming denotes the drowning of GNSS signals in noise by emitting radio frequency signals with higher power than GNSS. Dovis (2015) classifies the jamming signals based on their bandwidths into wideband, narrowband and continuous wave interference. Wideband interference covers a similar or larger bandwidth as GNSS, whereas narrowband interferer cover only a small portion of the spectrum in comparison to the GNSS band. Another definition of the classification can be done on the temporal behaviour of the jamming signal properties such as amplitude and frequency. The temporal variation of amplitude and frequency can be observed by using a timedependent PSD, the so called short-time-Fourier-transformation (STFT).
The power spectral density describes the distribution of power within the signal with respect to the frequency. There are several algorithms for computing a PSD such as Welch's method (Welch 1967). The PSD using the Fourier transformation from Equation 4.2 can be computed in the form

$$\texttt{PSD}(f) = \frac{1}{f_s \cdot N}|S(f)|^2, \tag{5.1}$$

where f_s is the sample frequency and N is the number of samples. A PSD uses the full signal length resulting in a high frequency resolution, thus having no temporal variation. A short-time-Fourier-transformation consists of several overlapping Fourier transformations over short time periods of the incoming signal s with N samples as shown in Figure 5.1.

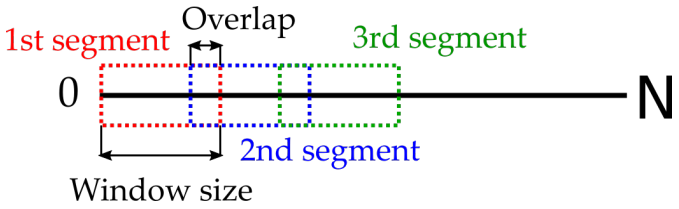

Figure 5.1: Short-time-Fourier-transformation

The number of segments a STFT uses is given by

$$N_{\texttt{segments}} = \frac{N - w}{w - o} + 1, \tag{5.2}$$

where N is the number of signal samples, w is the window size of the segments and o is the overlap. Each segment represents an epoch, thus the STFT shows how

the frequency components of a signal change over time.
Based on behaviour the following types of interfering signals can be distinguished.

Continuous wave (CW): CW jammers transmit signals with a constant frequency and amplitude as shown in Figure 5.2. These types of jammers can be characterized by their frequency offset which describes the difference between the centre frequency of the jammer and a GNSS centre frequency.

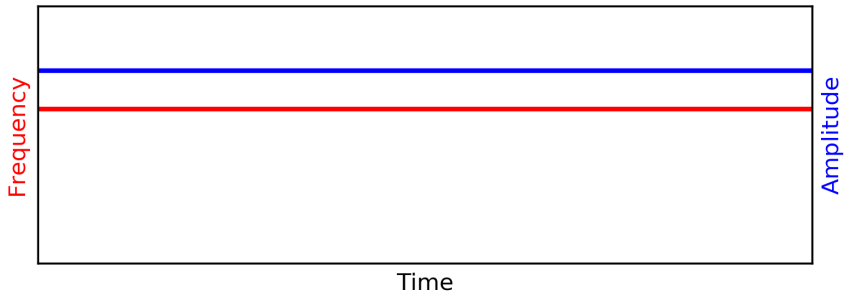

Figure 5.2: Continuous wave jammer

Amplitude modulated (AM): AM jammers show a constant frequency with a varying amplitude in the form of a sinusoidal wave as shown in Figure 5.3. AM jammers are characterized by the frequency offset, the modulation frequency and modulation index. The frequency offset is analogue to the frequency offset described by the CW jammer. The modulation frequency describes the modulated sinusoidal wave of the amplitude. The modulation index is the ratio between the biggest and smallest amplitude.

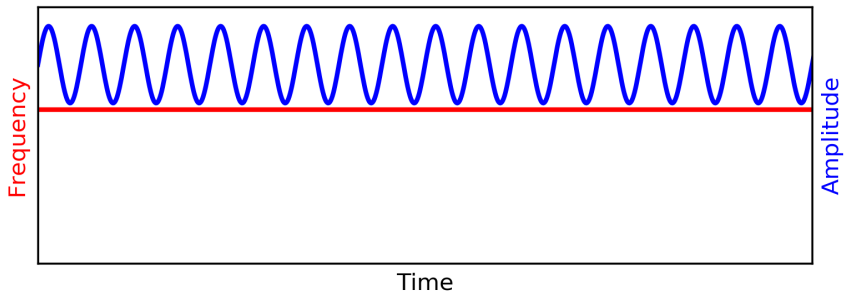

Figure 5.3: Amplitude modulated jammer

Swept continuous wave (SCW): This type uses a signal with constant amplitude and a varying frequency in the form of a sawtooth function as shown in Figure

5.4. A SCW jammer is defined by the frequency offset, the sweep bandwidth and the sweep duration. The frequency offset is the offset from a respective GNSS centre frequency. The sweep bandwidth describes range from the minimum to the maximum frequency it can sweep. The sweep duration describes the time it needs to complete one frequency sweep.

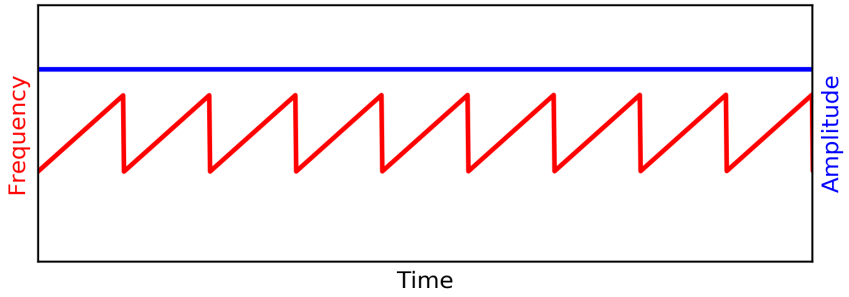

Figure 5.4: Swept continuous wave jammer

Frequency modulated (FM): FM jammers have a constant amplitude and a varying frequency in the form of a sinusoidal wave as shown in Figure 5.5. An FM jammer can be characterized by the frequency offset, the frequency deviation and the modulation frequency. The frequency offset is analogue to SCW jammers and the frequency deviation describes the minimum and maximum amplitude in the frequency with respect to the frequency offset. The modulation frequency describes the frequency of the sinusoidal wave.

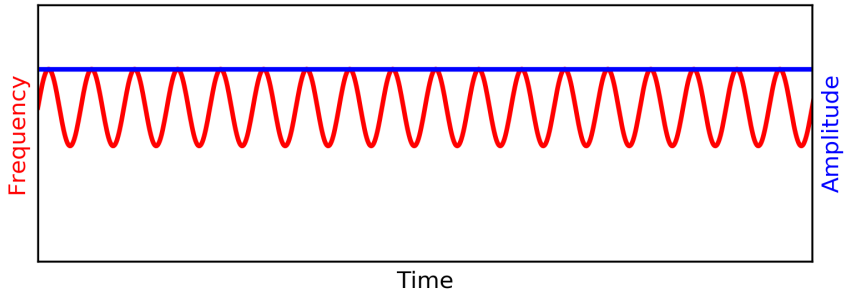

Figure 5.5: Frequency modulated jammer

5.2 Spoofing

Spoofing denotes the transmission of counterfeit GNSS signals with the aim of deceiving the receiver. The received counterfeit signals will be processed within a receiver as if they were authentic signals since the receiver cannot distinguish between the fake and the authentic signals. The tracking loops will switch from the authentic signals to the counterfeit ones and start computing measurements according to the spoofing signals which will then influence the PVT solution. At this point a spoofer can change the trajectory of the victim as desired. This process of swapping from the authentic to the counterfeit signals can be accomplished secretly making this type of attack so dangerous. A typical spoofing attack against a receiver consists of three stages as shown in Figure 5.6. At first the spoofer tries to align the counterfeit signal to the authentic GNSS signal with respect to the code phase and Doppler frequency. In the next step the output power of the spoofer is increased and thus the correlation peak of the spoofing signal, overpowers the authentic correlation peak. At this point the spoofer can change the position of the victim as desired.

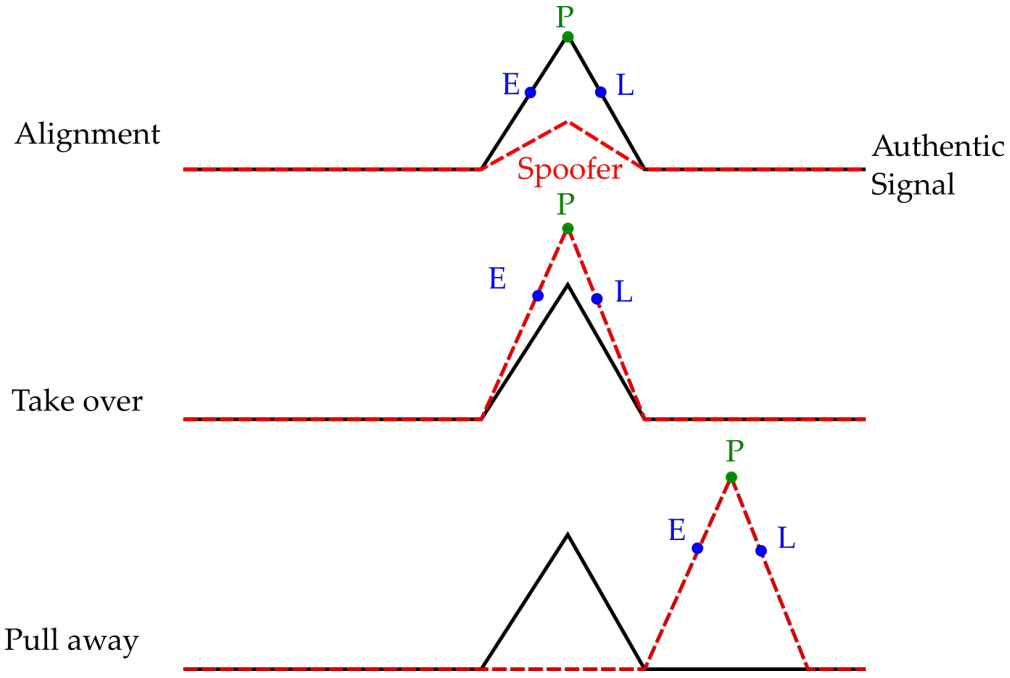

Figure 5.6: Principle of spoofing

Depending on the equipment, complexity and synchronization Dovis (2015) classi-

fies spoofing in three main categories: simplistic, intermediate and sophisticated spoofing attacks.

Simplistic: The simplistic attack emits signals without any knowledge of currently available satellite signals and precise time information. This leads to inconsistent ephemeris, code phase and Doppler values for the transmitted fake satellite signals. The alignment cannot be accomplished consistently since no time-synchronization is available. This spoofing attack is the easiest to detect due to faulty code phases, Doppler and timing. This type of attack only requires a GNSS signal simulator and transmitter.

Intermediate: The intermediate attack uses the knowledge of available satellite signals and correct timing information. A spoofer can accomplish this by using a GNSS receiver to derive the current time and ephemeris. Furthermore, an approximate position of the receiver is available for the correct alignment. The take over is done without Doppler frequency or code phase errors thus achieving a seemingless take over. The requirement of time synchronization and a-priori spatial knowledge of the victim requires a fundamental know-how in GNSS, signal processing and respective equipment making this form of attack rather complex to achieve. A detection possibility for this kinds of attacks is exploiting the fact that all counterfeit signals originate from a single RF source.

Sophisticated: The most complex form of attack uses the intermediate strategy in combination with several transmitters which are distributed over an area. The spoofing signal is received from multiple directions, time synchronized and aligned. In the optimum case each counterfeit signal is transmitted by an individual transmitter. Due to the equipment complexity and the requirement of all counterfeit signals being correctly aligned makes this attack the most complex one.

6 Quality of service monitoring

In recent years, GNSS applications have become the target of intentional interference attacks. Studies show that interference can cause both considerable economic and material damage, as interference signals can significantly influence the operation of GNSS. In general, the impact of interference can lead to degraded position and timing accuracies or to a total failure of the positioning. Mitigation techniques require a successful and reliable detection and classification of GNSS interference in advance. Classical approaches perform a continuous quality of service monitoring within the GNSS signal bands. Since the processing requirements and the amount of data to be processed is considered to be very high, a continuous monitoring is not suitable for all, especially low-cost, GNSS applications. Snapshot receivers on the other hand use short signals for processing, making them perfect for service monitoring of low-cost applications. An additional advantage of snapshot receivers over common ones is the full availability of the code-Doppler domain and correlation values. The disadvantage of using snapshot receivers is that no continuous monitoring is available and only instantaneous monitoring techniques have to be applied. Furthermore, the resulting positioning solution is slightly worse in comparison to receivers with tracking loops. Additionally snapshot receivers have no possible method of accomplishing phase measurements. According to Borio et al. (2016) interference detection can be categorized into three categories such as the hardware indicators, digital samples and post correlation. From this in general three quality assessments with respect to interference can be defined in a snapshot receiver:

Signal quality assessment: This quality assessment includes assessing the incoming signals with respect to the power, statistical distribution and anomalies such as jammers in the spectrum. For this several tools such as the PSD, STFT, statistical tests and statistical distributions can be used.

Code-Doppler domain quality assessment: The quality assessment for the code-Doppler domain includes quality of measurements, availability of satellites and correlation domain properties such as correlation peak strength and noise floor. This is accomplished by using statistical methods for comparing

measurements of different epochs and predictions, the symmetry of correlation peaks and comparing found satellites to possible available satellites.

PVT quality assessment: This type assesses the quality of positions with respect to accuracy, precision and change over time. For this statistical parameters such as the DOPs, distribution of position errors and confidence ellipses are available and can be statistically tested with different epochs.

6.1 Signal quality assessment

The signal quality assessment consists of a received power monitoring and a spectrum monitoring to provide insights into the received signal characteristics. Following Teunissen and Montenbruck (2017) the received power monitoring is an effective strategy for detecting interference. The power of an incoming signal can be computed by

$$P = \frac{\sum s[n]^2}{N}, \tag{6.1}$$

where $s[n]$ is the received signal and N being the number of samples. In the standard case the received power will only show slight fluctuations within a range of $\pm$ 1 dBW depending on the background variation according to Teunissen and Montenbruck (2017). Since jammers require to be several dBW stronger to effectively drown the GNSS signal, the energy detector would show a sudden increase in received signal power. A threshold can be computed using several epochs or defined by an expected value.

The spectrum monitoring is one of the strongest advantages of snapshot receivers in terms of looking for anomalies in the spectrum. The STFT can be used to determine if interference is present and also classify it. The algorithm is based on the classification algorithm of Bartl (2014) which uses the STFT for spectrum analysis as shown in Figure 6.1. The window size is responsible for the resolution in time and frequency. An AM or CW jammer requires a higher frequency resolution while a SCW and FM jammer requires a higher temporal resolution. Therefore, using the classification algorithm with different window sizes and combining the results this method provides the possibility of detecting jammers or other anomalies within the spectrum.

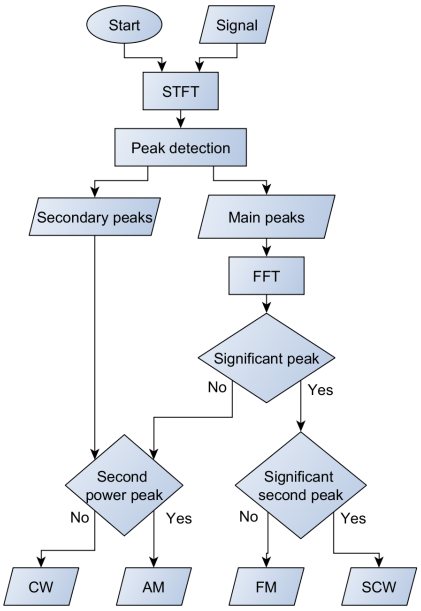

Figure 6.1: Jammer type estimation (c.f. Bartl 2014)

6.2 Code-Doppler domain quality assessment

The code-Doppler domain quality assessment uses a monitoring of the measurements, a monitoring of the correlation peak and a monitoring of the correlation peak-to-noise floor ratio (CPNR). The monitoring of the measurement uses previous measurement epochs and estimates of the current epoch to assess the present measurements of code phase and Doppler frequency. The disadvantage of this method is that several epochs and the receivers kinematic are required to be known for accurate estimates and comparisons. On the other hand the advantage of using this kind of monitoring is the simplicity of detecting outliers and discrepancies.
Since a snapshot receiver has full availability of the code-Doppler domain, this provides the possibility of monitoring the correlation properties such as peak deformations, presence of secondary peaks and noise floor behaviour combined in a correlation peak monitoring. A change within the correlation noise floor is an indication of the presence of interference. The additional jamming and counterfeit signals, if strong enough, increase the power of the correlation noise floor.
If a spoofing signal has a higher code offset of ± 1 chip in comparison to the authentic signal a secondary correlation peak can be found. This typically occurs during a drag away phase during a spoofing attack. A secondary peak detection can be accomplished by testing if any other correlation value exceeds the threshold

for acquisition or by peak to peak comparison with a given threshold. This easily detects a spoofing attack which has more than ±1 chips code offset in comparison to the authentic signal.
On the other hand if the spoofing signal is aligned with the authentic signal within ±1 chips a secondary peak will not be visible but the peak will show deformations due to the overlapping of the two peaks as shown in Figure 6.2.

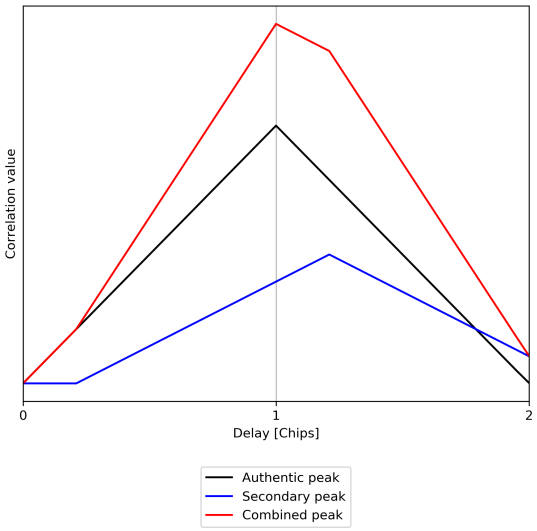

Figure 6.2: Deformed combined peak (red) resulting from the combination of the authentic peak (black) and a secondary peak (blue)

By using the symmetrical property of the correlation function this deformation can be found. One such method exploiting the symmetry to detect multipath is the slope asymmetry metric (SAM) to detect multipath and peak deformations proposed by Lopez-Salcedo et al. (2009). It compares the gradients of correlation peak flanks to detect deformations. Another form of exploiting the symmetry can be accomplished by using a theoretical correlation peak and correlating it to the estimated peak from the signal. Figure 6.3 shows the correlation result between the deformed and theoretical peak. It can be observed that a slight peak deviation results in an asymmetric correlation result in comparison to the correlation result between two authentic peaks. Within the code-Doppler domain quality assessment the CPNR monitoring algorithm compares CPNR and noise floor of previous and estimated epochs to the current set of values. This provides insights into the behaviour of the noise floor. If an interference signal is present the CPNR drops significantly in comparison to authentic epochs.

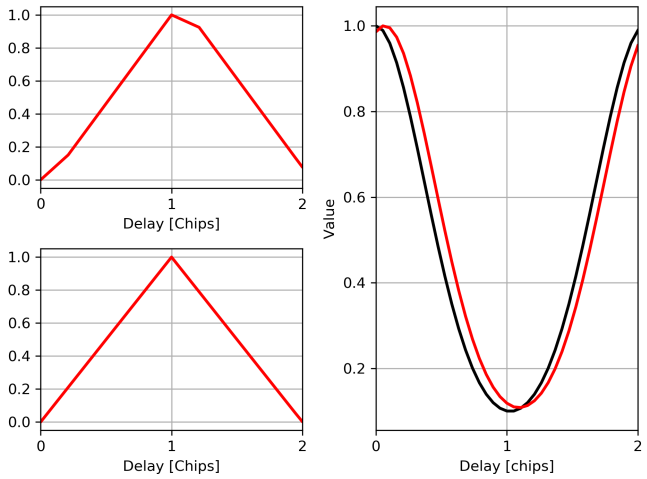

Figure 6.3: Correlation of a deformed correlation peak (top left) and a theoretical correlation peak (bottom left). The resulting absolute correlation values (red) show asymmetry in comparison to the correlation result of two theoretical correlation peaks (black)

6.3 PVT quality assessment

The quality of the position solution can be accomplished using statistical methods such as the confidence ellipse and statistical tests. Statistical tests are used for comparing estimated values with other independent estimated or theoretical values. Following Niemeier (2008) the test results indicate if a significant difference is present. A statistical test consists of a null hypothesis H_0, an alternate hypothesis H_A and an error probability α. One such test for deriving the PVT quality is the global model test according to Niemeier (2008) with the null hypotheses

$$H_0 = E(\mathbf{l}) = \mathbf{Ax}. \tag{6.2}$$

The estimated variance of unit weight σ is compared to an a-priori σ_0 by computing a test value in the form of

$$T = \frac{f \cdot \sigma}{\sigma_0} \sim (f)\chi^2, \tag{6.3}$$

where f is the degree of freedom and the test value being χ^2 distribution. The global model test is then conducted by comparing the test value to the quantile of the respective distribution in the form

$$P(T < \chi^2_{f,1-\alpha}) = 1 - \alpha. \tag{6.4}$$

A hypothesis test has one of four outcomes which depend on H_0 being true and accepted or H_A being true and accepted as shown in Table 6.1. The quantity β

describes the probability error for a false H_0 being accepted. More details can be found in Niemeier (2008).

Table 6.1: Results of hypothesis tests

Test decision	H_0 true	H_A accepted
H_0 accepted	Right decision with P = 1-$alpha$	Type 2 error with P = β
H_A accepted	Type 1 error with P = $alpha$	Right decision with P = 1-β

Another test for comparing different epochs is the congruence test proposed by Niemeier (2008). It tests whether two epochs show any movement within the null hypothesis

$$H_0 : \mathbf{x_1} - \mathbf{x_2} = \mathbf{0}, \tag{6.5}$$

where $\mathbf{x_1}$ is the position vector of the first epoch and $\mathbf{x_2}$ being the position vector of the second epoch. This test checks if the two estimated position solutions are the same with an estimated standard deviation. The test compares the distance between the estimated position solution to the standard deviations and if the distance is greater than the standard deviations with a certain error probability it can be concluded that the two positions are not the same and the resulting distance error is due to movement of the point. The test value can be computed by

$$F = \frac{\mathbf{d}^T \mathbf{Q_{dd}}^{-1} \mathbf{d}}{s_0^2 \cdot h}, \tag{6.6}$$

where $\mathbf{d} = \mathbf{x_1} - \mathbf{x_2}$, $\mathbf{Q_{dd}} = \mathbf{Q_{x_1x_1}} + \mathbf{Q_{x_2x_2}}$, $s_0^2 = \frac{\sigma_{x_1} + \sigma_{x_2}}{f1+f2}$ and $h = \mathtt{rg}(Q_{dd})$. This is then tested against the Fisher-distribution by

$$P(F > F_{h,f,1-\alpha}) = \alpha. \tag{6.7}$$

The Fisher distribution has to be used since the position solutions have both been estimated by the LSA and therefore having only estimated standard deviations. For static receivers this test can be applied without any issues. A dynamic receiver on the other hand requires the previous epoch to estimate the position the receiver will have in the next epoch to use this test. For this the dynamics of the receiver have to be known and a prediction algorithm such as the Kalmann filtering process is required. Furthermore, in case the receiver has not computed an epoch for a longer period of time while changing positions drastically, this test will fail.

7 Implementation considerations

For this thesis an open-loop snapshot SDR was developed in the Python programming language. More information on SDR can be found in Borre et al. (2007). Python was chosen because of it's easy ability to perform detailed analysis while maintaining computational speed. The results of the SDR depend on the signal properties such as sampling frequency, quantization and snapshot length. Within this chapter the impact of these properties will be explained and a brief overview of the developed software is provided.

7.1 Impact of signal properties

The quantization is used in the analogue-to-digital converter to map the analogue values to discrete values. It therefore describes the process of assigning continuous values to a predefined numbers of bit leves. This is accomplished by rounding the values to the closest given digital values as shown in Figure 7.1 for a two bit quantization.

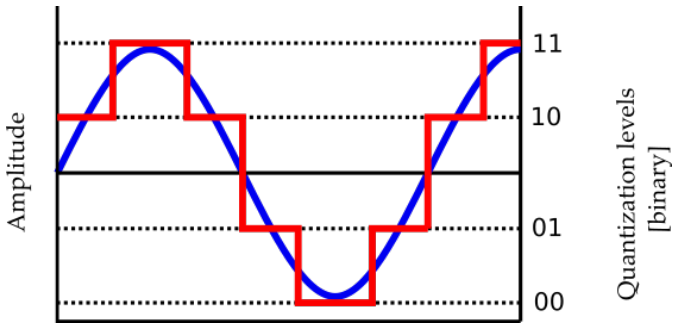

Figure 7.1: Quantization of a continuous signal

In GNSS receivers the quantization has a direct impact on the acquisition, according to He et al. (2008). The quantization influences the CPNR within the acquisition. Using less quantization levels decrease the CPNR and requires longer integration

time. Furthermore, it has a direct impact on the dynamic range. It also has an impact on the amount of data and required storage capacity. In snapshot receivers the number of bits used for the quantization can be selected to increase the signal length, saving memory or to decrease the noise. Furthermore, according to Teunissen and Montenbruck (2017) a higher quantization is always more preferable in case of present intentional interference.
The sampling frequency impacts the time and frequency resolution and limits the bandwidth according to the Nyquist (Shannon) theorem to

$$B < \frac{f_s}{s}, \tag{7.1}$$

where f_s is the sampling frequency. The impact on the time resolution is shown by the delay between adjacent samples in Figure 4.6. The sample frequency furthermore influences the interference detection especially the spectrum monitoring. The spectrum monitoring is done by a STFT as described in Section 5.1. The window size is the possible time resolution of the STFT and higher sampling frequencies allow higher time resolutions with the same window size in the spectrum monitoring as shown in Figure 7.2.

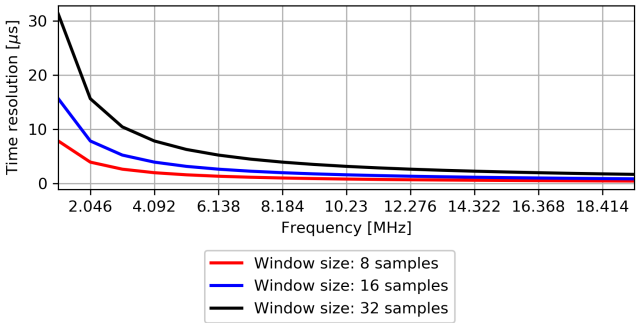

Figure 7.2: Sample frequency impact on the STFT time resolution

This is especially important for detecting SCW and FM jammers which require a higher time resolution in comparison to AM or CW jammers.
The snapshot length is especially important if the signal snapshots have to be transferred from the recording device to a central processing unit. The signal length determines the data size for a complex signal by

$$S = 2 \cdot Q \cdot L \cdot f_s, \tag{7.2}$$

where S is the data size, Q the quantization, f_s the sampling frequency and L the signal length in seconds. Figure 7.3 shows the data size in kB for different sample frequencies and an eight bit quantization per sample.

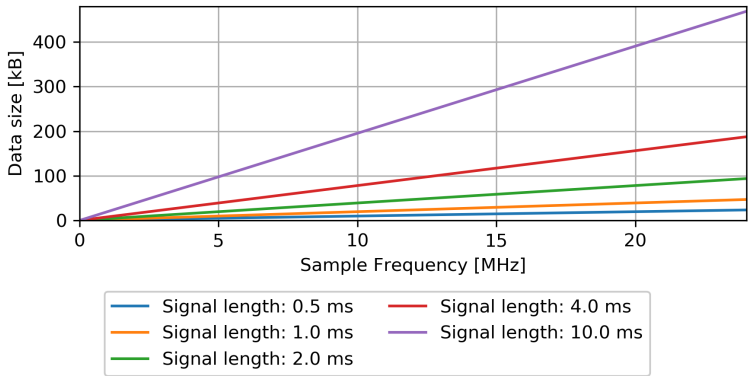

Figure 7.3: Data size of snapshot signals

A compromise of these properties has to be found prior to developing a snapshot receiver and in this thesis a quantization of 8 bit has been used.

7.2 Software design

The snapshot SDR was developed as shown in the flowchart in Figure 7.4. The SDR is implemented as process-based threading. It consists of a main process, a visualization and logging process and several acquisition modules.

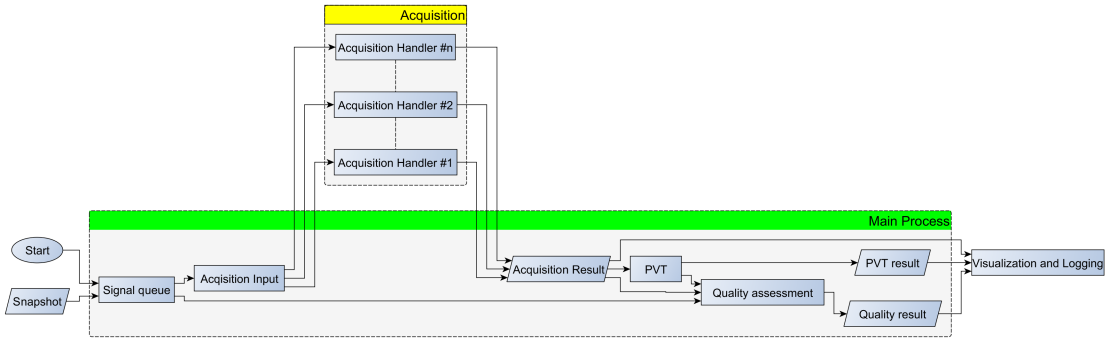

Figure 7.4: SDR snapshot architecture

The main process is responsible for the PVT computation, quality monitoring and creating the acquisition input for the different acquisition handlers. The acquisition input consists of satellite data such as ephemeris, estimated or last known Doppler and the respective code types to assist the acquisition process. The main process

then awaits the acquisition results from the acquisition handlers and computes the PVT and quality assessments. The results of the acquisition, PVT and quality assessment are then further processed in the visualization and logging processor. The acquisition is multi-processed by acquisition handlers and is responsible for computing the coarse and fine acquisition as described in Chapter 4.

8 Results and evaluation

In this chapter the results of the snapshot positioning and the interference monitoring using snapshot techniques are presented. For the evaluation simulations and real-world signals were used. The simulations have been created using the GNSS multisystem performance simulation environment (GIPSIE®). The simulator is capable of simulating digital GNSS signals with different sampling frequencies, different environment conditions as well as interference events (OHB Digital Solutions 2018). Table 8.1 shows the possible GNSS that can be simulated.

Table 8.1: Possible signal simulations with GIPSIE®

GNSS	Signals
GPS	L1 C/A, L2CL, L2CM, L5 I/Q
SBAS	L1 EGNOS/WAAS/MSAS
Galileo	E1B, E1C, E5a/b
GLONASS	G1, G2
BeiDou	B1, B2
QZSS	L1 C/A, SAIF, L2C, L5 I/Q, LEX
NAVIC	L5 and S-band

The real-world signals were recorded using the GTEC® radio frequency front-end (Rügamer et al. 2012), which is capable of recording digital GNSS signals as shown in Table 8.2.

Table 8.2: Possible signal recordings with GTEC®

GNSS	Signals
GPS	L1, L2, L2C
Galileo	E1, E5a/b, E5, E6
GLONASS	G1, G2, G3, G5
BeiDou	B1, B2, B3

The simulations were created for the same time span and antenna position as the recordings of the real-world signals. The settings for the simulations and recordings are summarized in Table 8.3.

Table 8.3: Settings used for the simulations and recordings

	Value
Observation start	4.4.2019 4:18:49 (GPST)
Observation end	4.4.2019 4:23:49 (GPST)
Static antenna-position [ϕ, λ, h]	47.09600422°N, 15.47425325°E, 481.282 m
Simulated f_s [MHz]	5.0, 10.23, 20.25
Recorded f_s [MHz]	20.25
Snapshot lengths [ms]	1.0, 2.0, 4.0, 8.0
Elevation mask	10°

The snapshot time gap, the time between two recorded snapshots, was set to 1 second. The AGC was enabled. For the simulations, the ionospheric and the tropospheric effects were taken into account and additive white Gaussian noise (AWG) was added. Furthermore, only satellites have been simulated which are currently available within the respective GNSS. For the evaluation of the scenarios the ephemeris downloaded from International GNSS Service (2019) were used. More precisely the data sets GOP600CZE_R_20190940000_01D_*N.rnx were used. Figure 8.1 shows the visible satellites for the ephemeris data for the given time span of 4.4.2019 4:18:49 (GPST) till 4.4.2019 4:23:49 (GPST).

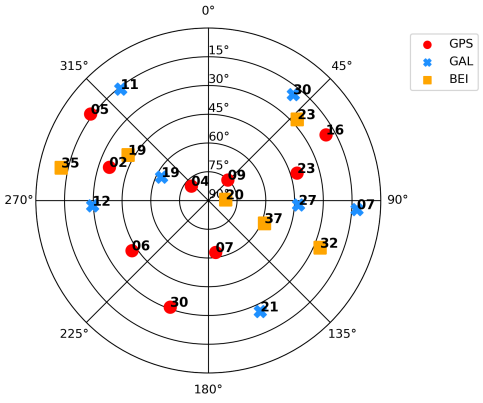

Figure 8.1: Skyplot of the visible satellites

For the comparison of the simulation and real-world data GPS L1 C/A and Galileo E1C signals were used. Figure 8.2 shows the number of acquired Galileo and GPS satellites and the resulting PDOP.

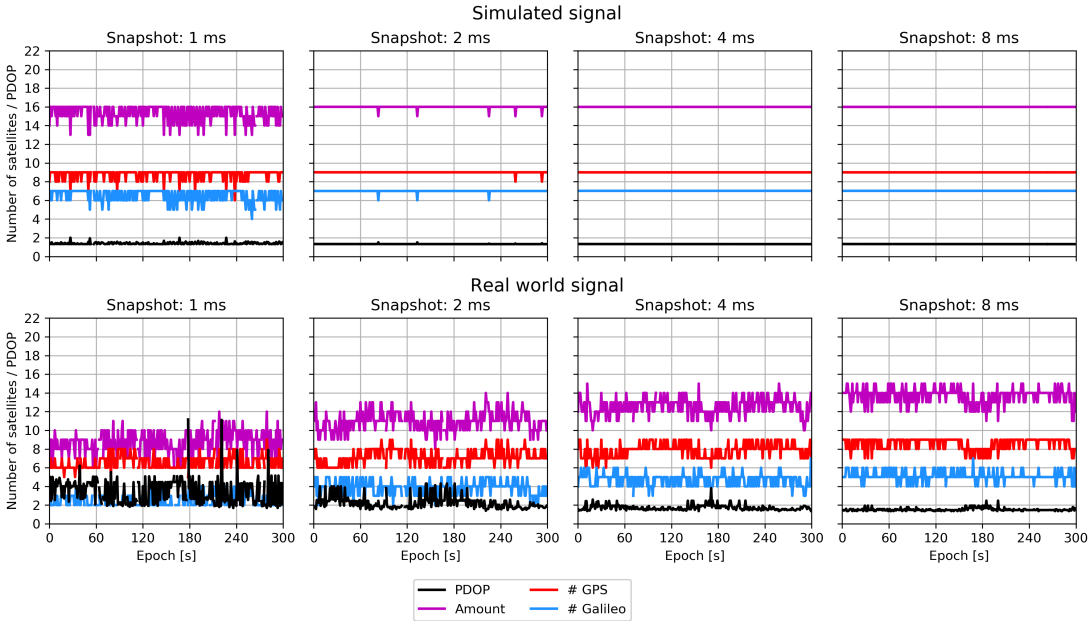

Figure 8.2: Number of acquired satellites and PDOP for the simulated and real-world signals

In general the number of acquired satellites using the real-world data is lower than for the simulations. This can be explained by the antenna being obstructed by trees and building causing a higher noise as well as blocking some signals completely. The PDOP shows high discrepancies for the 1.0 and 2.0 ms snapshot lengths with several measurement epochs having a PDOP of greater than four. This is due to the increasing noise using shorter snapshots, causing less visible satellites.

8.1 Snapshot positioning results

In this section the results of the time free Doppler and pseudorange positioning are presented and discussed. For all analyses evaluations the GPS L1C/A and Galileo E1C signals were used.

8.1.1 Time free Doppler positioning results

The time free Doppler positioning algorithm is evaluated with respect to applicability as initial position estimation for the time free pseudorange computation. For this an a-priori time of 4.4.2019 00:00:00 was selected and the correct time was searched within ± 12 hours using 1 hour intervals. For each time step a LSA with the time-free Doppler positioning model was computed. The result with the least squared sum of residuals and accepted global model test was chosen as the initial position and time.
The Doppler measurements were computed using the phase relation method according to Subsection 4.2.1. As shown in Figure 8.3 the phase relation method was used by splitting the signal in 1 ms parts, computing a phase angle for each part and estimating the Doppler with the following adjacent phase angle. As a last step these values were then averaged to obtain the final Doppler value.

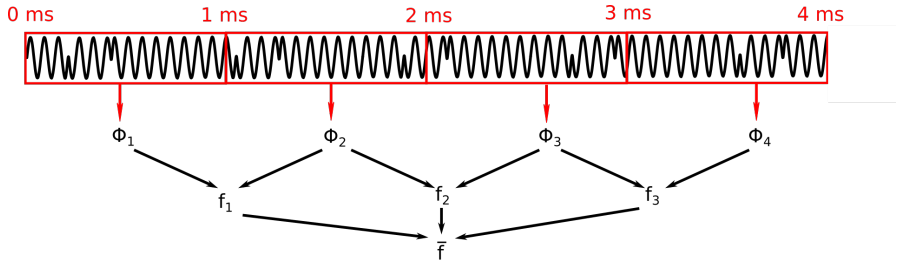

Figure 8.3: Phase relation Doppler estimation algorithm

The chosen snapshot lengths were 4.0 ms and 8.0 ms. These values were chosen to be consistent with the snapshot lengths of the time free pseudorange positioning results shown later and to investigate the behaviour of using less than within literature proposed, 5.0 ms of snapshot length. Figure 8.4 shows the position solutions in the local-level frame of the antenna. The results of the simulated signals for $f_s = 5.0$ MHz and $f_s = 10.23$ MHz differ only slightly from each other whereas using $f_s = 20.25$ MHz shows more precise results. The solution using real-world signals shows the least precise results but can be still used for an initial estimated position for the time free pseudorange positioning since the solution within ± 75 km. The lower precision using real-world signals is a result of less precise Doppler measurements due to noise and less visible satellites.
Table 8.4 summarizes the statistical values (i.e. mean value, standard deviation, outlier percentage) of the results.

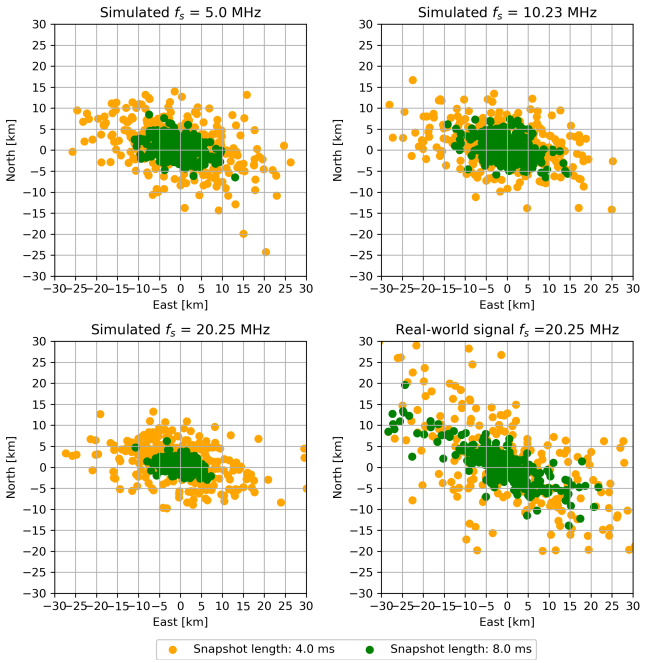

Figure 8.4: Time free Doppler positioning results for different snapshot lengths

Table 8.4: Summary of the time free Doppler positioning results

	fs [MHz]	Snapshot [ms]	Mean [km] N	Mean [km] E	Mean [km] U	Std. [km] N	Std. [km] E	Std. [km] U	Outliers [%]
Simulated	5.0	4.0	0.8	-0.3	-17.7	5.7	10.7	7.9	0.0
		8.0	0.4	-0.4	-5.7	2.3	4.2	3.2	0.3
	10.23	4.0	1.2	-0.9	-18.0	5.0	10.6	7.4	0.0
		8.0	0.4	-0.1	-5.5	2.7	4.7	3.6	0.3
	20.25	4.0	1.2	-0.1	-17.6	4.4	9.2	6.8	0.3
		8.0	0.4	-0.1	-5.6	1.5	2.5	2.1	0.3
Real -world	20.25	4.0	1.4	-0.2	-18.7	11.6	16.2	16.2	20.3
		8.0	0.4	-1.0	-6.7	6.0	11.5	9.9	4.7

Outliers are position results for which the global model test failed, the equation system became singular and thus a valid position could not be computed. The number of outliers using the real-world signals with a snapshot length of 4.0 ms is significantly higher in comparison to all other scenario and further more proves that more than 5.0 ms are necessary to compute reliable position results. Using the

algorithm as explained above $N-1$ Doppler values are estimated with N being the amount of ms. Since it is assumed that each measurement is done with the same standard deviation σ_{f_i} the precision of the averaged Doppler measurement $\sigma_{\bar{f}_s}$ is

$$\sigma_{\bar{f}_s} = \frac{\sigma_{f_i}}{\sqrt{N-1}}. \tag{8.1}$$

Thus, using at least 5.0 ms of snapshot lengths results in at least twice as precise averaged Doppler measurements than the individual measurement precision. Each scenario manages to fulfil the preliminary estimated position criteria (i.e. ± 75 km to receiver position) for the time free pseudorange position. Figure 8.5 shows the empirical cumulative density functions (CDF) for the position results. In the simulated scenarios increasing the sampling frequency did not lead to a significant improvement in precision. More important for an increase in precision was the chosen length of the snapshot.

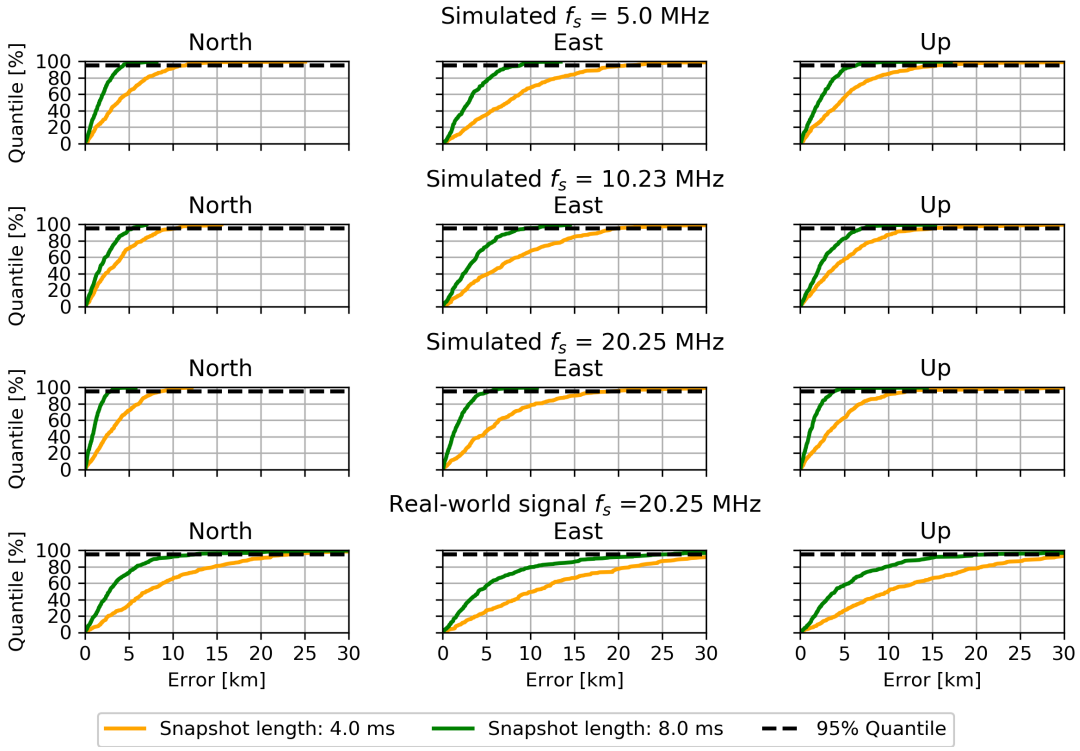

Figure 8.5: Empirical cumulative density function of the time free Doppler positioning results

The time results in comparison to the GPS time is shown in Figure 8.6.

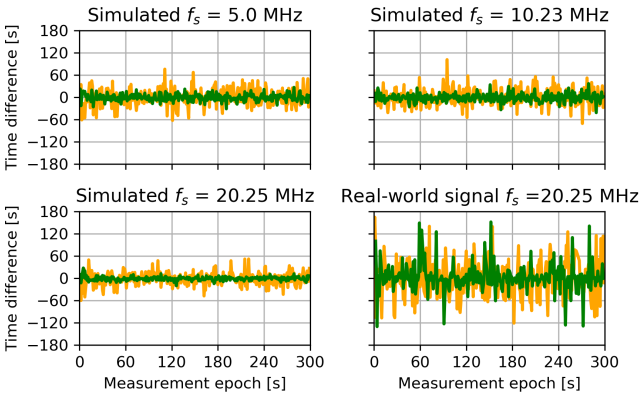

Figure 8.6: Estimated time difference

It can be observed that the solution using real-world signal shows the least precision, but according to Figure 8.7, 95% of the values are still within a range of 100 seconds. This is still acceptable for an initial time estimation for the time free pseudorange positioning.

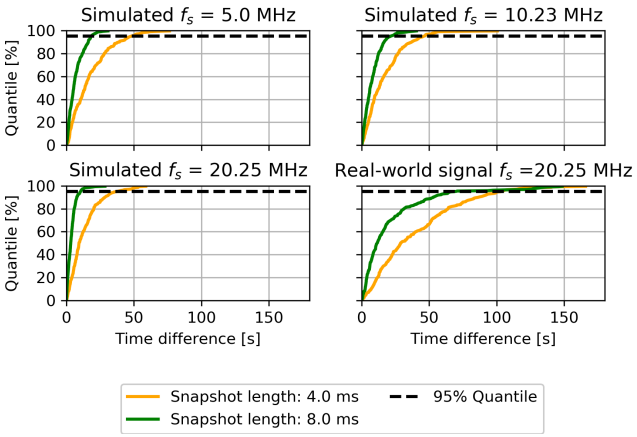

Figure 8.7: Empirical cumulative density function of the time differences

Table 8.5 summarizes the statistical values for each scenario. The solution using real-world signals and a snapshot length of 4 ms has the lowest precision and is the least favourable to be used for the initial estimation of time and position. Regarding the differences between simulated data and real-world data it is assumed

that a combination of less visible satellites, and the measurements beeing affected by noise cause a noisy estimation of the receiver clock drift in the LSA. Figure 8.8 shows the estimated Doppler common bias for the used RFFE.

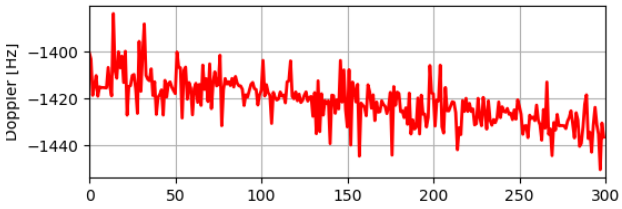

Figure 8.8: Estimated receiver clock drift

The estimated clock drift of the front-end is around -1410 Hz with a visible decrease within the short 5 minute time span. The high variations reach up to ± 10 Hz. Taking into account that 1 Hz results in 1 km position error these variations are assumed to be another factor lowering the precision. If an initial position has to be computed with given limited data size the signal could be decimated to a lower sampling frequency and thus increasing the possible snapshot length.

Table 8.5: Statistical results of the time difference

	fs [MHz]	Snapshot [ms]	Mean [s]	Std. [s]
Simulated	5.0	4.0	-0.4	22.6
		8.0	-0.3	9.1
	10.23	4.0	1.0	22.0
		8.0	-0.8	10.6
	20.25	4.0	-1.3	17.3
		8.0	-0.9	5.2
Real -world	20.25	4.0	-1.3	50.4
		8.0	3.1	34.6

The results of the time free Doppler positioning show that the sampling frequency is not as relevant as the length of the snapshot for the position accuracy. At least 8 ms should be used in order to obtain reliable results.

8.1.2 Time free pseudorange positioning results

For comparing the simulated and the real-world signals GPS L1 C/A and Galileo E1C signals were used without tropospheric or ionospheric corrections. This was done to show solutions without beeing affected by modelling errors. The code phase was fine estimated using a second degree polynomial according to Subsection 4.2.2. For the estimation of the main peak, the maximum peak value and the values from the adjacent samples have been used. Figure 8.9 shows the position solutions of the different scenarios within the local-level frame of the antenna.

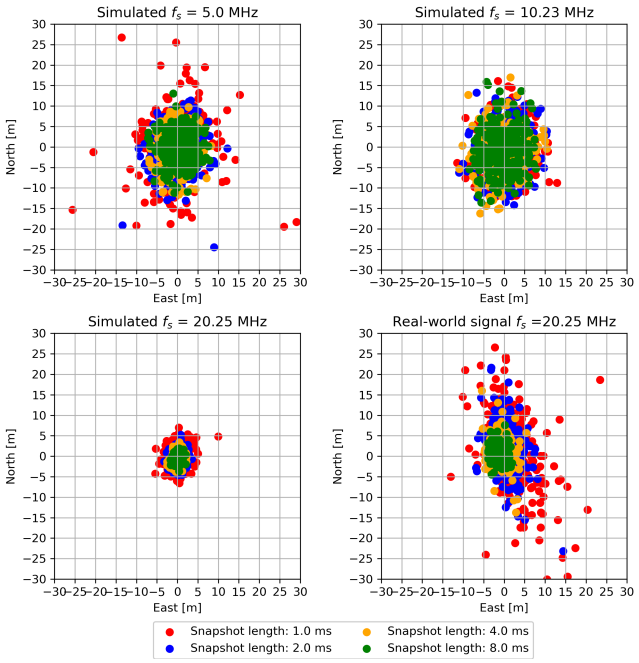

Figure 8.9: Time free pseudorange positioning results for different snapshot lengths

The 1.0 and 2.0 ms snapshot length solutions of the real-world signals are worse than the simulated once due to less visible satellites as shown in Figure 8.2. In case of GPS 6 to 8 satellites are visible while in case of Galileo most of the time only two satellites were successfully acquired which results in an average PDOP of three. The 2.0 ms snapshot scenario using the real-world signals shows slightly better results.
An increase of the sampling frequency from 5.0 MHz to 10.23 MHz, which also increases the sample accuracy from 60 m to 30 m did not increase the quality of the positioning results significantly. Both show the same accuracy and precision,

indicating that the correlation peak interpolation with a second degree polynomial is more efficient in improving the measurement for lower sampling frequencies. The statistical values for the mean positions, standard deviations and outliers are shown in Table 8.6.

Table 8.6: Pseudorange results

	fs	Snapshot	Mean [m]			Std. [m]			Outliers
	[MHz]	[ms]	N	E	U	N	E	U	[%]
Simulated	5.0	1.0	-0.8	0.1	10.7	8.1	6.0	17.8	1.0
		2.0	-0.7	0.2	11.2	5.0	3.8	11.2	0.0
		4.0	-0.2	0.2	11.7	4.2	2.8	8.5	0.0
		8.0	-0.2	0.5	11.7	3.9	2.8	7.3	1.0
	10.23	1.0	-0.4	0.3	12.8	5.3	4.0	10.8	1.0
		2.0	-0.6	0.1	12.2	5.3	3.8	10.7	0.0
		4.0	-1.4	-0.2	10.5	5.1	3.8	9.8	1.0
		8.0	-0.8	-0.2	12.0	4.9	3.5	8.9	1.0
	20.25	1.0	-0.5	0.2	12.2	2.4	1.8	5.5	0.0
		2.0	-0.5	0.2	12.1	1.7	1.1	3.2	0.0
		4.0	-0.5	0.1	12.0	1.2	0.8	2.5	0.0
		8.0	-0.5	0.1	12.0	0.9	0.7	1.8	0.0
Real-world	20.25	1.0	1.8	2.1	4.1	9.6	4.7	16.1	5.0
		2.0	1.8	0.4	4.8	5.3	2.8	8.8	2.0
		4.0	0.9	-0.7	8.0	3.2	1.8	5.7	1.0
		8.0	0.7	-1.2	9.0	1.7	1.2	3.3	0.0

In all scenarios, except for the ones using real-world data with a snapshot length of 1.0 and 2.0 ms an accuracy of the average values within one meter in north and east was achieved. The accuracy of the height is worse because no models for the ionosphere and troposphere were used. The statistical results show that the 5.0 MHz scenario and 10.23 MHz only slightly differ in accuracy and precision.
From the results for the real-world signals it can be observed that an accuracy of the average horizontal position solution below one meter cannot be accomplished using a snapshot length of 1.0 and 2.0 ms. The empirical cumulative density function of the positions as shown in Figure 8.10 shows that the position using real-world signals for short snapshots is worse than compared to the other scenarios. For snapshots with a length longer than 4.0 ms the accuracy is within $\pm$ 1.0 m in north and east.

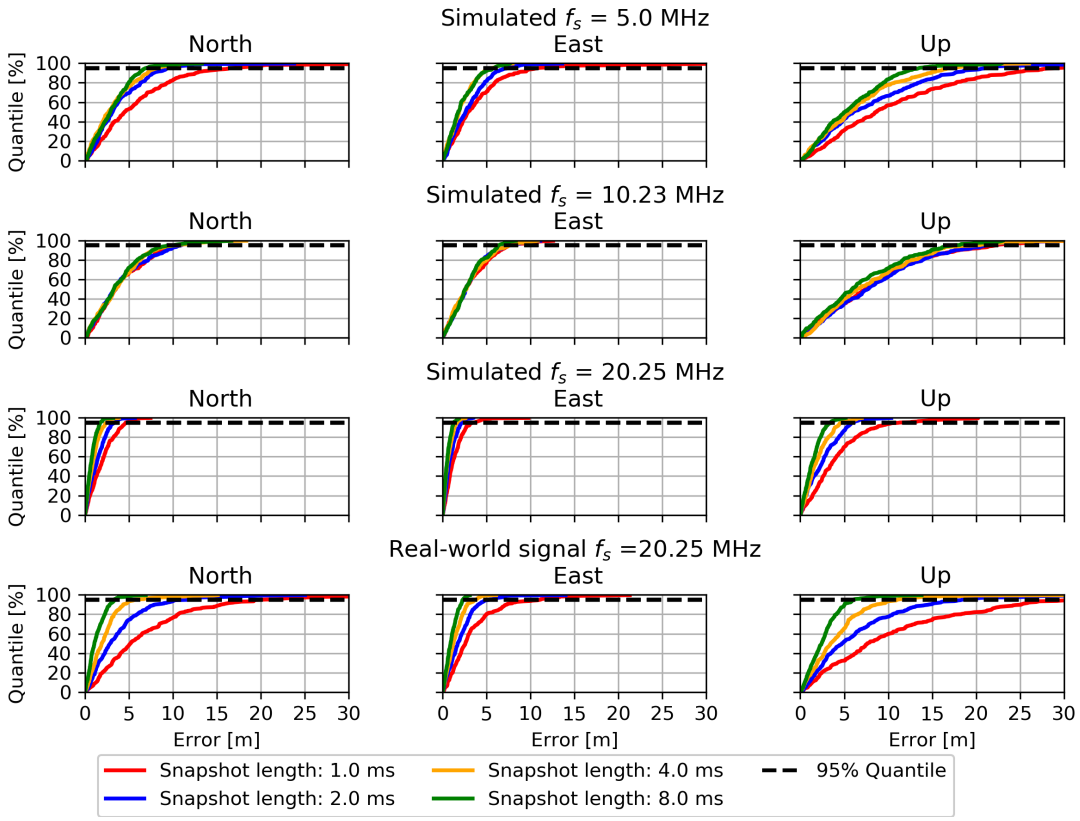

Figure 8.10: Empirical cumulative density function of the time free pseudorange positioning

In conclusion it can be stated that the position solution using real-world signals with two systems and a snapshot length shorter than 4 ms leads to accuracies above one meter and precisions up to 10 meters in north and east. A possible improvement of the position accuracy and precision can be achieved by using an additional system such as BeiDou $B1C_p$. By adding the BeiDou $B1C_p$ signal the available satellites and resulting PDOP improves to the values as shown in Figure 8.11.

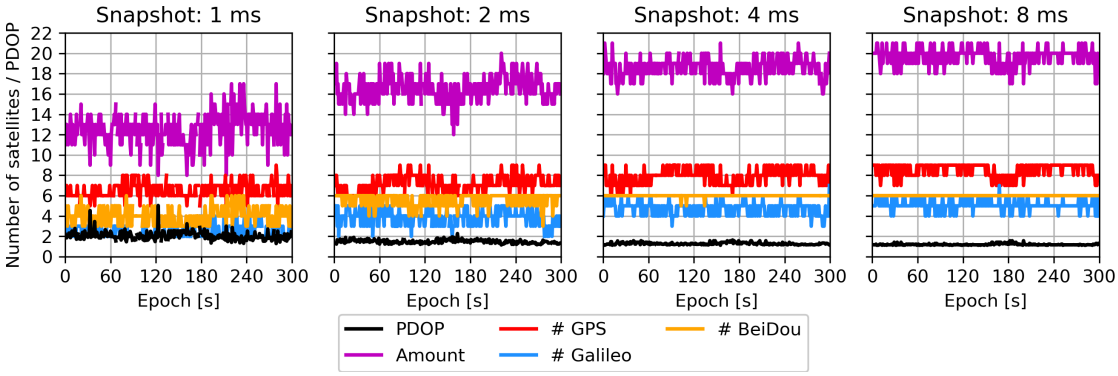

Figure 8.11: Number of visible satellites and PDOP when using BeiDou $B1C_p$ in addition

Compared to Figure 8.2 the PDOP is significantly better by adding the BeiDou signal. Additionally using the Klobuchar ionosphere model and the troposphere model developed by Collins (1999) and described in Subirana et al. (2013) the precision of the height estimation of the position solution can be increased. The position results in the local-level frame are shown in Figure 8.12. For all snapshot lengths the quality of the position solution increased as shown in Table 8.7. The accuracy and precision improvement can be observed especially in case of the 2.0 ms snapshot, which shows an accuracy below ± 1 meter in north and east. Furthermore, the precision is only slightly worse compared to the 4.0 ms snapshot. The additional system increased the PDOP and therefore the accuracy of the position solution and the additional atmospheric corrections further improved the height component of the solution.

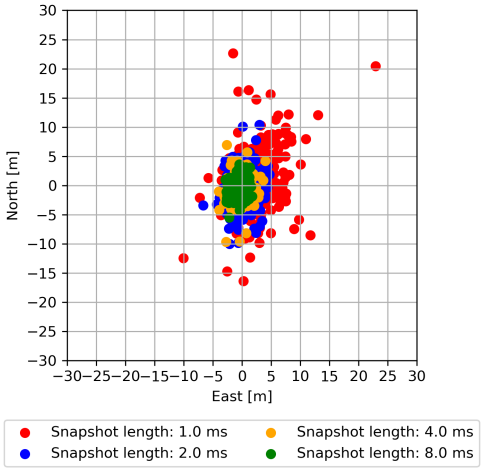

Figure 8.12: Time free pseudorange positioning results using GPS, Galileo and BeiDou

Table 8.7: Pseudorange results using BeiDou B1C$_p$ in addition to GPS L1 C/A and Galileo E1C

	fs [MHz]	Snapshot [ms]	Mean [m] N	Mean [m] E	Mean [m] U	Std. [m] N	Std. [m] E	Std. [m] U	Outliers [%]
Real-world	20.25	1.0	1.1	2.6	-3.2	5.1	3.4	8.9	2.0
		2.0	-0.6	0.2	-2.6	3.0	1.8	4.9	1.0
		4.0	-0.7	-0.4	-2.6	2.1	1.2	3.6	1.0
		8.0	-0.4	-0.6	-2.7	1.4	0.9	2.3	0.0

The improvements in the precision can be further observed in Figure 8.13. 95% of the position differences are within ±6 meters with north being worse than the east since there are no visible satellites in the north for any systems. In conclusion the higher the sampling frequency and the higher the snapshot length the better the position accuracy can be. The simulated signal position results were within 1 meter in north and east and show a maximum standard deviation of ±8 meters for the lowest sampling frequency and shortest snapshot length. Using additional systems and signals can increase the position quality for short snapshot lengths.

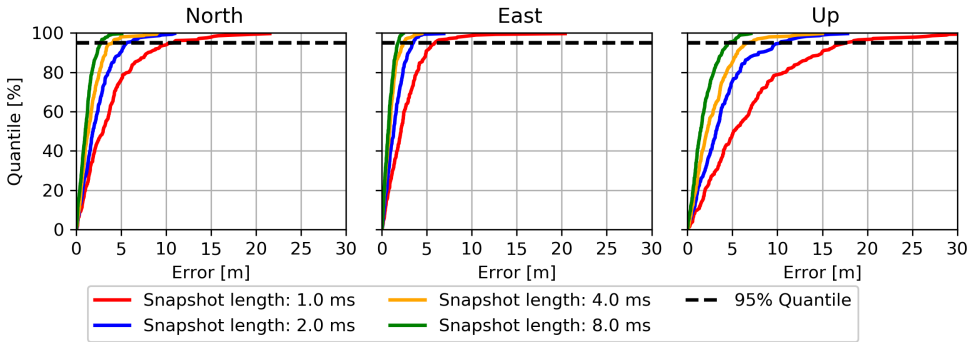

Figure 8.13: Empirical cumulative density function for the position solution with additional BeiDou signals

In comparison to the results above decreasing the snapshot length to 0.5 ms using the real-world signals results in a low number of visible satellites and a high PDOP as shown in Figure 8.14.

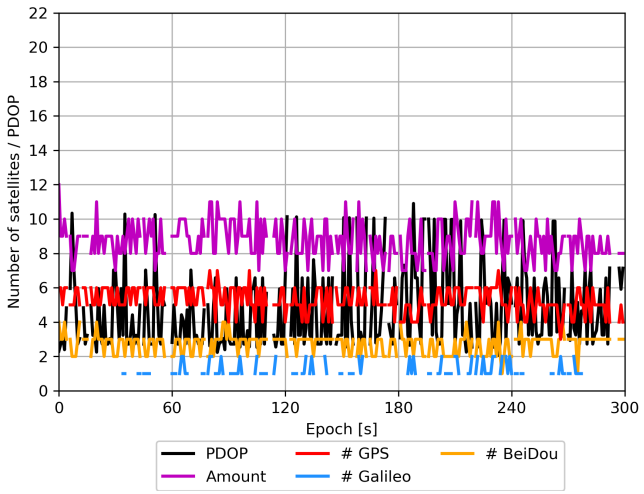

Figure 8.14: PDOP and nubmer of visible satellites per GNSS for 0.5 ms snapshot length

Galileo becomes nearly unavailable using this snapshot length due to the increasing noise in the acquisition. The position is, in nearly all cases, computed using the BeiDou B1C$_p$ and GPS L1 C/A signals. The position solutions with atmospheric corrections are shown in Figure 8.15

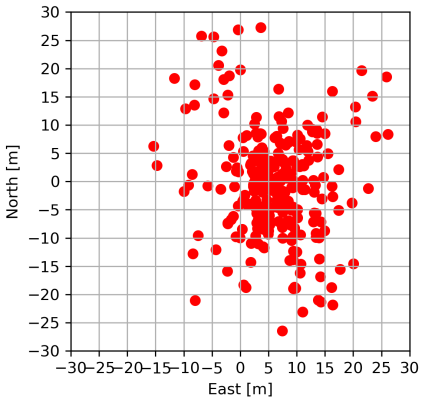

Figure 8.15: Local-level frame of the position results using a snapshot length of 0.5 ms

The position solution shows a significant decrease in accuracy and precision. The statistical values are presented in Table 8.8.

Table 8.8: Position results using a snapshot length of 0.5 ms

fs	Snapshot	Mean [m]			Std. [m]			Outliers
[MHz]	[ms]	N	E	U	N	E	U	[%]
20.25	0.5	0.2	6.3	-10.3	10.9	7.5	22.3	7.3

8.2 Interference detection

The analyses of the interference detection algorithms was performed using simulated scenarios for the same time frame. First the jamming detection capability using peak and spectrogram monitoring is presented followed by the spoofing detection and a validation with the real-world signals which are free of intentional interference.
The jamming detection results are based on snapshot lengths of 1.0, 2.0 and 4.0 ms for the simulated scenarios and GPS L1 C/A signals. At first detailed results for the scenario with a sampling frequency of 10.23 MHz are provided and discussed. Afterwards these detection results are compared to all other scenarios. The window size for the AM/CW spectrogram monitoring was chosen to be 1023 samples and for the FM/SCW spectrogram monitoring using 128 samples.

8.2.1 Jamming detection results

For the detection assessment four interference events have been simulated containing four different jamming signals. The interference signal properties are shown in Table 8.9.

Table 8.9: Setting and properties of the interference signals

	Jammer type			
	AM	CW	FM	SCW
Frequency offset [Hz]	0.0	0.0	0.0	0.0
Start epoch [s]	15	85	155	225
End epoch [s]	75	145	215	285
Modulation frequency [kHz]	1000	/	20	/
Modulation index [%]	60	/	/	/
Frequency deviation [MHz]	/	/	2	
Sweep duration [μs]	/	/	/	20
Bandwidth [MHz]	/	/	/	2

Figure 8.16 shows the change in signal power for each interferer event. The interfering signal powers are changed linear in order to analyse the minimum power required for the detectors to discover anomalies within the signal.

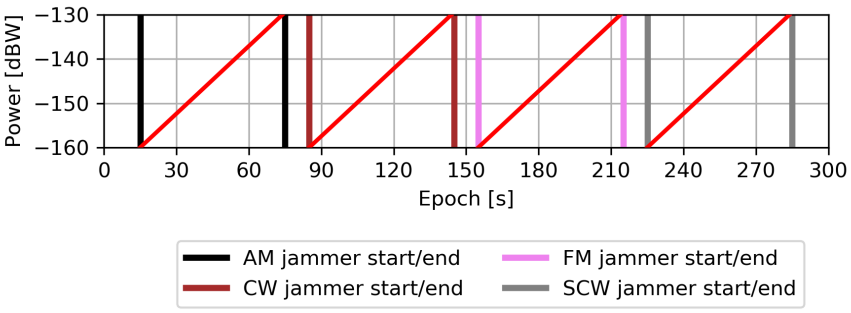

Figure 8.16: Power of the interferer events

The time series of the position results in the local-level frame of the antenna are shown in Figure 8.17.

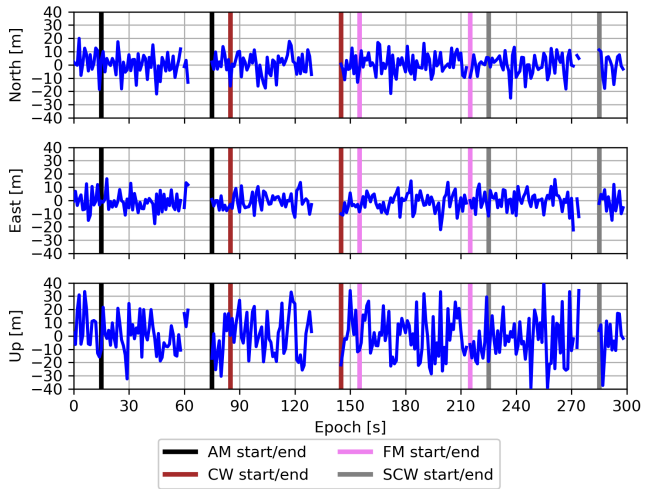

Figure 8.17: Time series of north east up positioning results during interference events

The position solutions show no significant outliers until the jamming signals are able to overpower the authentic signals. The AM and CW jammer deny the position solution at approximately the same power of -137 dbW. The FM jammer does not interference the results significantly. The chosen modulation frequency leads to the jamming signal not residing long enough on the centre frequency to successfully interfere with the authentic signal. The SCW jammer requires more than -135 dbW to affect the position solution. Figure 8.18 shows the CPNR in the acquisition stage and the respective threshold used for detecting visible satellites.

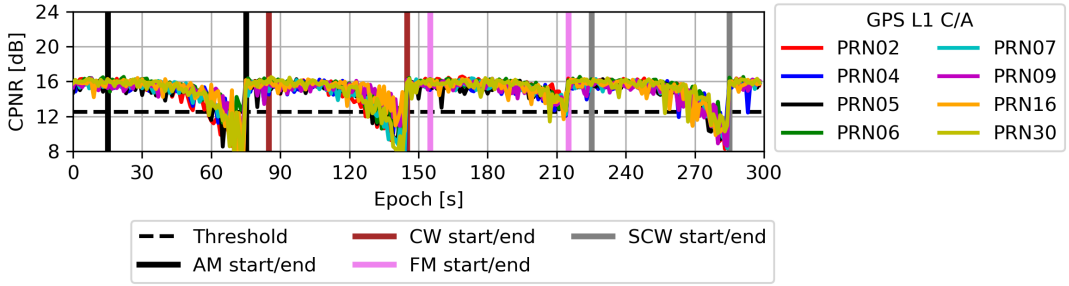

Figure 8.18: CPNR values in the acquisition stage during interference events

The CPNR values during the SCW and FM jamming events are slightly better than the CPNR values for the AM and CW events. The AM and CW jamming signals affect the position solution faster than the FM and SCW jammers.
Figure 8.19 shows the peak and spectrogram monitoring results.

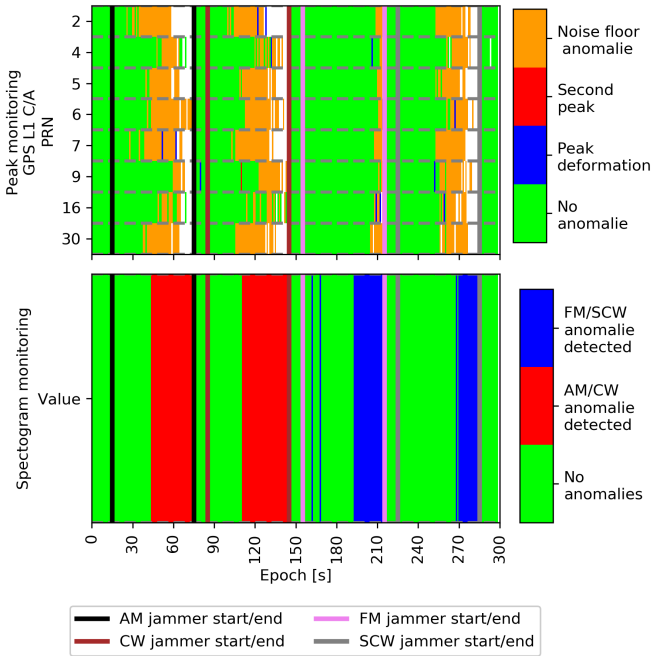

Figure 8.19: Peak monitoring (top) and spectrogram monitoring (bottom)

The peak monitoring shows detected anomalies for low elevation satellites earlier than for satellites close to the zenith. The earliest indication of an erroneous crosscorrelation is found at around 40 seconds where the jammer has around -147 dbW power. Slightly later the spectrogram monitoring correctly detects an AM or CW anomaly continuously for the duration of the interference event. The CW jamming event shows the same behaviour as the AM event.
Compared to the AM or CW jammer the peak monitoring indicates for the FM jammer nearly no anomalies and only the spectrogram monitoring detects the anomalies. The spectrogram monitoring detects FM jamming event at around 195 seconds, at which point the power of the jammer is around -142 dbW.
The SCW jammer is detected by the peak monitoring earlier than the spectrogram monitoring but still later than the AM or CW jammer. Like the FM jammer the SCW jammer does not reside on the centre frequency but only sweeps over it in certain intervals and thus it does not deny the centre frequency continuously. This leads to the jamming signal requiring more power to drown the authentic signal completely. The peak monitoring shows an earlier detection for low elevation satellites due to the lower received power from those satellites compared to satellites in the zenith. In all jamming events the interference was detected before the denial of service. AM, CW and SCW managed to completely deny the service, while

the FM jammer was completely ignored without quality drops in the position solutions. The SCW required a higher power compared to the AM or CW jammers to successfully deny a position solution. On the other hand the AM and CW jammers were easier to detect. The FM jammer was hard to detected in the peak monitoring and was only detected by the spectrogram monitoring. It is assumed that changing the properties of the SCW and FM jammers can lead to a decrease in required power to overpower the authentic signals.
The different results for the peak monitoring and spectrogram monitoring are shown in Figure 8.20 and Figure 8.21.

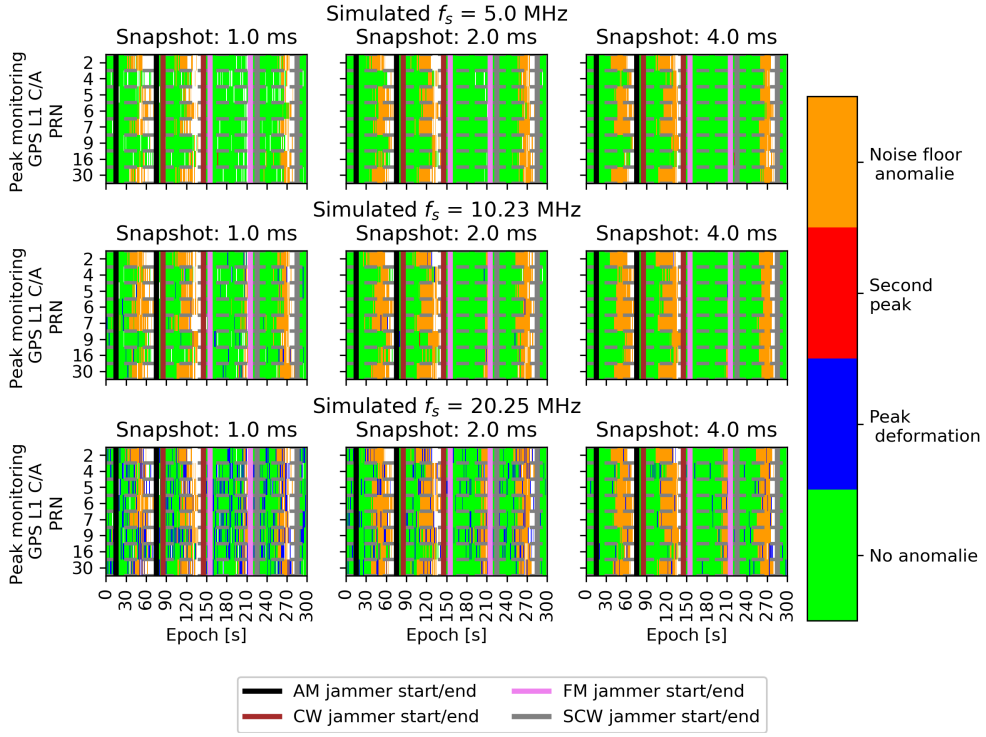

Figure 8.20: Peak monitoring results for all jamming scenarios

For jamming events the peak detector works better for longer snapshots. Increasing the sampling frequency also increases the detection speed, but also increases the false alerts. This is shown especially for shorter snapshot lengths. The spectrogram monitoring detects anomalies earlier with lower sample frequency and the result are independent from the snapshot length.

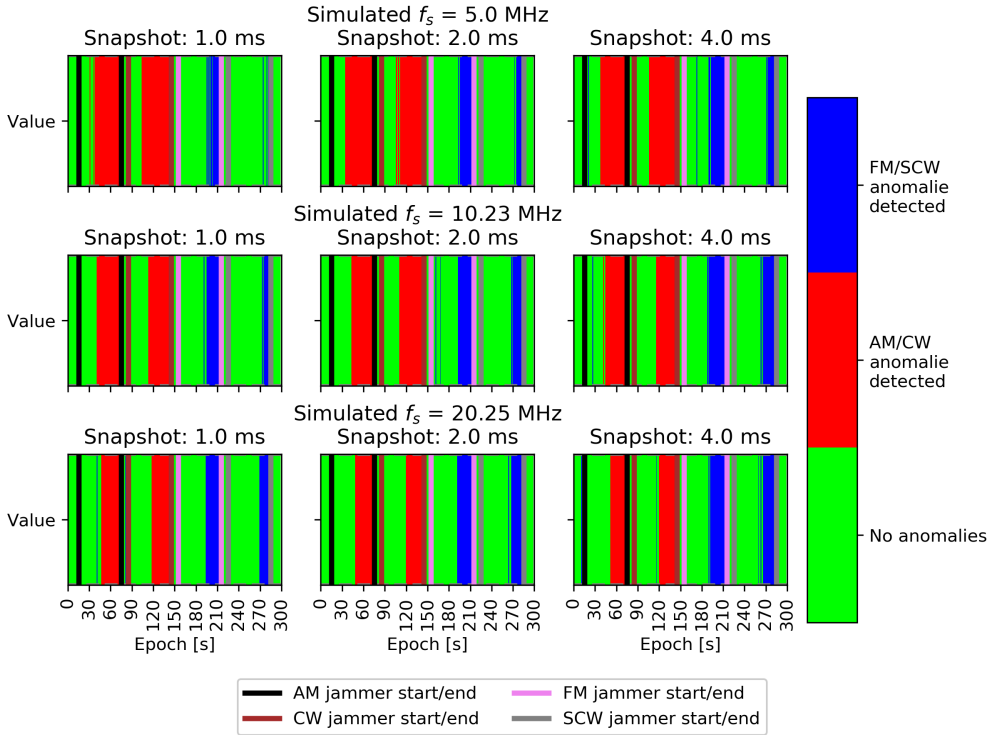

Figure 8.21: Spectrogram monitoring results for all jamming scenarios

8.2.2 Spoofing detection results

The spoofing detection results are first discussed for the 10.23 MHz scenario using a snapshot length of 2.0 ms and later compared to the other cases. The spoofing signal was simulated with the properties listed in Table 8.10.

Table 8.10: Setting and properties of the simulated spoofing signal

	Value
Start epoch[s]	30
Positioning	Same as receiver
Spoofed channels	GPS L1 C/A, Galileo E1B/E1C
Spoofing trajectory start [ϕ, λ, h]	47.09600422°N 15.47425325°E, 481.282 m
Spoofing trajectory end [ϕ, λ, h]	47.110287°N, 15.44861°E, 350.282 m
Spoofing power	3 dbW stronger than authentic signals

Figure 8.22 shows the position solution in the local-level frame of the antenna computed by the snapshot SDR during the spoofing attack.

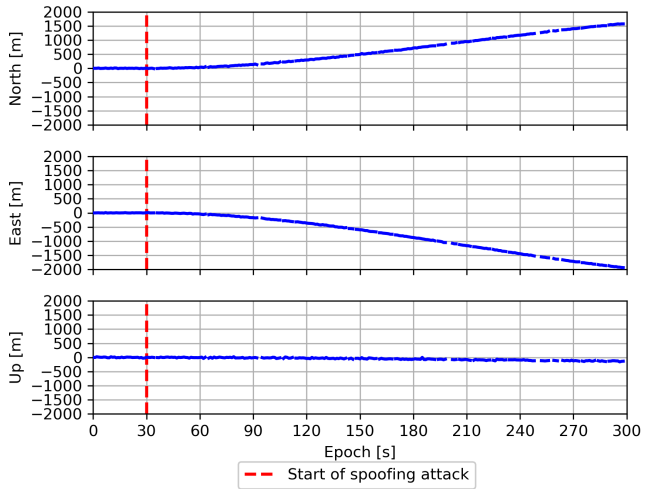

Figure 8.22: Position time series during the spoofing attack

The SDR computes counterfeited position solutions as the spoofer intended, but during several epochs no solution was possible. Figure 8.23 shows the estimated CPNR values in the acquisition stage during the spoofing attack. The CPNR values vary as soon as the spoofer is activated and tries to drag the receiver away.

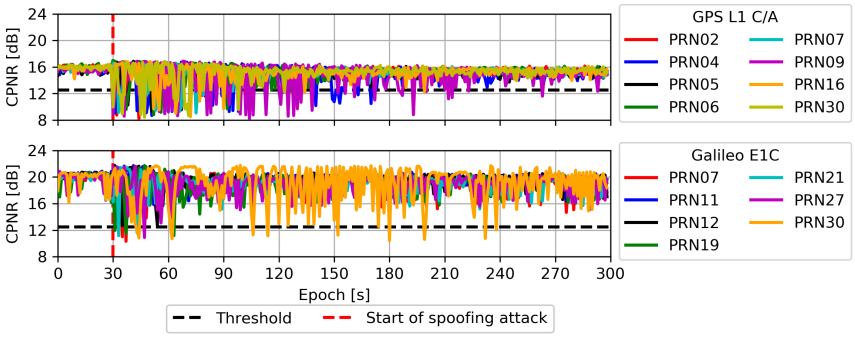

Figure 8.23: CPNR for GPS L1 C/A (top) and Galileo E1C (bottom) during the spoofing attack

The decrease in CPNR is due to the movement of the spoofing signals which creates a phase offset between the real and the spoofing signals which leads to a degradation and even cancellation of the signals. This is especially visible in the early stages of the spoofing attack where the peaks are aligned with each other. If the peaks are aligned with different phase angles the combined correlation peaks of the authentic and counterfeit signals will cancel each other due to different signs of I and Q respectively. If the peaks are not aligned the combination of the correlation values will only add additional noise thus the acquisition CPNR will show less variations as soon as the peaks are separated. The peak monitoring results during the spoofing attack for Galileo E1C and GPS L1 C/A are shown in Figure 8.24.

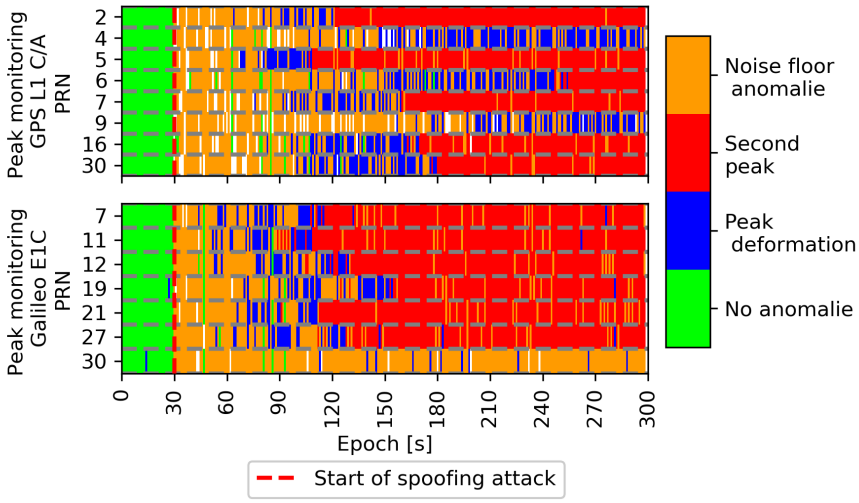

Figure 8.24: Peak monitoring GPS L1 C/A (top) and Galileo E1C (bottom) during the spoofing attack

Immediately after the start of the spoofing attack the peak monitoring detects an anomaly within the noise floor. Figure 8.25 shows the noise floor ratio with respect to the first epoch and it is obvious that the power of the noise floor changes as soon as the spoofing attack starts.

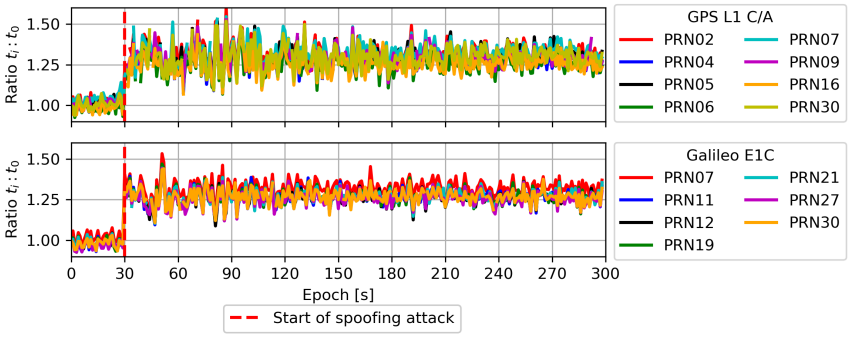

Figure 8.25: Noise floor ratio of the acquisition for GPS L1 C/A (top) and Galileo E1C (bottom)

After the initial noise floor detection an increase in peak deformation is detected until the authentic and fake peaks are completely separated. At this point the acquisition detects two possible peaks exceeding the decision threshold. Figure 8.26 shows the normalized correlation for the GPS PRN02 and PRN04 as well as Galileo PRN19 and PRN07. The GPS satellite PRN02 is at a low elevation angle and thus a faster seperation between the authentic and the spoofing correlation peak is possible. Shortly before the fake and authentic peaks become completely separated, the peak monitoring detects an increase in deformations which is also visible in the correlation results. The same behaviour can be observed for the other satellites. GPS satellite PRN04 is close to the zenith and therefore the distance to separate the original peak and spoofing peak is not achieved for this spoofing attack. Since the seperation is not achieved it is expected to show more peak deformation detections in comparison to the low elevation satellites. The Galileo correlation results show the same behaviour.

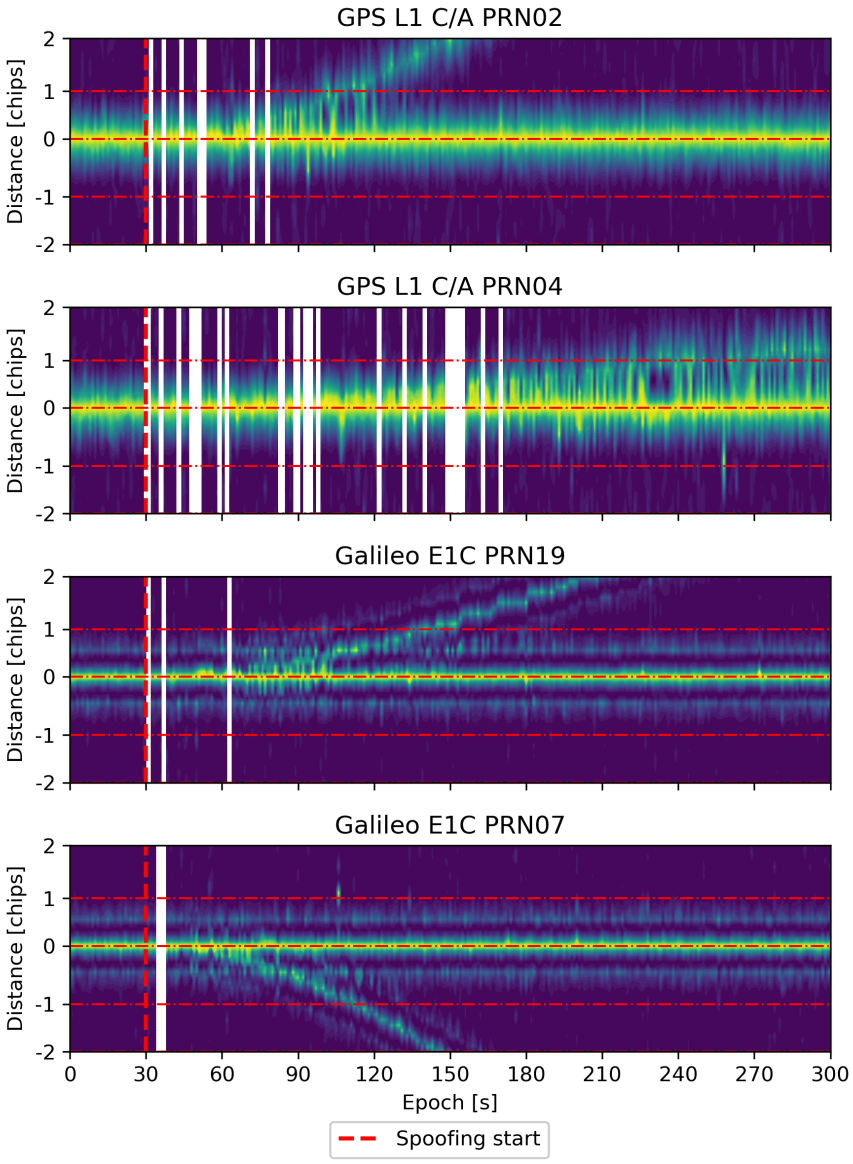

Figure 8.26: Normalized correlation results for selected satellites

The peak monitoring results for the different sample frequencies and snapshot lengths are shown in Figure 8.27 and Figure 8.28. These results show that lower sampling frequencies struggle with detecting the anomalies in the noise floor and peak deformations. Furthermore, it can be observed that longer snapshots are required to detect a secondary peak reliable.

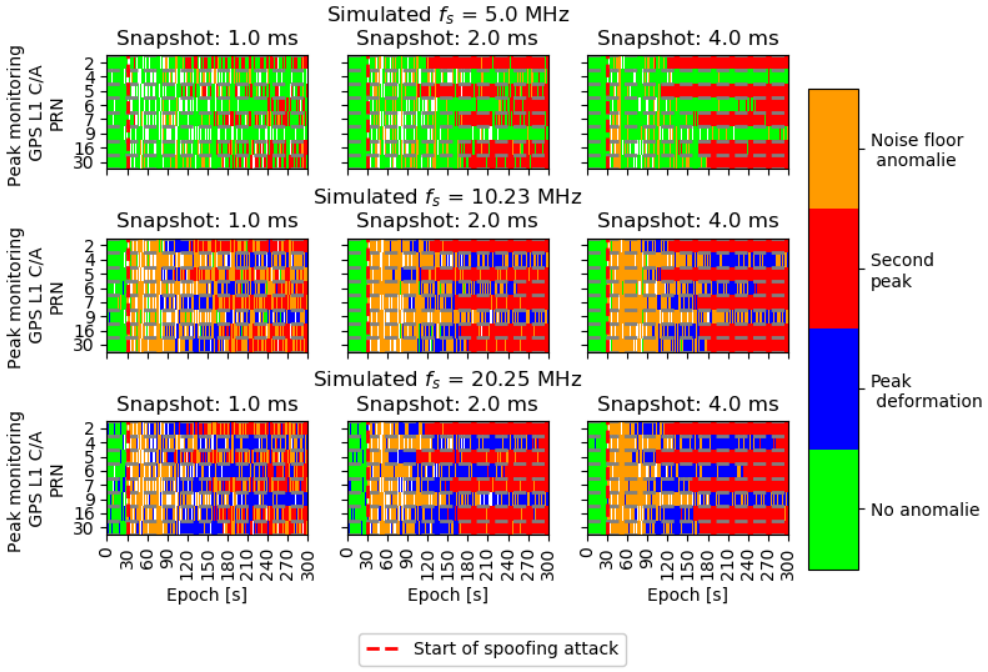

Figure 8.27: Peak monitoring results GPS L1 C/A during spoofing attack for all scenarios

In general, during the spoofing attack the following pattern can be observed: First a noise floor anomaly is detected followed by detected peak deformations which then leads to a complete secondary peak detection. Furthermore, the shorter the snapshot, the more often the secondary peak is not detectable and only a noise floor anomaly is detected instead. This happens due to the fact that the original peak becomes too weak to be found within the increasing noise floor. The longer the snapshot the more peak deformations are found before the separation of the authentic and fake correlation peaks. It can concluded that the sampling frequency is more important for the peak monitoring than the snapshot length.

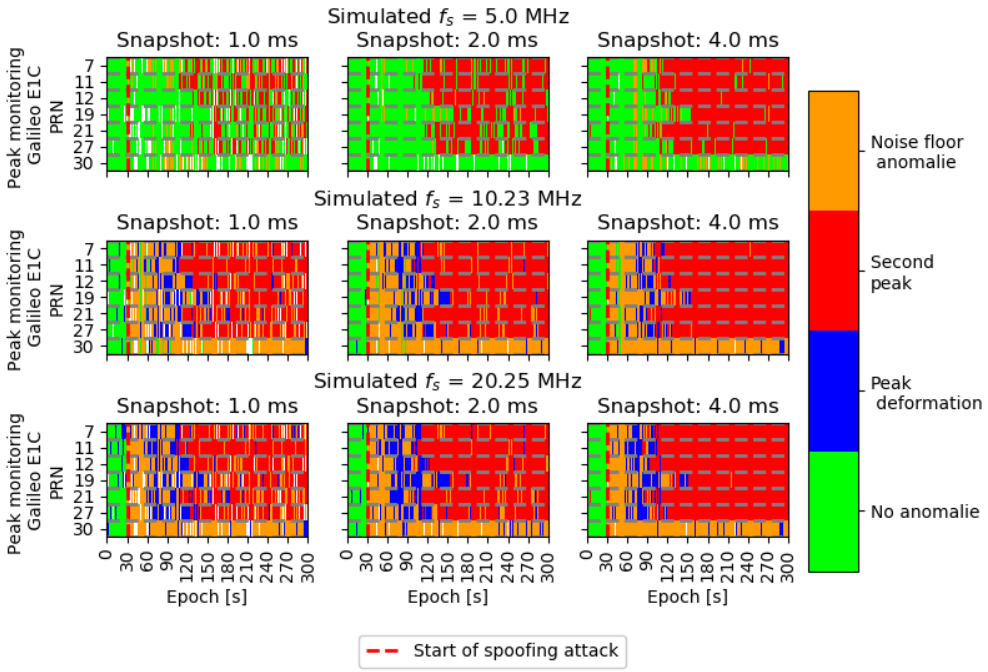

Figure 8.28: Peak monitoring results Galileo E1C during spoofing attack for all scenarios

8.2.3 Validation

To verify the applicability of the peak monitoring and the spectrogram monitoring Figure 8.29 shows the results for the peak monitoring for GPS L1 C/A , Galileo E1C and BeiDou $B1C_p$ for real-world signals. Figure 8.31 shows the corresponding spectrogram monitoring. The peak monitoring detects most of the anomalies for low elevation satellites. This is due to the fact that low elevation satellites are more influenced by noise and obstructions and thus deforming the correlation peaks. On the other hand satellites in the vicinity of the zenith are not influenced by obstruction and thus show few to no deformations as shown by GPS PRN09 and BeiDou PRN20 which have an elevation angle of 75° and 82° respectively. GPS PRN04 also has an elevation angle of 75° but shows, compared to the satellites mentioned before, significant more detected deformations. This indicates obstructions in the north-west direction and the same behaviour can be observed by comparing GPS PRN07 (south), Galileo PRN19 (north-west) and BeiDou PRN37 (south-east-east). These three satellites have the same elevation angle around 60° and Galileo PRN19 in the north-west shows the most detected deformations. This furthermore indicates obstruction in the north-west direction. The reason behind this has been found to be trees blocking the antenna in the north-west direction.

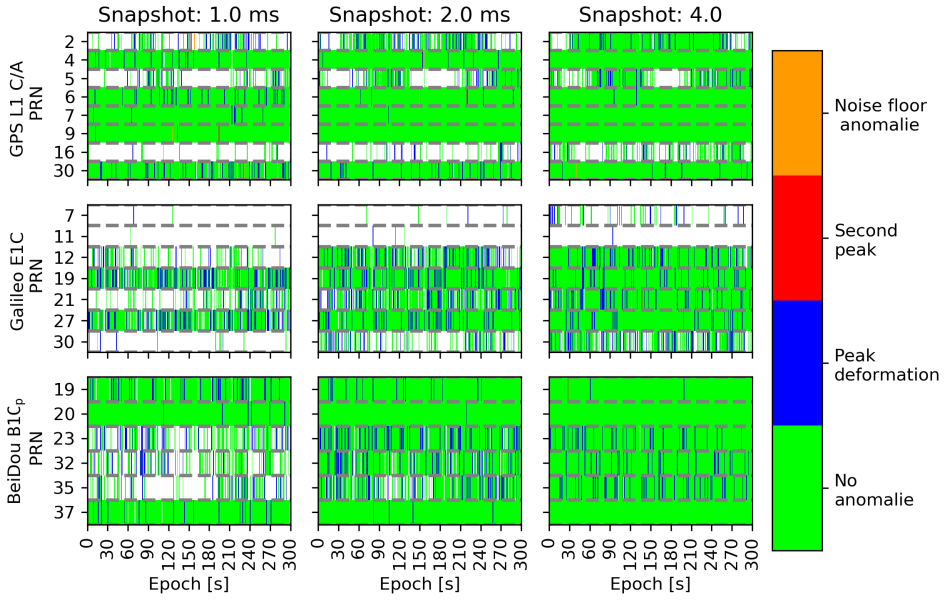

Figure 8.29: Peak monitoring results for GPS L1 C/A, Galileo E1C and BeiDOu B1C$_p$ for the real signal

Furthermore, by increasing the snapshot length, which increases the power of the GNSS signal the amount of detected anomalies decreases significantly.
Figure 8.30 shows the CPNR values for the three signal types using a snapshot length of 2.0 ms. It can be observed that satellites in the north-west direction show more variations within the CPNR compared to other satellites in other directions. In general the peak monitoring detects less deformations for real signals the longer the snapshot is and the less obstructed the arrivings signal are.

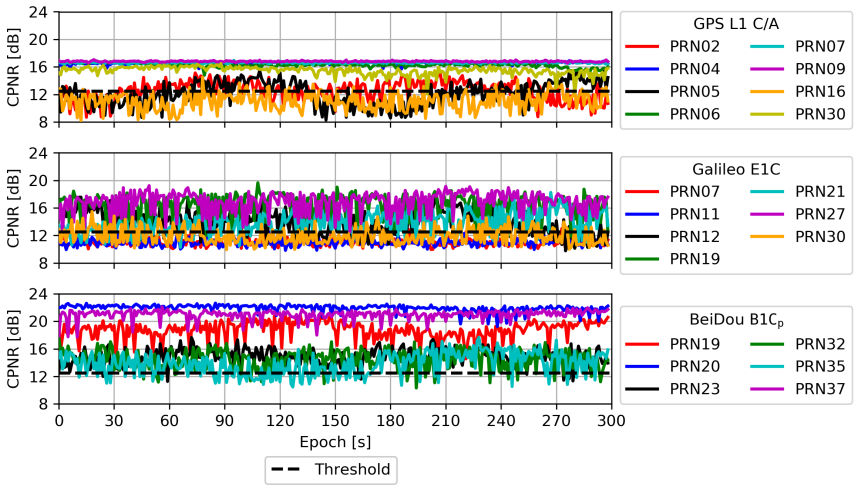

Figure 8.30: CPNR of the real signal for GPS L1 C/A (top), Galileo E1C (middle) and BeiDou B1C$_p$ (bottom) with a snapshot length of 2.0 ms

The spectrogram monitoring on the other hand shows increasing false detections with increasing snapshot length.

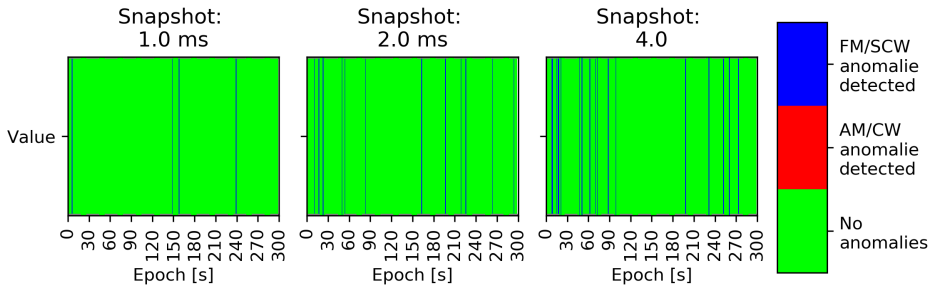

Figure 8.31: Spectrogram monitoring for the real signal

Table 8.11 summarizes the false alert rates for the different snapshot lengths for the spectrogram monitoring. It can be seen that with increasing snapshot length the false alarm rate increases. This means that the spectrogram monitoring should be combined with other monitoring techniques to decrease the false alarm rate, combine detections results over several epochs to validate the detection results or split longer snapshots into several shorter snapshots and combine the spectrogram monitoring results.

Table 8.11: False alert rates for the spectrogram monitoring

Snapshot length [ms]	False alert rate [%]
1.0	1.3
2.0	4.0
4.0	6.0

The spectrogram monitoring is an optimal tool for detecting jammers with GNSS snapshots but requires individual fine tuning of the parameters and final detection decision. A snapshot length of 2.0 ms with more than 5.0 MHz sampling frequency, and using three GNSS seems to be an optimal compromise between position accuracy, position precision, false alarms for the spectrogram monitoring, peak monitoring anomaly detections.

9 Conclusions and outlook

The use of GNSS and the associated permanent availability of position and precise time measurements as well become more and more a matter of course in many areas of everyday life. The information of GNSS satellites has become an important part in many applications and has become indispensable in today's information society. And yet most users are completely unaware of potential GNSS threats and their impacts. Studies show that an outage of GNSS can cause considerable economic and material damage. Successful mitigation techniques require a successful and reliable detection and classification of GNSS threats in advance. Classical approaches perform continuous quality of service monitoring within the GNSS signal bands which can lead to a considerable amount of data required to be processed. A different approach to decrease the data to be processed is the use of GNSS snapshot techniques. Snapshot techniques only process a short part of the continuous signal. The main goal of the thesis was to investigate GNSS snapshot technique and its potential regarding intentional interference monitoring. Within this thesis a python open-loop snapshot SDR has been developed in order to analyse snapshot algorithms in detail. Different positioning techniques unique to snapshot receivers have been implemented and tested. The GNSS quality monitoring focused on techniques not available in common receivers such as the monitoring of the code-Doppler domain or the signal spectrum.
Chapter 1 contains the introduction, state-of-the-art and the motivation for this thesis. Chapter 2 contains an introduction to GNSS, the signal structures, different systems and the basics for satellite-based positioning. Also design considerations for common receivers as well as snapshot receivers are elaborated.
Chapter 3 describes the snapshot positioning algorithms and discusses their advantages and limitations.
Chapter 4 explains common satellite acquisition strategies and provides detailed explanations on how to implement them. Furthermore, this chapter shows different possibilities of refining measurements after the acquisition process for snapshot receivers in detail.
Chapter 5 describes intentional and unintentional interference and elaborates jamming and spoofing in more detail. Furthermore, different types of jammers are discussed by their spectral characteristic and the basic principle of spoofing

is explained. Different spoofing categories, depending on their complexity, are listed. Chapter 6 explains the implemented techniques in this thesis for signal, code-Doppler domain and PVT quality assessment. Especially the peak monitoring and spectrogram monitoring are elaborated in more detail.
Chapter 7 explains the impact of signal properties and provides an overview on how a snapshot SDR can be developed.
Chapter 8 shows the result for time free Doppler and pseudorange positioning as well as quality of service monitoring results in regards to interference and jamming.
This thesis shows how snapshot techniques can be exploited in a SDR with accurate and precise positioning in combination of a quality of service monitoring. The focus was on making the quality of service monitoring as time independent as possible to have the availability of transferring the recorded snapshot to a central processing unit which then estimates the quality of GNSS service. For this transfer the lowest amount of required snapshot length and sampling frequency has been investigated and discussed. One innovation adapted in this thesis is the complete separation of data recording and signal processing with additional quality of service monitoring which provides the possibility of implementing given algorithms as a cloud service.
The time free Doppler positioning for the simulated signals has shown accurate horizontal positioning up to 1 km with precisions varying between 6 and 16 km depending on the snapshot length. The difference between the estimated time and real signal transmission time has shown promising accuracies up to 1 second with 95% showing smaller difference than 50 seconds. The results for the simulated signal as an initial position and time for the time free pseudorange position are more than satisfying. The results of the real-world signals on the other hand show the same accuracy but a worse precision and a lower reliability with shorter snapshot lengths. The worsened precision is a combination of less visible satellites in the real environment due to obstructions and the variation of the clock drift estimation which varies up to $\pm$ 10 Hz with a visible decline in the observed time frame. The less acquirable satellites result in higher DOP values and the varying clock drift results in 1 km error for 1 Hz error in its estimation. Therefore, it is assumed that the combination of these two factors are responsible for the slightly worse precision. Even with these two factors it has been shown that the estimated position and time still satisfy the conditions as an initial positioning for the time free pseudorange positioning technique.
The time free pseudorange positioning for the simulated signal shows promising horizontal accuracies up to 1 m with the worst precision being $\pm$8 m for the lowest sampling frequency and snapshot length. The highest chosen sampling frequency shows precisions varying between 1 and 3 m depending on the snapshot length. With a sample accuracy of $\pm$15 m for this sample frequency it is shown that the additional interpolation of the correlation peak can lead to a significant improvement

of the measurements and resulting positioning solutions. The real-world signals show slightly worse accuracies for shorter snapshot lengths and the same accuracy as the results for the simulated signals with longer snapshot lengths. The precision has worsened due to less visible satellites which results in higher DOP values. With additional atmospheric corrections to increase the accuracy in the height component and the usage of an additional signal from BeiDou to improve the precision the results show a significant improvement.
The later half of the evaluation shows the interference detection for a simulated jamming and spoofing scenario for different sampling frequencies and snapshot lengths. First the jamming scenarios are evaluated and show that the snapshot SDR is more sensitive to AM or CW jammers in comparison to FM or SCW jammers with the same jamming power. All jammers have been correctly detected, significant epochs before the position computation was no longer possible. The spectrogram monitoring has shown to be viable for all sample frequencies and snapshot lengths whereas the peak monitoring required longer snapshots.
For future work the spectrogram monitoring shall be fine tuned for different sample frequencies and include other jamming types such as white noise jammer. Further a final decision and detection metric in combination with other detection results should be implemented and tested.
For spoofing it is shown that a peak monitoring with the crosscorrelation in the code-Doppler domain is a reliable detection strategy. The noise floor, peak deformation and second peak detection have been found to have the same behaviour for all satellites during a spoofing attack. First the noise floor will significantly increase and once the spoofer drags the receiver position away a significant increase of peak deformation can be observed before the fake and authentic peaks are completely separated. Low sampling frequencies could not showcase this behaviour for the used snapshot lengths and only detected the spoofer with the second peak detection.
In the last part of this thesis the peak and spectrogram monitoring were applied to the real signal which is free of intentional interference to validate the behaviour of the monitoring techniques. It is shown that the spectrogram monitoring shows less false alarms with shorter signal snapshots while the peak monitoring shows more deformation detections with shorter snapshots especially for low elevation satellites. The longer the snapshot was, the less deformations have been detected by unobstructed satellites thus verifying that the detected deformations were due to noise or multipath. A compromise of at least 2.0 ms snapshot length and a higher sampling frequencies than 5.0 MHz have been found to be optimal for the monitoring techniques.
Future work will focus on the computational efficiency. The detection decision of the monitoring techniques will be refined and combined with additional detection methods in a detection and decision metric. Furthermore, a classification for

jamming shall be implemented since the jamming parameters are a necessity for mitigating the intentional interference. Additionally field tests with live jammers and spoofers should be exercised to validate the viability of the monitoring techniques. Additionally future work will focus on refinement of the measurements to increase the position and time estimations.

List of Figures

List of Tables

References

Ávila-Rodríguez J.A. (2008): On generalized signal waveforms for satellite navigation. PhD dissertation. University FAF Munich, Germany.

Bartl S. (2014): GNSS interference monitoring – detection and classification of GNSS jammers. Master thesis. Institute of Navigation, Graz University of Technology, Austria.

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

Berglez P. (2017): GNSS-Sicherheit - Chancen und Risiken. In: Österreichische Zeitschrift für Vermessung und Geoinformation, Heft 1/2017: 5–15.

Borio D., Dovis F., Kuusniemi H., Lo Presti L. (2016): Impact and detection of GNSS jammers on consumer grade satellite navigation receivers. In: Proceedings of the IEEE, Vol. 104, No. 6: 1233–1245.

Borre K., Akos D.M., Bertelsen N., Rinder P., Jensen S.H. (2007): A software-defined GPS and Galileo receiver - a single-frequency approach. Birkhäuser, Boston Basel Berlin.

C4ADS (2019): Above us only stars: Exposing GPS spoofing in Russia and Syria. Available at `https://www.c4reports.org/aboveusonlystars`.

Calcagno R., Fazio S., Savasta S., Dovis F. (2010): An interference detection algorithm for COTS GNSS receivers. In: Proceedings of the 5th ESA workshop on satellite navigation technologies and European workshop on GNSS signals and signal processing, NAVITEC 2010, ESTEC. Noordwijk, The Netherlands. December 8–10: 1–8.

China Satellite Navigation Office (2017): BeiDou navigation satellite system signal in space interface control document (OS B1C v.1.0). Available at `http://en.beidou.gov.cn/SYSTEMS/ICD/201806/P020180608519640359959.pdf`.

Collins J. (1999): Assessment and development of a tropospheric delay model for aircraft users of the global positioning system. Master thesis. University of New Brunswick, Fredericton, New Brunswick, Canada.

Dierendonck K. van, Al-Fanek O., Petovello M. (2018): What is snapshot positioning and what advantages does it offer? In: Inside GNSS 13.6: 28–33.

Diggelen F. van (2009): A-GPS: Assisted GPS, GNSS, and SBAS. Artech House, Norwood.

Dovis F. (2015): GNSS interference threats and countermeasures. Artech House, Boston London.

European Global Navigation Satellite Systems Agency (2016): European GNSS (Galileo) open service signal in space interface control document (Issue 1.3). Available at `www.gsc-europa.eu/system/files/galileo_documents/Galileo-OS-SIS-ICD.pdf`.

European Global Navigation Satellite Systems Agency (2017): GNSS market report. Publications Office of the European Union, Luxembourg.

European Global Navigation Satellite Systems Agency (2018): GNSS user technology report 2018. Publications Office of the European Union, Luxembourg.

Fernandez-Hernandez I. (2015): Snapshot and authentication techniques for satellite navigation. PhD thesis. Faculty of Engineering and Science, Aalborg University, Denmark.

Hartnett R., Peterson B., Ottoman G. (1995): GPS receiver structures for the urban canyon. In: Proceedings of the 8th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1995). Palm Springs, California. September 12–15: 1323–1332.

He Z., Zhai C., Zhan X. (2008): Signal quantization effects on acquisition process of GPS receiver: The analysis and simulation. In: Proceedings of the 2008 Congress on Image and Signal Processing. Sanya, Hainan, China. May 27–30: 197–200.

Higham N. (2002): Accuracy and stability of numerical algorithms. Society for Industrial and Applied Mathematics (SIAM), Philadelphia.

Hill J. (2001): The principle of a snapshot navigation solution based on Doppler shift. 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: 3044–3051.

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

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

Hofmann-Wellenhof B., Lichtenegger H., Wasle E. (2008): GNSS – global navigation satellite systems: GPS, GLONASS, Galileo, and more. Springer, Wien New York.

International GNSS Service (2019): GNSS broadcast ephemeris files. Available at `ftp://gssc.esa.int/gnss/data/daily/`.

Isoz O., Akos D., Lindgren T., Sun C.C., Jan S.S. (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.

Jiwon Seo (2017): South Korea Developing an eLoran Network to Protect Ships from Cyber Attacks. Inside GNSS, 1(8): 23–26.

Kaplan E.D., Hegarty C.J. (2006): Understanding GPS: Principles and applications. 2nd edition. Artech House, Boston London.

Leclère J., Botteron C., Farine P.A. (2013): Modified parallel code-phase search for acquisition in presence of sign transition. In: Proceedings of the International Conference on Localizatiion and GNSS (ICL - GNSS). Torino, Italy. June 25–27: 1–6.

Lopez-Salcedo J.A., Parro-Jimenez J.M., Seco-Granados G. (2009): Multipath detection metrics and attenuation analysis using a GPS snapshot receiver in harsh environments. In: Proceedings of the 3rd European Conference on Antennas and Propagation. Berlin, Germany. March 23–27: 3692–3696.

Lucas-Sabola V., Seco-Granados G., López-Salcedo J.A., Garcia-Molina J.A., Massimo C. (2016): Cloud GNSS receivers: New advanced applications made possible. In: Proceedings of the International Conference on Localization and GNSS (ICL-GNSS). Barcelona, Spain. June 28–30: 1–6.

Merwe J. van der, Rügamer A., Fernandez-Dans Goicoechea A., Felber W. (2019): Blind spoofing detection using a multi-antenna snapshot receiver. In: Proceedings of the International Conference on Localization and GNSS (ICL-GNSS). Nuremberg, Germany. June 4–6: 1–7.

Motella B., Presti L.L. (2014): Methods of goodness of fit for GNSS interference detection. IEEE Transactions on Aerospace and Electronic Systems, Vol. 50, Issue 3: 1690–1700.

Niemeier W. (2008): Ausgleichsrechnung: Statistische Auswertemethoden. 2nd edition. Walter de Gruyter, Berlin New York.

O'Connor A. et al. (2019): Economic benefits of the global positioning system (GPS). RTI Report Number 0215471. National Institute of Standards and Technology. Research Triangle Park, NC: RTI International.

OHB Digital Solutions (2018): GNSS multisystem performance simulation environment (GIPSIE®) core manual. Version 4.0.0.

Othieno N. (2012): Combined Doppler time free positioning for low dynamics GNSS receivers. Master thesis. Concordia University Montreal, Quebec, Canada.

Rügamer A., Förster F., Stahl M., Rohmer G. (2012): A flexible and portable multiband GNSS front-end system. In: Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012). Nashville, Tennessee. September 17–21: 2378–2389.

Russian Space Systems (2016): GLONASS ICD CDMA OS in L1 frequency band. Available at `http://russianspacesystems.ru/wp-content/uploads/2016/08/ICD-GLONASS-CDMA-L1.-Edition-1.0-2016.pdf`.

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.

Subirana J.S., Juan-Zornoza J.M., Hernández-Pajares M. (2013): GNSS data processing volume 1: Fundamentals and algorithms. ESA Communications, Leiden, The Netherlands.

Teunissen P., Montenbruck O. (2017): Springer handbook of global navigation satellite systems. Springer, Cham.

Tsui J. (2005): Fundamentals of global positioning system receivers: A software approach, Second Edition. Wiley, New York.

United States Department of Defense (2019): GPS signal in space interface specification (IS-GPS-200K). Available at `www.gps.gov/technical/icwg/IS-GPS-200K.pdf`.

Welch P. (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, Vol. 15, Issue 2: 70–73.

Yang Y., Zhou J., Loffeld O. (2011): Applying a fine Doppler acquisition method on software GPS receiver with field experiment. In: Proceedings of Electronics in Marine (ELMAR), 53rd International Symposium. Zadar, Croatia. September 14–16: 179–182.

Zheng R., Chen M., Ba X., Chen J. (2010): A novel fine code phase determination approach for a bandwidth limited snapshot GPS receiver. In: Proceedings of the Position, Location and Navigation Symposium. Indian Wells, California. May 4–6: 796–805.

Zhi-Feng W., Gai-Yun W., Lei C. (2013): Research on acquisition algorithms of GPS receiver. In: Proceedings of the Third International Conference on Intelligent System Design and Engineering Applications (ISDEA 2013). IEEE Computer Society, Hong Kong. January 16–18: 1148–1151.

Third-party software

Several third-party software components have been used for creating the content of this thesis. This chapter contains a list of the utilized software products together with some license and copyright information.

- **GIPSIE®**
  A simulation environment capable of simulating arbitrary digital intermediate frequency (IF) GNSS signals developed at OHB Digital solutions GmbH. The sampled signal is available as digital file, which can be up-converted to RF and replayed by a proprietary hardware simulator. The software contains a graphical user interface which provides all necessary functionalities to configure arbitrary GNSS simulation scenarios as well as a command line interface for easy automation of simulations. Version 4.0.0 used. More information on `https://www.ohb-digital.at/`

- **TEXstudio**
  An integrated writing environment for creating LaTEX documents. Version 2.12.10 used. Download available at `https://texstudio.org`

- **yEd Graph Editor**
  A powerful desktop application that can be used to quickly and effectively generate high-quality diagrams. Version 3.18.1 used. Download available at `https://yworks.com/products/yed`

- **Python**
  Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. Its high-level built in data structures, combined with dynamic typing and dynamic binding, make it very attractive for rapid application development, as well as for use as a scripting or glue language to connect existing components together. Download available at: `https://www.python.org/`