Mathias Duregger, BSc.

Detection strategies for GNSS spoofing attacks

Master's Thesis

to achieve the university degree of

Master of Science

(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

Institute of Geodesy

Co-supervisor

Dipl.-Ing. Dr.techn. Bakk.techn. Philipp Berglez

Graz, November 2018

Affidavit

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

Date

Signature

Eidesstattliche Erklärung

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

Datum

Unterschrift

Abstract

The use of Global Navigation Satellite Systems (GNSS) and the associated permanent availability of position and precise time measurements as well become more and more a matter of course in many areas of everyday life. The information from GNSS satellites is used in many applications like civil engineering, energy industry, telecommunication, banking, transport, surveying and many others. The number of GNSS devices is constantly increasing and forecasts show there will be one device per human in the next few years.

Due to the increasing number of applications and users, it becomes more important to consider also the weaknesses and risks of a satellite-based position determination. In recent years, GNSS applications have become the target of intentional interference attacks. In general, the impact of interference can lead to a degraded position and timing accuracy or to a total failure of the positioning service, possibly causing both considerable economic and material damage, as studies have shown. The term interference involves unintentional and intentional interference. Unintentional interference can be caused by the electron concentration in the ionosphere, other GNSS signals or out-of-band signals. In addition to unintentional interference, intentional interference of GNSS signals represents a high threat potential. Jamming, spoofing and meaconing are the known intentional interference types.

Spoofing is the broadcast of counterfeit GNSS signals with the intent that a target receiver misinterprets them as authentic ones. The victim might deduce a false position and time solution without disrupting operations. In order to maintain and increase the reliability of GNSS applications, detection and classification of counterfeit signals is the first step to reduce the impacts of such attacks and is helping to develop countermeasures.

This thesis deals with the investigation and classification of GNSS spoofing attacks in relation to their characteristics and threat potential. Within software simulations, state-of-the-art algorithms for detection were analyzed. Furthermore, a new mitigation strategy for stand-alone receivers was developed and implemented. The aim of this newly introduced countermeasure is to provide nominal receiver operations during an ongoing spoofing attack. Moreover, an algorithm for determining the direction of arrival of counterfeit signals was investigated. Real-world data sets of spoofing attacks were recorded during a measurement campaign to examine the capabilities of the implemented algorithms. In the end, the results were analyzed and discussed and conclusions were made together with a given outlook on the future topics in this area.

Zusammenfassung

Die Verwendung von Globalen Satellitennavigationssystemen (GNSS) und die daraus resultierende permanente Verfügbarkeit von präzisen Positions- und Zeitmessungen spielen eine immer wichtigere Rolle in vielen Bereichen unseres Alltags. Informationen von GNSS Satelliten werden beispielsweise in Bereichen des Bauwesens, in der Energieversorgung, der Telekommunikation, im Bank- und Transportwesen, in der Vermessung und vielen weiteren verwendet. Die Anzahl der GNSS-Empfänger steigt dabei stetig, wobei Prognosen voraussagen, dass in den nächsten Jahren im Durchschnitt jeder Mensch einen Empfänger besitzt.

Auf Grund der steigenden Zahl von Anwendungen und Nutzern ist es wichtig, nicht nur die Möglichkeiten, sondern auch die Schwächen und Risiken satellitengestützter Positionierung in Betracht zu ziehen. In den letzten Jahren wurden GNSS Anwendungen zu Zielen von absichtlichen Störangriffen. Allgemein kann der Einfluss von Interferenz zu einer schlechteren Positions- und Zeitgenauigkeit oder gar zum Totalausfall des Services führen, was erhebliche wirtschaftliche und materielle Schäden verursachen könnte, wie Studien zeigen. Der Ausdruck Interferenz umfasst unabsichtliche und absichtliche Interferenz. Unabsichtliche Interferenz kann von Elektronenkonzentrationen in der Ionosphäre, anderen GNSS Signalen oder von Signalen anderer Funkfrequenzsysteme verursacht werden. Im Gegensatz zu unabsichtlicher Interferenz stellen absichtliche Interferenzen ein großes Gefahrenpotential dar. Jamming, Spoofing und Meaconing sind die dabei bekannten Arten.

GNSS Spoofing ist das Aussenden von gefälschten Signalen mit der Absicht, dass ein GNSS Empfänger diese für authentische hält. Das Opfer könnte daraus eine falsche Positions- und Zeitlösung herleiten, ohne dass interne Rechenvorgänge dabei unterbrochen werden. Um die Verlässlichkeit von GNSS Applikationen aufrecht zu erhalten oder gar zu erhöhen, ist die Detektion und Klassifizierung von gefälschten Signalen der erste Schritt um die Einflüsse eines Angriffes zu reduzieren und hilft dabei, Gegenmaßnahmen zu entwickeln.

Die vorliegende Arbeit behandelt die Untersuchung und Klassifizierung von GNSS Spoofingangriffen in Bezug auf deren Eigenschaften und Bedrohungspotential. Mit Hilfe von Softwaresimulationen wurden State-of-the-art Algorithmen zur Detektion analysiert. Des Weiteren wurde eine neue Strategie zur Schadensbegrenzung für autarke Empfänger entwickelt und implementiert. Das Ziel dieser neu eingeführten

Gegenmaßnahme ist es, den Normalbetrieb eines Empfängers während einer Attacke weiterhin zu gewährleisten. Zudem wurde ein Algorithmus zur Bestimmung der Richtung der eintreffenden Signale untersucht. Dafür wurden reale Messdaten von Spoofingangriffen während einer Messkampagne aufgezeichnet, um die Fähigkeiten der implementierten Algorithmen zu untersuchen. Zum Schluss wurden die Ergebnisse analysiert und diskutiert und Schlussfolgerungen wurden zusammen mit einem Ausblick auf zukünftige Themen in diesem Bereich gemacht.

Contents

Acknowlegdements

At this point, my thanks go to all the people who helped me with the creation and elaboration of this thesis. I want to mention my supervisor Univ.-Prof. Dipl.-Ing. Dr.h.c.mult. Dr.techn. Bernhard Hofmann-Wellenhof, who arranged everything for my entry at TeleConsult Austria and who already gave me the opportunity to work in the scientific field of GNSS before.

Further, my appreciation goes to my co-supervisor Dipl.-Ing. Dr.techn. Bakk.techn. Philipp Berglez and to my co-worker Dipl.-Ing. Bakk.techn. Sascha Bartl, who both guided me throughout the whole development and revision of my thesis by giving advice to different topics and providing solutions to problems where otherwise I would have had a tough time with. The many technical conversations enhanced my knowledge of the scientific matter and inspired me to keep working in this field in the future.

Furthermore, I want to mention the rest of co-workers at TeleConsult Austria, who also supported me and helped me to regain my energy by clearing my mind during the coffee breaks.

My thanks go also to my family and friends, who made my graduation at the university successful in the first place. Without them, I would not be in the place where I am today.

Abbreviations

A/D	analog-to-digital
A-S	anti-spoofing
ACF	autocorrelation function
AGC	automatic gain control
ARNS	aeronautical radio navigation services
AWGN	additive white Gaussian noise
BMVIT	Bundesministerium für Verkehr, Innovation und Technologie
BOC	binary offset carrier
BPSK	binary phase-shift keying
C/A	coarse/acquisition
C/N_0	carrier-to-noise power density ratio
CCF	crosscorrelation function
CDMA	code division multiple access
CIA	central intelligence agency
DECODE	detection, countermeasures and demonstration of GNSS spoofing
DLL	delay locked loop
DME	distance measurement equipment
DOA	direction of arrival
DVB-T	digital video broadcasting - terrestrial
ESA	European space agency
FDMA	frequency division multiple access
FFT	fast Fourier transform
FM	frequency modulation
FOC	full operational capability
GIDAS	GNSS interference detection and analysis system
GLONASS	global'naya navigatsionnaya sputnikovaya sistema
GNSS	global navigation satellite system
GPS	global positioning system
GUI	graphical user interface
HAS	high accuracy service
HMI	hazardously misleading information
IMU	inertial measurement unit

ITU	international telecommunication union
JTIDS	joint tactical information distribution system
LFSR	linear feedback shift register
LOS	line-of-sight
LSA	least square adjustment
MBOC	multiplexed binary offset carrier
MEO	medium earth orbit
MIDS	multifunctional information distribution systems
MUSIC	multiple signal classification
NAVIC	navigation with Indian constellation
NLOS	non-line-of-sight
OFB	Oberste Fernmeldebehörde
OS	open service
PLL	phase locked loop
PRN	pseudorandom noise
PRS	public regulated service
PSD	power spectral density
PVT	position, velocity and time
QZSS	quasi-zenith satellite system
RAIM	receiver autonomous integrity monitoring
RF	radio frequency
RINEX	receiver independent exchange format
RMSE	root-mean-square error
RPM	received power monitoring
RSCN	real signal-complex noise
SAR	search and rescue
SBAS	satellite based augmentation system
SDR	software-defined radio
SIS	signal in space
SNR	signal-to-noise ratio
SQM	signal quality monitoring
TACAN	tactical air navigation
TDOA	time difference of arrival
TOW	time of week
UAV	unmanned aerial vehicle
UCA	uniform circular array
ULA	uniform linear array
UWB	ultra-wideband
WGS84	world geodetic system 1984

1 Introduction

Global navigation satellite systems (GNSS) are of great importance in today's economy, society and safety critical applications. Since its begin of development in the second half of the 20th century, this kind of positioning method has established a major role in many aspects of the modern world. It has become the most common and reliable method for position determination, since it offers permanent availability, cheap and easy access and high accuracy.

But like many new technologies with all their advantages and benefits, GNSS also have their flaws which can be exploited to cause damages and create dangerous situations. Although the spread spectrum GNSS signal design allows to mitigate a wide range of interference signals coming from other systems, it does not provide sufficient protection against high-power interferences (Hofmann-Wellenhof et al. 2008).

There are ways to interfere with the signal in their spectrum with small effort. Especially intentional interference, which is divided into jamming, spoofing and meaconing, is the biggest threat to GNSS based applications and the attempt to minimize or suppress the impacts is a current research focus throughout the industry and scientific institutions.

Spoofing is the broadcast of GNSS-like signals with the goal of fooling a target to compute a false position and time solution. In the past, it was a technique that has long been used to deceive a radar's target-ranging operation (Volpe 2001). Nowadays, in the field of GNSS, this technique offers certain advantages for its group of users. For instance, the crew of a fishing boat could intentionally spoof their own receiver in order to stay undetected in restricted waters (Psiaki and Humphreys 2016a).

Another field of application is to take over drones/unmanned air vehicles (UAV). Small drones appointed for private usage as well as military drones can be the target of a spoofing attack. Iranian forces claim to have spoofed a highly classified drone from the US central intelligence agency (CIA) in December 2011 to successfully land in their territory (Psiaki and Humphreys 2016a).

While in the past, spoofing remained difficult and could only be conducted by small groups of experts, the technique advances continuously making it attractive for a wider range of potential users. These days, by using software-defined radios

(SDR), it is no big hurdle for determined adversaries to adapt the technique for their own shadow activities.
Therefore, the development of countermeasures not only for spoofing, but for all kinds of intentional interference is mandatory. This thesis deals with the investigation on existing anti-spoofing strategies as well as the development of a new approach for detection and mitigation during receiver operations. Furthermore, the direction of arrival of counterfeit signals shall be computed, to provide the user with information about the location of its adversary. The aim is to minimize the impacts in order to keep the integrity of satellite positioning as high as possible in fields of applications where safety of lives or economic processes are of great concern.

1.1 Thesis outline

Chapter 1 states the motivation for this thesis by giving a short overview of the topic together with state-of-the-art work that has been done in the field of detection and mitigation. Furthermore, contributions to two related research projects, named DECODE and GIDAS, are presented. In Chapter 2, the basic principle of GNSS is explained together with the structure of GNSS signals.
Chapter 3 deals with the architecture of a software-defined radio (SDR), while Chapter 4 introduces the types of interference on GNSS signals together with their characteristics.
It is important to understand how GNSS spoofing works and what effects it can have on a receiver. Chapter 5 describes the impacts of spoofing on a SDR and gives an overview of publicly known incidents where spoofing has been used. In addition to that, countermeasures in Chapter 6 are introduced and explained, offering algorithms that are implementable in SDRs, to increase the protection level.
In Chapter 7 the implementation of a newly developed detection and mitigation strategy by the author is demonstrated, while Chapter 8 deals with the validation and discussion of the results based on software simulations as well as real-world scenarios.
At the end of the thesis, Chapter 9 concludes the obtained results and further lists future possibilities.

1.2 State-of-the-art

According to Dovis (2015), the development of spoofing detection and mitigation techniques is an active research topic in the GNSS community and the number of strategies for countermeasures is increasing steadily.

The most established way for protection is signal authentication. This method dates back to the first days of GNSS, considering the ability of the US military to encrypt some of its GPS signals, if needed, by activating the so called anti-spoofing (A-S) module. The European system Galileo also offers this kind of protection as part of its public regulated signals as well as some of its other services such as the open service (OS). However, most GNSS signals remain unencrypted and freely accessible to the user, making it prone for spoofing attacks.

Satellite-like signals emitted from a spoofer gain higher power compared to authentic ones. Due to this property, received power monitoring (RPM) serves as a first indicator for counterfeit signals as Dehghanian et al. (2012) has demonstrated.

Another way for detecting ongoing attacks is to monitor the position in static applications or to observe unusual behavior in the timing solution of a receiver. A further strategy is correlation peak monitoring, where several peaks resulting from one satellite indicate a possible attack (Psiaki and Humphreys 2016a).

By combining the two countermeasures of correlation peak monitoring and received power observations, the probability of false detection alarms can be decreased. If a spoofer tries to drag away its victim during satellite tracking, the resulting correlation peak experiences distortions and its symmetric shape vanishes. Wesson et al. (2013) has presented an approach where these two features are combined.

Assuming a static spoofer is located at a certain position, the principle of spatial correlation is another way of mitigating incoming signals. The fake GNSS signals emitted from a single spoofing source show a similar spatial signature making a distinction from authentic ones possible, as Broumandan et al. (2012) has demonstrated.

One of the safest options is not to rely on just one system, but combining several systems together in a multi-sensor environment as Dovis (2015) states. With complementary positioning systems, mutual quality control can be conducted. For example, absolute positioning service offered by GNSS can be extended by relative positions provided by an inertial measurement unit (IMU). This provides the opportunity to evade on a complementary system in case false measurements are produced due to any kind of malfunction or interference.

The usage of antenna arrays has several benefits compared to single antenna set ups. One such advantage is the possibility to estimate the direction of arrival (DOA), which has applications throughout many fields of signal processing. For the case, an attack by an interferer has been detected and successfully mitigated, the incident angles of the counterfeit signals can be processed, providing information about the direction of the spoofer relative to the user's position. Mathews and Zoltowski (1994) has described the topic of DOA determination applied for several types of antenna arrays.

1.3 Related work

This thesis contributes to two related research projects from TeleConsult Austria GmbH.
The first project, "GNSS Interference Detection and Analysis System" (GIDAS), is a scalable and flexible real time GNSS interference detection and analysis system which can be used as a stand-alone monitoring station for interference detection and which can be upgraded to a more complex network of stand-alone stations which allows interference detection and interferer localization. The system is independent from any other system and is designed to be easily deployed. The monitoring station receives all-in-view GNSS civil signals and automatically detects and classifies intentional interference sources within the dedicated GNSS signal band in real time (TeleConsult Austria GmbH 2018b). The GIDAS project has been supported and co-financed by the European space agency (ESA), contract number 4000122636/17/NL/MM.
The second project, "Detection, Countermeasures and Demonstration of GNSS Spoofing" (DECODE) had the goal to develop algorithms for detecting and mitigating spoofing attacks. In a first step, state-of-the-art algorithms for detection of spoofers were investigated. The existing algorithms were implemented in a software-based GNSS receiver and their reliability was tested by using simulations as well as the evaluation of the exact impacts of spoofers on receivers. The implementation was done by using a GNSS SDR, which offers the necessary flexibility for implementing diverse algorithms. After first tests, the most promising algorithms were developed further as well as, based on the newly gained knowledge, new detection methods were investigated, implemented and tested (TeleConsult Austria GmbH 2018b). The project DECODE was managed by the Austrian Research Promotion Agency (FFG) and received funding from the Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program line ASAP. The project was led by TeleConsult Austria, together with its partners Brimatech GmbH and the Austrian Ministry of Defence and was successfully completed in 2018.

2 Global Navigation Satellite Systems

Global navigation satellite systems have taken a major role in many aspects of our everyday lives. The development of the first systems started nearly 40 years ago. After the United States and the Soviet Union have set up first satellite-based navigation systems during the cold war, the development of the US NAVSTAR Global Positioning System (GPS) and the Russian Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS) system followed by using the gained knowledge (Hofmann-Wellenhof et al. 2008).

The basic principle of the two systems is the same: the travel time of an emitted radio signal is measured after its way through space and atmosphere, delivering range measurements. In combination with known satellite coordinates, the determination of a receiver's position in three-dimensional space can be acquired by trilateration. Nowadays, many additional GNSS have been set up by several countries for geopolitical reasons. The European Galileo and the Chinese BeiDou system are ambitious projects on taking the wheel in global satellite navigation. At the point of writing this thesis, these two systems are almost at full operational capability (FOC). All systems use the same concept and are continuously enhanced. While in the past, civil GNSS signals were broadcast only on one frequency, these days at least three carrier frequencies are provided by every system. This results in higher numbers of available observations as well as improved positioning accuracy. In addition to global systems, several countries also started to develop regional satellite systems, which are designed to cover the interests of their respective countries, like the Japanese Quasi-Zenith Satellite System (QZSS) or the Navigation with Indian Constellation System (NAVIC). Furthermore, several Satellite Based Augmentation Systems (SBAS) exist. These systems mostly consist of geostationary satellites and are designed to aid current GNSS and regional systems in terms of accuracy, integrity and availability.

In the following, the basic positioning principle is explained together with the signal structure of GPS and Galileo navigation satellites.

2.1 Basics

The basic concept of GNSS is the measurement of signal run time. The satellite in space broadcasts signals with a certain structure (see Chapter 2.2) that are measured by receivers on earth or in space. The signal run time

$$\Delta t_r^s = t_r - t^s \tag{2.1}$$

is the difference between the observation time t_r at the receiver and the transmitting time t^s at the satellite. By multiplying the time difference with the speed of light, the range ϱ between receiver and satellite can be computed, as shown in Figure 2.1. Since the satellite position $\boldsymbol{\varrho}^s$ is known, the unknown receiver coordinates $\boldsymbol{\varrho}_r$ can be computed.

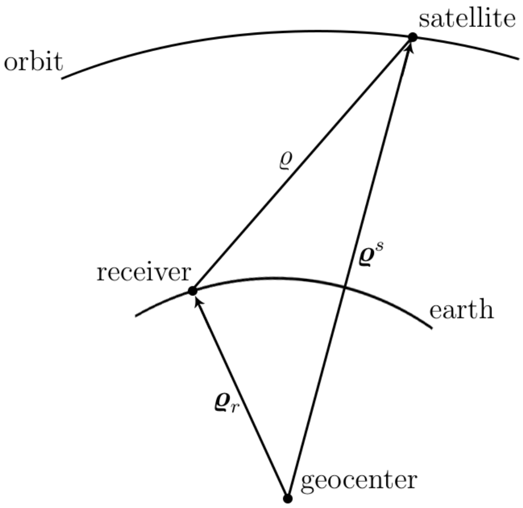


Figure 2.1: Principle of satellite-based positioning (c.f. Hofmann-Wellenhof et al. 2008)

Due to the fact, that satellite and receiver clocks are not synchronized, the run time of the signal is erroneous. Additional external influences, like the troposphere, ionosphere or multipath (reflection of signals from objects) also contribute to errors in the measured range. This biased range is denoted as pseudorange R_r^s. The simplified model for the pseudorange reads

$$R_r^s(t) = \varrho_r^s(t) + c\Delta\delta_r^s(t) + \epsilon(t), \tag{2.2}$$

with

$$\varrho_r^s(t) = \sqrt{(X^s(t) - X_r)^2 + (Y^s(t) - Y_r)^2 + (Z^s(t) - Z_r)^2}, \tag{2.3}$$

where $\varrho_r^s(t)$ is the true range and $\Delta\delta_r^s(t) = \delta_r(t) - \delta^s(t)$ is the combined clock error, with s and r being the super- and subscript for the satellite and receiver respectively, c being the speed of light in vacuum and X, Y and Z being the Cartesian coordinates of the satellite and receiver. Here, a static receiver is assumed, implying its coordinates are not a function of time. The term $\epsilon(t)$ in Equation 2.2 contains the before mentioned additional errors as well as Gaussian noise. For further explanations see Hofmann-Wellenhof et al. (2001).
The determination of the receiver position is acquired through a least square adjustment (LSA). The mathematical relation between observation, known satellite position and unknown receiver position is not free of errors. The goal is to obtain a solution, where the square sum of the residuals of the observations is minimal. To achieve this, the function is approximated by a Taylor series in a first step. The approximation of an arbitrary function $f(x)$ reads

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(x_0)}{n!} x^n, \tag{2.4}$$

where $f^{(n)}$ is the n-th derivative. The term x_0 implies the evaluation point of the function. In case of a LSA in GNSS positioning, the linearization of Equation 2.2 is aborted after the first term, as Hofmann-Wellenhof et al. (2001) states. The function is derived after every unknown parameter. This results in four derivations: three for the receiver coordinates and one for the receiver clock bias. The satellite clock error is modeled using a polynomial of second order and thus known. With this information, the design matrix $\mathbf{A}$ can be established as

$$\mathbf{A} = \begin{bmatrix} -\frac{X^{s_1}(t)-X_r}{\varrho_r^{s_1}} & -\frac{Y^{s_1}(t)-Y_r}{\varrho_r^{s_1}} & -\frac{Z^{s_1}(t)-Z_r}{\varrho_r^{s_1}} & c \\ -\frac{X^{s_2}(t)-X_r}{\varrho_r^{s_2}} & -\frac{Y^{s_2}(t)-Y_r}{\varrho_r^{s_2}} & -\frac{Z^{s_2}(t)-Z_r}{\varrho_r^{s_2}} & c \\ \vdots & \vdots & \vdots & \vdots \\ -\frac{X^{s_n}(t)-X_r}{\varrho_r^{s_n}} & -\frac{Y^{s_n}(t)-Y_r}{\varrho_r^{s_n}} & -\frac{Z^{s_n}(t)-Z_r}{\varrho_r^{s_n}} & c \end{bmatrix}. \tag{2.5}$$

Every row of this design matrix is associated with a certain satellite n. Due to the characteristic of Equation 2.2 being non-linear, approximated values for the receiver coordinates and clock bias are needed. To obtain a solution in real time, at least four observations are necessary.

Equation 2.6 shows the computation of the increments $\Delta\hat{\mathbf{x}}$ of the unknown parameters $\hat{\mathbf{x}}$.

$$\begin{aligned} &\Delta\hat{\mathbf{x}} = (\mathbf{A}^T\mathbf{P}\mathbf{A})^{-1}\mathbf{A}^T\mathbf{P}\Delta\mathbf{l} \\ &\hat{\mathbf{x}} = \mathbf{x_0} + \Delta\hat{\mathbf{x}} \end{aligned} \tag{2.6}$$

In this equation, the matrix $\mathbf{P}$ stands for the observation weight matrix. It can be used to reduce the impact of certain observations (e.g. signals from satellites with low elevation) on the solution. The vector $\Delta\mathbf{l}$ contains the reduced observations. It is the difference between measured observations and the ones that are computed with the help of the assumed values of the receiver. In the end, the increments are added to the known approximate values. This process is repeated several times, until there are no significant changes in the increments anymore.
For determining the precision of the computed coordinates and receiver clock bias, the variance of the weight unit is needed, which can be computed as

$$\hat{\sigma}^2 = \frac{\hat{\mathbf{e}}^T\mathbf{P}\hat{\mathbf{e}}}{n-m}, \tag{2.7}$$

where n is the number of given observations and m the amount of unknown parameters. The residuals $\hat{\mathbf{e}}$ are computed following

$$\hat{\mathbf{e}} = \mathbf{A}\Delta\hat{\mathbf{x}} - \Delta\mathbf{l}. \tag{2.8}$$

With this information the variance/covariance matrix is obtained by applying

$$\hat{\mathbf{\Sigma}}(\hat{\mathbf{x}}) = \hat{\sigma}^2(\mathbf{A}^T\mathbf{P}\mathbf{A})^{-1}. \tag{2.9}$$

Note that the constraint $\hat{\mathbf{e}}^T\hat{\mathbf{e}} = \min$ of a least square adjustment is still fulfilled.
A further observation type is the fractional part of the carrier phase from the emitted signal. The mathematical relation reads

$$\lambda\phi_r^s(t) = \varrho_r^s(t) + c\Delta\delta_r^s(t) + \lambda N_r^s. \tag{2.10}$$

Only the fractional part $\phi_r^s(t)$ is measured by the receiver while the full cycles of the incoming signal are unknown. This number is denoted as the integer ambiguity N_r^s. Note that both sides of equation 2.10 are multiplied with the nominal wavelength λ of the signal to obtain a dimension of a range. Computing a LSA by applying

Equation 2.10, a further parameter for the integer ambiguity needs to be estimated. The third measurable quantity is the Doppler frequency. The Doppler effect states the change in frequency of an emitted signal and occurs due to relative motion between satellite and receiver. The Doppler scaled to a range-rate can be derived from the time derivative of the phase measurement (Hofmann-Wellenhof et al. 2001) and reads

$$D_r^s(t) = \lambda\dot{\phi}_r^s(t) = \dot{\varrho}_r^s(t) + c\Delta\dot{\delta}_r^s(t). \tag{2.11}$$

Note that the integer ambiguity has vanished, since it is not dependent on time. Another way to describe the Doppler frequency shift is through the radial (line-of-sight) velocity $\dot{\varrho}_r^s$ between the satellite and the receiver and can be written as follows

$$\Delta f_r^s = f_r - f^s = -\frac{1}{c}\,\dot{\varrho}_r^s\, f^s. \tag{2.12}$$

The Doppler shift Δf_r^s is the difference between the emitted and received frequency. In Figure 2.2, the radial velocity $\dot{\varrho}_r^s$ equals the length of the projected relative velocity vector into the line-of-sight between satellite and receiver. The radial velocity is obtained by the scalar product

$$\dot{\varrho}_r^s = (\dot{\boldsymbol{\varrho}}^s - \dot{\boldsymbol{\varrho}}_r)\frac{\boldsymbol{\varrho}^s - \boldsymbol{\varrho}_r}{||\boldsymbol{\varrho}^s - \boldsymbol{\varrho}_r||}. \tag{2.13}$$

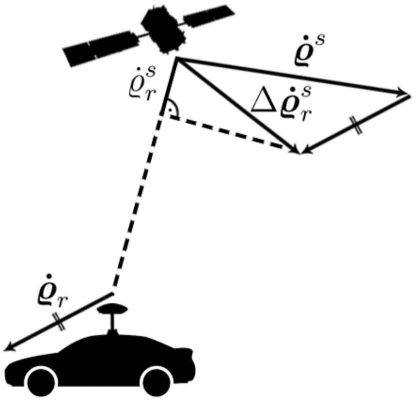

$\dot{\boldsymbol{\varrho}}^s$
$\dot{\varrho}_r^s$
$\Delta\dot{\boldsymbol{\varrho}}_r^s$
$\dot{\boldsymbol{\varrho}}_r$

Figure 2.2: Relation between relative and radial velocity

2.2 Signal structure of GPS and Galileo

A GNSS signal consists in general of three components: The first is the carrier wave, representing a sinusoidal wave. It is created by an on-board oscillator (atomic clock) at a certain frequency in the L-band (for further details see Hofmann-Wellenhof et al. 2003). This is due to the reason, that only waves with high frequencies are suitable for traveling through the atmosphere of the earth.
The second component, is the ranging code, also called pseudorandom noise (PRN) code. This code is not only used for determining the run time of the incoming signal at the receiver, but also to distinguish between individual satellites. This principle is called code division multiple access (CDMA). Another way of identification is to distinguish signals by their carrier frequencies. This so called frequency division multiple access (FDMA) is used i.a. by GLONASS satellites. Kaplan and Hegarty (2006) gives a detailed description on these techniques. The PRN code is basically a series of code chips. This pseudorandom sequence either states 0 or 1 (equaling -1 or 1 at signal level).
The third component is the data message. It is a sequence of bits containing information of the satellite ephemeris, satellite clock error, ionospheric parameters and almanac data.
These three signals are combined by the principle of phase modulation as shown in Figure 2.3.

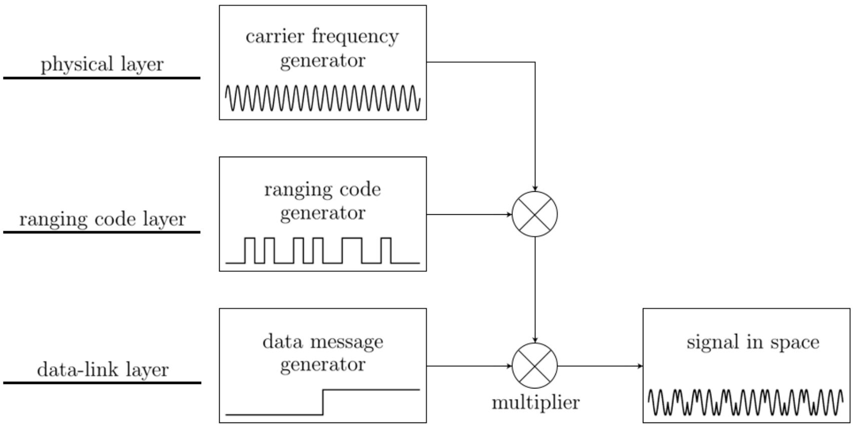


Figure 2.3: GNSS signal generation (c.f. Hofmann-Wellenhof et al. 2008)

The PRN code signals are either generated by a linear feedback shift register (LFSR) or stored as memory codes on board. In order to determine the run time of the signal, the incoming PRN code is correlated with a locally generated replica.

For that reason, the ranging codes between all satellites must maintain a low crosscorrelation to make an exact distinction possible. This condition is fulfilled by the so called Gold codes and is further explained in Borre et al. (2007). Equation 2.14 shows the multiplexing of a signal for the in-phase I and quadrature-phase Q and reads

$$s(t) = \sqrt{2P_I}D_I(t)C_I(t)\cos(2\pi ft) - \sqrt{2P_Q}D_Q(t)C_Q(t)\sin(2\pi ft). \tag{2.14}$$

Here, P denotes the power of the signal and D and C are the data and ranging code respectively, while f denotes the carrier frequency.

BPSK vs. BOC modulation

There exist many modulation techniques in signal processing. Here, two of them are introduced which are used by several GNSS, including GPS and Galileo. The first method that modulates the two codes on the carrier wave is the scheme of binary phase-shift keying (BPSK). Basically, whenever a chip jump occurs in either the PRN code or the data message, the phase of the carrier wave is shifted by 180°. The second one is the scheme of binary offset carrier (BOC) modulation. The main difference to BPSK is the use of an additional binary code sequence, called sub-carrier. Figure 2.4 shows the BOC-modulation principle.

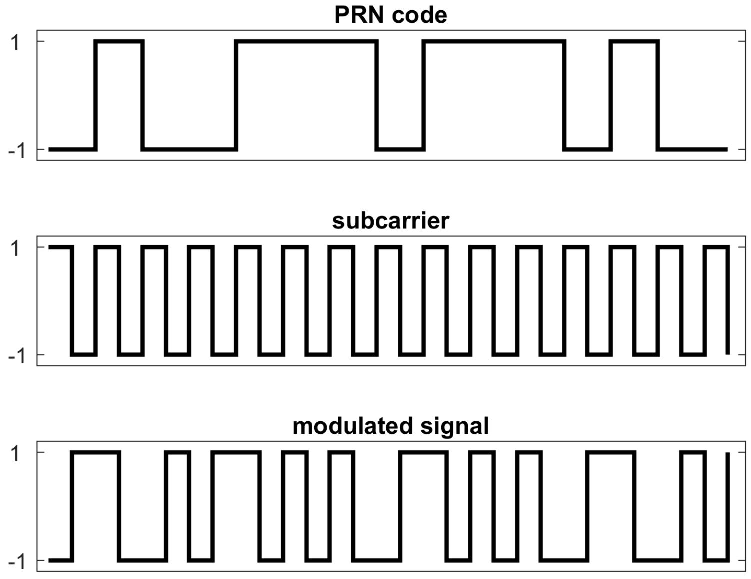


Figure 2.4: Binary offset carrier modulation

This modulation depends on the relation between the used sub-carrier frequency f_S and the chipping rate f_C of the PRN code. Therefore, the BOC modulation can be written as a function of these two quantities BOC(f_S,f_C).
The difference of the signal modulations has certain reasons. The power spectral density is a quantity to describe the distribution of a signals' power with respect to its frequency. It can be computed by the Fourier transform of the autocorrelation function of the signal

$$S(f) = \int_{-\infty}^{\infty} R(\tau) e^{-2\pi f \tau} d\tau, \tag{2.15}$$

as Borre et al. (2007) states. Figure 2.5 shows the power spectral density of a BPSK and a BOC modulated signal respectively.

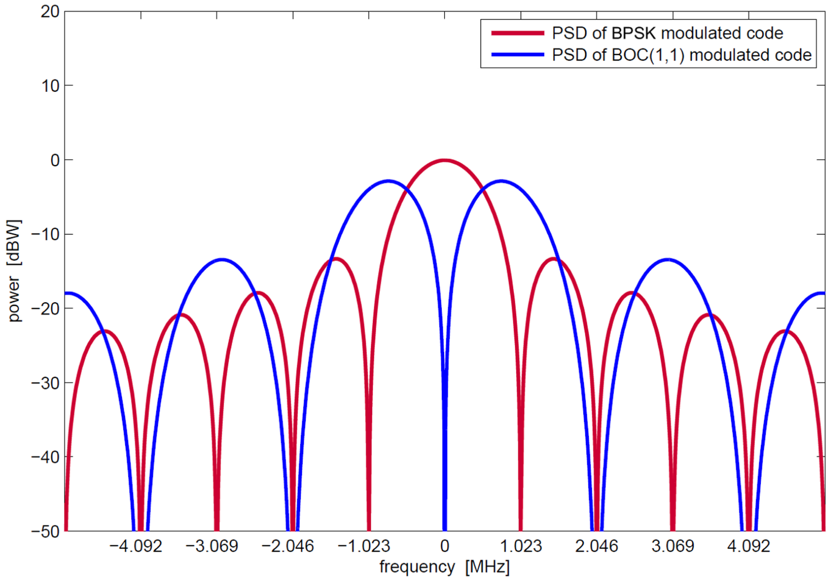


Figure 2.5: Comparison of PSD for BPSK (red) and BOC (blue) modulation

As can be seen, the main lobe of the BPSK signal is exactly at the center frequency, while the BOC signal has zero power there. Instead, two main side lobes on the left and right side of the center are present with lower power. In exchange, the remaining side lobes show higher powers compared to the BPSK signal.
Due to this property, BOC signals show a better resistance against interference. Here, an interferer needs to cover a larger bandwidth to make sure, all side lobes of

the signal are suppressed. Consider an interferer broadcasting on a small bandwidth around the center frequency of a certain signal. While a big part of the main lobe of a BPSK signal would be drown in noise, a BOC modulated signal would stay unaffected for most parts.
Moreover, several BOC signals can be modulated to one signal, denoted as multiplexed binary offset carrier (MBOC). For example, a BOC(1,1) signal and a BOC(6,1) signal can be combined to a MBOC(6,1,1/11) one. The power spectral density of such a signal reads

$$|S(f)|^2 = \frac{10}{11}|S_{\text{BOC}(1,1)}|^2 + \frac{1}{11}|S_{\text{BOC}(6,1)}|^2. \tag{2.16}$$

The signal power is 10/11 for BOC(1,1) and 1/11 for BOC(6,1). With this method, additional power can be achieved in the side lobes of the PSD, making it easier for receivers to track the signal. More details on this topic are given in Berglez (2013).

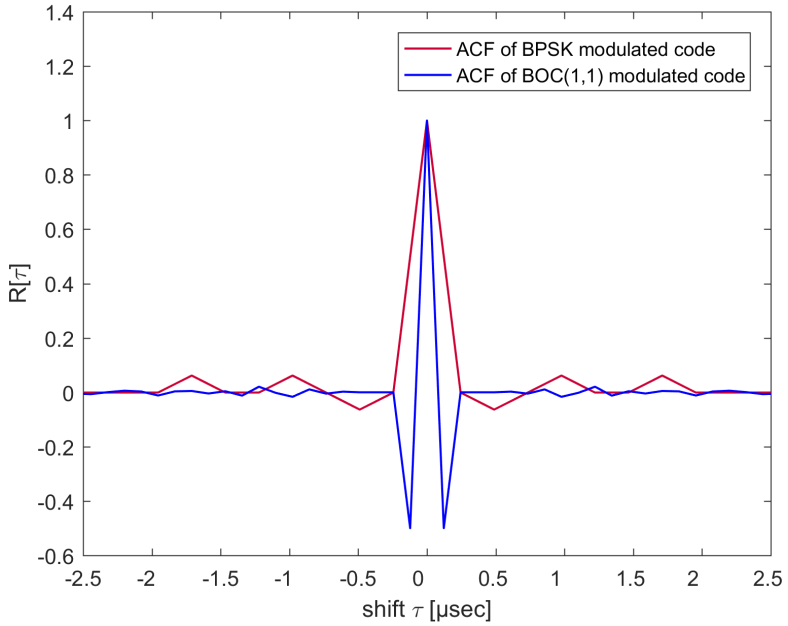


Figure 2.6: Comparison of ACF for BPSK (red) and BOC (blue) modulation

Figure 2.6 shows the autocorrelation function (ACF) of a BPSK and a BOC(1,1) modulated signal respectively. The crosscorrelation function (CCF) is used to compute the time shift between two identical signals. By this principle, the signal run time from satellite to receiver can be determined. The CCF of two discrete signals reads

$$R[\tau] = \frac{1}{N} \sum_{n=0}^{N-1} C_1[n] C_2[n+\tau], \tag{2.17}$$

where τ denotes the shift. If C_1 equals C_2, the CCF turns to the ACF.
Every GNSS has its own definition of carrier frequencies and signals. In the following, the main characteristics of the US GPS and European Galileo system are briefly explained.

Global Positioning System GPS has a nominal constellation of 24 satellites placed in six equally spaced orbital planes. The satellites are operating in a medium earth orbit (MEO) with an average altitude of 20200 km and an orbit inclination of 55° relative to the equator. The orbits are nearly circular and the period of a satellite is about 11 h and 58 min (Subirana et al. 2013). The system broadcasts signals on three carrier frequencies. These three carrier waves are derived from a fundamental frequency f_0 being 10.23 MHz, as shown in Table 2.1.

Table 2.1: GPS carrier frequencies (United States Department of Defense 2018)

Link	Factor	Frequency [MHz]	Wavelength [cm]
L1	$154 \cdot f_0$	1575.42	19.0
L2	$120 \cdot f_0$	1227.60	24.4
L5	$115 \cdot f_0$	1176.45	25.5

Based on these three carrier frequencies, several signals are modulated and broadcast by the satellites. While in the past, only one civil signal was broadcast by GPS satellites, many additional signals have been introduced during modernization, opening new fields of applications. Table 2.2 gives an overview of the current civil signals.

Table 2.2: Civil GPS signals (Berglez 2013)

Link	PRN code	PRN code length [chip]	Modulation	Bandwidth [MHz]	Data rate [bps]
L1	C/A	1023	BPSK(1)	2.046	50
L1	$L1C_D$	10230	MBOC(6,1,1/11)	4.092	50
L1	$L1C_P$	$10230 \cdot 1800$	MBOC(6,1,1/11)	4.092	–
L2	L2CM	10230	BPSK(1)	2.046	25
L2	L2CL	767250	BPSK(1)	2.046	–
L5	L5I	102300	BPSK(10)	20.46	50
L5	L5Q	102300	BPSK(10)	20.46	–

In addition, secured signals named P(Y) code and the new military M code are also broadcast but due to encryption only usable by military receivers.

Galileo The Galileo system has a nominal constellation of 27 satellites in three equally spaced orbital planes with an inclination of 56°. The satellites also operate in MEOs with an average altitude of 23222 km. This results in a period of 14 h and 4 min. Compared to GPS, Galileo broadcasts on five different carrier frequencies with some of them being the same as in GPS, as shown in Table 2.3.

Table 2.3: Galileo carrier frequencies (European Global Navigation Satellite Systems Agency 2016)

Link	Factor	Frequency [MHz]	Wavelength [cm]
E1	$154 \cdot f_0$	1575.420	19.0
E6	$125 \cdot f_0$	1278.750	23.4
E5	$116.5 \cdot f_0$	1191.795	25.2
E5a	$115 \cdot f_0$	1176.450	25.5
E5b	$118 \cdot f_0$	1207.140	24.8

The Galileo system provides a variety of signals that are offered in four services. Every signal is designed to fulfill the requirements of a specific service. Referring to Subirana et al. (2013), the services are shortly introduced in the following:
The Open Service (OS) is free of charge to users worldwide. Up to three separate signal components are offered within it. The service is designed for combining Galileo with other GNSS measurements.
The Public Regulated Service (PRS) is intended for security authorities (e.g. police, military) and thus under governmental control. Through encryption and enhanced signal modulation, robustness against jamming and spoofing is provided. When Galileo has reached FOC, two PRS navigation signals with encrypted ranging codes

and data messages will be available.

The High Accuracy Service (HAS) is a service that, compared to the OS, provides an additional navigation signal and added-value services in a different frequency band. The signal can be encrypted in order to control the access to the Galileo HAS (European Global Navigation Satellite Systems Agency 2018a).

The Search and Rescue (SAR) service will be part of the international COSPAS-SARSAT system. A distress signal will be relayed to the rescue coordination center and Galileo will inform users that their emergency call has been detected (Subirana et al. 2013).

Table 2.4: Galileo OS signals (European Global Navigation Satellite Systems Agency 2016)

Link	PRN code	Channel	Primary code length [chip]	Secondary code length [chip]	Modulation
E1	E1B	data	4092	1	MBOC(6,1,1/11)
E1	E1C	pilot	4092	25	MBOC(6,1,1/11)
E5	E5a-I	data	4092	20	BPSK(10)
E5	E5a-Q	pilot	4092	100	BPSK(10)
E5	E5b-I	data	4092	4	BPSK(10)
E5	E5b-Q	pilot	4092	100	BPSK(10)

Table 2.4 provides an overview of the freely accessible signals used by the Open Service of Galileo. The signals are divided into a data and a pilot channel. The pilot channel is missing the data message. The aim is to achieve a longer integration time, helping receivers to acquire signals with low signal-to-noise ratios (SNR) in obstructed environments like cities, forests, indoor etc.

3 Design of a software-defined radio

A software-defined (SDR) radio is a rapidly evolving technology that is getting enormous recognition and is generating widespread interest in the receiver industry (Borre et al. 2007). The main advantage compared to a conventional hardware-based receiver is the ability to change the radio's properties without modifying or replacing hardware components. Furthermore, fast bug-fixing and software updates can be made, resulting in substantial economic benefits. Nonetheless, hardware parts like the analog front-end and the antenna, are still needed.

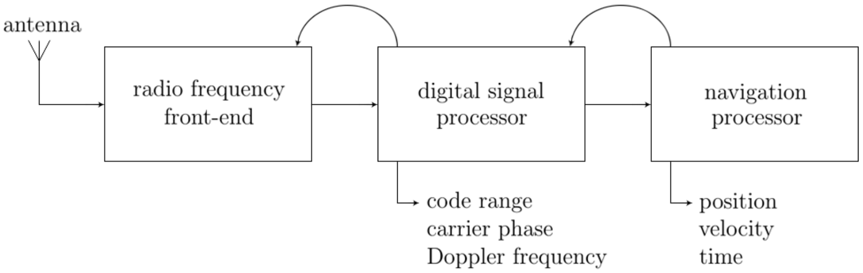


Figure 3.1: Functional blocks of a SDR (c.f. Hofmann-Wellenhof et al. 2008)

Figure 3.1 shows the basic functional blocks of a SDR: the radio frequency (RF) front-end converts the incoming high frequency signal from the antenna to a lower intermediate frequency (IF) and converts the analog signal to digital by means of an analog-to-digital (A/D) converter. Inside the digital signal processor, every visible satellite in the signal is acquired and tracked. After passing the tracking results to the navigation processor, pseudoranges and phase measurements are computed as well as satellite positions and other parameters which are extracted from the navigation message. Finally, a position, velocity and time (PVT) solution is computed and provided to the user.

3.1 Radio frequency front-end

The receiver's antenna is connected to a RF front-end, where the incoming data is either recorded or streamed. Though the high frequency of satellite signals is good for propagating through space and atmosphere, it is not suitable for data processing. Thus, the incoming signals are converted to a lower frequency (often denoted as IF) by mixing them with the frequency of the local oscillator of the receiver. The down-converted signal is held at a constant power level by using an automatic gain control (AGC). In the last stage, the analog data are converted to digital by sampling it with a suited frequency f_S. This sampling frequency has to be at least twice as high as the bandwidth B of the incoming signal in order to fully reconstruct it without any loss of information ($f_S \geq 2B$). This principle is known as Nyquist (Shannon) theorem (Kaplan and Hegarty 2006).

3.2 Digital signal processor

The digital signal processor is the core element of a SDR, where the signals from all visible satellites are extracted and their offset in the Doppler and code domain is determined. By using these quantities, the basic observables like pseudoranges and phase measurements can be computed. In a first step, the receiver needs to know, which satellite signals are present in order to track them. This is realized in the acquisition stage.
Coarse values for the Doppler frequency shift and code phase are obtained through the following principle: for every nominal satellite a local sequence of the PRN code is generated on a certain carrier frequency. The local carrier frequency varies from the incoming one due to relative motion between satellite and receiver. This Doppler deviation can go up to ±10 kHz in the worst case (Borre et al. 2007). The receiver generates local PRN codes on predefined frequency intervals. One such interval is often denoted as frequency bin Δf. Furthermore, the PRN code sequence is generated for every chip delay $\Delta\tau$, denoted as code-offset. Figure 3.2 illustrates the described search space for code-offset and Doppler.
There are several ways to perform the acquisition. Three different techniques are listed below:

- Serial search acquisition
- Parallel frequency space search acquisition
- Parallel code phase search acquisition

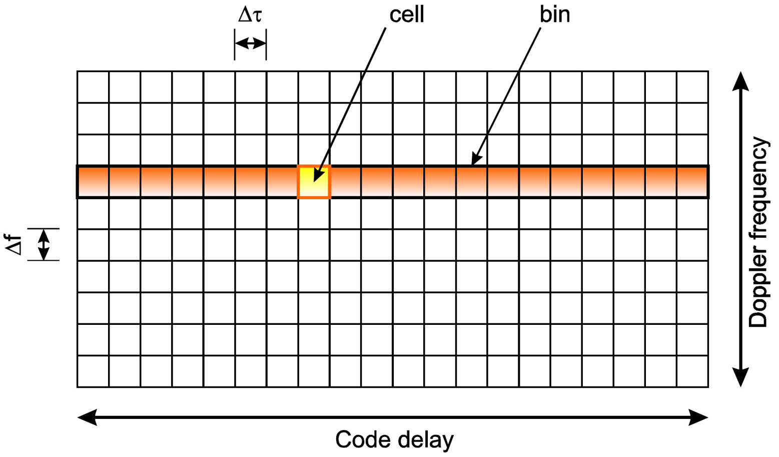


Figure 3.2: Acquisition search space for Doppler and code phase (Berglez 2013)

While the parallel code phase search acquisition is the most complex of these three, it is also the fastest. For further information on this topic refer to Kaplan and Hegarty (2006).

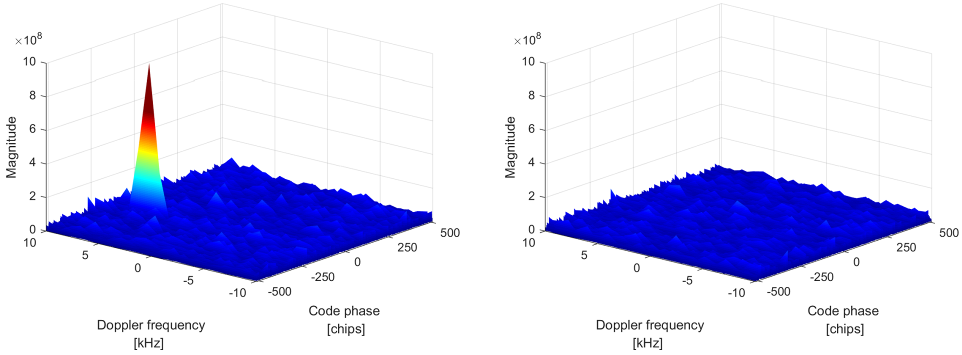


Figure 3.3: Correlation peak search (left: PRN11 found, right: PRN20 not found)

Figure 3.3 shows the result during an acquisition search. The PRN code of every satellite is known and a local replica is generated for testing, if a certain satellite is present in the incoming IF signal. On the left side of the figure, PRN11 is found which results in a clear peak coming out from the noise floor. In the right part of Figure 3.3, PRN20 is searched but not found.

To make sure, a satellite is present, the found peak is compared to a given threshold. There are several ways for defining a proper threshold, for instance conducting a hypothesis test. More information on peak detection can be found in Pany (2010). The acquired coarse values for code-offset and Doppler shift of the found satellites

are handed over to the tracking stage.
The goal for a tracking loop is to keep track of the code- and carrier phase of the acquired satellite signal and refine these values. The output is an aligned replica of the code. Typically, three local codes, the early, prompt and late code, are generated and correlated with the incoming IF signal, aided by the coarse values from the acquisition in a first step.

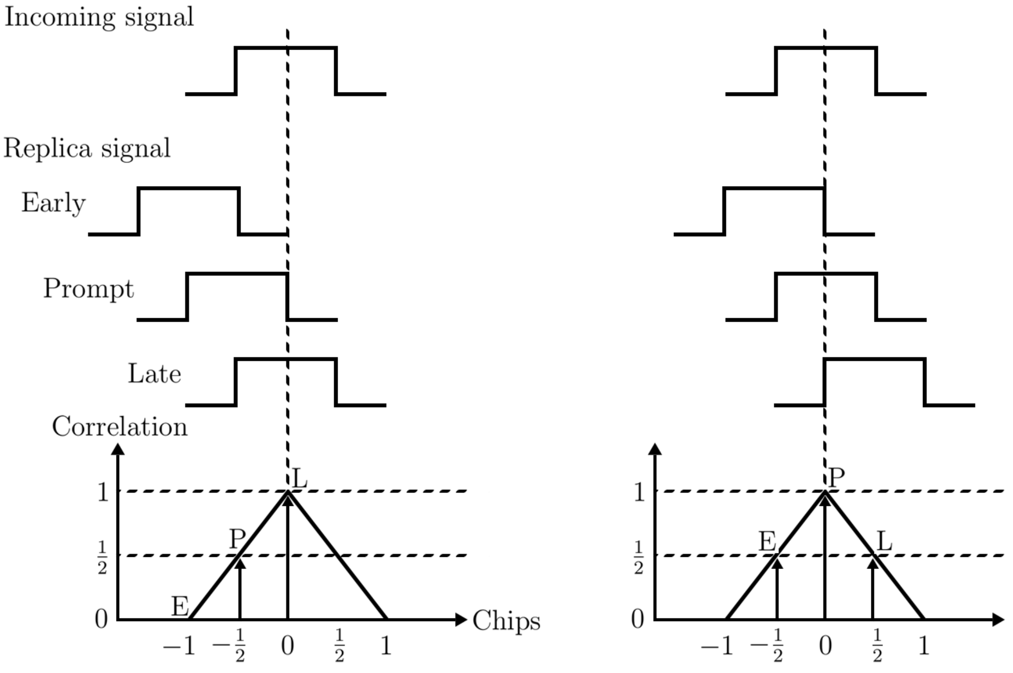


Figure 3.4: Early, prompt and late code correlation principle (c.f. Borre et al. 2007)

The left side of Figure 3.4 shows the late code having the highest correlation. This means, the code phase must be decreased – resulting to the right side of the figure, where the prompt code is well aligned with the incoming signal. The tracking of the PRN code happens inside the so called delay locked loop (DLL). This loop is combined with a phase lock loop (PLL). The PLL is responsible for tracking the carrier wave, by aligning the local carrier with the baseband signal.

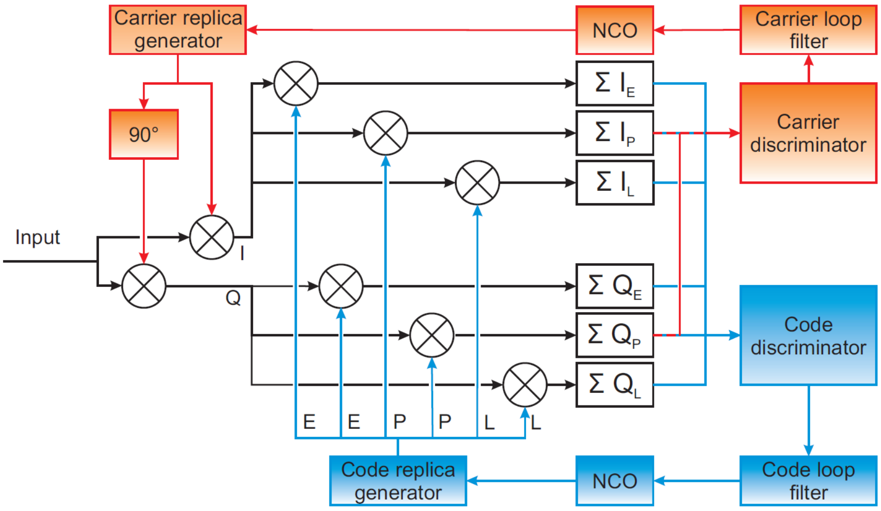


Figure 3.5: Tracking loop block diagram with six correlator outputs (Berglez 2013)

An illustration of such an implementation is shown in Figure 3.5. Here, the DLL and PLL have six correlator arms. For both, the in-phase and quadrature-phase, three local codes are generated and correlated. The PLL and the DLL work hand in hand by using the correlator outputs to compute a feedback for the local code generators. This feedback is generated through discriminator functions. These functions can either be computed from all correlator outputs or just from a subset. More information can be found in Borre et al. 2007.

3.3 Navigation processor

The navigation processor is responsible for decoding the information that is held in the data message and delivering a PVT to the user. After demodulating the PRN code and carrier from the incoming signal, the data message is left. Since the output of the tracking loops are code and carrier phases, it is necessary to convert them into pseudorange or phase measurements, which can be used within the receiver position computation (Kaplan and Hegarty 2006).

The navigation message is divided into frames in case of GPS. In order to find the beginning of the message, the incoming data is correlated with a known synchronization pattern, also called preamble. This preamble is located at the beginning of each frame. After determining the start of a frame, the necessary information for PVT computation (i.e. transmission time, satellite ephemeris, ionospheric parameters, almanac data) can be extracted from the bit sequence.

The time of signal transmission is encoded at the beginning of every subframe and denoted as time of week (TOW). Together with the reception time acquired by the receiver clock, the pseudorange $R_r^s(t)$ can be computed via the time difference Δt_r^s. For more information refer to Berglez (2013).

The navigation solution is separated in several steps: At first, the code and phase measurements are filtered, in case cycle slips occurred or in case code and carrier smoothing is applied. Moreover, the measurements are corrected for tropospherical and ionospherical influences as well as for satellite clock errors. Using the broadcast ephemeris, position and velocity of the visible satellites are computed. In the end, receiver position, velocity and time is calculated in sense of a LSA or Kalman filter together with their statistical parameters (e.g. standard deviation of position). Furthermore, a receiver autonomous integrity monitoring (RAIM) can be conducted, to ensure erroneous measurements are detected and excluded from the PVT.

4 Interference

It is well known that several phenomena may affect the quality of the pseudorange estimation that is based on the measurement of the propagation time of a signal from a satellite to the user (Dovis 2015). Electromagnetic waves that interact with GNSS signals interfere with them in a sense, where they contribute to distortions and erroneous propagation time. Following Volpe (2001), RF interference can be distinguished in two groups: unintentional and intentional interference.

The first group consists of interference based on natural, inter- and intra, out-of-band and in-band interference. While these kinds of interactions with the signals are not uncommon, their effects are well known and can be modeled in a way to keep the impacts as small as possible.

The second group is called intentional interference. This kind of threat to RF signals is gaining more attention and is especially in the GNSS sector a current research topic. The impacts on receiver operations are still investigated and a proper protection against this menace is demanded for the near future. If neglected, the consequences can be tremendous and damages can be caused in most fields of application where GNSS are of relevance.

4.1 Unintentional interference

Unintentional interference on GNSS signals can occur due to several reasons. The most common causes are listed in the following.

Natural sources of interference Natural interference refers to interactions caused by solar storms and the earth's atmosphere, divided into the ionospheric and the tropospheric layer. Inside the ionosphere, the ionization of electrons (due to solar storms) causes erroneous signal travel times. On single frequency measurements, parameter models can be used to compensate the impacts. Since the ionosphere is a dispersive medium (the propagation of the RF wave is dependent on its frequency), dual frequency measurements can be exploited to eliminate the impacts (Hofmann-Wellenhof et al. 2008). Moreover, electron density irregularities, also called scintillations, appear during high solar and geomagnetic activities, which can lead to further fluctuations in amplitude and phase of the signal (Dovis 2015). Inside the troposphere, the weather interferes with the signal. The influences on the propagation time can also be corrected by introducing parameter models depending on temperature, air pressure and water vapor.

Multipath Multipath is basically the reception of reflected signals in contrary to direct line-of-sight (LOS) signals. Multipath measurements can be considered as replicas of the true signals which are caused by objects like buildings, that are located near the receiver. Due to this fact, multipath can be considered as self-interference to a certain extent (Dovis 2015).

Intra- and intersystem interference Intrasystem interference is considered as interaction of signals broadcast by satellites of the same system, e.g. Galileo. Theoretically, the PRN codes are designed to be orthogonal to each other in order to be distinguished by the receiver. But this mentioned orthogonality is not perfect, yielding residual powers causing interactions between the signals.
Intersystem interference on the other hand is denoted as the interaction of signals between different systems (e.g. GPS and Galileo). The reason for that is due to the shared carrier frequencies, where signal power from one system can disrupt operations from the other. These two types of interference are considered during the signal design phase and are strictly regulated by the international telecommunication union (ITU).

External interference Harmonics out-of-band signals can generate interference in GNSS bands. Common sources are e.g. analog TV channels, DVB-T signals, very high frequency and satellite communications, FM harmonics, cell phones, pagers, airport navigation/communications systems and many more. Equation 4.1 shows the definition of out-of-band interference (f_{int}) in relation to the GNSS bandwidth (B_{GNSS}) and frequencies (f_{GNSS}).

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

In-band interference is caused by systems that operate inside the GNSS bands. Examples are military systems and aeronautical radio navigation services (ARNS) like distance measurement equipments (DME), tactical air navigation (TACAN) or joint tactical information distribution systems (JTIDS) and multifunctional information distribution systems (MIDS). For more details on ARNS see Hofmann-Wellenhof et al. (2003). Furthermore, ultra-wideband (UWB) signals also cause in-band interactions.

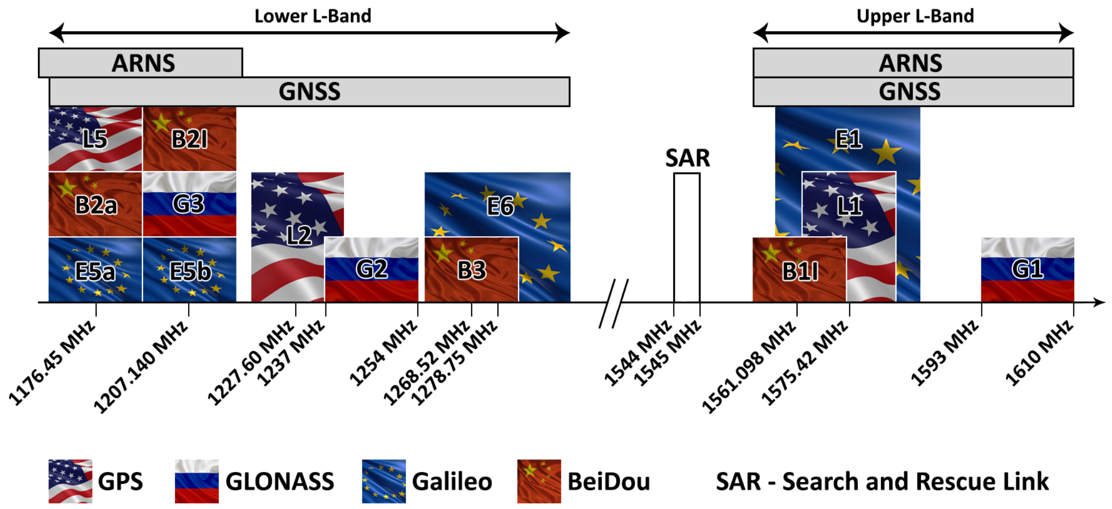


Figure 4.1: Overview on GNSS and ARNS frequency bands (c.f. Subirana et al. 2013)

Figure 4.1 shows the frequency bands of GPS, GLONASS, Galileo and BeiDou as well as the bands of ARNS. Many of the before mentioned ARNS broadcast in the lower bottom and the upper L-band like GNSS does, causing in-band interference. Equation 4.2 shows the definition of in-band interference in relation to the GNSS bandwidth frequencies.

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

Wasle et al. (2009) has dealt with the topic of analyzing the impacts of radio navigation satellite system signal modulation on interference.

4.2 Intentional interference

Intentional interference on the other side, is transmitted by adversaries to interfere with GNSS signals on purpose. The goal is to disrupt or change nominal receiver operations to benefit the needs of the attacker. The three kinds of this interference type are described subsequently.

Jamming The goal of jamming is to mask GNSS signal bands with noise in order to deny navigation or timing service. During a jamming attack, the receiver loses tracking of the satellites and a re-acquisition is not possible. Jammers broadcast high-powered RF noise on certain frequencies and bandwidths to interfere with nearby receivers. These devices can be classified by their power source (e.g. chargeable battery, external power supply), the number of covered GNSS frequencies or the type of jamming signal itself (Dovis 2015).

A jamming signal can, for example, be a continuous wave, with constant frequency and amplitude, a swept continuous wave, where the frequency has the shape of a saw-tooth function or an amplitude/frequency modulated signal.

Figure 4.2 shows the carrier-to-noise power density ratio (C/N_0) of some GPS satellites during several jamming events. The C/N_0 is a quantity, that represents the incoming power of a satellite signal with respect to the noise floor. During a jamming event, the power drops rapidly, coming near the value of 30 dBHz or even below. If this limit is undercut, the receiver loses lock of the tracked signals and nominal operations are disrupted. In Figure 4.2, four frequency modulated jamming events are present with each having a duration of 10 seconds. The C/N_0 depends on the jammer power and its characteristics. During the first event, the threshold of 30 dBHz is undercut by three satellites.

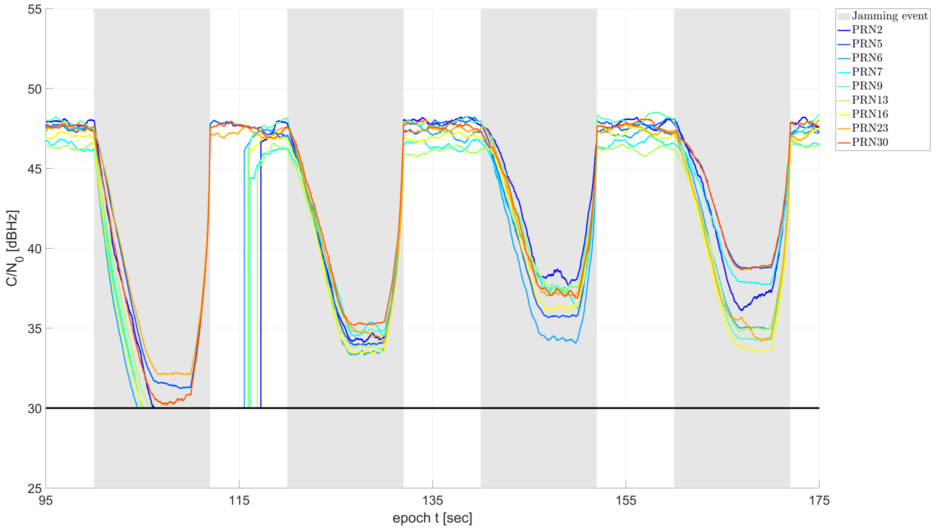


Figure 4.2: C/N_0 during jamming event

Many research materials on jamming detection and mitigation exist. Filtering the incoming interference signal by means of adaptive notch filtering has proven to be one effective countermeasure. Moreover, the principle of pulse blanking, where unwanted parts of the signal are cut out, has also proven to be a reliable strategy in the field of unintentional interference (e.g. ARNS interfering with GNSS). More information on this topic can be found in Bartl (2014).

Meaconing Meaconing is the broadcasting of delayed authentic signals. A meaconer first receives incoming signals and later rebroadcasts them with a certain time delay. The number of counterfeit signals in general equals the satellites in view of the victim with having stronger power and a constant delay. Meaconing can be seen as environmental multipath since it has the same effects on the receiver.

Spoofing Spoofing is the transmission of fake GNSS signals. The intention is to take over a chosen victim so it produces a false PVT without disrupting operations on receiver's site. What makes this kind of interference more dangerous compared to others is the fact that a properly conducted spoofing attack could stay undetected. Damages could be tremendous considering e.g. safety critical or economic applications. The countermeasures are currently a scientific research topic. Many counter strategies like signal encryption, the use of multi-sensor environments, or algorithms on stand-alone receivers are investigated. The following chapter describes the impacts of spoofing on GNSS receivers followed by state-of-the-art defense strategies in Chapter 6.

5 Spoofing

Spoofing is the transmission of GNSS-like signals with the aim to produce a false position and timing solution at a victim receiver. In general, during an ongoing attack, nominal receiver operations continue, without showing any indications to the victim. This is what makes spoofing so dangerous. Damages could be tremendous if safety critical applications (e.g. air navigation, public emergency services), or economic processes (e.g. timing at stock market, container shipment) are the targets.

Considering that the US GPS already offers the encrypted military P(Y) code as an anti-spoofing (A-S) strategy for several years, this threat is not new. What has changed is the fact, that nowadays with advanced technologies in digital signal processing, it has never been as easy to perform an attack as before. Another reason is the steadily growing number of GNSS devices that are in most cases unprotected against any kind of interference (e.g. smartphones).

Though only a handful of spoofing attacks are publicly known and have been proven to be real, more of these are likely to occur in the near future.

5.1 Principle of spoofing

For performing a spoofing attack, a GNSS signal simulator (in some cases in combination with a receiver) is used to generate and broadcast counterfeit signals of authentic satellites that are in the victim's view. In a first step, the spoofer tries to alter Doppler and code-offset of its broadcast signals to align with the ones from the visible authentic satellites. After a successful alignment, the correlation peak of the fake signal overlays with the authentic one. At this point, the power of the spoofing signals is still kept low, showing no indications to the victim. Now the attacker slowly increases the power of its signals until the victim receiver's tracking loop locks onto them. Once the receiver has been taken over, the spoofer can drag away its correlation peak by altering the broadcast signal properties again, yielding to a false PVT computation at victim receiver's site.

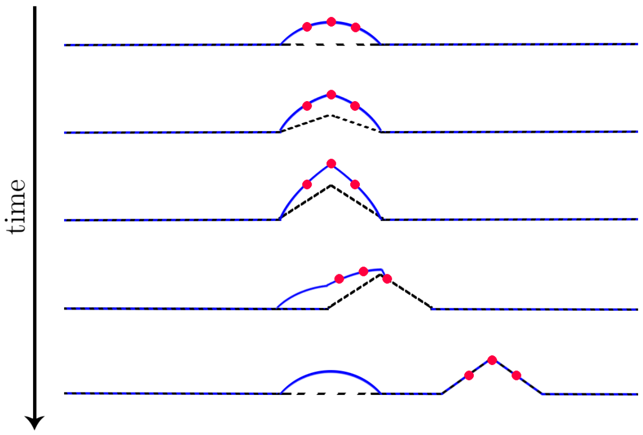


Figure 5.1: Spoofing attack viewed from victim receiver's correlation level (c.f. Psiaki and Humphreys 2016a)

Figure 5.1 shows the correlation function of a tracking channel of a victim receiver during a spoofing attack sequence. The black dash-dotted curve is the spoofing signal and the blue is the sum of authentic and spoofed satellite. If the receiver has been taken over, the drag-off begins and the black curve is drawn away from the authentic correlation peak. The three red dots indicate the early, prompt and late correlators within the tracking loop.
The incoming signal at the RF front-end during a spoofing attack is basically the sum of all authentic and spoofed satellites. Equation 5.1 shows the received complex signal s at receiver site for an epoch t:

$$\begin{aligned} s(t) = & \sum_{i=1}^{L} \alpha_i^A(t) A_i^A(\mathbf{p}(t), t) D^A(t - \Delta\tau_i^A) C_i(t - \Delta\tau_i^A) e^{j(2\pi f_i^A t + \theta_i^A)} \\ & + \sum_{i=1}^{L} \alpha_i^S(t) A_i^S(\mathbf{p}(t), t) D^S(t - \Delta\tau_i^S) C_i(t - \Delta\tau_i^S) e^{j(2\pi f_i^S t + \theta_i^S)} \\ & + \omega(t), \end{aligned} \tag{5.1}$$

where the index i denotes a specific PRN and L the total number of visible satellites. The superscripts A and S represent the authentic and spoofing signals. The term α is a random complex scintillation applied to the signal and the term A stands for the channel gain, which is a function of the antenna phase center position $\mathbf{p}$ and time t. D and C are the data message and PRN ranging code respectively and functions of time and code-offset $\Delta\tau$. f denotes the Doppler frequency and θ the

initial phase of the signal. The term ω is considered as additive white Gaussian noise (AWGN). If the spoofing attack is properly conducted, the victim should receive for every visible satellite a signal that is emitted by the spoofer.
The number of reported spoofing incidents is steadily grown. In the following, some incidents are presented together with a classification of attacks. Furthermore, the impacts on the digital signal and navigation processor are described to give the reader an overview of the technical aspects that happen inside a receiver during an attack.

5.2 Known incidents

As already mentioned in the introduction, the spoofing threat is no fiction but has rather become reality in recent years. Several incidents have been reported in the past. Although in most cases the use of spoofing was just an assumption, it is plausible that only this kind of interference could lead to such results in those situations.

Spoofed ships in the Black Sea Between June 22nd–24th, 2017 several ships in the Black Sea reported that their indicated location jumped from waters to an airport near the coast. At first, several speculations where made on what exactly had happened until the idea of spoofing came to authorities minds. Though these are just speculations, as no one ever took the claim for the spoofing, it is assumed that the Russian federation is responsible for it, since the vessels navigated near their territory. But what reason could the Russian Federation have to let the vessels think they are at an airport? One explanation could be the security of their borders. Since airports are restricted areas for drones to fly over, many UAVs have build in mechanisms to stop operations as soon as they are over or near one. This results in either landing them immediately or fly in opposite direction. So the main target could not been the vessels but rather drones that could fly near the border to spy over territory. For more information refer to Jones (2017).

US drone capture by Iranian forces Iranian forces claim to have taken over a US drone, operated by the CIA, and successfully landed it in their territory in December 2011 (Shepard et al. 2012). Though the US government never officially confirmed the incident, it could be possible that Iranian forces have the knowledge and equipment to perform such an attack. The attackers let the drone think it flew back safely to it's Afghan military home base while in reality they landed the drone inside their borders. Though the drone has taken some damages during landing, this example shows that even the US military was not prepared for dealing with such kind of assault on their equipment.

US vessel capture by Iranian forces In January 2016, Iranian forces seem to have faked GPS signals again with the purpose to send two US Navy patrol boats off course into their waters. Ten US soldiers were captured and pictures of the captives went viral. Although the soldiers were released shortly after the capture, the search for explanations on what has happened has started. The US Department of Defense made some implausible assumptions resulting in a final statement saying the soldiers on both vessels simply ”misnavigated” on their trip between Kuwait and Bahrain. Taken into account that the highly trained troopers were more than 50 miles off their planned course, this seems unrealistic. While it will never be fully clear what exactly happened, a spoofing attack is one plausible explanation to this curios incident (Psiaki and Humphreys 2016b).

Spoofing a yacht at university of Texas Due to these allegedly incidents, the US Department of Homeland Security started to investigate in the spoofing topic soon after. A team of scientists at university of Texas lead by Humphreys and Psiaki began an experiment, where a spoofing attack on a yacht was conducted with the goal to fool the vessel's computers by indicating a false course. An automatic course correction by the systems entailed that the real trajectory now diverged from the nominal one. The experiment, which was set in international waters, became well known throughout the media and showed for the first time that the threat was plain reality. The second goal of the team of scientists during this attempt was to implement and test a detection scheme for spoofing attacks, with it being also successful. Further information on this topic can be found on Psiaki and Humphreys (2016b).

5.3 Classification of spoofing attacks

According to literature, spoofing attacks are classified into categories. Dovis (2015) categorizes them into simplistic, intermediate and sophisticated attacks, as illustrated in Figure 5.2. Another division is the distinction between synchronized (where the spoofed signals are synchronized with the authentic ones) and unsynchronized attacks. Although each classification can be diverged in further branches, the three main categories are introduced in the following.

Simplistic attack For this kind of attack, a GNSS signal simulator is needed in combination with a signal emitting RF front-end. Due to unknown information of

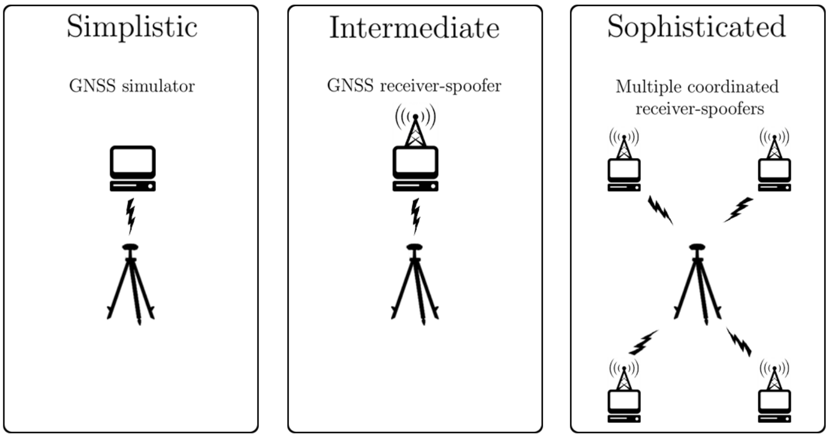


Figure 5.2: Categories of spoofing attacks (c.f. Dovis 2015)

authentic satellite ephemeris in real time, the simulated signals are inconsistent. Moreover, without having precise time information, a time-synchronous broadcast of the fake signals is impossible. Many receivers may stay unaffected and a detection is more likely. Another disadvantage are residual modulation effects like additional Doppler frequencies or code-offsets. On the contrary, little equipment is needed yielding to low costs and complexity.

Intermediate attack Compared to a simplistic attack, this one is more complex due to the fact that a GNSS receiver is used in combination with a signal simulator. By using the obtained satellite ephemeris and time information from the received signals, the synchronization of the locally generated counterfeit codes and carriers is aided, gaining more plausible spoofing signals. For a successful attack, the coarse position of the victim receiver must be known to adjust the alignment of the counterfeit signals with respect to the real ones. This can be achieved by varying the code-offset by additional lengths over a time period. If the alignment is accurate enough, no additional Doppler effects and code-offsets can be seen in the received signals. One drawback of an intermediate attack is, that only a single source is used as spoofer making it prone for detection strategies based on spatial correlation.

Sophisticated attack The third category is an extension of an intermediate attack by using several spatially distributed GNSS simulators. In an optimal scenario, every counterfeit signal is transmitted by an individual spoofer. This implicates that the fake signals' spatial signature in terms of correlator outputs, Doppler values, etc. is not correlated anymore if all spoofers are distributed evenly in space, imitating real satellites. This prevents advanced detection schemes like multi-antenna arrays from finding a single RF source. On the contrary, this method comes with high hardware complexity as well as practical efforts due to the fact that all spoofers must be in phase-lock and evenly distributed around the target to perfectly mimic authentic satellite signals.

5.4 Effects on receiver operation

Undeniable, an attack on GNSS receivers with counterfeit signals impinges several effects that can be seen during the digital signal and navigation processing.

Digital signal processor At the signal acquisition stage, the receiver is looking for coarse estimates of code-offset and Doppler from satellites. During an attack one or more additional peaks per satellite occur in case the power of the counterfeit signal is around the same as the authentic one. Otherwise the spoofed peak would be drowned in noise or vice versa. Additional peaks can most likely be seen during the drag-off phase of an attack.

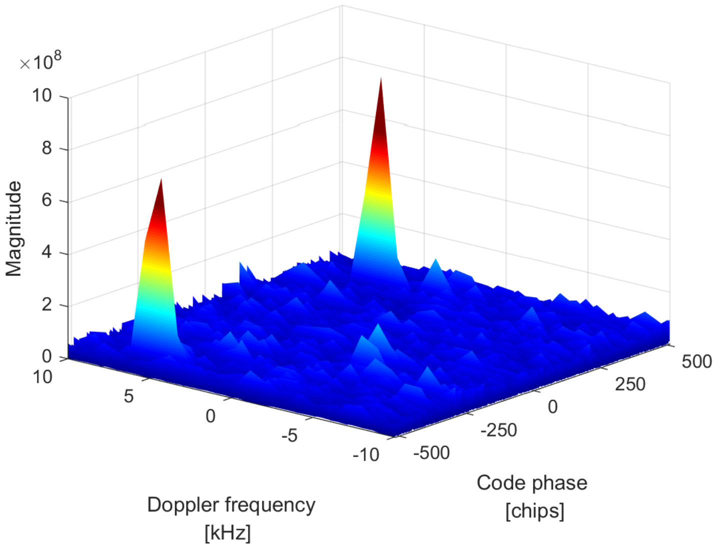


Figure 5.3: Signal acquisition during spoofing attack (two visible peaks for PRN11)

Figure 5.3 shows the acquisition result during an ongoing spoofing attack. In this example, two peaks on the same frequency but with a large code-offset are visibly emerging from the noise floor. To successfully lock the tracking loop on

the counterfeit peak, the power has to be equal or higher, making the authentic satellite signal drown in noise. For illustration purposes the two peaks in Figure 5.3 have the same magnitude.
Furthermore, effects also occur inside the tracking loop during the early-, prompt- and late correlator computation. Figure 5.4 shows the two-dimensional correlation function of the replica prompt code with the incoming baseband signal in case of an ongoing spoofing event. The dotted red and blue curve indicate the authentic and spoofed correlation peak, respectively, with the spoofed peak being slightly higher in power compared to the authentic one. The actual correlation function is a combination of these two and is represented by the black curve. On the top left of the figure, the spoofer has aligned its signals with the authentic ones resulting in an unusually high correlation peak. Afterwards the drag-off begins. On top right, the counterfeit correlation peak is half a chip, on bottom left one chip and on bottom right already two chips apart. During this drag-off phase, the overlaid peak experiences distortions. This behavior can be used for detection algorithms by observing the symmetric difference of correlation functions. For further details on this topic, see Chapter 6.

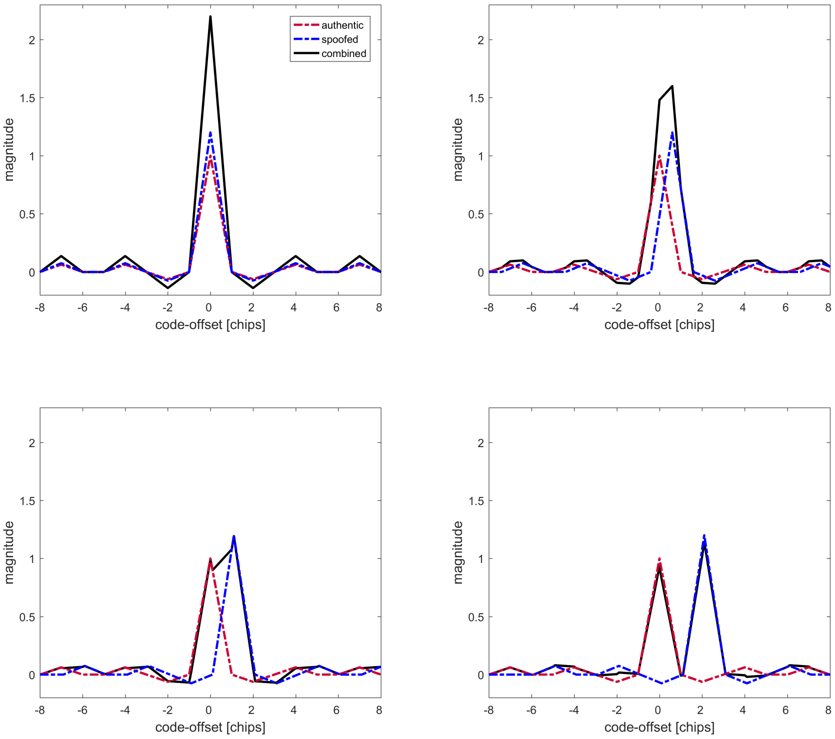


Figure 5.4: Correlation of prompt replica code with incoming baseband signal

Also, in case of a spoofing attack, the DLL and PLL outputs will diverge from their theoretical values. During the takeover, the tracking result accuracies will decrease. Shortly after that phase, the tracking loop's accuracy increases again due to the correlators locking on the new peak. This behavior can be observed and exploited as detection scheme. However, accuracies can be disturbed due to multipath or other signal power decreasing influences like jamming and therefore additional detection methods for a robust and reliable detection are needed.

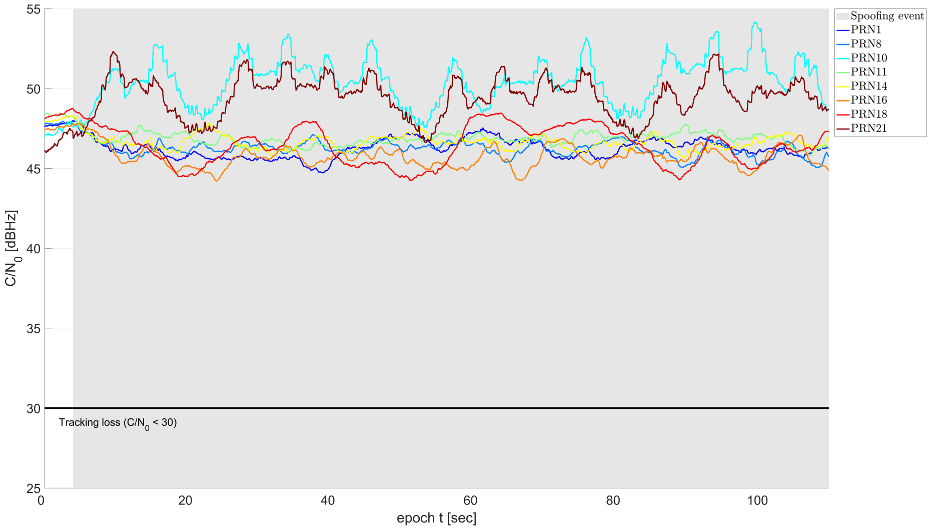


Figure 5.5: C/N$_0$ during spoofing event

Further, the carrier-to-noise power density ratios show increased values under certain circumstances if a spoofing attack is ongoing. Figure 5.5 shows the computed C/N$_0$ values of several GPS satellites. The two signals of PRN10 and PRN21 are emitted by a spoofing source with their power being 7 dB higher relative to the authentic signals. Significantly higher power values with over 50 dBHz indicate the presence of an interferer and can be exploited for further detection schemes of an ongoing attack.

Navigation processor After the attack was successfully conducted, the opponent can alter the victim receiver's position to his favor. In some cases not every authentic signal is spoofed. These authentic observations combined with the spoofed ones go inside the LSA, for position and velocity computation. If the receiver has the availability to perform a RAIM, then these authentic observations are seen as outliers and excluded from the PVT solution. The same principle goes vice versa in case only a few spoofed signals are present. Furthermore, in the case a time spoofing attack is conducted, unusual behaviors like sudden jumps on the estimated receiver clock bias can also indicate the presence of counterfeit signals.

6 Countermeasures to spoofing

As a result of the high demand in offering protection against spoofing, several state-of-the-art algorithms have been developed and introduced in literature. Many of them are either based on the principles of signal quality monitoring (SQM) or received power monitoring (RPM). After a detection, the user is informed in case the receiver is producing hazardously misleading information (HMI). In a next step, mitigation algorithms aim to provide the user with genuine PVT solutions during ongoing events. Moreover, the source of emitting fake signals can be estimated and thus, information about the spoofer position can be given.
Every algorithm has its benefits in terms of functionality, implementation complexity, hardware requirements (e.g. single vs. antenna array) or field of application (e.g. static vs. kinematic). For that reason, a combination of several complementary counter strategies is preferred to raise the robustness and reduce the false alarm rate. This chapter gives an overview of several established algorithms divided into categories of both, detection and mitigation.

6.1 Spoofing detection

The detection of counterfeit signals is a prerequisite for mitigation algorithms and serves as an important information for the user, as the produced PVT output from the receiver should not be trusted.

Position, velocity and time monitoring Since the goal of a spoofing attack is to produce HMI at receiver's side resulting in a false position and timing, the most obvious measure is to monitor the PVT output and compare it with nominal values in case of a static receiver. Alternatively, a direct comparison of position and velocity of two consecutive epochs is also possible for a static scenario. A detection alert can be raised if these quantities diverge from each other for a certain significance level by implementing a hypothesis test. A multipath creating environment has to be taken into account by modeling the reflections in order to lower false alarm rates.

Another statistical approach would be the comparison of a given a-priori variance of the weight unit with the a-posteriori variance resulting from the LSA. This method is denoted as RAIM. Within the Hewitson test, for example, the two variances are compared using a hypothesis test, with a predefined probability of false alarm rate α (Gmeindl 2011). The hypotheses are defined as follows: H_0 (null hypothesis) states that the observations used inside the LSA are free of outliers. H_1 (alternative hypothesis) states the opposite. This test can either be one-sided, where the computed metric is compared to one threshold, or two-sided, where the metric is tested against an interval. Figure 6.1 shows the probability density functions of a normal distribution for a one- and a two-sided test with limits defined by a false alarm rate of 5%.

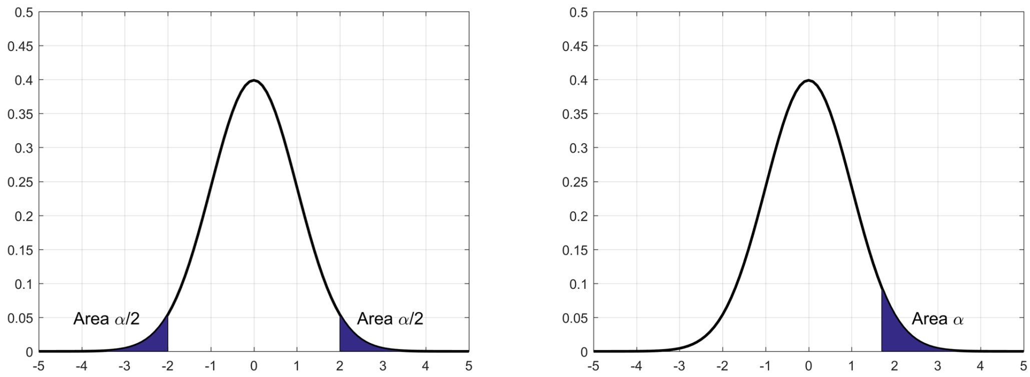


Figure 6.1: Normal probability density functions of hypothesis test

In general, a hypothesis test has one of four outcomes. The outcome depends on H_0 either being true or false and whether H_0 is accepted or refused. Table 6.1 gives an overview of the possible cases. The quantity β describes a type 2 error, where a false H_0 is being accepted. The probability $1 - \alpha$ is called the significance level, while $1 - \beta$ is known as the power (Gmeindl 2011).

Table 6.1: Possible cases for a hypothesis test

Test decision	H_0 true	H_1 true
H_0 accepted	Right decision with $P = 1 - \alpha$	Type 2 error with $P = \beta$
H_1 accepted	Type 1 error with $P = \alpha$	Right decision with $P = 1 - \beta$

The Hewitson test consists of two parts: the first is a global test, telling if any outliers are present in the PVT output. The second part, is a test for localizing

the faulty observations and excluding them from the LSA.
The computed variance of the weight unit $\hat{\sigma}^2$, as defined in Equation 2.7, is used together with an a-priori defined variance σ_0^2 to compute a test metric

$$T_{\chi^2} = (n-m)\frac{\hat{\sigma}^2}{\sigma_0^2} \sim (n-m)\chi^2, \tag{6.1}$$

where $n-m$ is the degree of freedom and the metric being χ^2-distributed. If a two-sided test is conducted, H_0 is true, if the metric lies inside the interval

$$P\left(F_{\chi^2}^{-1}\left(\frac{\alpha}{2}, n-m\right) < T_{\chi^2} < F_{\chi^2}^{-1}\left(1-\frac{\alpha}{2}, n-m\right)\right) = 1-\alpha. \tag{6.2}$$

If the null hypothesis is rejected, a second test is performed to locate the outliers. One of these tests can be the ω-test. Every residual is standardized and compared against a normal distribution with a false alarm rate of α_0. The new false alarm rate is calculated using the former one of the global model test in combination with the redundancy of the model. The computation of α_0 is defined by

$$\alpha_0 = \frac{\alpha}{r}, \tag{6.3}$$

with

$$r = \mathrm{tr}(\mathbf{R}) = \mathrm{tr}(\mathbf{Q}_{\hat{e}}\mathbf{P}). \tag{6.4}$$

The matrix $\mathbf{Q}_{\hat{e}}$ is the covariance matrix of the residuals and is given through

$$\mathbf{Q}_{\hat{e}} = \mathbf{P}^{-1} - \mathbf{A}(\mathbf{A}^T\mathbf{P}\mathbf{A})^{-1}\mathbf{A}^T. \tag{6.5}$$

With this information, for every residual i, a standardized value ω_i can be calculated using

$$\omega_i = \frac{\mathbf{d}_i^T\mathbf{P}\hat{\mathbf{e}}}{\sqrt{\mathbf{d}_i^T\mathbf{P}\mathbf{Q}_{\hat{e}}\mathbf{d}_i^T}}, \tag{6.6}$$

were, $\mathbf{d}_i$ is a vector of the length of the residuals, where the ith value is set to 1 and the others to 0. The hypothesis test

$$|\omega_i| > N_{1-\alpha_0/2}(0,1) \tag{6.7}$$

is conducted by assuming a normal probability distribution function depending on the false alarm rate α_0. If the threshold is exceeded, the observation is excluded and the LSA is repeated together with the global model test. The process continues, until the global test is accepted and no outliers are present, meaning the PVT does not contain any inconsistent observations anymore. More information on RAIM and hypothesis testing can be found in Gmeindl (2011).
Assuming a scenario, where not all authentic satellite signals are overpowered by the spoofer, the receiver might also track the authentic signals, resulting in a distorted PVT. For that case, if a statistical hypothesis test does not detect any inconsistency inside the geometry, a further look on the estimated receiver clock bias can help. The LSA smears the errors into the estimated parameters with the receiver clock bias being the most affected. In an optimal scenario, an epoch wise estimation of the clock bias should result in a linear trend with a constant offset over time.

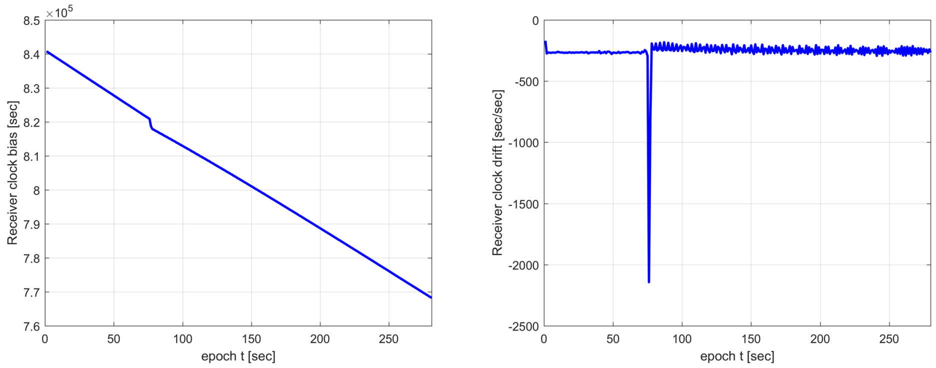


Figure 6.2: Receiver clock bias (left) and drift (right) during spoofing attack

Figure 6.2 shows the resulting clock bias and its time derivative from a receiver under a spoofing attack. A significant jump at around epoch 75 can be seen after the receiver has been taken over. Reasons for this behavior could be wrong satellite ephemeris or the signals not being time-synchronously broadcast with respect to the authentic ones.

Doppler monitoring A detailed look on Doppler measurements can also make a detection possible by comparing them with the theoretical Doppler in case the receiver is not in motion. A static receiver observes a Doppler that only consists due to relative satellite motion, neglecting clock drifts. If the position vector of the antenna is known and its velocity is assumed to be zero, the radial velocity can be calculated using Equation 2.13 and thus the resulting Doppler shift. For this, the absolute satellite velocity is needed. Similar to satellite position determination, the velocity can also be computed via the broadcast ephemeris. Further information can be taken from Hofmann-Wellenhof et al. (2008).

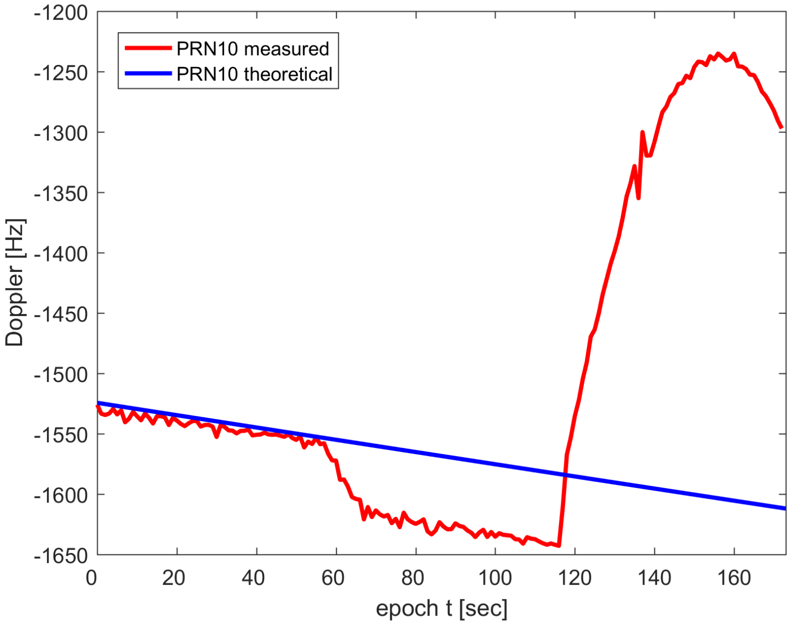


Figure 6.3: Theoretical vs. measured Doppler

Figure 6.3 shows the comparison of the measured Doppler values resulting from the tracking loop vs. the theoretical ones. The noisy observations scatter below the theoretical values. After epoch 55, the receiver has been taken over. A quick change of the Doppler inside the tracking loop happens due to the spoofer dragging away the receiver from its position. The measured Doppler values in this scenario are caused by a code-sweep of the spoofer, where the additional code-offset on the counterfeit signals is varied over time. The measurements diverge from the theoretical values by several hundred Hertz, indicating an unusual behavior caused by the spoofing signal.

Correlation peak monitoring Multipath effect is denoted as a composition NLOS received signals, leading to erroneous PVT solutions. Such signals produce similar results compared to fake ones emitted by a spoofer. Before issuing an alarm, a spoofing detector would need to verify that the observed distortion is not explainable as mere multipath (Psiaki and Humphreys 2016a). In an unspoofed and multipath-free scenario, for every visible satellite, one correlation peak in the two-dimensional search space of Doppler and code-offset is present. Assuming, reflected signals from surfaces near the receiver overlay with the LOS signals, additional peaks may appear near the authentic one. In case the receiver is moving, these peaks are not constant and vary quickly over time causing distortions on the main peak.
During the drag-off phase of a spoofing attack, a clear second peak with higher magnitude appears, if code-offset and Doppler between the two signals are big enough. If the peak is present for a certain amount of time with the same signal characteristics, its source can be assumed to be a spoofer.
If more than one peak is visible, the receiver has probably locked onto the false signal already inside the tracking loop. Due to a permanently changing code-offset of the spoofed peak, additional Doppler effects occur, caused by the relative motion between the two peaks. This provides further information of an ongoing spoofing event.
If both peaks are close to each other, they are merged to one distorted peak with significantly higher power, as depicted in Figure 5.4. These distortions result in asymmetric correlation functions which can be exploited for detection. Following Huang et al. (2016), the implementation of a ratio test metric

$$M(t) = \frac{I_E(t) + I_L(t)}{\epsilon I_P(t)}, \tag{6.8}$$

measures distortions, where I_E, I_P and I_L are the early, prompt and late in-phase correlator outputs and ϵ being a constant factor that represents the slope of the correlation function.

Received power monitoring GNSS-like signals emitted by a spoofer need to overpower the authentic ones in order to force a takeover of the victim receiver. One quantity that describes the power of a GNSS signal is the carrier-to-noise power density ratio (C/N$_0$). It is essential for determining the status of the tracking loop. For example, tracking loops experience a rapid increase of tracking errors at low C/N$_0$, e.g. below 30 dBHz, until they completely lose lock (Petovello 2010). The ratio is computed on the post-correlation stage of the tracking loop utilizing the prompt correlator output. Assume a discrete sample stream from a complex signal

$$r_C[n] = \sqrt{P_d}D[n] + \sqrt{P_n}\eta[n], \tag{6.9}$$

where $D[n]$ are the navigation bit samples containing a residual carrier phase error, P_d and P_n being the power of the data and noise respectively, and $\eta[n]$ being the noise of the complex signal. The computation of the C/N$_0$ reads

$$\frac{C}{N_0} = \lambda_C \cdot B_{eqn}, \tag{6.10}$$

where $\lambda_C = P_d/P_n$ is the signal-to-noise ratio (SNR) and B_{eqn} represents the normalized equivalent noise bandwidth of the system. There are several methods to acquire the SNR (Petovello 2010). One of such is the real signal-complex noise (RSCN) estimator. The estimated power of the noise

$$\hat{P}_n = \frac{2}{N}\sum_{v=1}^{N} |r_{C,Im}[v]|^2 \tag{6.11}$$

is calculated via the quadrature-phase (imaginary) samples of the prompt correlator output. By forming the total signal power

$$\hat{P}_{tot} = \frac{1}{N}\sum_{v=1}^{N} |r_C[v]|^2, \tag{6.12}$$

the SNR λ_C is given by

$$\lambda_C = \frac{\hat{P}_{tot} - \hat{P}_n}{\hat{P}_n}, \tag{6.13}$$

and thus the carrier-to-noise power density ratio can be computed using Equation 6.10. Further information on C/N$_0$ calculation can be taken from Petovello (2010). On the pre-correlation side, the power spectral density (PSD) can provide an insight on the power characteristics of the incoming signal. Since a spoofing signal needs to be around the same power as authentic ones, its characteristics are below the thermal noise and thus cannot be seen in the PSD. Therefore, PSD monitoring is more suitable for detecting jamming events, rather than spoofing attacks.

Symmetric difference combined with received power monitoring Considering only the received signal power, an explicit distinction between a spoofer and jammer cannot be made. On the other side, distorted correlation peaks, as created by spoofers during the drag-off phase, can also occur in multipath environments. By combining the two strategies of RPM and symmetric difference, the disadvantages of each method are compensated.
Wesson et al. (2013) has developed a strategy where metrics of the symmetric difference of the correlator outputs are combined with the measured signal strength. The symmetric difference at a certain epoch t is defined as

$$D_t(\tau_s) = r_t(\tau_c - \tau_s) - r_t(\tau_c + \tau_s), \tag{6.14}$$

where r_t is the correlator output dependent on the center tap offset τ_c and the symmetric difference tap offset τ_s. Under ideal noise-, multipath-, and spoofing-free conditions, $D_t(\tau_s)$ is close to zero. Large values can indicate the presence of a spoofer. Depending on the correlator spacing, tracking performance and multipath sensitivity is influenced. A narrow correlator spacing improves the performance and is thus preferred. The power P_t at a certain epoch is the power spectral density estimate of the received signal. Together with the metric $D_t(\tau_s)$, a single detection statistic

$$z_t = [D_t(\tau_s), P_t]^T \tag{6.15}$$

can be formed. This statistic is tested against three hypotheses: H_0, being AWGN, H_1, being mutlipath and H_2, being spoofing. For every hypothesis, an empirical probability distribution $p_{z|H_i}(\psi|H_i)$ for $i = 0, 1, 2$ needs to be defined. The probability of false alarm P_f is acquired via the distributions of H_0 and H_1:

$$P_f = \frac{1}{2} \int_R (p_{z|H_0}(\psi|H_0) + p_{z|H_1}(\psi|H_1)) d\psi. \tag{6.16}$$

The region of the integral R is defined where H_i and H_2 share the same probability mass and where $p_{z|H_i}(\psi|H_i) < \lambda$ for $i = 0, 1$ and a particular choice of λ (Wesson et al. 2013). In order to lower the false alarm rate, representative data sets for every hypothesis are needed, to get the best results for this detection strategy.

Closely spaced correlators Enhancing the symmetric difference, the principle of closely spaced correlators is introduced. Citing Khan et al. (2017), a legacy three-arm correlator does not generate enough information to capture all the details to estimate signal quality for spoofing detection purpose. To compensate that, a high number of correlators on both sides of the prompt correlator is defined, separated by a small chip spacing. Under ideal conditions, the correlation function of the prompt code has a triangular shape. The principle of this approach is to measure the Euclidean distance between the ideal symmetric difference $D_t^{ideal}(\tau_s)$ and the measured one $D_t^{meas}(\tau_s)$ for every tap offset τ_s by applying

$$M_{CSC} = \sqrt{\sum_{\tau_s=-k}^{k} (D_t^{ideal}(\tau_s) - D_t^{meas}(\tau_s))^2}. \tag{6.17}$$

Considering an ideal scenario without the presence of spoofing or multipath,

$$D_t^{meas}(\tau_s) = D_t^{ideal}(\tau_s) + \omega(t) \tag{6.18}$$

is valid, with $\omega(t)$ being AWGN. This yields to a detection metric

$$M_{CSC} = \sqrt{\sum_{\tau_s=-k}^{k} (\omega(t))^2}. \tag{6.19}$$

Using this information, a detection threshold η can be computed by

$$\eta = C \cdot \sqrt{\sum_{\tau_s=-k}^{k} (\omega(t))^2}, \tag{6.20}$$

where C is a constant, which can be determined with the inverse normal cumulative density function by using a chosen probability of false alarm P_f, a mean value μ and standard deviation σ of an interference-free scenario. The computation of the constant reads

$$C = F^{-1}(P_f, \mu, \sigma). \tag{6.21}$$

Figure 6.4 shows the calculated metric for GPS PRN14 acquired by 20 symmetric differences with a chip spacing of 0.2 chips for a SDR under attack.

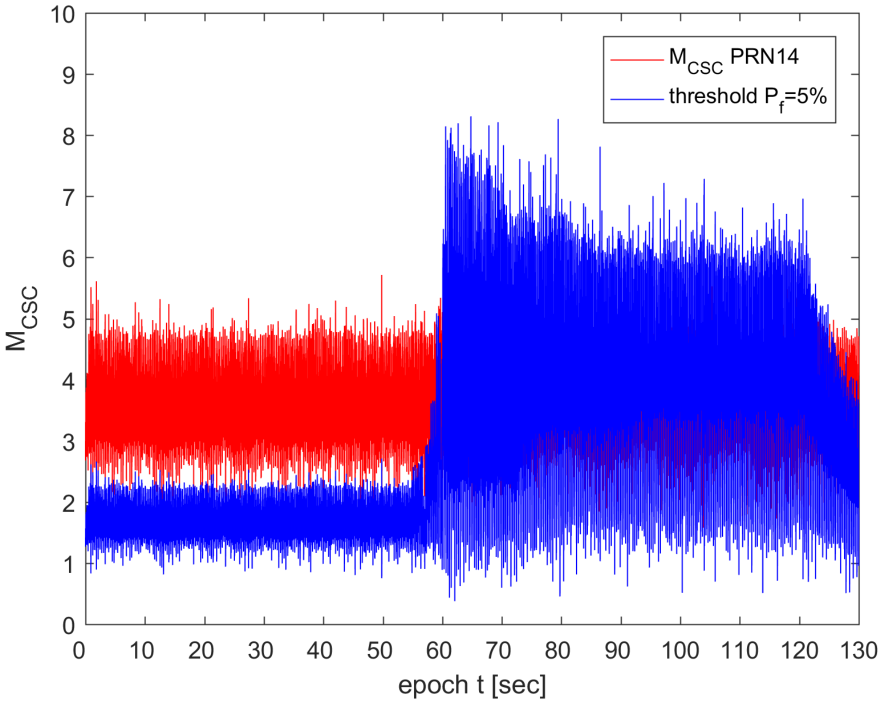


Figure 6.4: Closely spaced correlator detection metric during spoofing event

After 55 seconds, the spoofer increased its power from -10 dB to 10 dB relative to the authentic signal power. The threshold ($P_f = 5\%$) is quickly exceeded. After 60 seconds, the drag-off phase starts, where to spoofer slowly drags away the locked on peak by adding a varying additional code-offset to its signals. After 120 seconds, the metric M_{CSC} quickly decreases again. At this point the authentic and counterfeit correlation peaks are well separated from each other causing no more distortions and the SDR is now tracking the fake signals.

6.2 Spoofing mitigation

Mitigation algorithms aim to maintain nominal receiver operations and try to guarantee that no HMI is produced and used. Furthermore, the source of the emitted false signals can be located. With this information, the user can take further actions.

Signal authentication Signal authentication of both, the ranging code and navigation message, based on encryption, is the safest way to cope with the threat of intentional interference of spoofing. For that reason, the US Department of Defense already started to encrypt some of its GPS signals in the early days and further spends a lot of time and money in the modernization of the system by establishing the new M-Code for military receivers. Embracing this idea, the European system Galileo will also be offering navigation message authentication to signals that are part of the OS after reaching FOC (Chatre and Verhoef (2018)). Nonetheless, highly encrypted signals can still be easily jammed, denying any PVT service.
The main objective of navigation message authentication is to guarantee that the signal has been generated by a trusted source. The basic principle is the encryption of the navigation message which can only be decrypted with a proper key. The generation of this authentication signature can be divided into two categories: symmetric key and asymmetric key techniques. In the symmetric technique, the transmitter and receiver share a secret key while the asymmetric technique splits the secret key into two parts. Those two parts consist of a private key, only known to the transmitter and a public key, which is distributed publicly. The private key is used to generate the authentication message and the public key serves in the verification step (Petovello 2018).
Referring to O'Hanlon et al. (2012), a spoofing detection scheme based on correlation between two civil GPS receivers has been presented. Here, the presence of a spoofing attack is determined by mixing and accumulating the baseband quadrature channel samples from two spatially separated civil receivers. The detection aims at the crosscorrelation of the encrypted P(Y)-code, which should be present in both signals in the absence of spoofing.

Spatial correlation This principle exploits the property of high correlation between signals emitted by the same source. Referring to Broumandan et al. (2012), measurements coming from a single source have essentially the same PSD and virtually the same channel gain for any space-time point. If a receiver is static, all channel gains of the authentic and spoofed pairs are similar and thus highly

correlated. But as soon as the receiver starts moving, the gains based on the authentic satellites quickly decorrelate over time. This makes a distinction between real and fake signals possible.
Assuming the incoming complex signal at the receiver has the structure of Equation 5.1. After despreading the carrier and PRN code inside the tracking loop, the correlator output corresponds to

$$\begin{aligned} x_i^A(t) &\approx \alpha_i^A(t) A_i^A(\mathbf{p}(t), t) + \omega_i^A(t), \\ x_i^S(t) &\approx \alpha_i^S(t) A_i^S(\mathbf{p}(t), t) + \omega_i^S(t), \end{aligned} \tag{6.22}$$

for authentic and spoofed signals respectively with the same definition as in Section 5.1. Here, the terms $\omega_i^{A/S}(t)$ denote the noise. By collecting correlator outputs over a snapshot interval $t \in [0, T]$ divided into M subintervals with a duration of ΔT, every m-th subinterval extends over the interval of $[(m-1)\Delta T, m\Delta T]$ for $m \in [1, 2, ..., M]$. Figure 6.5 describes the sampling process for a moving antenna on a random trajectory (Broumandan et al. 2012).

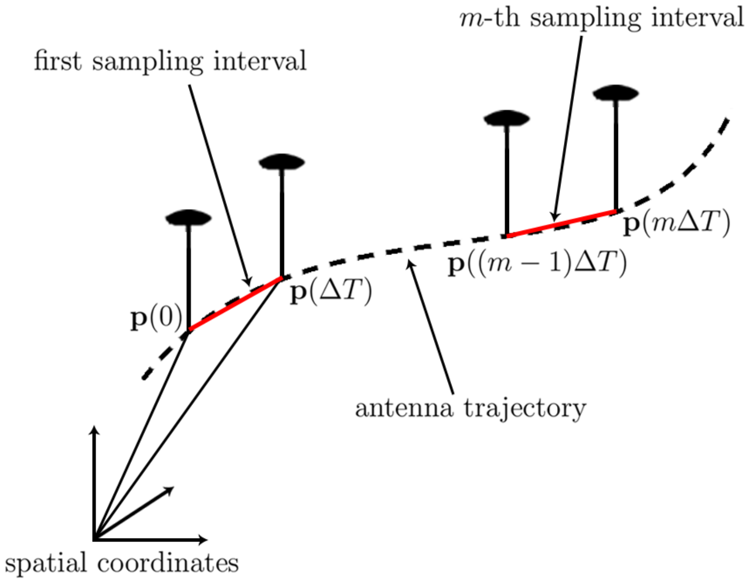


Figure 6.5: Spatial sampling of antenna trajectory (c.f. Broumandan et al. 2012)

The sampled values within the subintervals can be summed up to vectors so that the detection problem can be defined as

$$\mathbf{x}_i = \begin{cases} \mathbf{a}_i^A \odot \boldsymbol{\alpha}_i^A + \boldsymbol{\omega}_i^A = \boldsymbol{\Lambda}_i^A + \boldsymbol{\omega}_i^A & H_0 \\ \mathbf{a}_i^S \odot \boldsymbol{\alpha}_i^S + \boldsymbol{\omega}_i^S = \boldsymbol{\Lambda}_i^S + \boldsymbol{\omega}_i^S & H_1, \end{cases} \tag{6.23}$$

where $\mathbf{a}_i$ and $\boldsymbol{\alpha}_i$ are the channel gains and complex scintillation vectors respectively for a certain PRN i. The operator $\odot$ denotes the Hadamard vector product. During antenna movement, the spatial signature inside $\mathbf{a}_i$ is the same for all L counterfeit signals, resulting in the following definition

$$\begin{array}{ll} E[\boldsymbol{\Lambda}_i^{A^H}, \boldsymbol{\Lambda}_j^A] \approx \delta_{ij} & \text{for } \ 1 \leq i, j \leq L, \\ E[\boldsymbol{\Lambda}_i^{S^H}, \boldsymbol{\Lambda}_j^S] \approx 1 & \text{for } \ 1 \leq i, j \leq L, \end{array} \tag{6.24}$$

where $E[\,\cdot\,]$ denotes the expectation operator, the superscript H the Hermitian matrix transpose and δ_{ij} the Kronecker-delta. By setting up a matrix

$$\mathbf{x} = \begin{bmatrix} x_{1,1} & x_{2,1} & \cdots & x_{2L,1} \\ x_{1,2} & x_{2,2} & \cdots & x_{2L,2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,M} & x_{2,M} & \cdots & x_{2L,M} \end{bmatrix}, \tag{6.25}$$

with the spatial snapshots of the correlator outputs for a possible set of $2L$ satellites (authentic and spoofed set), the correlation coefficient can be calculated using

$$\rho_{ij} = \frac{E[\mathbf{x}_i, \mathbf{x}_j^H]}{\sqrt{E[\mathbf{x}_i, \mathbf{x}_i^H]}\sqrt{E[\mathbf{x}_j, \mathbf{x}_j^H]}}. \tag{6.26}$$

This metric indicates whether a satellite pair has the same spatial signature or not. When the value is near one, a high spatial correlation between a signal pair is present, whereas zero indicates the opposite.

An implementation of this method can also be based on Doppler values. By comparing the measured Doppler frequency and the theoretical one, the spatial correlation of the spoofer signals is high due to receiver kinematics. Figure 6.6 shows the difference between measured Doppler frequencies and theoretical ones (residual Doppler) during a spoofing event, where two satellites (i.e. PRN8 and PRN21) have been spoofed.

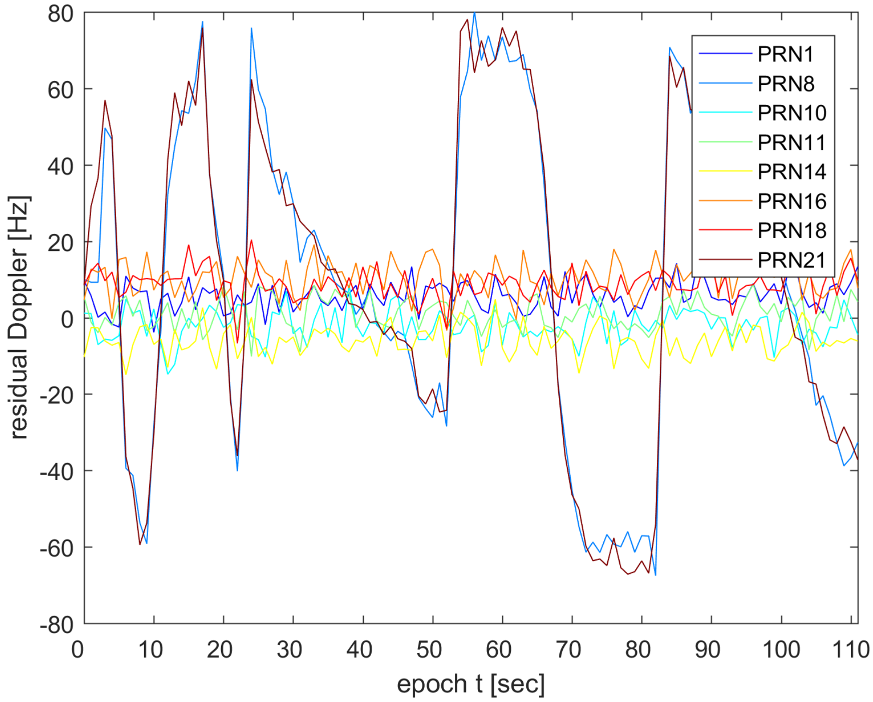


Figure 6.6: Difference between measured and theoretical Doppler

While the residual Doppler values sourcing from the authentic satellites randomly scatter near zero, the two spoofed satellites experience deviations of up to 80 Hz. Furthermore, the correlation is high during the whole time span of around two minutes due to the same relative movement. Figure 6.7 depicts this effect, where the crosscorrelation coefficient between PRN8 and PRN21 is one, while the rest are close to zero. Note that the correlation for every signal with itself (autocorrelation) also yields one.

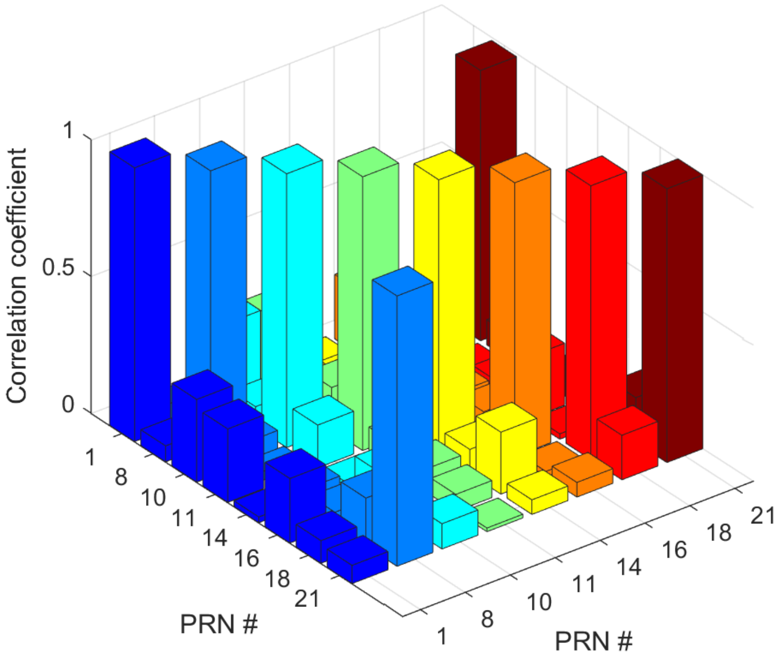


Figure 6.7: Spatial correlation coefficient for residual Doppler

If just one satellite is spoofed, no correlations between any signal combinations would be seen. The presence of one counterfeit satellite can be compensated by an implemented RAIM algorithm to avoid producing any HMI.

Direction of arrival estimation By using multi-antenna arrays, the direction of arrival (DOA) of incoming signals can be estimated. Some algorithms offer the estimation of several signal sources simultaneously depending on the number of array elements. For the case of real GNSS satellites, every signal impinges from a different direction at receiver site. In case of an intermediate spoofing attack, all signals emerge from one source. In case, an attack has been detected, multi-antenna arrays can be utilized to determine the source of the high-powered counterfeit signals and thus, the direction of the spoofer.

There are several types of antenna arrays. The most used ones are uniform linear or circular arrays (ULA, UCA). The more elements an array contains, the more stable the estimation of the DOA parameters is. Referring to Broumandan et al. (2007), the element spacing is important to avoid ambiguities in the estimated direction angles. For proper results, a spacing of equal or less than half the wavelength λ of the incoming signal is preferred. This limits the size of arrays in case of GNSS

DOA estimation, where high frequencies for signal propagation are used.
Krim and Viberg (1996) describes several techniques for DOA estimation. As examples, beamforming techniques and subspace-based methods are mentioned. The latter one has proven to deliver reliable results in case of closely spaced signal sources. One of these subspace-based methods is the multiple signal classification (MUSIC) algorithm. Considering the covariance matrix of the incoming signals computed via N samples for a certain number of M array elements

$$\mathbf{R}_x = \frac{1}{N}\sum_{t=1}^{N} \mathbf{x}(t)\mathbf{x}(t)^H, \tag{6.27}$$

where $\mathbf{x}(t)$ denotes the complex signal column vector of the array elements and H the Hermitian transpose. The sample covariance matrix is formed by the steering matrix $\mathbf{S}$ and the nominal covariance matrix $\mathbf{R}_I$ yielding

$$\mathbf{R}_x \approx \mathbf{S}\mathbf{R}_I\mathbf{S}^H. \tag{6.28}$$

The matrix $\mathbf{S}$ contains D interference steering vectors depending on the number of signal sources. Its spectral decomposition can be written as

$$\mathbf{R}_x \approx \mathbf{U}_s\mathbf{\Lambda}_s\mathbf{U}_s^H + \sigma^2\mathbf{U}_n\mathbf{U}_n^H, \tag{6.29}$$

where $\mathbf{U}$ is a matrix consisting of the eigenvectors and $\mathbf{\Lambda}$ a diagonal matrix with the eigenvalues of the covariance matrix. The subscripts s and n denote the signal sources impinging on the array and the noise, respectively. The distinction between signal and noise is based on the known number of signal sources D. By doing a first spectral decomposition, the resulting eigenvalues are sorted by ascending order. The D largest eigenvalues with its eigenvectors form the signal subspace matrices, while $M - D$ values are assigned to the noise subspace. This implies, that the number of estimable signal sources D cannot be greater than the number of array elements M. The estimation of the signal number is a well addressed problem and as such referred to Mathews and Zoltowski (1994). By forming the spectrum function

$$P_{\text{MUSIC}} = \frac{1}{\mathbf{s}(\theta)^H\mathbf{U}_n\mathbf{U}_n^H\mathbf{s}(\theta)} \tag{6.30}$$

for a varying DOA parameter θ, the power of the incoming direction of a signal can be estimated. The D largest values indicate the emitting sources in the spectrum. In case of an UCA, the steering vector $\mathbf{s}(\theta)$ for a certain signal source takes the form

$$\mathbf{s}(\theta) = \mathbf{s}(\vartheta, \varphi) = \begin{bmatrix} e^{-i\xi\cos(\varphi-\gamma_0)} \\ e^{-i\xi\cos(\varphi-\gamma_1)} \\ \vdots \\ e^{-i\xi\cos(\varphi-\gamma_{M-1})} \end{bmatrix}, \tag{6.31}$$

with

$$\xi = \frac{2\pi}{\lambda} r \cos\vartheta, \tag{6.32}$$

where ϑ and φ denote the elevation and azimuth of the impinging signal respectively, λ the wavelength of the incoming signal and r being the radius of the circular array. For every array element, the circular angle γ is computed by

$$\gamma_m = \frac{2\pi m}{M} \quad \text{for} \quad m \in [0, 1, ..., M-1]. \tag{6.33}$$

Phase mode excitation-based beamforming is the basis for the development of the UCA-RB-MUSIC (real beamspace) algorithm that requires only real-valued eigenvalue decompositions to obtain signal and noise subspace estimates (Mathews and Zoltowski 1994).
A beamformer is needed, to transform the steering vector $\mathbf{s}(\theta)$ from element space to beamspace. By doing this, an improved estimator performance in correlated source scenarios as well as a lower computational complexity is provided, as samples of the two-dimensional beamspace MUSIC spectrum corresponding to a given elevation can be obtained via fast Fourier transform (FFT). For the single computation steps of phase mode excitation for UCA, refer to Mathews and Zoltowski (1994).
According to Tang (2014), the MUSIC algorithm offers several advantages compared to conventional DOA estimates listed as follows:

- Ability to simultaneously estimate multiple signal sources, where the number of estimable sources equals the number of array elements
- High precision estimates
- High resolution for antenna beam signals
- Achievable real time processing

Besides DOA based on subspace and beamforming techniques, the position of an interferer can further be acquired through the principle of time difference of arrival (TDOA). It is the inverse principle of classical hyperbolic radar systems, where multiple receivers are combined with one transmitter. The TDOA is computed via crosscorrelation of the received signals at different monitor stations. Considering two signals

$$\begin{aligned} r_1(t) &= s(t) + \omega(t), \\ r_2(t) &= a \cdot s(t+\tau) + \omega(t), \end{aligned} \tag{6.34}$$

measured at two monitor stations 1 and 2, where $s(t)$ is the emitted signal by an interferer, a the attenuation at the second monitor station, τ the time delay between the stations and $\omega(t)$ being AWGN. Through the principle of triangulation and the known monitor station coordinates, the position of the transmitter can be computed. Correlating the signals by applying Equation 2.17, the time delay can be estimated. In order to achieve that, the clocks at monitor station's side need to be synchronized. Since the receiver clocks are not free of errors, the biases need to be known beforehand. Through calculating a GNSS PVT, the estimated receiver clock bias is provided.

7 Implementation of a detection and mitigation algorithm

Within this thesis, a developed algorithm for detection and mitigation of spoofing attacks is presented. The proposed algorithm is suitable for moving stand-alone single-antenna receivers (e.g. mounted on a car, plane, drone or carried by foot). The basic principle is based on monitoring the incoming signal's spatial signature based on Doppler measurements. Additionally, by combining several antennas to an uniform circular array, a provided DOA of the spoofing signals emitter is obtained, in case a spoofing attack has successfully been detected and mitigated.
The algorithm was developed and tested in the programming language MATLAB. The fundamental SDR structure was provided by Borre et al. (2007) and enhanced by the proposed algorithm. Furthermore, preprocessed receiver independent exchange format (RINEX) files were used for validating the algorithm's performance and functionality. For investigating different scenarios, simulations and real-world record data sets, based on raw GNSS smartphone measurements were used. In the following, a detailed description of the single algorithm steps is given.

7.1 Overall concept

The concept of the proposed counter strategy is illustrated by the flow chart in Figure 7.1. The incoming GNSS signals are gathered through an enhanced acquisition process in a first step. A search for several peaks in the two-dimensional Doppler/code-offset domain for every PRN is made. If only one peak per channel is acquired, a nominal PVT computation with RAIM is carried out together with the calculation of the correlation coefficient based on the difference between theoretical and measured Doppler, as described in Section 6.2. In case, a high correlation between the individual PRN channels is present, the algorithm returns to the acquisition stage, where additional correlation peaks should now be visible. The receiver tracks all peaks that are present, meaning authentic and spoofed signals are processed simultaneously.

In a next step, the tracked signals are coarsely divided into two sets based on the C/N_0 output from the tracking loop: an authentic set, including the tracked PRNs with nominal received power and a spoofed set, where the associated power is significantly higher.

The classification of the two sets based on the C/N_0 values can be verified. If required, a PVT with the minimum configuration of four chosen satellites is calculated for every possible combination out from both sets in a first step. This results in 2^n possible combinations, where $n = 4$, since measurements from at least four satellites are needed to compute a PVT in case of GNSS. With every obtained PVT solution, the spatial correlation coefficients are calculated based on the theoretical Doppler values. The set with the lowest correlations should now consist of authentic satellite signals only.

In a second step, an iteration is carried out by assigning one further PRN out of both sets to the authentic set and repeating a PVT computation. By comparing the two solutions, the authentic satellite can be sought out. In the end, all signals are correctly classified according to their source. Two separately computed PVTs are provided, with one being the true solution based on real GNSS satellites and the other being HMI, generated by a spoofer, assuming that both authentic and spoofed signals are tracked.

At the same time, a DOA based on the subspace technique of the MUSIC algorithm is executed, in case high correlations are present and a UCA is set up. The DOA is acquired by combining the incoming complex signals at every array element.

To aid the proposed algorithm, further measures can be utilized to lower detection false alarm rate. For example, the spatial signature of the correlator outputs can be observed as well. Furthermore, a ratio test metric combined with closely spaced correlators can help to indicate asymmetric behavior in the correlation functions.

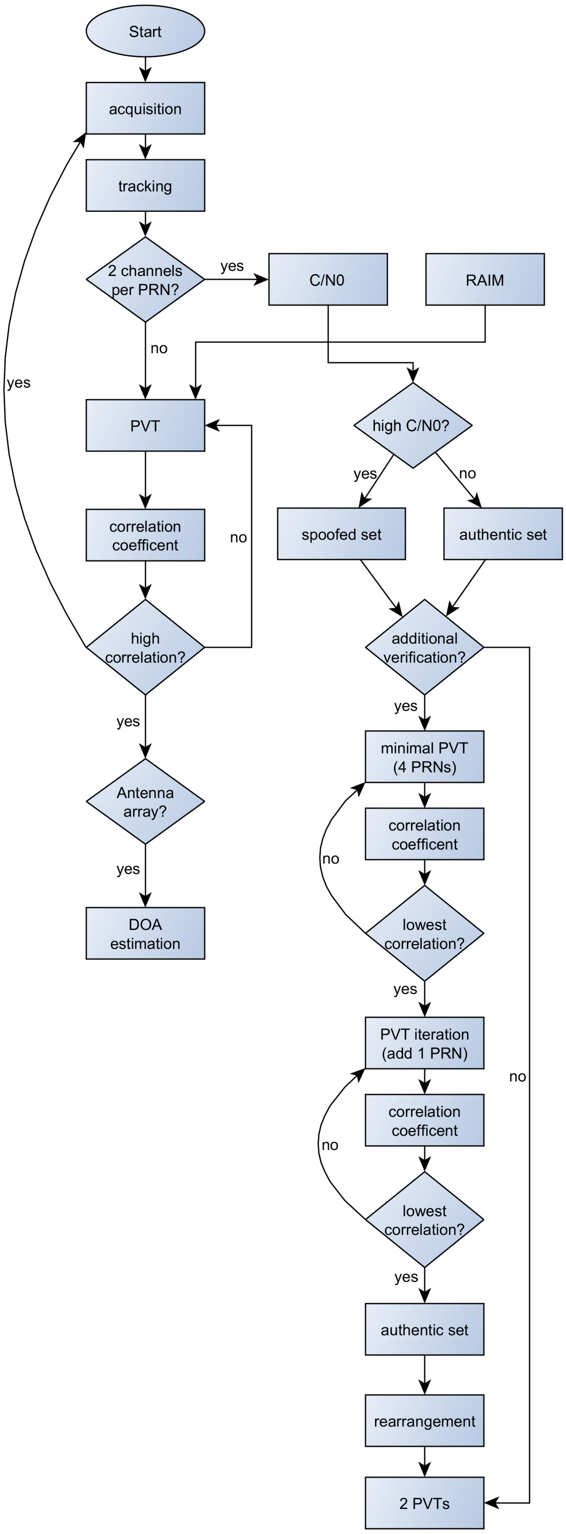


Figure 7.1: Overall concept of the proposed algorithm

8 Results and evaluation

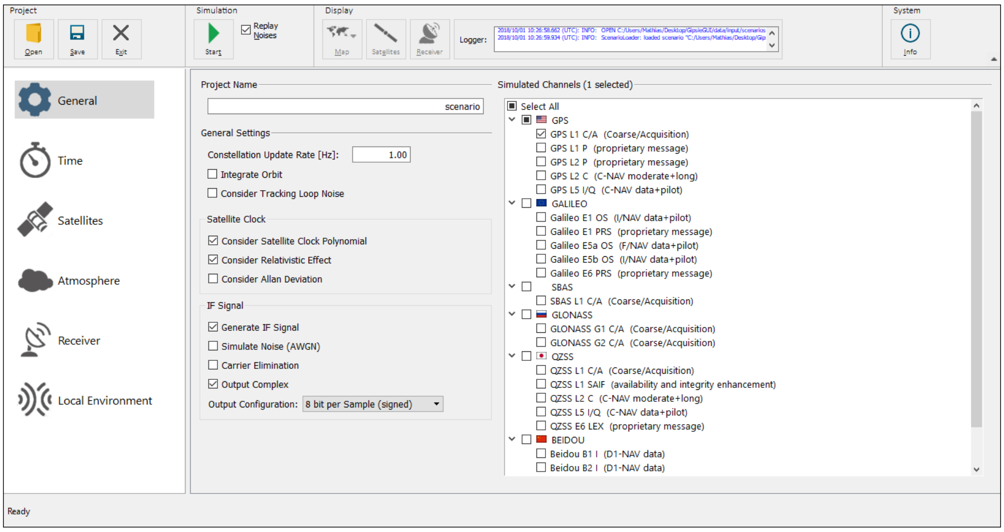
In the present chapter, the results based on simulated and real-world measurements are discussed. The developed algorithm, proposed in Chapter 7, is investigated for different simulated scenarios. Furthermore, the direction of arrival of a possible spoofer has been conducted, based on a simulated circular antenna array. In the end, a recorded real-world spoofing attack with raw GNSS smartphone measurements has been evaluated.

8.1 Data acquisition

Simulation data based on GIPSIE® For testing and validating the presented state-of-the-art algorithms in Chapter 6 and testing the proposed mitigation strategy depicted in Figure 7.1, data scenarios have been generated by the GNSS multisystem performance simulation environment (GIPSIE®), a software developed by TeleConsult Austria GmbH. The environment is capable of simulating arbitrary digital IF GNSS signals (TeleConsult Austria GmbH 2018a). The sampling frequency can be fully adjusted for the resulting digital file, making it possible for upconverting it to RF and replaying it by a proprietary hardware simulator. The software can be controlled either through a graphical user interface (GUI) or by command prompt. All necessary functionalities to configure arbitrary GNSS scenarios are provided together with an easy automation of simulations.

The environment can simulate the following GNSS signals:

- GPS: L1 C/A and P; L2 L2C and P; L5 I/Q
- SBAS: L1 EGNOS/WAAS/MSAS
- Galileo: E1B and E1C; E5a/b
- GLONASS: G1, G2
- BeiDou: B1, B2
- QZSS: L1 C/A and SAIF, L2C, L5 I/Q, LEX
- NAVIC: L5 and S-band



☑ Replay Noises

Logger:

```
2018/10/01 10:26:58.662 (UTC): INFO:   OPEN C:/Users/Mathias/Desktop/GipsieGUI/data/input/scenarios
2018/10/01 10:26:59.934 (UTC): INFO:   ScenarioLoader: loaded scenario "C:/Users/Mathias/Desktop/Gip
```

Project Name: scenario

General Settings

Constellation Update Rate [Hz]: 1.00

☐ Integrate Orbit

☐ Consider Tracking Loop Noise

Satellite Clock

☑ Consider Satellite Clock Polynomial

☑ Consider Relativistic Effect

☐ Consider Allan Deviation

IF Signal

☑ Generate IF Signal

☐ Simulate Noise (AWGN)

☐ Carrier Elimination

☑ Output Complex

Output Configuration: 8 bit per Sample (signed)

Simulated Channels (1 selected)

▣ Select All
- ▣ GPS
  - ☑ GPS L1 C/A (Coarse/Acquisition)
  - ☐ GPS L1 P (proprietary message)
  - ☐ GPS L2 P (proprietary message)
  - ☐ GPS L2 C (C-NAV moderate+long)
  - ☐ GPS L5 I/Q (C-NAV data+pilot)
- ☐ GALILEO
  - ☐ Galileo E1 OS (I/NAV data+pilot)
  - ☐ Galileo E1 PRS (proprietary message)
  - ☐ Galileo E5a OS (F/NAV data+pilot)
  - ☐ Galileo E5b OS (I/NAV data+pilot)
  - ☐ Galileo E6 PRS (proprietary message)
- ☐ SBAS
  - ☐ SBAS L1 C/A (Coarse/Acquisition)
- ☐ GLONASS
  - ☐ GLONASS G1 C/A (Coarse/Acquisition)
  - ☐ GLONASS G2 C/A (Coarse/Acquisition)
- ☐ QZSS
  - ☐ QZSS L1 C/A (Coarse/Acquisition)
  - ☐ QZSS L1 SAIF (availability and integrity enhancement)
  - ☐ QZSS L2 C (C-NAV moderate+long)
  - ☐ QZSS L5 I/Q (C-NAV data+pilot)
  - ☐ QZSS E6 LEX (proprietary message)
- ☐ BEIDOU
  - ☐ Beidou B1 I (D1-NAV data)
  - ☐ Beidou B2 I (D1-NAV data)

Figure 8.1: GUI of GIPSIE® software

Figure 8.1 illustrates a part of the GUI, where the satellite systems and signals can be selected for simulation. More information on GIPSIE® can be found at TeleConsult Austria GmbH (2018a).

A spoofer needs to know an approximate position of its victim receiver in order to take it over. By correctly adapting the code-offset and Doppler in its broadcast signals, the target receiver can be captured. Within the simulation environment GIPSIE®, the spoofer and receiver position can be defined. Furthermore, the target position can be set, which is the spoofer's assumed position of its victim. If the spoofer has good knowledge of the victim receiver, the receiver and target position overlap. In case the receiver is moving randomly, the trajectory is unknown and thus the broadcast signals do not perfectly match with authentic signals in the two-dimensional correlation domain.

This condition is illustrated in Figure 8.2. Here, the assumed target point is not aligned with the actual receiver position. This results in an additional code-offset Δ_ρ. The distance between the spoofer and the receiver (victim) is denoted as Δ_{SV}, while the distance between spoofer and target is Δ_{ST}.

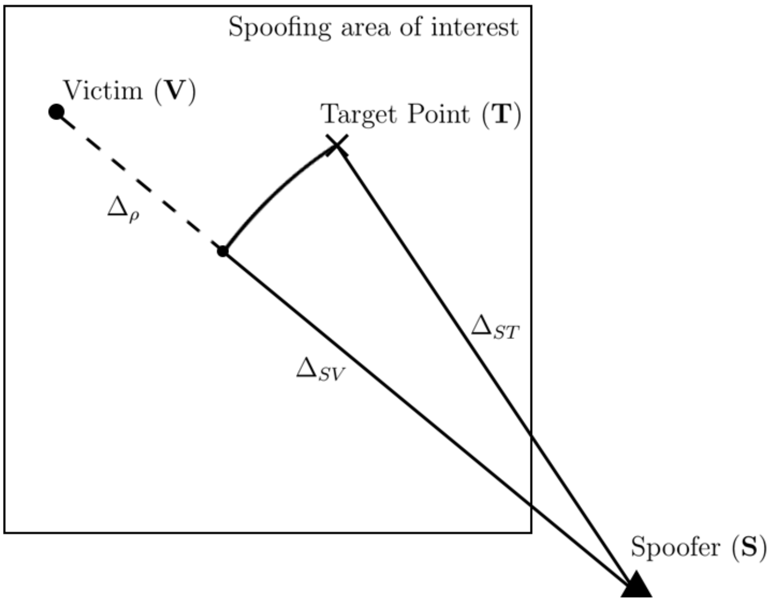


Figure 8.2: Spoofing scheme of GIPSIE® software

In case the spoofer has no precise knowledge of the receiver position, an area of interest can be defined, where the victim's location is assumed. Within this area, the spoofer can vary its code-offset over time to move its correlation peak. The variation in the code-domain also changes the Doppler. This is denoted as code-sweep. By applying this strategy, the receiver can be captured once the authentic and spoofed peaks fall together for all satellites. Due to random movement, the receiver experiences additional Doppler effects in its received signal. These signals have the same spatial signature, if emitted by a single source. This makes a detection possible, if the spoofer has no exact knowledge of the receiver trajectory and thus, cannot cancel out these additional effects.

Recorded real-world data A measurement campaign was conducted at the military training area at Seetaler Alpe, Styria in September 2018 in the cause of the DECODE project together with the Austrian armed forces. With permission of the Oberste Fernmeldebehörde (OFB) and Bundesministerium für Verkehr, Innovation und Technologie (BMVIT), different test measurements for jamming and spoofing attacks were set up and executed. The attacks were recorded by high-end GNSS receivers as well as smartphones that support raw GNSS measurement logging.

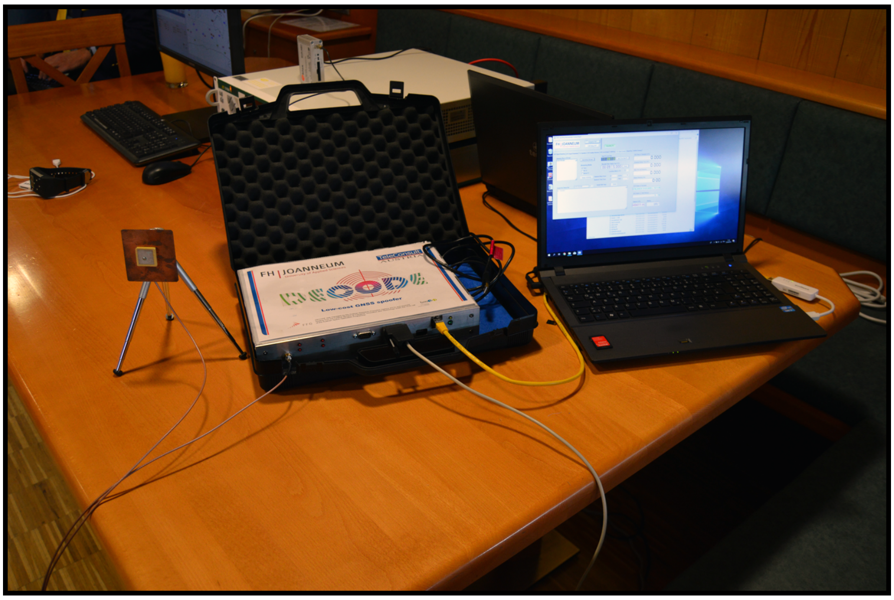
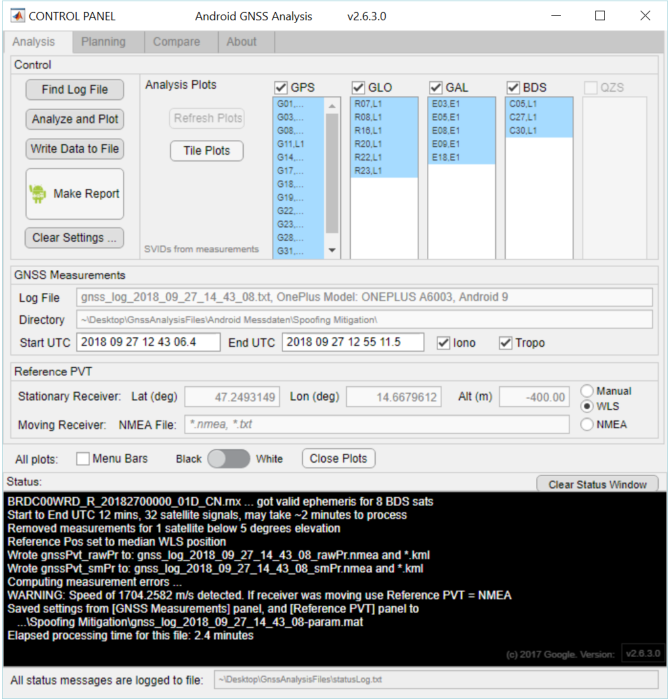


Figure 8.3: DECODE spoofing hardware

The used spoofing hardware, which was developed within the DECODE project, is shown in Figure 8.3. In general, a scenario for a predefined receiver trajectory is simulated with GIPSIE® for a chosen time span. Actual satellite ephemeris for the scenario are utilized for generating the signals contained in the binary IF file. The scenario is transferred to the hardware, which then upconverts the IF signals to RF and broadcasts them via an antenna. For deploying a time-synchronous spoofing attack, a GNSS reference receiver is connected to the hardware to provide precise timing information based on authentic satellites. The hardware is operated by a computer to adjust the starting point of the attack as well as the transmission power of the fake signals and other parameters.

For this thesis, an analysis of spoofing attacks on smartphones was conducted. In May 2016, Google announced the availability of GNSS raw measurements for the operating system Android 7. For the first time, developers could access carrier and code measurements together with decoded navigation messages from mass-market devices (European Global Navigation Satellite Systems Agency 2018b). The usage of raw GNSS measurements on smartphones has several advantages such as an increased performance, where more advanced GNSS processing techniques can be applied. These properties were reserved to professional receivers in the past.



☑ GPS: G01,... G03,... G08,... G11,L1 G14,... G17,... G18,... G19,... G22,... G23,... G28,... G31,...
☑ GLO: R07,L1 R08,L1 R16,L1 R20,L1 R22,L1 R23,L1
☑ GAL: E03,E1 E05,E1 E08,E1 E09,E1 E18,E1
☑ BDS: C05,L1 C27,L1 C30,L1
□ QZS

GNSS Measurements

Log File: gnss_log_2018_09_27_14_43_08.txt, OnePlus Model: ONEPLUS A6003, Android 9
Directory: ~\Desktop\GnssAnalysisFiles\Android Messdaten\Spoofing Mitigation\
Start UTC: 2018 09 27 12 43 06.4 End UTC: 2018 09 27 12 55 11.5 ☑ Iono ☑ Tropo

Reference PVT

Stationary Receiver: Lat (deg) 47.2493149 Lon (deg) 14.6679612 Alt (m) -400.00
Moving Receiver: NMEA File: *.nmea, *.txt
○ Manual ● WLS ○ NMEA

All plots: □ Menu Bars Black ○ White

Status:

```
BRDC00WRD_R_20182700000_01D_CN.rnx ... got valid ephemeris for 8 BDS sats
Start to End UTC 12 mins, 32 satellite signals, may take ~2 minutes to process
Removed measurements for 1 satellite below 5 degrees elevation
Reference Pos set to median WLS position
Wrote gnssPvt_rawPr to: gnss_log_2018_09_27_14_43_08_rawPr.nmea and *.kml
Wrote gnssPvt_smPr to: gnss_log_2018_09_27_14_43_08_smPr.nmea and *.kml
Computing measurement errors ...
WARNING: Speed of 1704.2582 m/s detected. If receiver was moving use Reference PVT = NMEA
Saved settings from [GNSS Measurements] panel, and [Reference PVT] panel to
  ...\Spoofing Mitigation\gnss_log_2018_09_27_14_43_08-param.mat
Elapsed processing time for this file: 2.4 minutes
```

(c) 2017 Google. Version: v2.6.3.0

All status messages are logged to file: ~\Desktop\GnssAnalysisFiles\statusLog.txt

Figure 8.4: Google GNSS Analysis Tool®

The GNSS Analysis Tool®, provided by Google, offers an evaluation of the raw measurements together with a PVT computation. The application is a desktop GUI, based on the coding language MATLAB, realised using MATLAB RUNTIME. Figure 8.4 shows the main window of the application. Furthermore, Google provides the open source code of the tool for comprehending certain processing algorithms and offering the possibility to extend it by various additional components. For more information refer to European Global Navigation Satellite Systems Agency (2018b).

8.2 Simulation results

Spoofing mitigation For testing the developed mitigation algorithm presented in Chapter 7, which is based on the observation of residual Doppler correlations, different simulations have been made within the GIPSIE® software. For every test scenario, a complex digital signal with an IF of 0 MHz and a sampling frequency of 4.092 MHz has been generated. Within these simulations, GPS C/A code measurements on the L1 frequency have been processed. The time span for each test scenario was around 2 minutes. For the first test case, an authentic scenario has been simulated, where eight GPS satellites were visible for an arbitrary receiver trajectory. The receiver's average velocity was 40 km/h. Figure 8.5 shows the ellipsoidal coordinates (WGS84) of the receiver's trajectory, which have been calculated using the authentic measurements by the SDR.

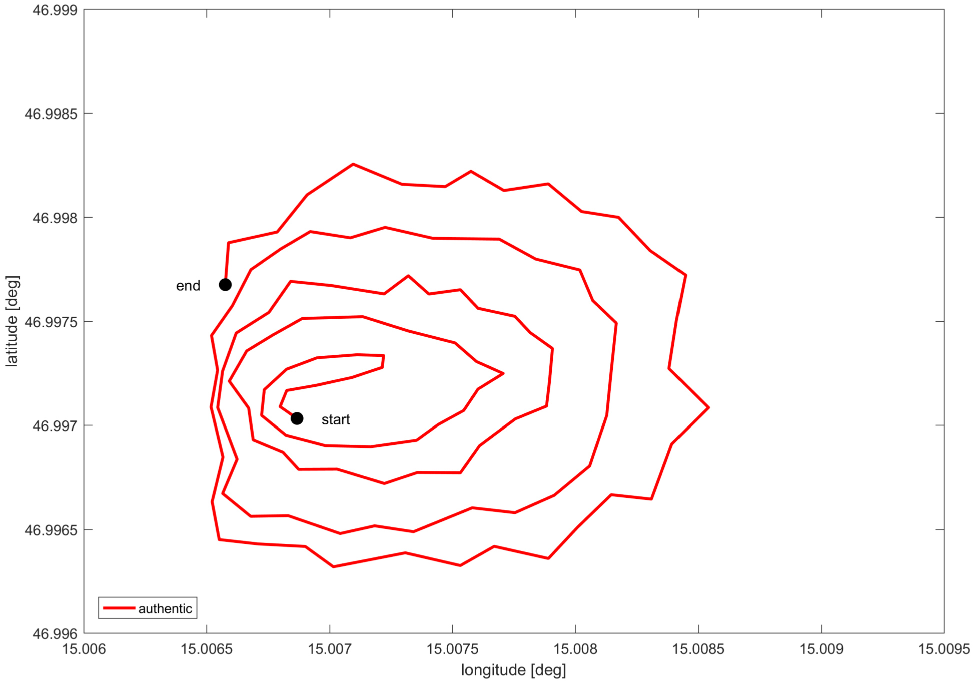


Figure 8.5: Authentic receiver trajectory in case of no spoofing

Due to the receiver's movement relative to the spoofer, additional Doppler effects with a highly correlated pattern should be visible during an attack. Within the GNSS receiver, the theoretical Doppler can be estimated based on the position and velocity of the satellites and receiver, respectively, as well as the clock drifts and ionospheric effects. By subtracting all impacts from the Doppler measurements resulting from the tracking loop, residual values remain. These values scatter normally distributed around zero, in case of an authentic scenario, without showing high correlations or systematic behavior. The scattering range of the values is dependent on the tracking loop's accuracy of the receiver. Figure 8.6 shows the residual Doppler of the simulated spoofing-free scenario, where no significant deviations are present for the whole time span.

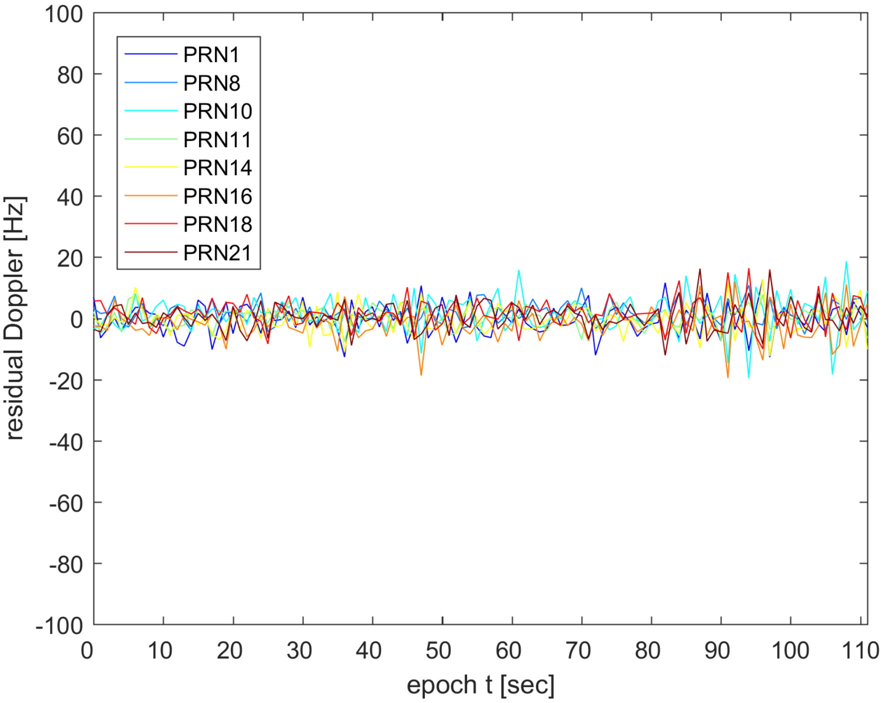


Figure 8.6: Residual Doppler measurements in case of no spoofing

The Doppler contributions of satellite and receiver motion as well as satellite and receiver clock drift were considered. The influences of the clock drifts were computed by multiplying the drift coefficients with the nominal carrier frequency of the signal and read

$$\begin{aligned}\Delta f^s_{\text{clock}} &= a^s_1 \cdot f^s,\\ \Delta f^r_{\text{clock}} &= a^r_1 \cdot f^s.\end{aligned} \tag{8.1}$$

The satellite clock drift coefficient a_1^s is transmitted within the navigation data message together with two further coefficients a_0^s and a_2^s, corresponding to the bias and drift rate. By forming a polynomial of second order with these coefficients, the satellite clock error is modeled and applied on the measurements. The receiver clock drift coefficient a_1^r can be estimated together with the receiver velocity by utilizing range-rate measurements in a least square adjustment, similar to the position solution stated in Equation 2.6. By utilizing this information, the differences between the measured and theoretical Doppler can be calculated.

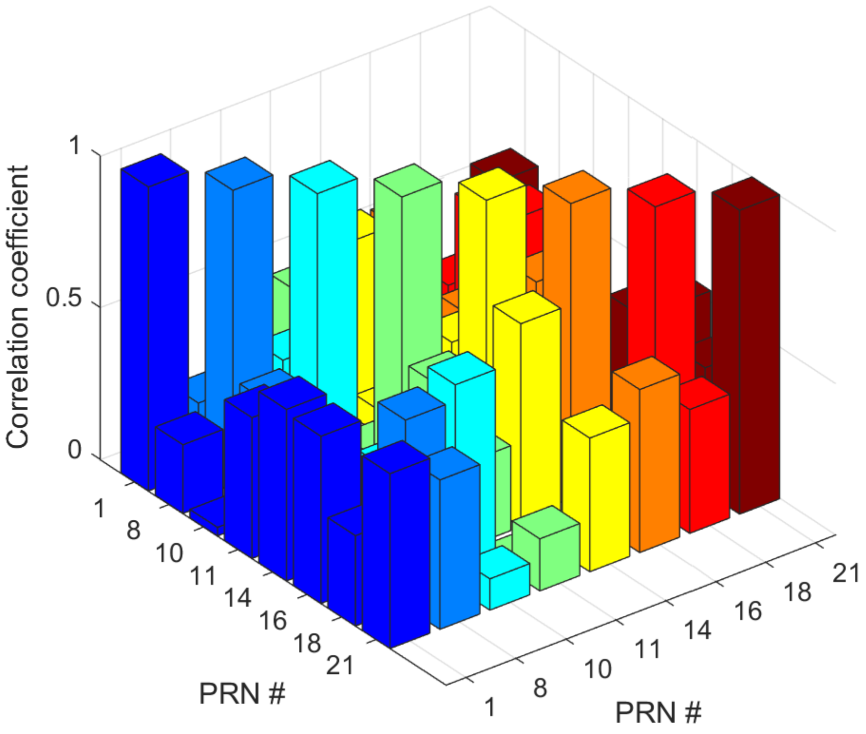


Figure 8.7: Residual Doppler correlation coefficients in case of no spoofing

Figure 8.7 depicts the computed absolute correlation coefficients of the signal's residual Dopplers. As expected, no significant correlations exist, meaning all signals origin from different sources. Nonetheless, some signal pairs show higher correlations than others. The reason for this behavior is due to the fact, that the satellites of these pairs have similar azimuth and elevation angles, resulting in a higher spatial correlation of their signal's signature.

The satellite skyplot of the authentic scenario in Figure 8.8 shows that several space vehicles share a similar direction of arrival. For example, PRN1 and PRN14 are spatially close to each other, resulting in the high correlation bar in Figure 8.7. PRN16 and PRN18 share almost the same elevation but a different azimuth. This results in higher negative correlation values. Due to the fact, that only the absolute correlation coefficents are plotted in Figure 8.7, the negative values are also shown as positive.

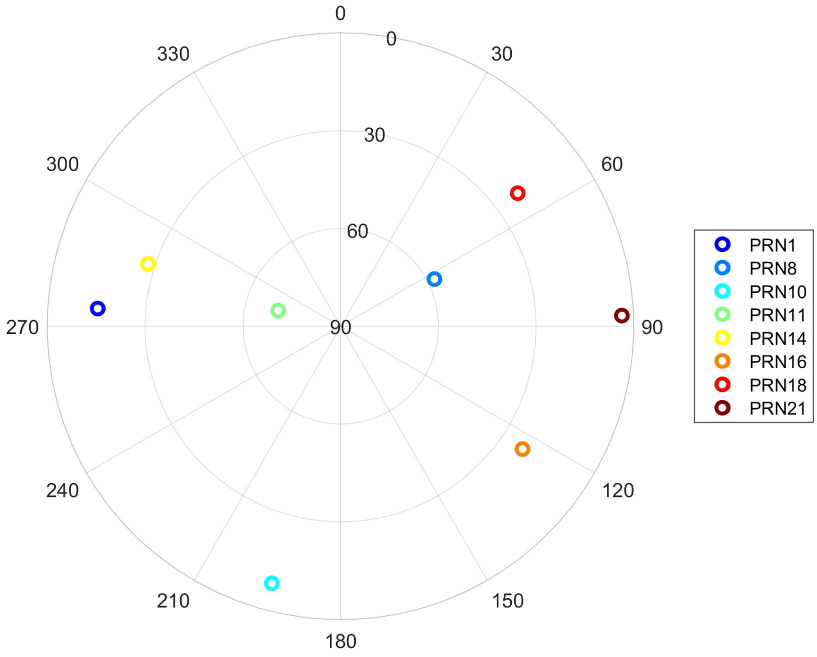


Figure 8.8: Skyplot of GPS satellites of simulated scenario

For the second scenario, a spoofing attack was simulated, where the relative power of the counterfeit signals was 10 dB higher compared to the authentic ones. The spoofed receiver's trajectory shared to same path as the real one for the first 20 seconds. Afterwards, it is diverging from the authentic path leading the victim to a false destination. Figure 8.9 shows the authentic and spoofed receiver trajectories, respectively. Furthermore, the target path, which is set to be the same as the spoofed receiver trajectory, is displayed.

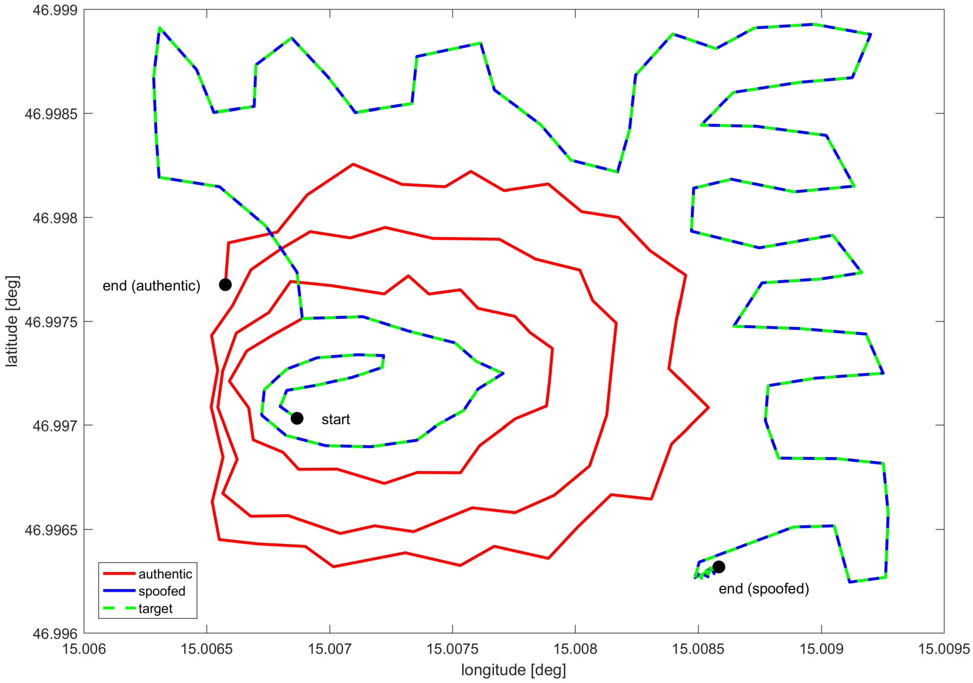


Figure 8.9: Trajectories in case of spoofing (target path equal to spoofed path)

As already explained in Section 8.1, the target position is the spoofer's assumed position of its victim. For this spoofing scenario, the spoofer has no knowledge of the real receiver's path. Here, the spoofed and the target trajectory are overlaid. This property results in a high correlation between the residual Doppler values as soon as the authentic and spoofed paths diverge. Figure 8.10 shows the Doppler residuals and their corresponding correlation coefficients, where significantly high correlated patterns are visible in the residuals. Therefore, the correlation coefficients for all pairs are one.

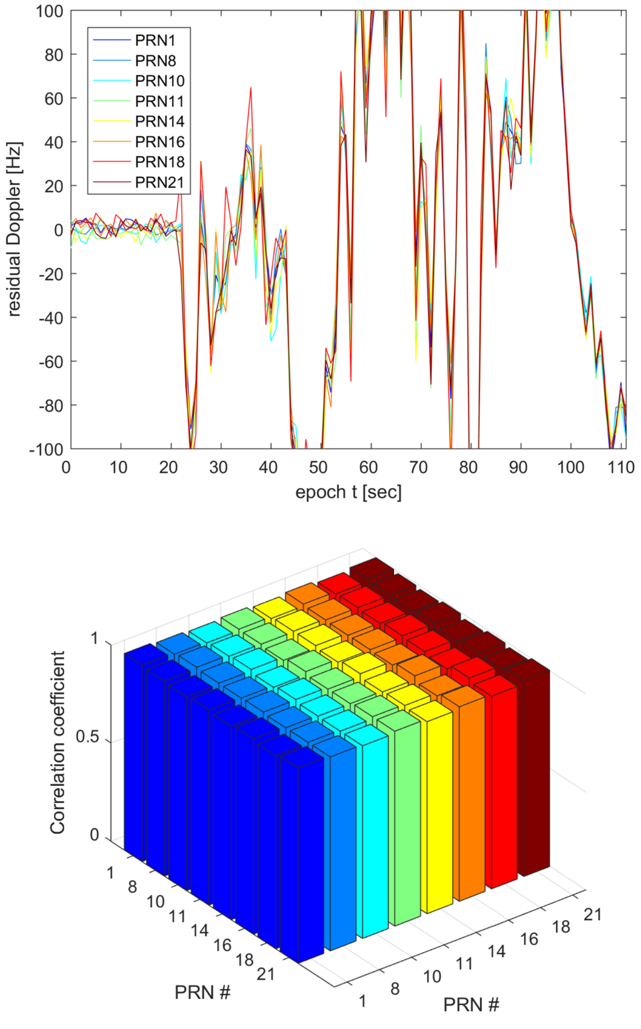


Figure 8.10: Doppler residuals (top) and correlations coefficients (bottom) in case of spoofing (target path equal to spoofed path)

The third scenario's properties are the same as the second one's with one difference: now the target path is the same as the authentic one from the receiver. This means, the spoofer now has knowledge of the receiver's movement and can thus alter its signals to compensate the additional Doppler effects induced by the relative movement. Figure 8.11 shows again the spoofed and authentic trajectories but now the target path is overlaid with the real path.

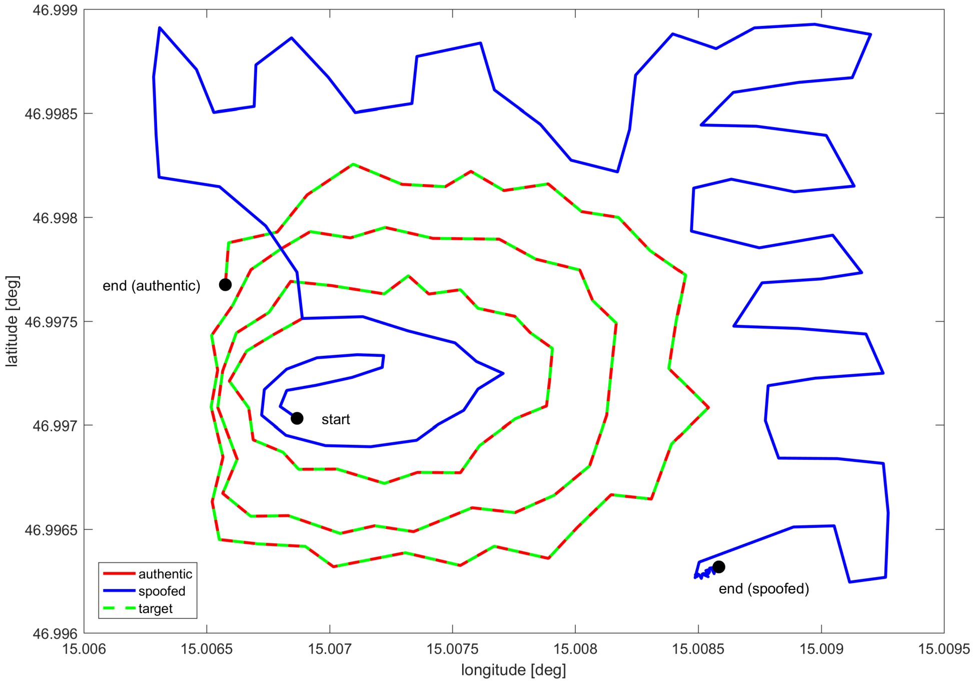


Figure 8.11: Trajectories in case of spoofing (target path equal to authentic path)

This measure ensures that no significant correlations between the Doppler residuals exist, as Figure 8.12 shows. The fact, that the spoofer has to know the receiver's path beforehand and that the movement of the receiver can be arbitrary, makes a full disguise of the spoofer in a real-world attack impossible, since additional Doppler effects due to the relative movement cannot be fully modeled.

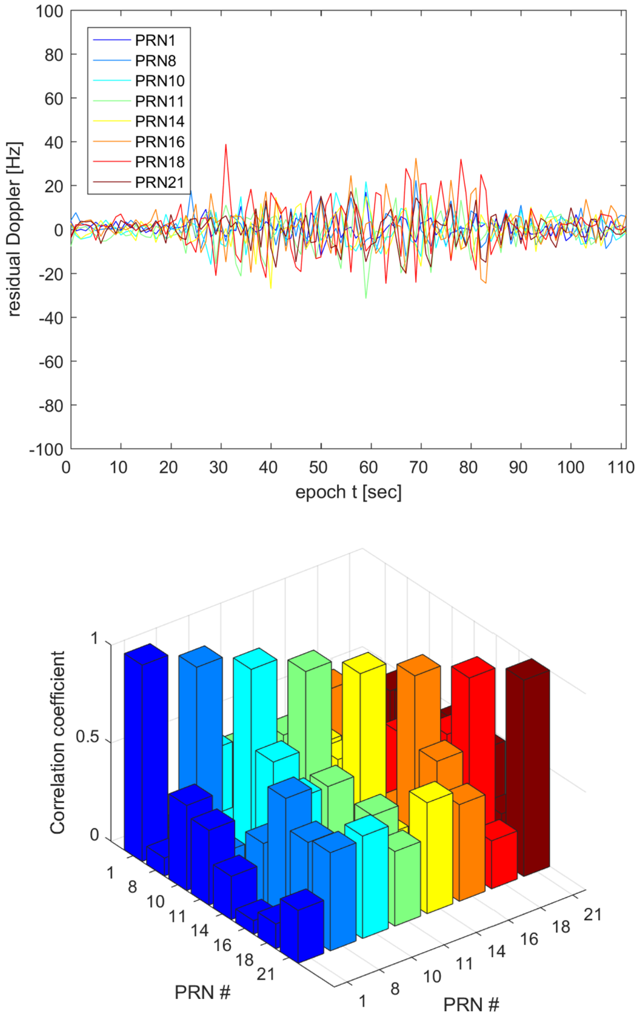


Figure 8.12: Doppler residuals (top) and correlations coefficients (bottom) in case of spoofing (target path equal to authentic path)

For investigating the performance of the proposed algorithm in Chapter 7, two scenarios, an authentic and a spoofing attack, have been generated. The used IF was 0 MHz and the sampling frequency was 4.092 MHz for both scenarios. Again, only GPS C/A code signals on the L1 frequency have been simulated for eight satellites. This time the simulated receiver movement was an arbitrary motion pattern with an average velocity of 40 km/h. For the spoofing attack, the target and spoofed position were both set static. These two scenarios imitated all signals tracked inside a SDR during an attack. In Figure 7.1, the flow chart of the proposed algorithm shows a coarse classification of the signals based on their carrier-to-noise power density ratio. In case a false classification was made, a further distinction based on iteration was executed. For this test, a worst case scenario was generated, where two sets (eight satellites per set) were misclassified by the algorithm based on the C/N$_0$ values. This resulted in each set consisting of four authentic and four spoofed signals.

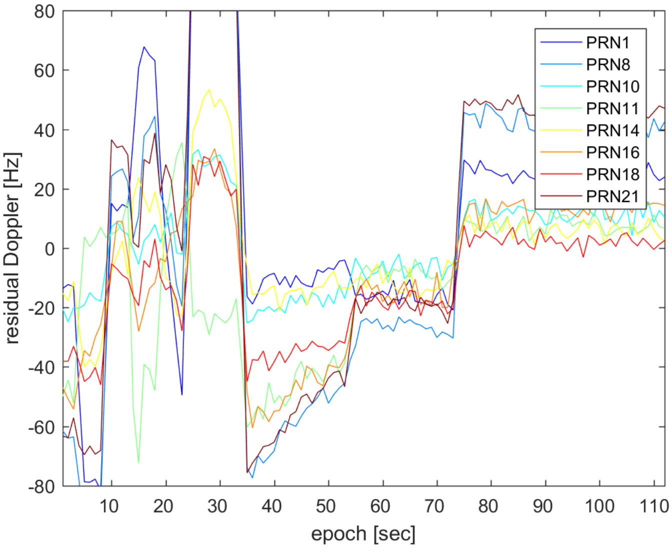


Figure 8.13: Doppler residuals for misclassified PVT set (50% authentic, 50% spoofed)

Figure 8.13 shows the resulting Doppler residuals for a time span of around two minutes, where the theoretical Doppler values were processed through a false PVT output due to misclassification. PRN1 to PRN11 are authentic satellites, whereas PRN14 to PRN21 are spoofed.

Afterwards, the algorithm started its sorting process. For more details on the single steps of the mitigation algorithm refer to Chapter 7. The whole time series was divided into data snapshots of equal length, where each snapshot was processed individually.

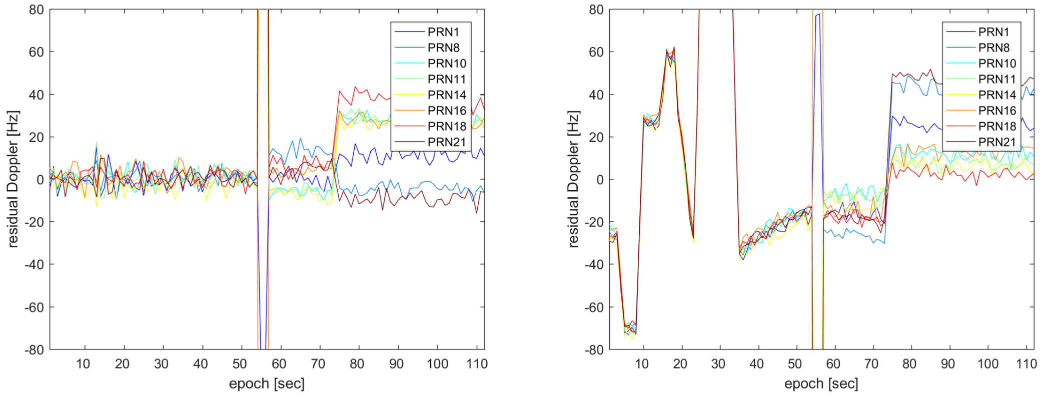


Figure 8.14: Rearranging misclassified authentic (left) and spoofed (right) PVT set

Figure 8.14 shows Doppler residuals of the two processed data sets, where the first half of the time series has already been correctly sorted. As can be seen on the left, no correlations between the single signal pairs are present. After 55 seconds, the Doppler residuals on the right exceed the values of ±80 Hz due to the inconsistency of the data sets. Figure 8.15 shows the final result after the algorithm has processed all data snapshots. As expected, the algorithm has correctly classified the tracked signals. The Doppler residuals show a highly correlated pattern for the spoofed set, representing the relative motion of the receiver. The sudden jumps in the values occur whenever the receiver changed its direction in the trajectory.

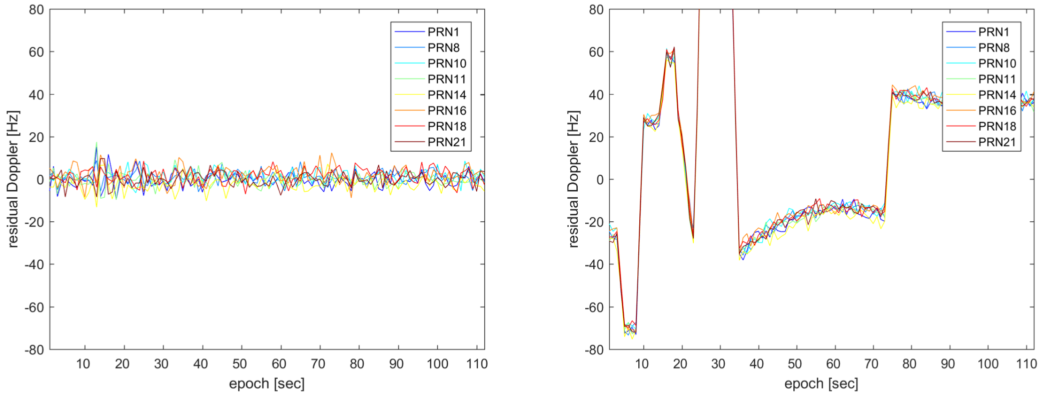


Figure 8.15: Correctly sorted authentic (left) and spoofed (right) PVT set

Direction of arrival The DOA finding based on the MUSIC algorithm described in Chapter 6 was tested by using a simulated antenna array generated in GIPSIE$^{\circledR}$. For investigation purposes, three spoofers have been simulated to test the performance and accuracy of the algorithm. Table 8.1 shows the position of the center of the uniform circular array (UCA), as well as the radius and the number of used antennas for the circle.

Table 8.1: DOA properties of simulated UCA

	North [deg]	East [deg]	Height [m]	Number of array elements (antennas)	Array radius [m]
UCA	47	15	350	8	0.09

The positions of the three spoofers as well, as the reference azimuth and elevation between the center of the UCA and the respective spoofer are listed in Table 8.2. Furthermore, the relative power between the emitted counterfeit signals and the authentic ones is given along with the distances. As can be seen, the distances between every spoofer and the center of the UCA is the same. Note that all positions are given as WGS84 coordinates.

Table 8.2: DOA properties of simulated spoofers

	North [deg]	East [deg]	Height [m]	Azimuth [deg]	Elevation [deg]	Rel. power [dB]	Distance [m]
SP1	46.99477	15.00739	938	136	36	20	1000
SP2	47.00055	15.00081	1346	45	85	16	1000
SP3	47.00372	14.98834	558	295	12	18	1000

A UCA-RB-MUSIC estimation has been performed for three scenarios, where signals from one, two and three spoofers where arriving at the array. For peak searching, a grid resolution of 0.5 degrees was used. Beamforming was applied, to increase the performance of the algorithm as well, as the spatial resolution of the spectrum in case of coherent signals. Data snapshots of one second were used to establish the sample covariance matrix $\mathbf{R}_x$. The preset sampling frequency for all simulations was 2.046 MHz. This resulted in a size of 2046000 complex signal samples for the covariance matrix.

Figure 8.16 shows the three-dimensional MUSIC spectrum with one spoofer (SP1) present. The algorithm determines a peak near the reference values for an azimuth of 136 degrees and elevation of 36 degrees (c.f. Table 8.2). The estimated azimuth angle is 136.5 degrees and the corresponding elevation is 36.5 degrees with a spoofer's relative signal power of 20 dB and a distance of 1000 m.

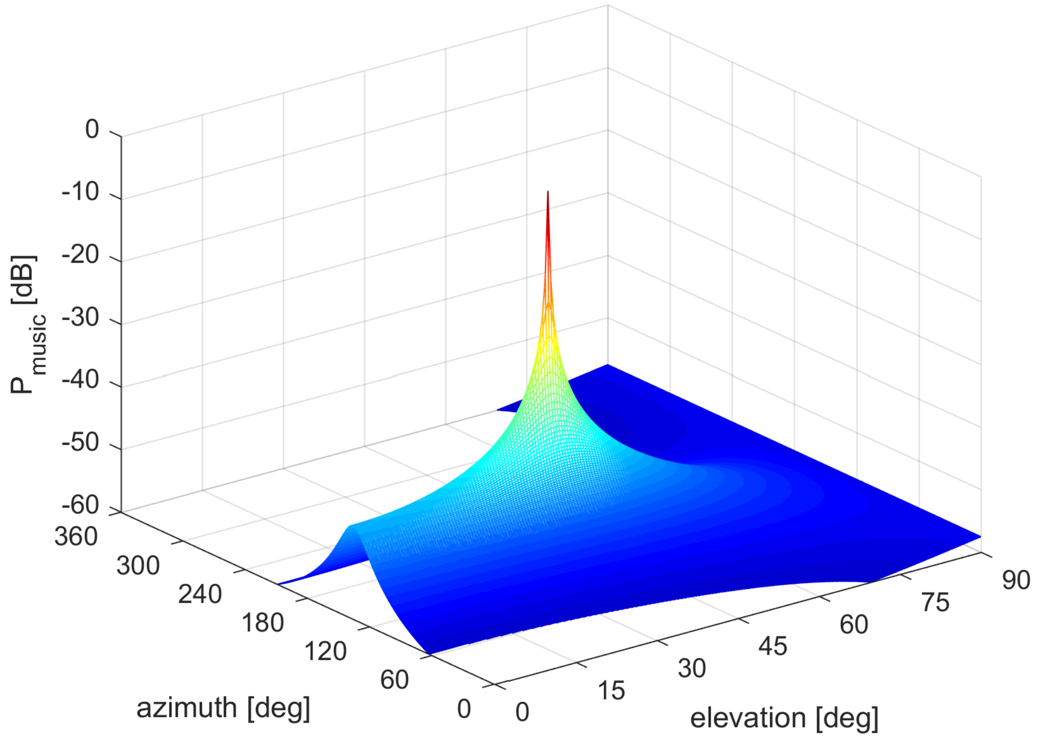


Figure 8.16: 3D MUSIC spectrum for one spoofer

The peak is clearly visible above the noise floor. By searching for the maximum inside the spectrum, the direction of arrival was determined.

Figure 8.17 depicts the two-dimensional spectrum respectively, making a visual determination of the estimated azimuth and elevation easier. The asymmetric structure of the spectrum along the elevation axis indicates that the accuracy of this angle is poorer compared to the azimuth. The right choice of the radius from the circular array is important for getting a proper result of the elevation during the computation. The connection between the radius and the elevation angle is stated in Equation 6.32.

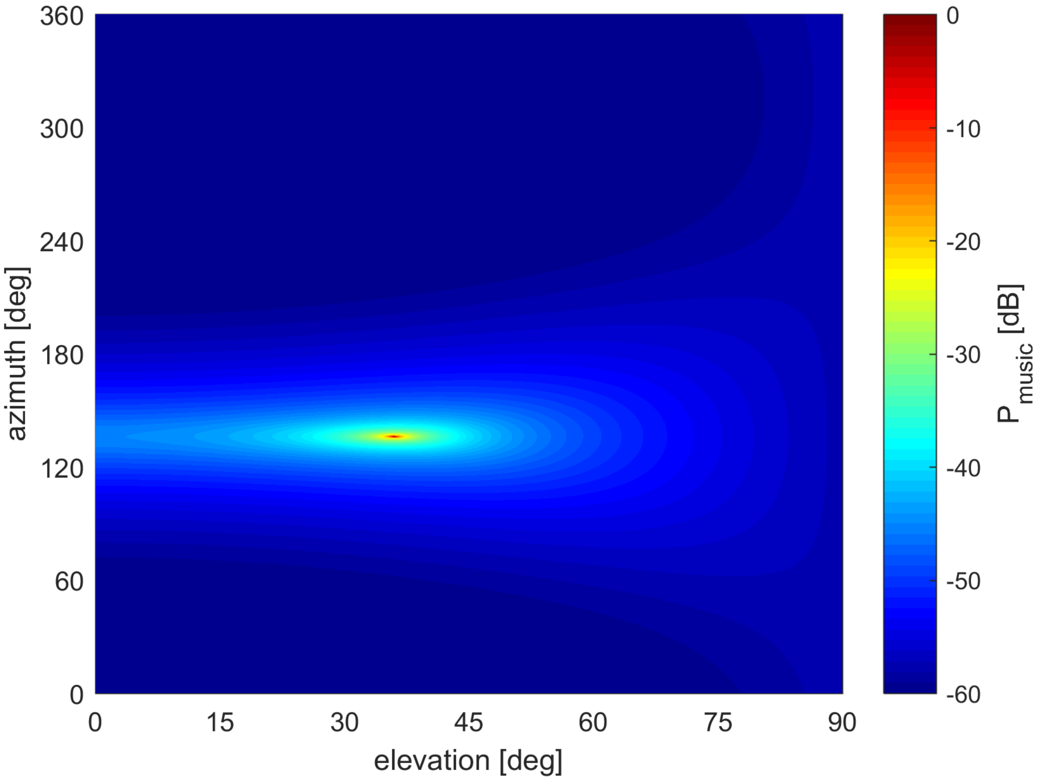


Figure 8.17: 2D MUSIC spectrum for one spoofer

In Figure 8.18, the 2D and 3D spectrum of a scenario of two broadcasting spoofers (SP1 and SP2) are shown. Again, the determination of the DOA resulted in clear maximums in the spectrum. Noticeable is a connecting region between the two peaks, where the power is significantly higher compared to the noise floor. This effect occurs due to a correlation between the two coherent signal sources. As already stated in Chapter 6, the maximum number of estimated signal sources equals the number of the set up antennas of the array. therefore, the estimated DOA from the two signal sources is well-handled by MUSIC with an eight element antenna array.

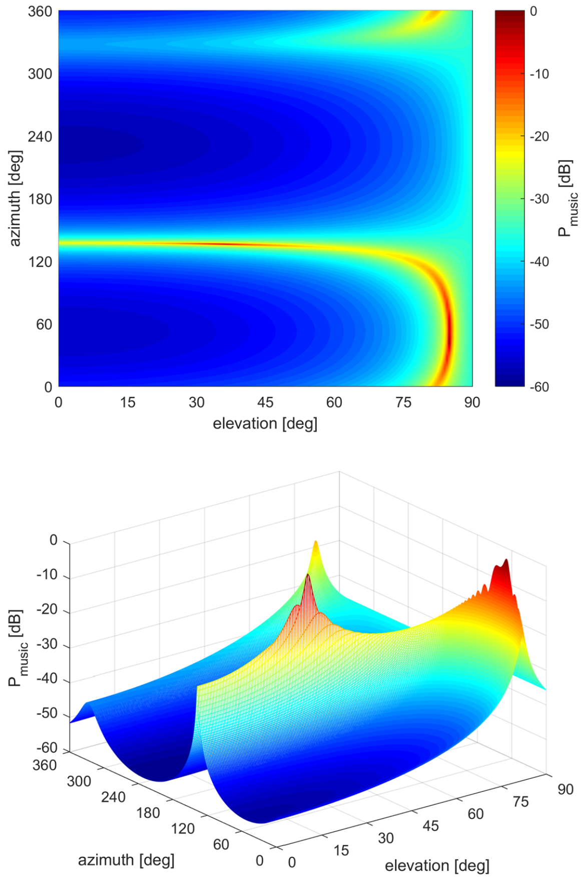


Figure 8.18: 2D (top) and 3D (bottom) MUSIC spectrum for two spoofers

The estimated azimuth and elevation angle for spoofer 1 (SP1) are 136.5 and 37 degrees and for spoofer 2 (SP2) 43.5 and 85.5 degrees, respectively.

For the third scenario, the presence of three spoofers was simulated. Figure 8.19 shows the according spectrum. Again, the algorithm had no problem determining the correct angle pairs of the sources. Remarkable is, that the second spoofer (SP2) has the worst resolution, especially in its azimuth. The reason for this is the weaker power of this spoofer compared to the others (4 dB weaker to SP1 and 2 dB weaker to SP3). Again, all present spoofers are correlated, with connecting regions where the spectrum is around -30 dB.

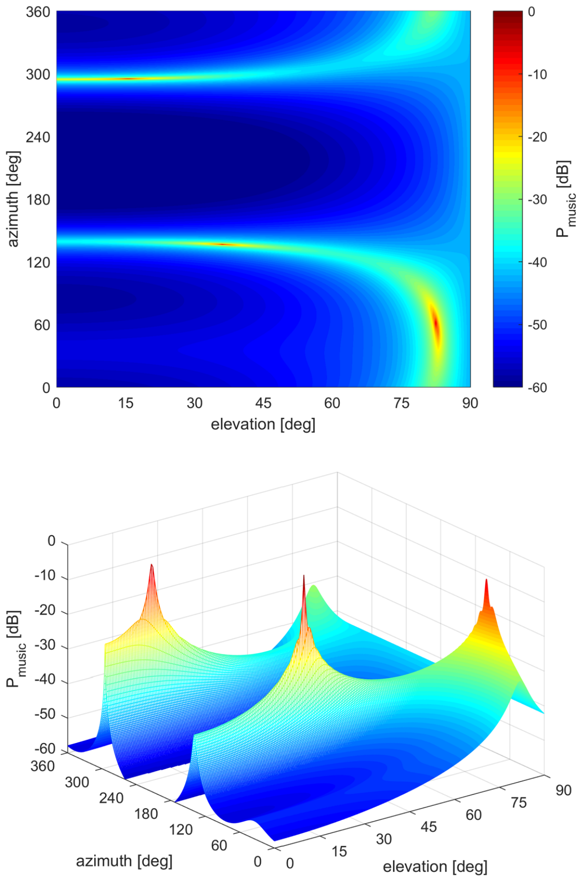


Figure 8.19: 2D (top) and 3D (bottom) MUSIC spectrum for three spoofers

For investigating the performance of the MUSIC algorithm in respect to the relative power of a spoofer, the root-mean-square error κ (RMSE) for the direction of arrival for different power levels has been evaluated. For this scenario, one spoofer (SP1) was emitting signals. The RMSE is computed by the reference DOA θ_{ref} and reads

$$\kappa = \sqrt{\frac{\sum_{k=1}^{n}(\hat{\theta}_k - \theta_{ref})^2}{n}}, \tag{8.2}$$

where $\hat{\theta}_k$ is either the estimated azimuth $\hat{\varphi}_k$ or the elevation $\hat{\vartheta}_k$ for a certain snapshot k. For evaluation purpose, DOA estimates for $n = 10$ data snapshots were executed. Therefore, the snapshot length was restricted to 0.1 seconds. The power of the spoofing signals in respect to the authentic ones was continuously decreased by 2 dB within the range of +20 to −10 decibels.

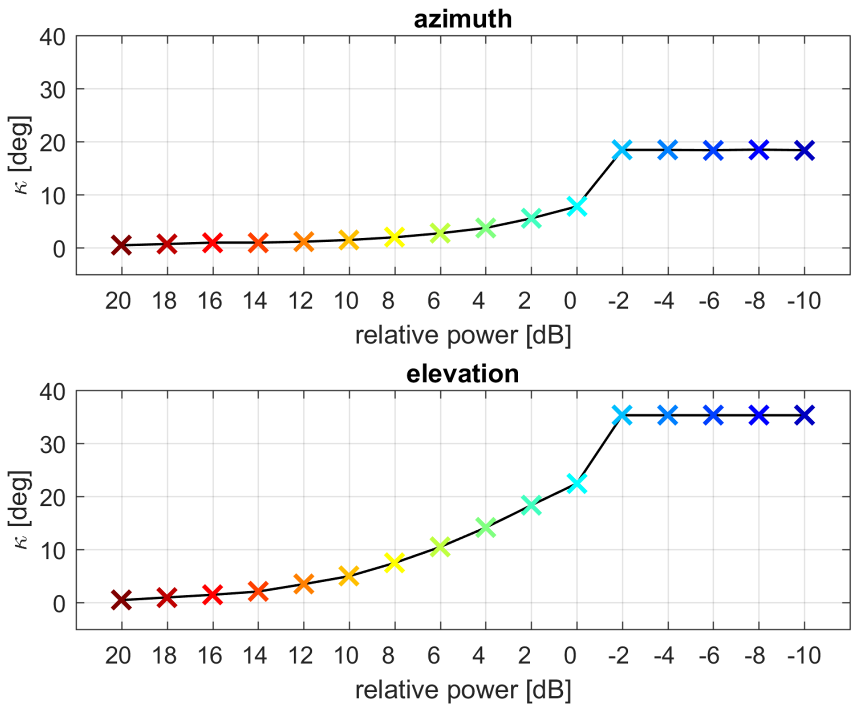


Figure 8.20: DOA RMSE for different power levels

Figure 8.20 shows the calculated RMSE. As can be seen, a decrease in power has the similar impacts on the accuracy for both angles. In general, the accuracy of the elevation angle is lower by the factor of 2. One reason is the relation between the array radius and the elevation angle, which has a greater dependency on the signal power. In order to acquire proper results for both angles, the relative power of the spoofer compared to the satellite signals has to be over 10 dB. After the spoofer's power is below the one of the satellites, the RMSE for both angles does not change anymore. At this point, the counterfeit signals are too weak compared to the authentic signals and the MUSIC algorithm esimates the DOA parameters for the satellite with the strongest signal power.

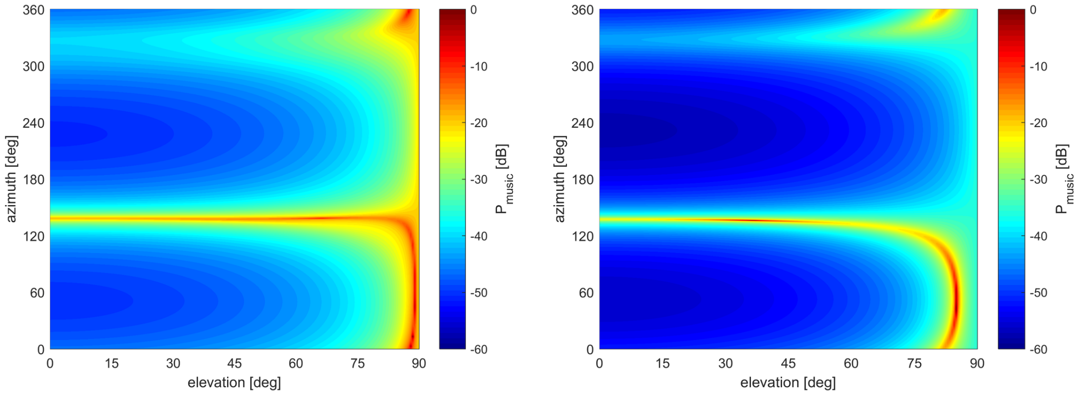


Figure 8.21: DOA element space (left) vs. real beamspace (right)

Comparing the 2D standard element space spectrum with the 2D real beamspace spectrum with three present spoofers in Figure 8.21, the element space spectrum of the DOA angles shows a higher noise floor. Moreover, no FFT based spectrum calculation can be executed, meaning the element space version has a higher computation time. Also, the resolution of the peaks is decreased significantly, resulting in less accurate values for the estimated angles.

In case, two sources are coherent and thus, spatially correlated, both versions of the MUSIC algorithm (element space and real beamspace) fail. This effect is depicted in Figure 8.22, where the MUSIC spectrum containing spoofer SP1 with an azimuth of 136 and 36 degrees and a second spoofer with 139 and 39 degrees, respectively, is visible. To overcome this issue, spatial smoothing is advised. Wax and Sheinvald (1994) has developed a strategy for spatial smoothing of coherent signals in the case of uniform circular arrays.

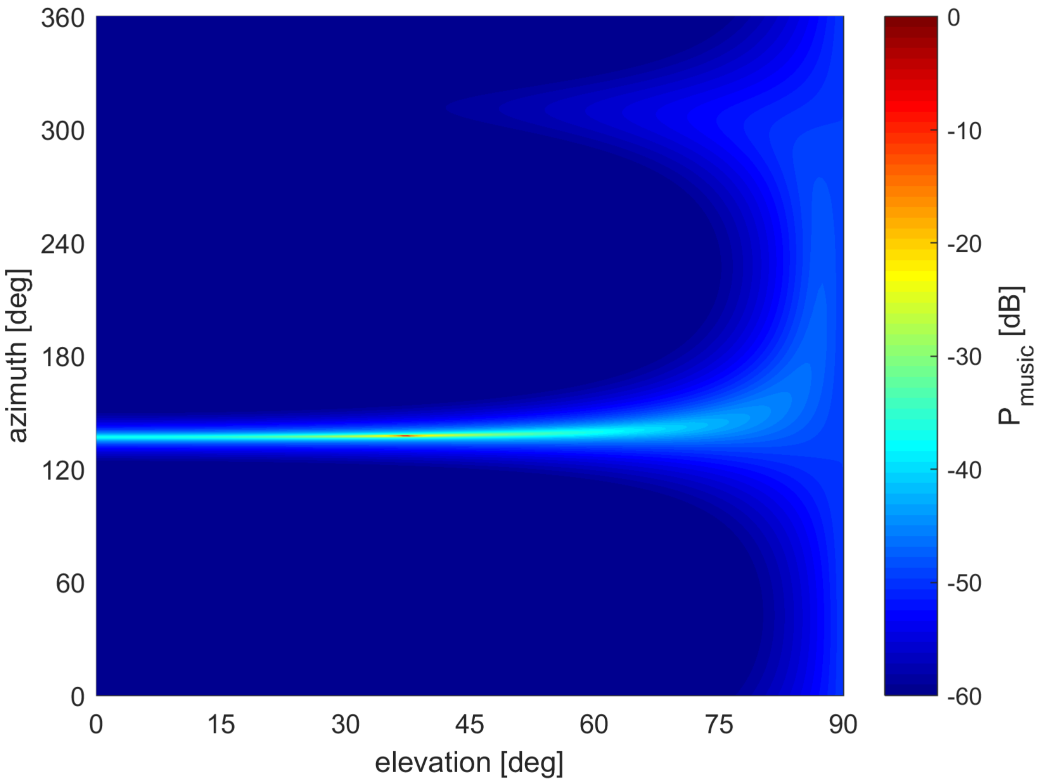


Figure 8.22: DOA MUSIC estimation for two spatially correlated spoofing sources

8.3 Real-world tests

For generating a real-world recorded data set, a spoofing scenario was simulated and broadcast at the military training area Seetaler Alpe. For the scenario, a spoofed receiver trajectory in the shape of an eight was created. The spoofing attack was recorded by an Android OnePlus 6 A6003 smartphone that supports GNSS raw measurement logging. The starting point of the simulated receiver path was at the position of the smartphone. After the attack was started, the spoofed position was moved towards north-east, doing a bow after around 1 km and coming back to the initial position. There, the counterfeit correlation peak fell together with the authentic one and stayed for a few seconds until it moved again heading south-west this time. In the end, a closed trajectory in the shape of an eight with a diameter of around 2 km was done. Figure 8.23 shows the aerial view of the spoofed receiver path.

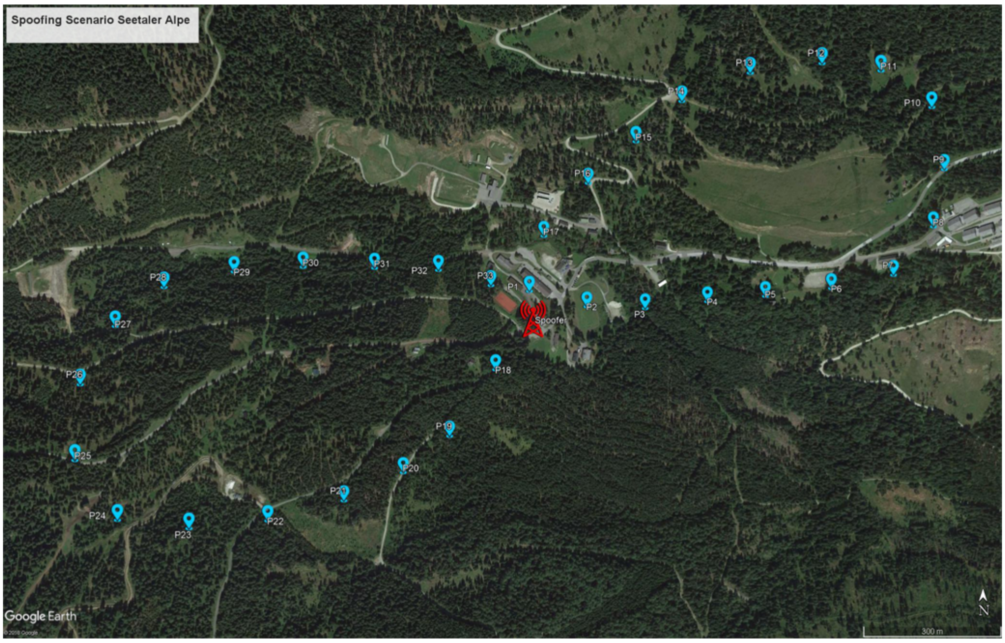


Figure 8.23: Simulated spoofing scenario at Seetaler Alpe (overlaid with Google$^{\text{TM}}$ Earth)

By stopping the spoofed peak at the same position as the authentic one, the spoofer had several chances to take over the receiver. For this scenario, a signal with an IF of 0 MHz and a sampling frequency of 2.046 MHz was generated and broadcast. Moreover, only GPS C/A code signals on the L1 frequency were spoofed, whereas other GNSS bands and signals were ignored. The attack had a total duration of 10

minutes. The single frequency smartphone measurement logging was started around two minutes before the launch of the spoofing attack. Throughout the attack, the smartphone was moved around in order to induce a spatial correlation on the received spoofing signals. Due to technical issues, only a time asynchronous attack could be conducted. This had several influences on the processed measurements by the victim receiver, which will be further explained in the following pages.
As described in Chapter 6, received power monitoring provides a good first insight on the signal's characteristics. Therefore, a look at the received C/N_0 values for each satellite signal indicates an ongoing attack. In Figure 8.24 the mean values of the five strongest carrier-to-noise power density ratios of GPS, GLONASS and Galileo are depicted.

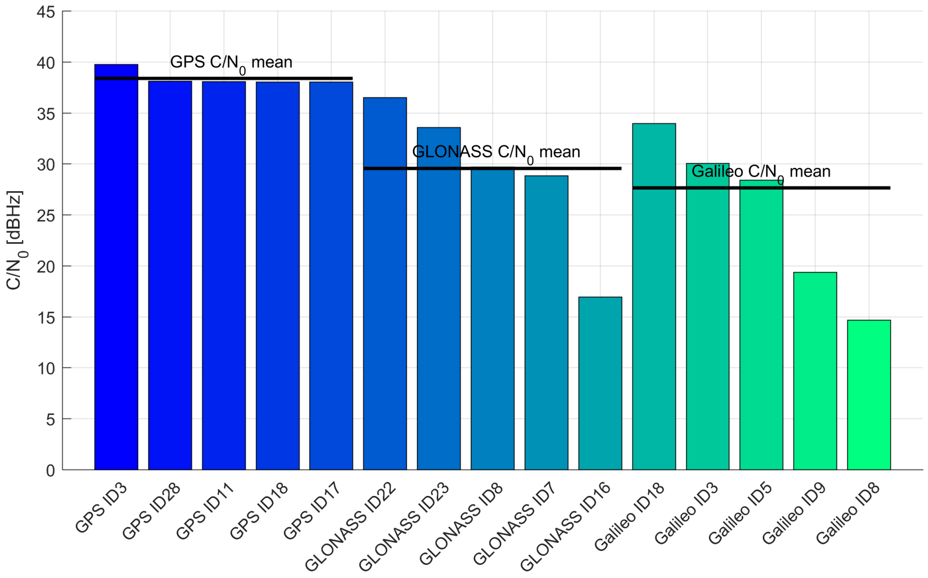


Figure 8.24: Strongest five C/N_0 for different GNSS during spoofing attack at Seetaler Alpe

While the latter two show normal power levels, the spoofed GPS satellites experience a significantly higher ratio. All five satellites show a C/N_0 of about 40 dBHz. Moreover, the mean values of each system indicate that spoofed signals were present. With GLONASS and Galileo signals being around the same power level, an offset of approximate 10 dB is seen between the mean values of them and the spoofed GPS signals. By increasing the spoofer's power, the counterfeit signals also serve as a kind of jammer, by pushing down the power levels from other systems.

By looking at the plotted time series of the C/N$_0$ values in Figure 8.25, a significant difference between the spoofed signals and the authentic can be seen in the power level. The black dotted line marks the start of the attack. At several epochs no observables from the GLONASS system were recorded anymore. The reason for that is the high transmitting power of the spoofer, which jamms the signals from other systems. This effect can be seen even clearer by looking at the Galileo measurements, where a total failure of the service happens during a big part of the attack. Figure 4.1 shows that the GLONASS G1 band has not the same center frequency as the GPS L1/Galileo E1 band. Therefore, the high spoofer power had less influence on the satellite signals of the Russian system.

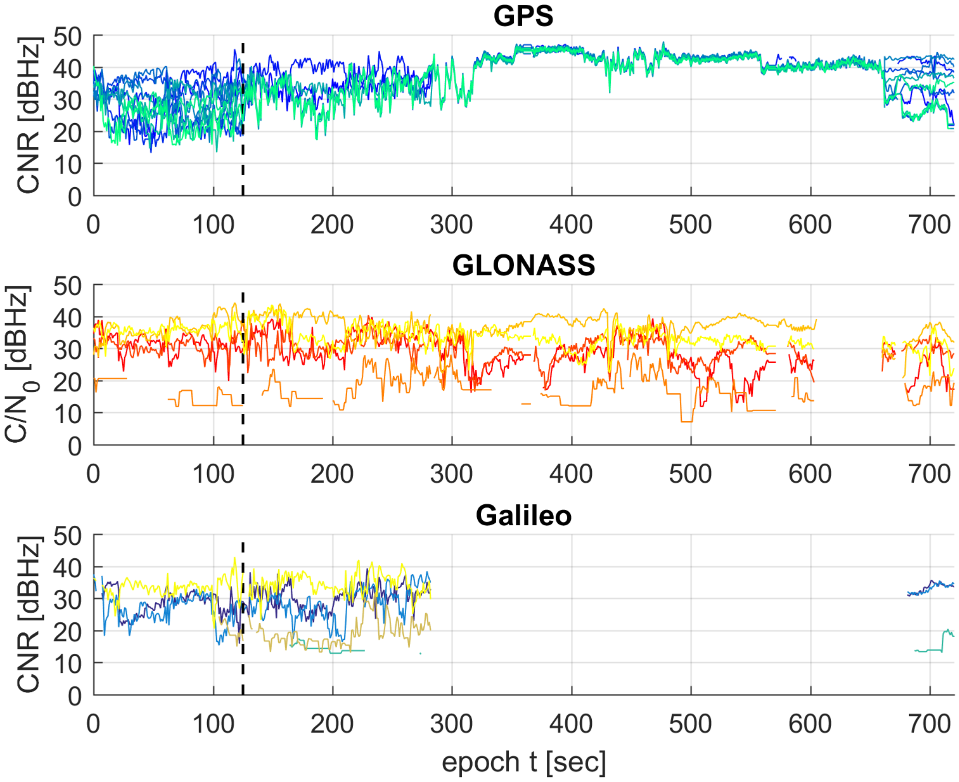


Figure 8.25: C/N$_0$ for different GNSS during spoofing attack at Seetaler Alpe

Remarkable is the fact, that also high correlations appear between the spoofed C/N$_0$ values, once the attack has been launched. Generally, the received C/N$_0$ from smartphones show a larger scattering range compared to that of conventional GNSS receivers, due to the poorer accuracy of the tracking loops.

Figure 8.26 illustrates the derived raw pseudoranges for the three systems. By looking at the GPS measurements, at the start of the attack (black dotted line) at epoch 125, all pseudoranges except for one are off by several thousand kilometers. This big offset results due to the time asynchronous broadcast (around half a second off) of the counterfeit GPS signals. Many receivers use the GPS time of week as a reference for processing the measurements from other GNSS. This property can also be seen here, where to pseudoranges from GLONASS experience the same offset at the exact moment, all GPS signals have been successfully taken over at epoch 280. The Galileo measurements are again not available, due to the spoofer's high power.

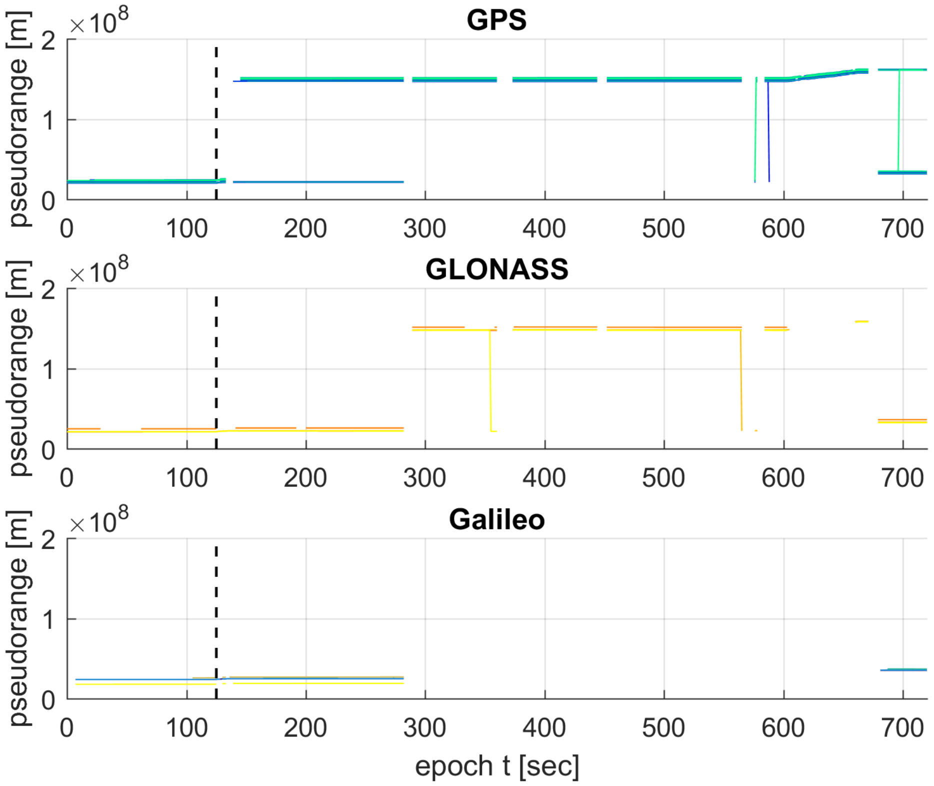


Figure 8.26: Raw pseudoranges for different GNSS during spoofing attack at Seetaler Alpe

At some points during the time series, even the GPS measurement logging stopped. At these points, the smartphone was moved too close to the spoofer transmitting antenna, resulting in a jamming of the receiver.

In order to compute a PVT during the spoofing attack, a constant time offset of 0.35 seconds, which resulted from the asynchronous broadcast, was applied to the logged receiver time stamps of the GPS measurements. Figure 8.27 shows the GPS only authentic and spoofed positions of the receiver, respectively. The spoofed positions were processed, after all GPS satellites have been successfully taken over. As can be seen, the trajectory which the receiver estimated, is the same as the one which was defined for the generation of the spoofer's IF signal in Figure 8.23. Again, the data gaps lead to a denial of the PVT computation at some epochs, which can be seen especially at the end of the spoofed trajectory.

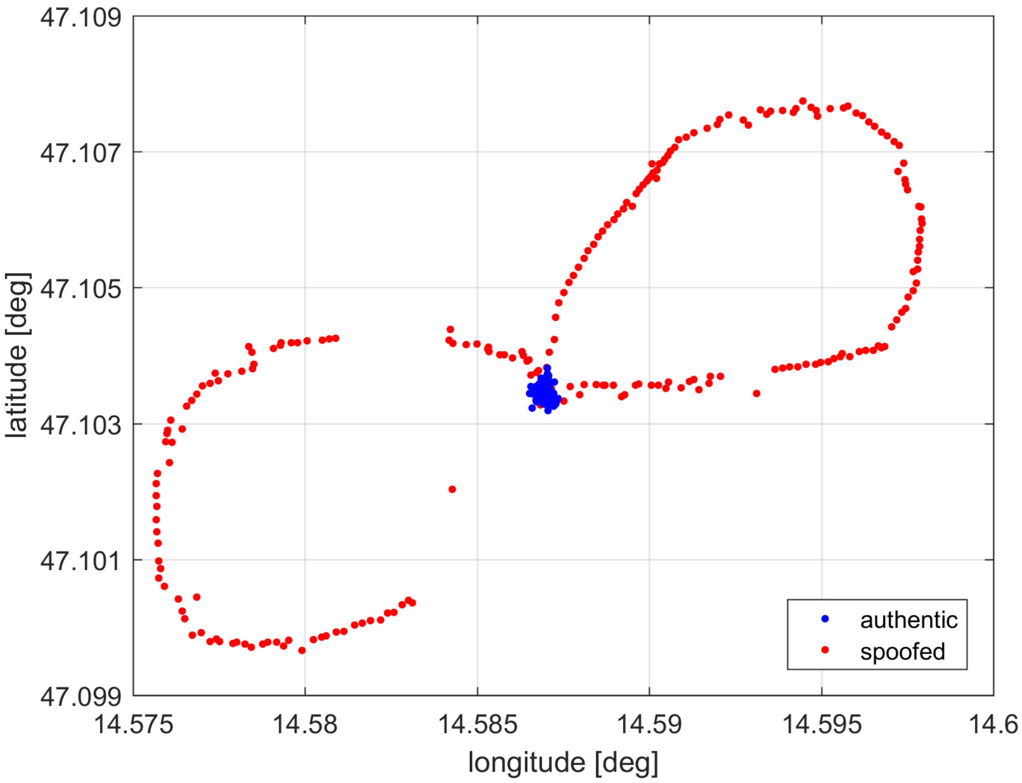


Figure 8.27: Authentic and spoofed GPS receiver positions at Seetaler Alpe

High correlations due to relative movement of the receiver with respect to the spoofer influence the structure of Doppler measurements. Figure 8.28 shows the residual Doppler values (measured minus theoretical) for all GPS satellites. Here, the same behavior as in the simulations can be seen. The attack's launch is marked by the black dotted line. The values show a high correlation, with most Doppler residuals having a similar systematic structure over time after the attack has been started. Again, it can be seen, that not all signals have been successfully taken over after the launch of the attack at epoch 125. At epoch 280, after the tracking loop has locked on all counterfeit signals, almost all Doppler residuals show high deviations of several hundred Hz with a correlated pattern.

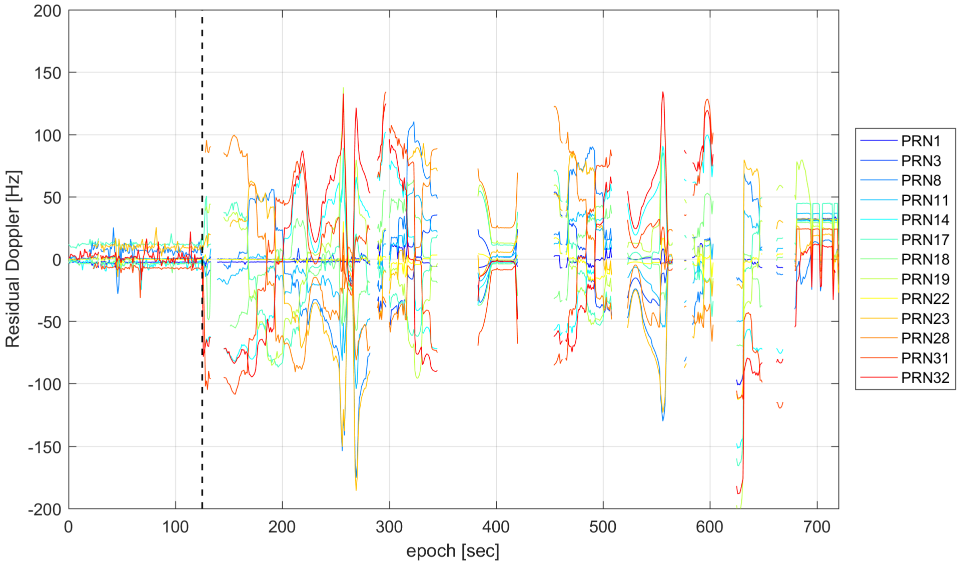


Figure 8.28: Residual Doppler frequencies for GPS during spoofing attack at Seetaler Alpe

Data gaps can be seen again for the same epochs as before. By applying Equation 6.26 on the measurement samples, a distinction based on the correlation coefficient can be done.

In Figure 8.29 the computed correlation coefficients of the Doppler residuals for the time span before and after the start of spoofing attack are shown. The set of correlation coefficients at the top of the figure corresponds to the authentic positions in Figure 8.27, whereas the bottom set is assigned to the spoofed PVT. As already expected from the simulation results as well as Figure 8.28, high correlations for most of the spoofed signal pairs are present. Still, some pairs show very low crosscorrelations. Especially, the PRNs, which have not been spoofed from the very beginning of the attack, are less correlated with each other.

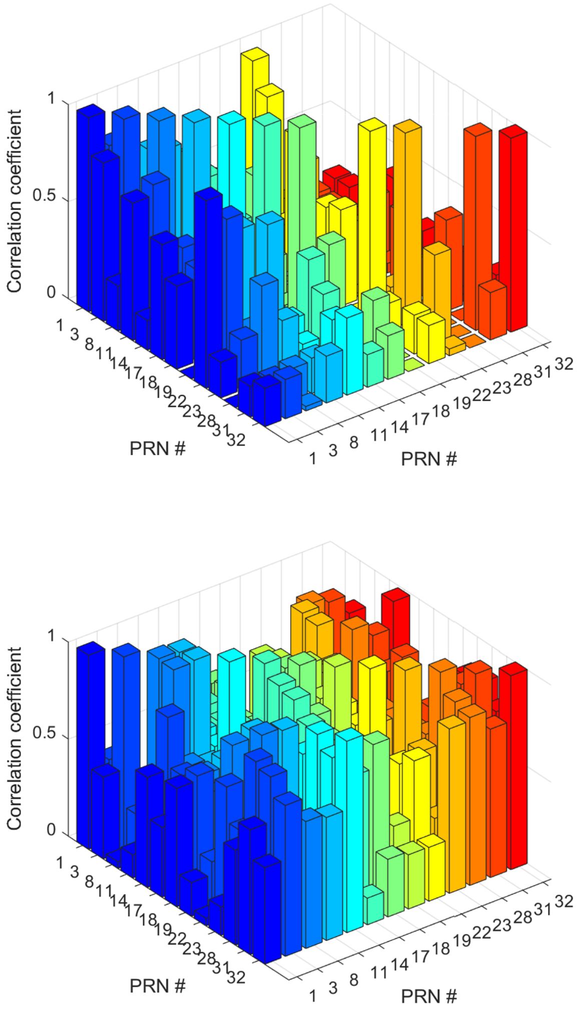


Figure 8.29: GPS correlation coefficients authentic (top) vs. spoofed (bottom) at Seetaler Alpe

In general, a significantly high correlation is given for the spoofed data sets, whereas the coefficients of the authentic set are low for the most part. Some signal pairs though show relatively high correlations. Especially PRN1, PRN3 and PRN22 are highly correlated. The reason lies again in the constellation of the GPS satellites. These three satellites have almost the same azimuth and similar elevations, as Figure 8.30 depicts. PRN19 and PRN28 were not present during the time span of authentic measurements, therefore they are missing.

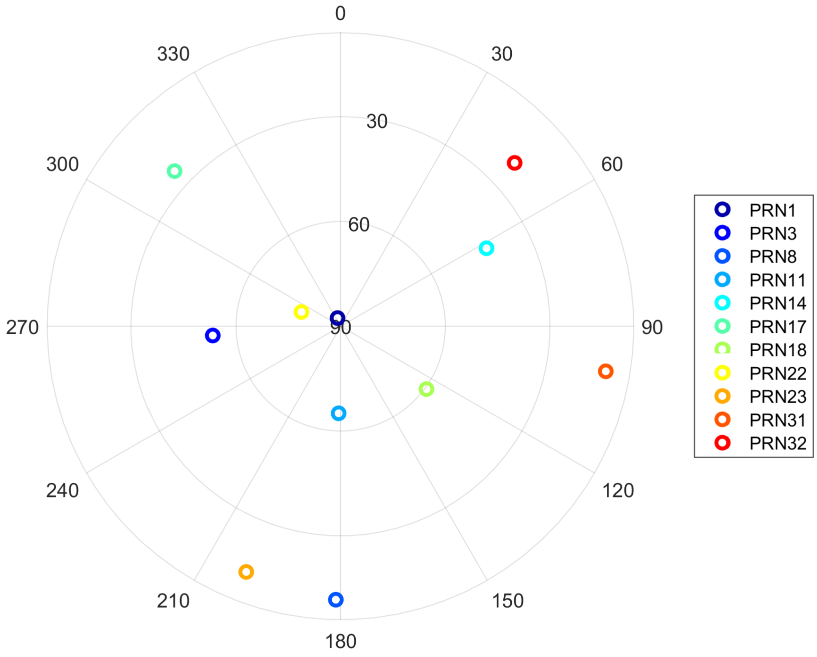


Figure 8.30: Skyplot of authentic GPS satellites at Seetaler Alpe

The implemented algorithms showed promising results for both, simulated and real-world tests, making them suitable for detecting and mitigating incoming spoofing attacks.

9 Conclusions and outlook

This thesis deals with the investigation of different state-of-the-art spoofing detection algorithms as well as the development of a reliable mitigation strategy, where an authentic PVT can be guaranteed during an ongoing attack. The need for intentional interference countermeasures is crucial. Many safety critical applications depend on satellite-based navigation and precise timing solutions. For a long time, the threat of GNSS spoofing has been neglected. But recent reports on successful attacks show that the threat has become a real issue and that the number of incidents will raise in the near future.

Several state-of-the-art algorithms for spoofing detection have been investigated. Most of these methods showed promising results. In case of a static receiver application, simple PVT monitoring can be utilized for detecting unusual behavior caused by a spoofing attack. Moreover, received power monitoring in combination with the observed outputs from the tracking loop's correlation functions serves as reliable countermeasure, where the false alarm rate is lowered, by considering jamming attacks as well as multipath effects. Many of these strategies can be combined in order to increase the robustness of detection for receivers during ongoing attacks.

The demanded development of a new detection and mitigation strategy for spoofing attacks has been successfully achieved. Based on the spatial signature of the incoming signals for a moving receiver, the correlations of Doppler residuals have been exploited to successfully detect an ongoing attack and further mitigate it by correctly classifying the tracked signals into authentic and spoofed sets. The algorithm was applied on real-world measurements and the results were consistent with the ones based on the simulations. The flowchart in Chapter 7 shows all necessary steps for implementing the algorithm inside a SDR, making a realization easy for developers.

Besides single-antenna set ups, the usage of antenna arrays has a long tradition in signal processing and is recently gaining more attention in the field of GNSS. Especially uniform circular arrays have proven to be reliable for estimating two-dimensional direction of arrival parameters. The antenna element spacing is dependent on the frequency of the incoming signals. In case of GNSS, where signals in the L-band are processed, the size of UCAs can be restricted to decimeter level.

The application of subspace direction of arrival techniques, such as MUSIC, provides an estimation of several signal sources simultaneously, compared to time difference of arrival techniques, where only a single source can be determined. In this thesis, a DOA estimation based on MUSIC for several spoofers has been successfully demonstrated with a simulated antenna array. The estimated angles of the incoming spoofing signals differed less than one degree from the reference values. With the simulated eight-element array, directions of arrival for three spoofers were simultaneously determined without performance losses in terms of accuracy and computation time. The comparison between the element space and real beamspace MUSIC algorithm showed that the latter one offers an improved estimator performance for correlated signals sources, while the angles determined in element space had significantly lower accuracies.

The idea of antenna arrays could, in a further step, be realized through virtual arrays, by moving a single antenna in the shape of certain structures. Broumandan et al. (2007) has developed a strategy, where the direction of arrival of an interferer was computed by setting up a synthetic UCA through antenna rotation. With this strategy, the costs can be reduced, since only one antenna is required. Moreover, no calibration of antenna elements needs to be done in advance. On the contrary, the accuracy of the derived DOA parameters is dependent on the accuracy of the antenna movement following a certain array structure.

In a next step, the newly developed mitigation strategy based on Doppler residuals will be implemented inside a SDR for the GIDAS project. In order to further test its performance, simulations as wells as real-world recordings of different kinds of spoofing attacks will be investigated.

For validating the acquired simulation results of the DOA estimation based on antenna arrays, a UCA set up can be used to test the performance of the MUSIC algorithm with real-world measurements.

The upcoming support of raw GNSS measurements by smartphones also opens wide fields for new approaches on PVT processing. The resulting advantages not only affect the solutions in terms of achievable accuracy, but also in terms of security, where raw measurement observation can be utilized for detecting and mitigating ongoing attacks.

List of Figures

List of Tables

References

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.

Borre K, Akos DM, Bertelsen N, Rinder P, Jensen SH (2007): A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach. Birkhäuser, Boston Basel Berlin.

Broumandan A, Jafarnia-Jahromi A, Dehghanian V, Nielsen J, Lachapelle G (2012): GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation. In: Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium. Myrtle Beach, South Carolina. Apr 24–26.

Broumandan A, Lin T, Moghaddam A, Lu D, Nielsen J, Lachapelle G (2007): Direction of Arrival Estimation of GNSS Signals Based on Synthetic Antenna Array. In: Proceedings of the 20th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2007). Fort Worth, Texas. Sept 25–28.

Chatre E, Verhoef P (2018): Galileo Programme Status Update. In: Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2018). Miami, Florida. Sept 24–28: 733–767.

Dehghanian V, Nielsen J, Lachapelle G (2012): GNSS Spoofing Detection based on Receiver C/N0 Estimates. In: Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012). Nashville, Tennessee. Sept 17–21.

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). Version available at `www.gsc-europa.eu/system/files/galileo_documents/Galileo-OS-SIS-ICD.pdf`.

European Global Navigation Satellite Systems Agency (2018a): Galileo System Services. More information on `www.gsa.europa.eu/galileo/services`.

European Global Navigation Satellite Systems Agency (2018b): Using GNSS raw measurements on Android devices. White Paper. Available at `www.gsa.europa.eu/system/files/reports/gnss_raw_measurement_web_0.pdf`.

Gmeindl D (2011): Analysen zu RAIM – Receiver Autonomous Integrity Monitoring. Bachelor thesis. Institute of Navigation, Graz University of Technology, Austria.

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.

Huang J, Presti LL, Motella B, Pini M (2016): GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky. In: ICT Express 2.1: 27–40. DOI: `10.1016/j.icte.2016.02.006`.

Jones M (2017): GPS World: Spoofing in the Black Sea: What really happened? In: GPS World. Oct 11. Available at `www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened`.

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

Khan AM, Iqbal N, Khan MF (2017): Spoofing Detection for GNSS Signal using SQM through Closely Spaced Correlators. Article. Department of Electrical Engineering, National University of Sciences and Technology, Islamabad, Pakistan. Available at `www.researchgate.net/publication/310490016_Spoofing_Detection_for_GNSS_Signal_using_Signal_Quality_Monitoring_through_Closely_Spaced_Correlators`.

Krim H, Viberg M (1996): Two Decades of Array Signal Processing Research. In: IEEE Signal Processing Magazine 13.4: 67–94. DOI: 10.1109/79.526899.

Mathews CP, Zoltowski MD (1994): Eigenstructure Techniques for 2-D Angle Estimation with Uniform Circular Arrays. In: IEEE Transactions on Signal Processing 42.9: 2395–2407. DOI: 10.1109/78.317861.

O'Hanlon BW, Psiaki ML, Humphreys TE (2012): Real-Time Spoofing Detection Using Correlation Between Two Civil GPS Receiver. In: Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012). Nashville, Tennessee. Sept 17–21.

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

Petovello M (2010): Carrier-to-Noise Algorithms. Inside GNSS, 5(1): 20–27.

Petovello M (2018): What is navigation message authentication? Inside GNSS, 13(1): 26–31.

Psiaki ML, Humphreys TE (2016a): GNSS Spoofing and Detection. In: Proceedings of the IEEE 104.6: 1258–1270. DOI: 10.1109/JPROC.2016.2526658.

Psiaki ML, Humphreys TE (2016b): GPS Lies. More information on spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation.

Shepard D, Bhatti JA, Humphreys TE (2012): Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle. In: GPS World. Aug 1. Available at www.gpsworld.com/drone-hack.

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

Tang H (2014): DOA estimation based on MUSIC algorithm. Bachelor thesis. Institutionen för Fysik och Elektroteknik, Umeå University, Sweden.

TeleConsult Austria GmbH (2018a): GNSS Multisystem Performance Simulation Environment (GIPSIE®) Core Manual. Version 4.0.0.

TeleConsult Austria GmbH (2018b): The Navigation and Mobility Experts. More information on www.tca.at.

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

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

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

Wax M, Sheinvald J (1994): Direction Finding of Coherent Signals via Spatial Smoothing for Uniform Circular Arrays. In: IEEE Transactions on Antennas and Propagation 42.5: 613–620. DOI: `10.1109/8.299559`.

Wesson K, Evans B, Humphreys T (2013): A Combined Symmetric Difference and Power Monitoring GNSS Anti-Spoofing Technique. In: IEEE Global Conference on Signal and Information Processing. Austin, Texas. Dec 3–5.

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.

- **GCC C++ compiler**
  Standard C++ compiler for Ubuntu Linux, used in version 4.8, GNU general public license. Download available at: `https://gcc.gnu.org`

- **Cmake**
  Cross-platform build tool for C++, used in version 3.0.2, BSD 3-clause license. Download available at: `http://cmake.org`

- **Qt framework**
  Cross-platform application and user interface framework for C++ including Qt-Creator software, used in version 5.3.2, GNU general public license v3 license. Download available at: `http://qt-project.org`

- **GIPSIE®**
  A simulation environment capable of simulating arbitrary digital intermediate frequency (IF) GNSS signals developed at TeleConsult Austria 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://tca.at`

- **GNSS Analysis Tool®**
  An application, developed by Google, for processing and analyzing GNSS raw measurements from Android smartphones. The application is based on MATLAB RUNTIME. Version 2.6.3.0 used. Download available at: `https://github.com/google/gps-measurement-tools`

- **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`

- **Matlab**
  A desktop environment tuned for iterative analysis and design processes by using a programming language that expresses matrix and array mathematics directly. Version R2016b used. More information on: `https://mathworks.com/products/matlab.html`

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