UCGE Reports

Number 20385

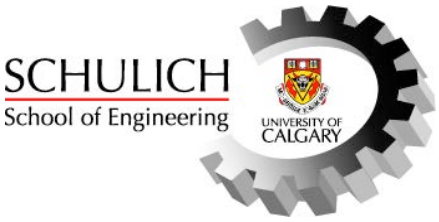
Department of Geomatics Engineering

GNSS Signal Authenticity Verification in the Presence of Structural Interference

by

Ali Jafarnia Jahromi

September 2013



UNIVERSITY OF CALGARY

GNSS Signal Authenticity Verification in the Presence of Structural Interference

By

ALI JAFARNIA JAHROMI

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF GEOMATICS ENGINEERING

CALGARY, ALBERTA

September 2013

Abstract

GNSS dependant timing and positioning systems have become widespread in various civilian applications such as communication networks, smart power distribution grids and vehicular and airplane navigation systems. However, GNSS signals are quite vulnerable to different types of interference since they are very weak once received on the earth surface. Among various intentional interference signals, structural interferences (e.g. spoofing and meaconing) are much more dangerous since they are designed to mislead their target receiver(s) that are not aware of the attack and this can lead to disastrous consequences in scores of applications.

Spoofing and meaconing signals' features are very similar to those of authentic GNSS signals; therefore, it is very difficult for a GNSS receiver to discriminate their presence. This dissertation analyses the effects of spoofing signals on different processing levels of civilian GPS L1 C/A receivers and accordingly proposes some possible countermeasure techniques. It is shown that the presence of spoofing interference increases the power content of structural signals within the GNSS frequency bands and this feature can reveal the presence of spoofing interference before the despreading process of the receiver.

Spoofing and meaconing interference can affect the acquisition process of a GNSS receiver. It is shown that monitoring the absolute received power of received GNSS signals is highly effective to reduce receiver vulnerability to spoofing attack during the acquisition process. Spoofing signals can also compromise the tracking process of GNSS receivers by generating synchronized higher power PRN signals. The effects of different

spoofing attacks on a tracking receiver are analysed and two possible countermeasure techniques have been proposed to detect the interaction between spoofing and authentic signals. Furthermore, the effect of spoofing signals has been analysed on the position level observables of a GNSS receiver and it is shown that these observations can practically reveal the presence of a spoofed position/timing solution for a moving receiver.

The performances of the proposed authenticity verification techniques are validated using several real data collection and processing scenarios. Finally, a possible structure for a spoofing aware GPS receiver is proposed that checks the authenticity of received GNSS signals at different processing layers without imposing extensive hardware or software modifications to conventional GNSS receivers.

Preface

This thesis includes some materials (e.g. figures, tables, formulas and texts) previously published, accepted or submitted in two conference papers and three journal papers

Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen and G. Lachapelle (2012) "GPS Spoofer Countermeasure Effectiveness based on Using Signal Strength, Noise Power and C/N0 Observables" *International Journal of Satellite Communications and Networking*, July, vol 30, no 4, pp. 181–191

Jafarnia-Jahromi, A., T. Lin, A. Broumandan, J. Nielsen and G. Lachapelle (2012) "Detection and Mitigation of Spoofing Attacks on a Vector Based Tracking GPS Receiver," *Proceedings of International Technical Meeting of the Institute of Navigation (ION ITM 2012)*, 30 January-1 February, Newport Beach, CA, pp. 790-800

Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen and G. Lachapelle (2012) "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques" in the International Journal of Navigation and Observation, Hindawi Publishing Corporation, vol 2012, 16 pages

Jafarnia-Jahromi, A., S. Daneshmand, A. Broumandan, J. Nielsen and G. Lachapelle (2013) "PVT Solution Authentication Based on Monitoring the Clock State for a Moving GNSS Receiver" in the European Navigation Conference (ENC2013), April 23-25, Vienna, Austria, 11 pages

Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen and G. Lachapelle "Pre-Despreading Signal Quality Monitoring towards GPS Authenticity Verification" Submitted to NAVIGATION: the journal of the Institute of Navigation, August 2013

The above papers were produced by the author during the research phase of this thesis. The co-authors' valuable collaboration on the above materials is acknowledged. Use of the above material in this thesis is allowed by the co-authors and the journal/proceedings publishers.

Acknowledgments

Foremost, I would like to express my deepest appreciation to my supervisor, Professor Gérard Lachapelle, for his continuous support during my PhD study and research, his positive attitude, understanding, caring, and immense knowledge. His guidance helped me at all the time of research and writing of this thesis. I have learned a lot from him in academic, professional and personal aspects of my life.

I would like to thank my co-supervisor, Professor John Nielsen, for his encouragement, enthusiasm and sharing his insights in different parts of this research. This study would not have been possible without his knowledge and assistance.

My sincere gratitude goes to my advisor, Dr. Ali Broumandan, for his friendship, patience, insightful comments and very helpful discussions and advice he provided me throughout this research. This research would have been much more challenging without his endeavours and support.

I owe special thanks to Mahshid Sadat Mohammadi, my lovely wife, for her continuous support and for her constant love during my education. She was the reason of my happiness and peace. Also, special thanks to my parents without whose support I would never have gotten this far. This thesis is a dedication to them and to their unconditional love. Besides, I would like to thank my siblings for their kind support and encouragements during my study.

I would also like to convey my thanks to Alberta Innovates Technology Futures (AITF) for providing me with financial support during the last two years of my studies.

Finally, I would like to extend a heartfelt thanks to all my friends and work colleagues in the Position, Location and Navigation (PLAN) Group at the University of Calgary. Specifically, I would like to thank Dr. Vahid Dehghanian, Dr. James T. Curran, Srinivas Bhaskar, Dr. Nima Sadrieh, Peng Xie, Hatef Keshvadi, Behnam Aminian, Negin Sokhandan, Mohammad Mozaffari, Billy Chan, Dr. Tao Lin and Anup Dhital for their encouragement and support during this research. I am particularly grateful for the collaborative work and illuminating discussions with my friend and colleague, Dr. Saeed Daneshmand, during different stages of my PhD studies.

Dedication

To my beloved wife, Mahshid, my parents, Maryam and Mohammad Jafar, my brother Mehdi, and my sisters Afrooz and Yasaman.

Table of Contents

List of Tables

List of Figures and Illustrations

List of Symbols

Symbol	Definition
$r(nT_s)$	Complex discrete baseband signal received by an antenna
p_m^a	Power of mth authentic signal
p_q^s	Power of mth spoofing signal
$\eta(nT_s)$	Complex sampled circularly symmetric AWGN
σ^2	The variance of $\eta(nT_s)$
T_s	Sampling interval
τ_m^a	Code delay of mth authentic signal
τ_q^s	Code delay of qth spoofing signal
f_m^a	Doppler frequency of mth authentic signal
f_q^s	Doppler frequency of qth spoofing signal
$h_m^a(nT_s)$	Data bit of mth authentic signal
$h_q^s(nT_s)$	Data bit of qth spoofing signal
$c_m^a(nT_s)$	Spreading Code of the mth authentic PRN signal
$c_q^s(nT_s)$	Spreading Code of the qth spoofing PRN signal
ϕ_m^a	Initial carrier phase for the *m*th authentic signal
ϕ_q^s	Initial carrier phase for the *q*th spoofing signal
u_l	Complex correlator output for the *l*th PRN
D_l	Squared amplitude of correlator output for the *l*th PRN
Λ_l	Signal to noise ratio (SNR) for the *l*th correlator output

H_0	The null hypothesis which refers to the absence of spoofing signals
H_1	The alternative hypothesis which refers to the presence of spoofing signals
$\mathbf{J}^a$	Authentic signals set
$\mathbf{J}^s$	Spoofing signals set
ς_{ij}	Correlation coefficient between *i*th and *j*th correlator outputs
$\mathbf{b}$	Steering vector toward spoofing source
$\mathbf{f}$	Array gain vector orthogonal to spoofer's direction
$\mathbf{a}_m$	Steering vector toward *m*th authentic signal
$I_0(\bullet)$	Modified zero order Bessel function of the first kind
N_c	Number of CAF cells
β_s	Scaling Factor for Carrier Aiding
R_c	Code Chip Rate
$E[\bullet]$	statistical expectation
χ^2_N	Central Chi-Square Distribution with *N* degrees of freedom
$\chi^2_N(\lambda)$	Non-central Chi-Square Distribution with *N* degrees of freedom and non-centrality factor of λ
$Q_{\chi^2_N}(\bullet)$	Right tail probability for a Chi-square random variable with *N* degrees of freedom
$Q^{-1}_{\chi^2_N}(\bullet)$	Inverse of the right tail probability for a Chi-square random variable with *N* degrees of freedom
P_D	Probability of detection
P_{FA}	Probability of false alarm
$\mathbf{I}_2$	A 2×2 identity matrix
$\mathrm{N}_c(\mathbf{A},\mathbf{C})$	Circularly symmetric complex Gaussian distribution with the mean

	vector of **A** and the covariance matrix of **C**.
T_c	Chip duration of GPS L1 C/A PRN signals
T_e	Epoch length of GPS L1 C/A PRN signals
γ	Detection threshold
$PR_i(t)$	Pseudorange observation corresponding to PRN *i* at time (t)
$\rho_i(t)$	Range between *i*th satellite and user's antenna
$\rho_{su}(t)$	Range between the spoofer transmit antenna and target receiver's antenna
$dT_u(t)$	User clock bias at time *t*
c	Speed of light (m/s)
dt_i	Clock error corresponding to the *i*th satellite
$\mathbf{P}_s[n]$	Spoofer's position at time instant *n*
$\mathbf{P}_u[n]$	User's position at time instant *n*
$\mathbf{H}$	Design matrix
$\mathbf{x}$	Vector of observations
$T(\mathbf{x})$	Detection test statistic

List of Abbreviations

Abbreviation	Definition
ADC	Analog to Digital Converter
AGC	Automatic Gain Control
AOA	Angle of Arrival
ASIC	Application-Specific Integrated Circuit
AWGN	Additive White Gaussian Noise
C/A	Coarse Acquisition
CAF	Cross Ambiguity Function
CDF	Cumulative Density Function
CDMA	Code Division Multiple Access
CWI	Continuous Wave Interference
DAC	Digital to Analog Converter
DAM	Delay and Multiply
DLL	Delay Locked Loop
DOA	Direction of Arrival
DOP	Delusion of Precision
DS-CDMA	Direct Sequence CDMA
DSP	Digital Signal Processing
DVB-T	Digital Video Broadcast - Terrestrial
GLRT	Generalized Likelihood Ratio Test
GNSS	Global Navigation Satellite System
GOF	Goodness of Fit
GPS	Global Positioning System
GSM	Global System for Mobile

IF	Intermediate Frequency
i.i.d.	Independent Identically Distributed
IMU	Inertial Measurement Unit
KF	Kalman Filter
LBS	Location Based Service
LLR	Log Likelihood Ratio
LO	Local Oscillator
LOS	Line of Sight
MLE	Maximum Likelihood Estimate
Msps	Mega Sample per Second
NCO	Numerically Controlled Oscillator
NI	National Instruments
OCXO	Oven Controlled Crystal Oscillator
PANOVA	Phase only Analysis of Variance
PCWI	Pulsed Continuous Wave Interference
PDF	Probability Density Function
PDOP	Position Dilution of Precision
PLAN	Position, Location and Navigation group
PLL	Phase Locked Loop
PPD	Personal Privacy Device
PRN	Pseudorandom Noise
PSD	Power Spectral Density
PVT	Position, Velocity and Time
RAIM	Receiver Autonomous Integrity Monitoring
RF	Radio Frequency

RFI	Radio Frequency Interference
RMS	Root Mean Square
RSS	Received Signal Strength
ROC	Receiver Operating Characteristics
SAPR	Spoofing to Authentic Power Ratio
SIC	Successive Interference Cancelation
SINR	Signal to Interference and Noise Ratio
SNR	Signal to Noise Ratio
SSNR	Structural Signal to Noise Ratio
SQM	Signal Quality Monitoring
TAP	Total Authentic Power
TCXO	Temperature Controlled Crystal Oscillator
TOA	Time of Arrival
TSP	Total Spoofing Power
UAV	Unmanned Aerial Vehicle
VIAS	Vulnerability Index Against Spoofing
VMS	Vessel Monitoring System
VSA	Vector Signal Analyzer
WAAS	Wide Area Augmentation System
WSMR	White Sands Missile Range

Chapter One: Introduction

Position, velocity and time (PVT) provided by global navigation satellite systems (GNSS) now impact most aspects of human life. Nowadays, most mobile phones as well as vehicles are equipped with positioning and navigation systems utilizing GPS. In addition, countless time tagging and synchronization systems rely primarily on GPS. Various civilian applications such as vehicular and personal navigation, electrical power distribution grids, digital communication networks, aircraft navigation and landing systems, marine and ground transportations, police and rescue services, dangerous offender tracking, wild-life tracking, vessel monitoring systems (VMS), location based services, stock exchange transactions, car rental industry and many more are relying on GPS signals as well. As a consequence, such a ubiquitous system is becoming an increasingly attractive target for illicit disruption by terrorists and hackers.

1.1 GNSS and Interference Signals

GNSS signals are vulnerable to interference due to being extremely weak when they are received on the earth's surface. Therefore, even low-power interference can easily jam or spoof commercial GPS receivers within a range of several kilometres. These interfering signals can originate from different sources such as TV transmitters, radio amateur equipment and personal privacy devices (PPDs). Consequently, anti-interference mechanisms are becoming increasingly important to develop for modern GNSS applications. There are several types of interference signals that can adversely affect GNSS operation and they can be categorized in different groups such as intentional and unintentional, wide-band and narrow-band interference.

1.1.1 Un-intentional interference

Radio frequency interference (RFI) generated by malfunctioning or noncompliant electronic equipment can potentially disrupt GNSS receivers within a certain area. Two main sources of unintentional interference are spurious and out-of-band emissions of electronic and telecommunication equipment (Wildemeersch et al 2010). For example, the harmonics of digital video broadcast- terrestrial (DVB-T) signals can highly interfere with GNSS signals and disturb the positioning capability of corresponding receivers (Borio et al 2006). The probability of occurrence for this type of interference is high since many types of electronic equipment with different manufacturing qualities are transmitting signals near GNSS frequency bands.

Another category of unintentional interference is multipath reflection that seriously degrades the positioning performance of GNSS receivers. Multipath signals are mostly generated by terrestrial reflectors such as buildings in downtown areas. The interaction between multipath and line of sight (LOS) signals can distort the shape of the correlation peaks and subsequently affect the pseudorange measurements of the GNSS receivers.

1.1.2 Intentional interference

Intentional interference signals are specially designed to deny or mislead GNSS service within a certain area. The most common type of intentional interference is jamming signals which can be generated in several formats such as continuous wave (CW), pulsed continuous wave (PCW) and additive white Gaussian noise (AWGN). This type of interference aims to prevent GNSS receivers from providing position and timing solutions. PPDs are well-known examples of civilian GNSS jammers that can be

purchased online at very low cost. Although the nominal power of these transmitters is low, they can deny the GNSS service within a radius of tens of metres which is beyond the personal space and affects other receivers in the vicinity (Grabowski 2012). The availability of such interference generating devices compounds the interference issue and hence, interference countermeasures are becoming an increasingly important research topic.

Spoofing and meaconing signals are structural types of wideband intentional interference that try to misdirect their target GNSS receivers into generating falsified position and/or timing solutions while the receiver is not aware of this attack. Meaconing signals are a replayed version of previously recorded genuine GNSS signals whereas spoofing signals are counterfeit GNSS signals that are specially designed to mimic the authentic GNSS signals in different aspects such as temporal and spectral characteristics. Spoofing and meaconing are insidious and potentially more damaging than jamming since the receiver is not aware of the threat and will produce wrong information that could lead to dire consequences. In other words, under a spoofing or meaconing attack, a GNSS receiver is providing position and timing solutions with fairly good signal quality measures however, the position solutions do not represent the actual location of the receiver.

Figure 1-1illustrates a spoofing attack on a GPS receiver mounted on a vehicle. Herein, the illustrated GPS equipment is receiving both authentic and spoofing signals; however, the higher power of spoofing signals can mislead the GPS receiver toward tracking them. It is observed that spoofing signals are transmitted via a local single antenna spoofing source and they are trying to induce a fake trajectory to the vehicle's onboard GPS

receiver. The fake trajectory is shown in red whereas the actual trajectory of the receiver is depicted as a green line. In this scenario, the spoofing source may be mounted on the vehicle in case that the driver wants to intentionally misdirect the GPS equipment of his/her vehicle.

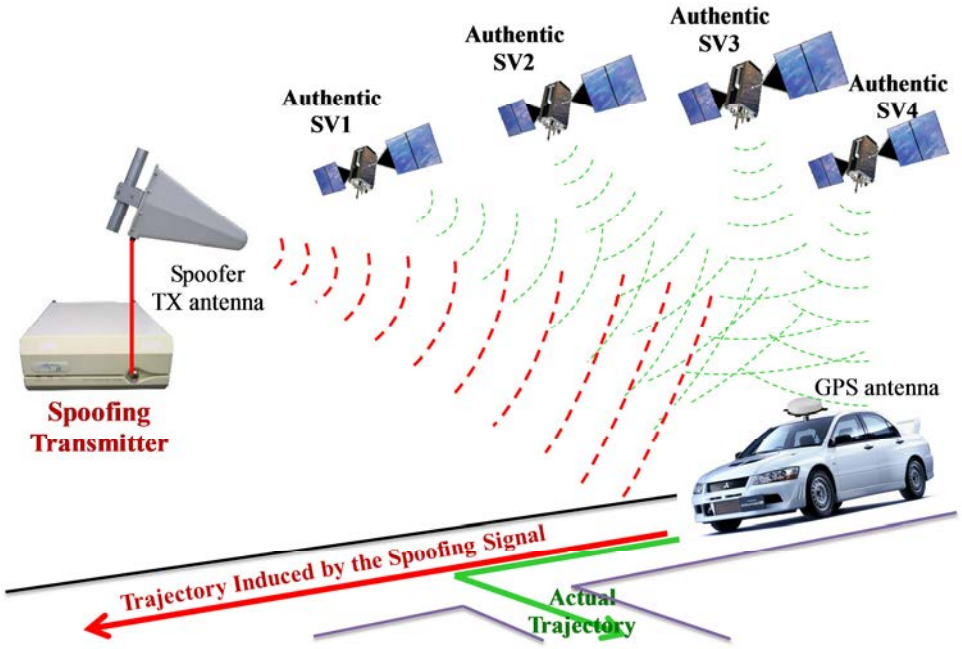


Figure 1-1 Illustration of a GPS spoofing attack on a vehicle

1.2 Motivations

Due to the recent rapid increase in the application of civilian GNSS dependant systems, motivation has increased to spoof these signals for illegal or concealed transportation, fishing and hunting in prohibited areas, misleading receiver timing being used by power distribution grids and cellular networks and interrupting stock exchange transactions. The structure of most civilian GNSS signals is known to the public (IS-GPS 200F & IS-GPS-705) and due to the recent rapid advances in software defined radio (SDR) technology, designing a portable GNSS spoofer has become more feasible and less costly

(Humphreys et al 2008, Mitch et al 2011). Therefore, spoofing is turning to a more serious type of threat for the future of GNSS systems and this necessitates proper countermeasure techniques that can be practically implemented in GNSS receivers without requiring high computational power or additional costly/massive hardware.

In recent years, several research groups and companies have focused on GNSS interference countermeasures and several articles have been published in this regard. The special case of spoofing countermeasures has recently attracted considerable research interest as spoofing is such a potential menace. However, civilian commercial GNSS receivers remain generally defenceless against this type of interference. The main focus of the research in the field of GNSS spoofing countermeasure is to answer the following questions: “How can a GNSS receiver make sure that it is providing a valid position solution?” and “How can this receiver recover its positioning capability once it is exposed to counterfeit GNSS signals?”.

1.3 Previous Research on Anti-Spoofing

Spoofing signals are very similar to authentic GNSS signals in various aspects such as signal structure and received signal strength (RSS). However, spoofing signals should be wisely designed so that they can effectively misdirect their target GNSS receiver(s) and at the same time avoid being detected by spoofing countermeasure techniques. For example, the RSS of spoofing signals should be slightly higher than that of the authentic signals, but it should not be significantly higher in order to prevent being suspicious because of exceeding the normal RSS range of authentic GNSS signals.

Several spoofing countermeasure techniques have been proposed in the open literature and they can be generally divided into two main categories, namely spoofing detection and spoofing mitigation (Humphreys et al 2008, Montgomery et al 2009). Spoofing detection algorithms concentrate on detecting the presence of spoofing attack while spoofing mitigation techniques aim to neutralize the spoofing threat and help the target GNSS receiver to recover its positioning capability. Spoofing countermeasures can take place at any of the operational layers of a GNSS receiver, namely at the signal processing level, data bit level and/or position solution and navigation level (Jafarnia et al 2012c).

Spoofing countermeasure methods look for specific features of spoofing signals that make them different from the authentic ones. Some of the previously proposed countermeasure techniques can be enumerated as received signal strength (RSS) monitoring, received signal time of arrival (TOA) monitoring, spatial coherency analysis of received GNSS signals, signal quality monitoring (SQM), cryptographic authentication, receiver autonomous integrity monitoring (RAIM) and consistency check among different sensors and constellations (Scott 2003, Wen et al 2005, Wesson et al 2011, Ledvina et al 2010, Pini et al 2011). The following paragraphs briefly discuss some of the most important existing anti-spoofing methods and their associated limitations.

RSS based spoofing countermeasure techniques rely on the assumption that the power level of spoofing signals is higher than authentic GNSS signals in order to be able to misdirect their target GNSS receiver(s). Shepard et al (2011) have observed that a spoofing signal can effectively misdirect a GNSS receiver if its power is at least 1.1 dB higher than the authentic signals. As the path loss between spoofer and target receiver is

highly variable, it is difficult for a spoofer to estimate the transmit power required to impose sufficient signal strength at the target receiver while not excessively exceeding the typical power level of the authentic GPS signals. Nielsen et al (2012), Dehghanian et al (2012) and Wen et al (2005) have proposed SNR monitoring as a good indicator of the presence of higher power spoofing signals. Akos (2012) has shown that the presence of additional power of spoofing signals can affect the automatic gain control (AGC) component of the target receiver and this can be an effective measure for spoofing detection. RSS based spoofing countermeasure methods are powerful means of detecting the presence of spoofing signals, however, as it will be shown in Chapter 4, SNR measurements are not always a good measure of RSS since the spoofer is able to transmit higher power PRN signals combined with an elevated noise floor. Furthermore, AGC level information might not always be available to the user (e.g. for the case of a GNSS software receiver working on digitized IF samples) and this can limit the applicability of such a processing method.

TOA based techniques rely on the assumption of the presence of an inevitable delay between authentic signals and the spoofer generated GNSS signal replicas. This delay can be observed in the PRN code offset and in data bit transition boundaries. Cho et al (2008) have designed a TOA based authentication method that looks for unusual data bit transitions within the intervals of less than 20 ms for GPS L1 C/A signals. This technique can be useful in the case that both spoofing and authentic signals are observable by the target receiver at a comparable power level and the spoofer does not predict the GNSS data bits.

Spatial processing spoofing countermeasure techniques rely on the assumption that the spoofing source is a single antenna transmitter emitting several PRN signals. Therefore, the spoofing PRNs are spatially coherent which means that they are all received from the same direction. Spatial processing using either physical or synthetic antenna arrays has been recently considered in several papers (Hartman 1995, Montgomery et al 2009, Nielsen et al 2011, Broumandan et al 2012, Daneshmand et al 2012, McDowell 2007, Chang 2012, Meurer et al 2012, Hornbostel et al 2013, Konovaltsev et al 2013). These papers have employed several approaches such as angle of arrival (AOA) estimation and verification, pairwise correlation of different PRNs and observation and comparison of phase variations of correlation peaks to countermeasure the spoofing threat. Using appropriate antenna array processing techniques, spoofing signals can be also mitigated by steering a null toward the direction of the spoofer (McDowell 2007, Daneshmand et al 2011, 2013).

Antenna array processing is one of the most effective means of spoofing detection and mitigation. However, these methods increase the hardware complexity of a GNSS receiver because of requiring additional antenna branches along with their corresponding RF front-ends and analogue to digital converters (ADCs). Furthermore, some of the previously proposed multiple antenna processing techniques require precise antenna array calibration which makes them more complicated to be implemented in real world scenarios. For the case of synthetic array spatial processing methods, accurate modelling of the receiver's clock state as well as Doppler frequency estimation are two limiting

factors that can considerably affect the ideal performance of spoofing countermeasure techniques.

Consistency check methods are also a very powerful category of spoofing countermeasure techniques. Consistency check of the position layer observables with the measurements coming from external sensors such as inertial measurement units (IMUs) can reveal the presence of counterfeit positioning signals (Gao & Bobye 2013, White et al 1998). Verifying the solutions consistency between multiple GNSS signals such as GPS, GLONASS, Galileo and BeiDou can be also an effective means of detecting counterfeit spoofing signals. Most of the consistency verification techniques require additional hardware for multi-sensor navigation and/or multi-constellation GNSS reception which might not be affordable for many classes of GNSS receivers.

1.4 Objectives and Contributions

The main contribution of this thesis is analysing the effect of structural interference on different stages of GNSS receivers' signal processing and proposing possible countermeasure techniques toward reducing the vulnerability of civilian GNSS receivers to this type of interference. The research is focused on proposing practical authenticity verification techniques that can be implemented on commercial GNSS receivers without requiring additional hardware or extensive processing burden. Herein, the word "structural interference" refers to spoofing and meaconing signals whose structure is quite similar to the genuine GNSS signals and they are designed to force GNSS receivers into generating an incorrect position and/or timing solution. The effect of structural interference is investigated on raw signal samples, signal acquisition, signal tracking, and

finally on position layer observables of a typical GNSS receiver. Possible countermeasure methods have been proposed for each stage in order to detect the presence of structural interference and alert the user of potentially falsified position and timing solutions. Most of the analyses have been performed on line of sight (LOS) propagation environments; however, in the next steps, they can be extended to more practical scenarios such as multipath propagation. Since GPS L1 C/A signals are widely used in different civilian GNSS based applications, without loss of generality different analyses and countermeasure techniques have been developed for this signal. However, due to the similarity of different GNSS signals, the proposed methods can be easily generalized to other satellite positioning systems. The following objectives have been considered for this thesis:

a) Pre-despreading Structural Interference Detection

In order to be effective, a GPS spoofing/meaconing source should transmit at least four pseudorandom noise (PRN) codes each of which having more power compared to the authentic GPS signals. Therefore, a consistent navigation solution can be generated consisting entirely of spoofing sources. In most cases, to be more effective, a spoofer might transmit as many as 10 synchronized PRN signals with consistent features. Therefore, the presence of a spoofing source can considerably increase the power content of structural signals within the GPS bandwidth. However, since counterfeit GPS signals might be also buried under the noise floor similar to the authentic ones, it is very challenging for a GPS receiver to verify the authenticity of its received raw signal

samples before signal acquisition, tracking and position solution. However, having such a capability at a low computation cost can be very advantageous for a GPS receiver.

To this end, a low computational complexity authenticity verification method is proposed that takes advantage of specific features of GPS signals in order to detect the presence of spoofing interference in the received signal set before being processed by a GPS receiver. This method requires a calibration phase involving the measurement of the typical test statistic value for genuine GPS signals and this value will be further utilized for setting the detection threshold. This detection technique can be also employed by an inline signal quality assurance module that can alert a GPS receiver to the presence of possibly misleading interference signals.

b) Spoofing Analysis and Detection during Acquisition Process

During the acquisition process, GPS receivers try to come up with a rough estimate of the received signal's Doppler and code delay. To this end, the receiver performs a two-dimensional search over different code delays and Doppler shifts for each PRN and searches for the highest power correlation peak which is above the detection threshold. The presence of spoofing signals can lead to the observation of additional correlation peaks in the cross ambiguity function (CAF) and also it can increase the noise floor of the receiver. To mislead the acquisition procedure, the spoofing correlation peak must be more powerful than the authentic one and therefore they might be miss-acquired by the GPS receiver. Furthermore, the cross correlation terms caused by higher power spoofing signals can elevate the receiver's noise floor and subsequently reduce the effective SNR

of authentic signals. These effects can adversely affect the GPS acquisition performance in two ways, it can either mislead the acquisition process into estimating an incorrect code delay and/or Doppler frequency or it can reduce the detection performance due to SNR value degradation for the authentic GPS signals.

The research is concentrated on the assessment of spoofing signals' effect on the acquisition process of a typical GPS receiver and it will be shown that the SNR based spoofing discrimination methods are of limited effectiveness and with small circuit modifications, the receiver can measure the absolute power of the correlation peaks which is an effective means of detecting and discriminating spoofing signals. The vulnerability region of both spoofing countermeasure methods is compared using illustrative figures and it will be shown that absolute power monitoring considerably reduces the vulnerability of GPS receivers against spoofing interference.

c) Spoofing Analysis and Detection during the Tracking Process

During the tracking procedure, a GPS receiver tries to come up with a fine estimate of the Doppler shift and code delay corresponding to each acquired PRN. To this end, the receiver employs delay locked loops (DLLs) and phase locked loops (PLLs) focusing on the authentic correlation peak. Therefore, the receiver is not much vulnerable to additional correlation peaks caused by spoofing. To mislead a tracking receiver without forcing it to lose lock, a spoofer must align its correlation peaks to those of authentic signals and then gradually lift-off the tracking point of the receiver by moving away its

higher power correlation peaks (Humphreys et al 2008). This case can be achieved by a synchronized spoofing source that exactly knows the position of its target receiver.

This part of the research analyses the effect of the interaction between spoofing and authentic correlation peaks and proposes a spoofing countermeasure technique that is able to detect this interaction based on the statistical analysis of early, late and prompt correlator outputs. It will be shown that for consistent Doppler and code rates of the spoofing signals, the interaction between spoofing and authentic signals causes amplitude fluctuations. These fluctuations affect the typical distribution of correlation peaks thereby revealing the presence of synchronized spoofing interference. In addition, a detection test has been proposed in order to check the consistency between code rate and Doppler frequency of correlation peaks which are currently tracked by the GNSS receiver. Hardware simulator signals have been utilized to simulate a spoofing attack on a tracking receiver and verify the effectiveness of this proposed countermeasure technique.

d) Spoofing Signal Detection in the Position Solution Layer

Structural interference signals are different from other types of GNSS interference signals since they transmit multiple navigationally consistent PRN coded signals that yield a location. This feature can be used for detection and even localization of spoofing source using spoofed pseudorange measurements. Due to logistical limitations, a spoofing source usually employs a single antenna to transmit several counterfeit PRN signals and consequently all these PRNs experience the same propagation channel and the same delay from the spoofer antenna to the target receiver's antenna.

This part of the research is focused on detecting the presence of spoofed position solutions based on monitoring the clock bias of a moving receiver. It is shown that the pseudorange measurements corresponding to the spoofing PRN signals experience common variations as a function of the receiver antenna movement. These common variations affect the clock state of the position solution and this feature can be utilized to differentiate between spoofed and authentic position solutions. Different motion scenarios in the presence of different local oscillator (LO) qualities are considered for performance evaluation of this authenticity verification technique.

1.5 Thesis Outline

The dissertation is organized in seven chapters and the outline of upcoming chapters is as follows:

Chapter 2 starts with a review on different categories of spoofing generation methods namely GNSS signal simulator, receiver based spoofer and sophisticated receiver based spoofer. Then, Section 2.3 investigates the vulnerability of GPS signals to spoofing interference in a multi-layer approach (i.e. signal processing, data bits and position solution/navigation layers). Section 2.4 provides the received signal model for GPS L1 signals in the presence of spoofing interference for single and multiple antenna receivers. Section 2.5 is dedicated to a literature review on spoofing countermeasure techniques under the categories of spoofing detection and spoofing mitigation. Several techniques including received power monitoring, TOA discrimination, spatial processing, multiple frequency consistency check and vestigial signal detection are discussed in this section. Section 2.6 discusses different test scenarios that have been already adopted to evaluate

spoofing countermeasure methods and finally, summarizing notes are discussed in Section 2.7.

Chapter 3 concentrates on pre-correlation authenticity verification of GPS signals based on signal structure (IS-GPS-200G). After a brief introduction in Section 3.1, the problem formulation is discussed in Section 3.2 where spectral properties of GPS L1 signals and their delay and multiply (DAM) property are introduced. Section 3.3 discusses the proposed authentication technique which consists of four steps, namely differential Doppler removal, signal filtering, noise filtering, compensating the effect of AGC and finally spoofing detection. Simulation results are then provided in Section 3.4 and real data collection scenario and its processing results are presented in Section 3.5. Section 3.6 introduces TEXBAT data sets and their processing results based on the proposed authentication method. The concluding notes are finally provided in Section 3.7.

Chapter 4 analyses the effect of spoofing signals on the acquisition process of GPS receivers. Section 4.1 provides an introduction to the topic and then the system model is introduced in Section 4.2. After that, Section 4.3 provides a brief discussion on GPS signal acquisition as a GLRT detection problem. Section 4.4 analyses the noise floor elevation due to the cross correlation effect of spoofing signals. Section 4.5 analyses the received signal to noise ratio of authentic signals in presence of spoofing interference. Section 4.6 discusses the vulnerability of GPS acquisition in the presence of a spoofing attack. This section consists of two subsections that analyse the vulnerability of the acquisition process in two cases, namely common authentic and spoofing PRNs and uncommon authentic and spoofing PRNs. Section 4.7 introduces two spoofing

countermeasure methods that are based on the SNR monitoring and absolute power monitoring of received GPS signals and then compares the vulnerability region of these two methods. Section 4.8 provides real data collection and analysis results and finally the concluding notes of the preceding discussions are provided at Section 4.9.

Chapter 5 analyzes the effect of a synchronized spoofing attack on a tracking receiver and then proposes two spoofing countermeasure techniques based on the statistical analysis of correlator outputs and Doppler and code rate consistency check during the tracking process. Section 5.1 provides an introduction to the chapter materials and then Section 5.2 analyzes a spoofing attack on a tracking receiver. Section 5.3 discusses the problem formulation and provides mathematical analysis of the interaction between spoofing and authentic signals. Section 5.4 introduces the proposed spoofing detection techniques for the two cases of locked Doppler and consistent Doppler spoofing scenarios. Section 5.5 introduces the data collection and simulation of spoofing scenarios using the Spirent hardware simulator. Section 5.6 presents the data processing results and finally, Section 5.7 provides the summary and concluding notes.

Chapter 6 proposes a PVT authenticity verification method based on the clock state monitoring of a moving GPS receiver. Section 6.1 provides a brief introduction on the topic and its importance. Section 6.2 introduces the problem formulation and compares the equations for spoofed and authentic pseudoranges for two scenarios of non-aligned and aligned spoofing attacks. Section 6.3 presents the proposed position solution authentication tests based on monitoring receiver's clock bias for different motion scenarios, namely known trajectory, circular trajectory, random walk motion, linear

trajectory and finally completely unknown trajectory. The simulation results are provided in Section 6.4 and the data collection and processing in presence of different motions and different oscillator qualities are shown in Section 6.5. Concluding notes are finally presented in Section 6.6.

Chapter 7 provides a summary of the research results presented in previous chapters. Section 7.1 proposes a possible structure for a spoofing aware GPS receiver that employs that employs spoofing countermeasure techniques at different operational layers in order to reduce its vulnerability to structural interference signals. Section 7.2 discusses the possibilities for future research in the context of GNSS signal authenticity verification.

Chapter Two: A Review on Spoofing Countermeasure Techniques

2.1 Introduction

Spoofing signals were considered a threat for military GNSS signals from the start however, due to the ever increasing civilian applications of GNSS, it is of critical importance to verify the authenticity of PVT solutions provided by related equipment. Spoofing signals try to induce falsified timing and position solution to their target receivers and they are designed to mimic different features the authentic GNSS signals in order to prevent detection. The ubiquity of GNSS has generated the motivation for spoofing attacks and generating this type of interference has become more feasible and less costly due to advances in software defined radio (SDR) technology. As such, many researchers have started analysing the vulnerability of GNSS systems to spoofing attack and developing spoofing discrimination and mitigation techniques (Humphreys et al 2008, Nielsen et al 2011, Montgomery et al 2009, Scott 2003, Chen et al 2012, Shepard et al 2012, Kim et al 2012, Wullems 2012, Motella et al 2010, and Tippenhauer et al 2011).

This chapter first provides a brief review on different spoofing generation techniques. Subsequently, the vulnerability of civilian GPS receivers to spoofing attacks will be investigated in different operational layers. Then, a brief review on previously anti-spoofing techniques will be provided in terms of spoofing detection and spoofing mitigation. Finally, some test scenarios will be presented that are useful for testing the spoofing/anti-spoofing algorithms.

2.2 Classification of Spoofing Generation Techniques

Spoofing generation can be divided into three main categories (Humphreys et al 2008, Montgomery et al 2009, Ledvina et al 2010)

2.2.1 GNSS Signal Simulators

This category of spoofing attack consists of a GNSS signal simulator connected to an RF transmitter. The signals generated by this kind of spoofers are not essentially synchronized to real GNSS signals. In other words, the spoofing correlation peaks are not essentially aligned with the authentic ones. Therefore, this type of spoofing signals looks like noise for a GNSS receiver operating in the tracking mode (even if the spoofer power is higher than the authentic signals). However, this type of spoofers can adversely affect the acquisition process of conventional GNSS receivers and degrade their performance especially if the spoofing signal power is higher than that of the authentic signals. A GPS signal simulator is the simplest GPS spoofer and it can be detected by different anti-spoofing techniques such as amplitude monitoring, consistency check among different measurements and consistency check with IMUs.

2.2.2 Receiver Based Spoofers

A more advanced type of spoofer consists of a GNSS receiver concatenated with a spoofing transmitter. This system first synchronizes with the current GNSS signals and extracts the position, time and satellite ephemeris, and then generates the spoofing signal knowing the 3D pointing vector from its transmit antenna toward the target receiver's antenna. The correlation peaks generated by this type of spoofer can be aligned to the authentic correlation peaks and as a result, the tracking receivers can be also misled.

Figure 2-1 shows the receiver based spoofer structure proposed by Scott (2003) and Humphreys et al (2008).

Figure 2-1 Receiver based spoofing attack on a GNSS receiver

Signals from this kind of spoofer are difficult to discriminate from the authentic signals and the spoofer is more complicated than the first category. The main challenge toward realization of this kind of spoofer is projecting the spoofing signals to the intended victim receiver with the correct signal delay and strength. It should be noted that the spoofing power should be higher than the authentic signal power in order to successfully mislead the target receiver but it should not be much higher than the typical power of GNSS signals in order to prevent being detected by RSS methods.

Aligning the carrier frequency and phase to the authentic GPS signals, minimizing the self-jamming effect and suppressing relative data bit latencies are other limitations that a receiver based spoofer should deal with (Humphreys et al 2008). As it will be discussed in Chapter 5, phase alignment between the spoofing replica and the authentic peak is a very challenging process that requires centimetre level knowledge of the 3D pointing vector from the spoofer antenna phase centre toward the target receiver's antenna. Therefore, it would be a great advantage in this case if the spoofer antennas were placed very close to the target receiver antenna or if there is a fixed distance between the spoofer antenna and its target receiver's antenna. This type of spoofers is relatively hard to detect since they are synchronized to the real GPS satellites.

2.2.3 Sophisticated Receiver Based Spoofers

This category is the most complex and effective type of the spoofing generation methods. Herein, the spoofer is assumed to know centimetre level position of the target receiver's antenna phase centre to perfectly synchronize the spoofing signal code and carrier phase to those of authentic signals at the receiver (Ledvina et al 2010). This type of spoofer can take advantage of several transmit antennas in order to defeat angle of arrival (AOA) based anti-spoofing techniques. In this case, the spoofer needs to synthesize an array manifold that is consistent with the array manifold of the authentic signals to defeat AOA discriminating spoofing countermeasure methods.

The complexity of materializing such a spoofer is much higher than the two previous categories discussed above. The effectiveness area of this type of spoofer is much more limited since the PRN signals generated by different spoofer antennas must conform together so that their corresponding pseudorange measurements converge to a position solution. This criterion might be achieved in a very small region in case spoofer's antennas have a considerable separation. Carrier phase alignment and array manifold synchronization are two other limiting parameters that might be achieved only for a very small region where target receiver antennas are located. In addition to the previously mentioned factors, there are some physical limitations regarding the spoofer antenna placement relative to the target receiver antenna(s) and their synchronization. As such, the realization of this type of spoofers is very difficult and in many cases impractical due to the geometry and movement of the target receiver antenna(s).

2.3 GPS Vulnerability against Spoofing Attack

The vulnerability of GPS to spoofing can be investigated in three operational layers namely the signal processing, data bit and position/navigation solution levels.

2.3.1 GPS Vulnerability to Spoofing at the Signal Processing Level

The structure of civilian GPS signals, including the modulation type, PRN signals, transmit frequency, signal bandwidth, Doppler range, signal strength and many other features are publicly known (IS-GPS-200G & IS-GPS-705C). Furthermore, GPS is a backward compatible technology whose L1 signal features does not significantly change through different generations of GPS satellites. GPS receivers are equipped with some form of automatic gain control (AGC) block that compensates the power variations in the received GPS signal. However, AGC can increase the vulnerability of GPS receivers against higher power spoofing signals since it automatically adjusts the receiver input gain according to the more powerful spoofing signals (Wen et al 2005). Therefore, knowing the general structure and operational basics of a civilian GPS receiver, a spoofer module can generate counterfeit signals that are similar to the authentic GPS signals so as to effectively mislead its target GPS receiver(s).

2.3.2 GPS Vulnerability to Spoofing at the Data Bit Level

The framing structure of the GPS signals is publicly known. The navigation frame consists of different parts such as almanac and satellite ephemeris. This information does not change rapidly during short time intervals; for example, the satellite ephemeris information can be acquired in less than 1 minute but it remains unchanged for 12.5 minutes (Jun et al 2009). Therefore, the spoofer can take advantage of this stability in

order to regenerate the GPS data frame. In addition, the satellite health status bits can be manipulated by a spoofer in order to mislead the receiver toward rejecting valid satellite signals (Xi-jun et al 2009).

Nighswander et al (2012) have discussed several possible software attacks on GPS L1 C/A signals by manipulating navigation data bits in order to confuse target GPS receivers. They have investigated the vulnerability of several commercial and industrial grade GPS receivers against their proposed spoofing methods and have shown that all of these receivers are vulnerable to software attacks and can be spoofed through the manipulation of ephemeris information. Since software attacks via navigation data are not predicted in the design of most of the conventional GPS receivers, this type of spoofing can cause permanent damage on some of these receivers.

2.3.3 GPS Vulnerability to Spoofing at the Position Solution Level

The spoofer can inject counterfeit pseudorange measurements into the receiver observations, leading to a wrong PVT solution. In case that the number of spoofed pseudorange measurements is very small (e.g. 1 or 2), the receiver autonomous integrity monitoring (RAIM) techniques can detect and discard the presence of counterfeit spoofed measurements (Ledvina et al 2010). However, for the case of a higher number of spoofed measurements, RAIM methods may fail to detect the presence of spoofing signals.

Based on the analysis provided by Juang (2009), spoofing signals can impose PVT deviation on the solution provided by a GPS receiver before it is detected by RAIM techniques. It is discussed that the PVT error is proportional to the range residuals

multiplied by a geometry related factor. This author has developed a vulnerability index against spoofing (VIAS) that indicates the geometric relationship between GPS constellation and the spoofer position that results in receiver position solution deviations. It is shown that the VIAS changes over time and position and that it has a higher value where the position dilution of precision (PDOP) value is high. Based on the discussions provided by Juang (2009), the VIAS index can be used in the design and development of anti-spoofing methods.

In some applications, GPS receivers are strictly used for timing synchronization such as power distribution networks and CDMA/GSM cell towers. In many cases, a timing receiver is a static receiver whose coordinates are completely known by the spoofer. Therefore, the spoofing attack can align its signals to the authentic ones and gradually misdirect the target receiver into tracking a spoofing correlation peak. In this case, the spoofed position coordinates can still remain the same while the timing information gradually deviates from its genuine value.

2.4 Received Signal Model

Anti-spoofing techniques can be generally investigated for two receiver categories namely: single antenna and multiple antenna receivers. This section describes the received signal model for these receivers in the presence of spoofing attacks.

2.4.1 Single Antenna Receiver

Considering the GPS L1 C/A code, the received signal subjected to a spoofing attack can be modeled as

$$r(nT_s) = \sum_{m \in \mathbf{J}^a} \sqrt{p_m^a} F_m^a(nT_s) + \sum_{q \in \mathbf{J}^s} \sqrt{p_q^s} F_q^s(nT_s) + \eta(nT_s), \tag{2-1}$$

where

$$\begin{aligned} F_m^a(nT_s) &= h_m^a(nT_s - \tau_m^a) c_m^a(nT_s - \tau_m^a) e^{j\phi_m^a + j2\pi f_m^a nT_s}, \\ F_q^s(nT_s) &= h_q^s(nT_s - \tau_q^s) c_q^s(nT_s - \tau_q^s) e^{j\phi_q^s + j2\pi f_q^s nT_s}, \end{aligned} \tag{2-2}$$

and $\mathbf{J}^a$ and $\mathbf{J}^s$ are authentic and spoofing signal sets, respectively. T_s is the sampling interval and ϕ, f, p and τ are the carrier phase, Doppler frequency, signal power and code delay of the received signals, respectively and the superscripts s and a refer to the spoofing and authentic signals, respectively. In this model, $h(nT_s)$ is the transmitted navigation data bit and $c(nT_s)$ is the PRN sequence at time instant nT_s. The subscripts m and q correspond to the mth authentic signal and the qth spoofing signal, respectively. $\eta(nT_s)$ is the complex additive white Gaussian noise with variance σ^2 and j is the square root of -1.

2.4.2 Multiple Antenna Receiver

Assume an arbitrary N-element antenna array configuration in which one antenna is chosen as the reference antenna. Without loss of generality it can be assumed that the reference coordinate system is located at the reference antenna (r_1) as shown in Figure 2-2. Here, it is assumed that the spoofer uses a single antenna to transmit several PRN signals from the same direction. Therefore, the complex baseband representation of N received spatial samples of authentic and spoofing signals impinging on the antenna array before de-spreading can be written in vector form as

$$\mathbf{r}(nT_s)=\begin{bmatrix} r_1(nT_s) \\ \vdots \\ r_N(nT_s) \end{bmatrix}=\sum_{m=1}^{N_{Auth}}\mathbf{a}_m\sqrt{p_m^a}F_m^a\left(nT_s\right)+\mathbf{b}\sum_{q=1}^{N_{Spoof}}\sqrt{p_q^s}F_q^s\left(nT_s\right)+\boldsymbol{\eta}\left(nT_s\right), \tag{2-3}$$

where $\boldsymbol{\eta}$ is the $N\times 1$ complex additive white Gaussian noise vector with covariance matrix $\sigma^2\mathbf{I}$ and $\mathbf{I}$ represents a N by N identity matrix. Herein, it is assumed that all the spoofing PRN signals are transmitted from the same antenna. $\mathbf{a}_m$ and $\mathbf{b}$ are steering vectors incorporating all spatial characteristics of the antenna array for authentic and spoofing signals, which can be written as

$$\mathbf{b}=\begin{bmatrix} 1 \\ b_2 \\ \vdots \\ b_N \end{bmatrix}=\begin{bmatrix} e^{-j\frac{2\pi\mathbf{d}_{11}^{ant}\bullet\hat{\mathbf{d}}^{spoof}}{\lambda}} \\ e^{-j\frac{2\pi\mathbf{d}_{21}^{ant}\bullet\hat{\mathbf{d}}^{spoof}}{\lambda}} \\ \vdots \\ e^{-j\frac{2\pi\mathbf{d}_{N1}^{ant}\bullet\hat{\mathbf{d}}^{spoof}}{\lambda}} \end{bmatrix},\quad \mathbf{a}_m=\begin{bmatrix} 1 \\ (a_m)_2 \\ \vdots \\ (a_m)_N \end{bmatrix}=\begin{bmatrix} e^{-j\frac{2\pi\mathbf{d}_{11}^{ant}\bullet\hat{\mathbf{d}}_m^{sat}}{\lambda}} \\ e^{-j\frac{2\pi\mathbf{d}_{21}^{ant}\bullet\hat{\mathbf{d}}_m^{sat}}{\lambda}} \\ \vdots \\ e^{-j\frac{2\pi\mathbf{d}_{N1}^{ant}\bullet\hat{\mathbf{d}}_m^{sat}}{\lambda}} \end{bmatrix}, \tag{2-4}$$

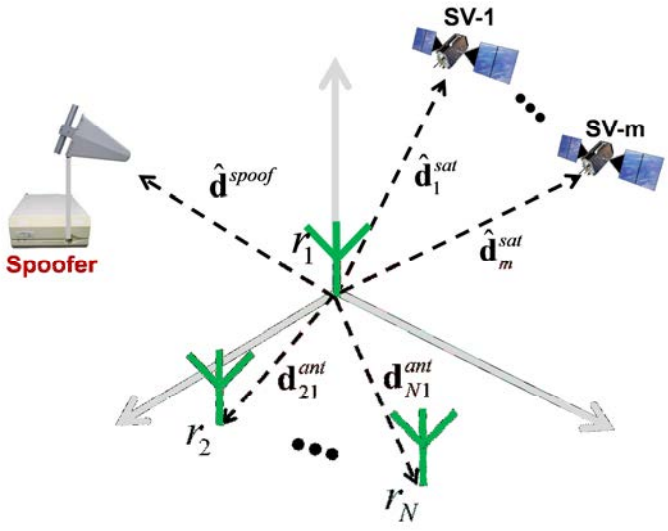


Figure 2-2 Multiple antenna receiver configuration

where $\mathbf{d}_{i1}^{ant}$ represents a vector pointing from the origin (reference antenna phase centre) to the *i*th antenna phase centre. $\hat{\mathbf{d}}_{m}^{sat}$ and $\hat{\mathbf{d}}^{spoof}$ represent the unit pointing vectors from the origin to the *m*th authentic satellite and spoofing source respectively; λ represents the signal carrier wavelength.

2.5 Classification of Anti-Spoofing Techniques

Several anti-spoofing techniques have been proposed in the open literature and as it was discussed in Chapter 1, they can generally be classified into two main categories, namely *spoofing detection* and *spoofing mitigation*. In the following sub-sections a brief introduction is provided on different techniques proposed for each category.

2.5.1 Spoofing Detection

2.5.1.1 Received Signal Strength Monitoring

In open sky conditions, satellites movement and ionosphere variations can cause gradual smooth changes in the received signal strength (RSS).However, when the receiver starts tracking a higher power spoofing signal, a jump might be observed in the RSS that indicates the presence of a spoofer. Akos (2012) has proposed a spoofing countermeasure method based on monitoring the receiver's AGC gain level. He has shown that the presence of spoofing signals increases the power content of the received signal set and this changes the AGC level. Based on the analyses provided by Akos (2012), AGC monitoring is a powerful measure for detecting the presence of spoofing signals especially if their power level is considerably higher than that of the authentic ones.

Most GPS receivers employ C/N_0 measurements as a parameter that characterizes the RSS. Nielsen et al (2012) and Dehghanian et al (2012) have proposed spoofing countermeasure techniques based on C/N_0 analysis. They have shown that the effectiveness area of GNSS spoofers reduces when the receivers are equipped with C/N_0 monitoring techniques. A spoofing aware receiver can continuously monitor the received C/N_0 and look for any unusual variation that can be a sign of a spoofing attack. A GPS receiver can store a time history of measured C/N_0 values and subsequently detect undesired variations in the received C/N_0. However, as it will be discussed in the upcoming chapters, the presence of higher power spoofing signals does not essentially affect the received C/N_0 of a GNSS receiver, therefore, there are some limitations for C/N_0 based spoofing detection techniques.

2.5.1.2 RSS Variations versus Receiver Movement

Based on the free space propagation law, the received power of a signal propagated in free space is proportional to the inverse of the squared propagation distance. GPS satellites are about 20,000 kilometres away from the earth surface; therefore, a receiver moving on the earth surface in low multipath open sky environment and calm ionospheric situation does not experience considerable changes in the received power from authentic satellites. However, as discussed before, the spoofing signal is usually transmitted from a single directional antenna located much closer to the receiver compared to the GNSS satellites. Therefore, the movement of the receiver with respect to the spoofer antenna can considerably change the C/N_0 value received from spoofing signals (Wen et al 2005).

Figure 2-3 illustrates the variations of spoofing and authentic received C/N_0 values versus the receiver's distance from spoofer antenna. It is observed that when the spoofer is very close to its target receiver, even a slight movement between spoofer and the target receiver can considerably affect the received spoofing signal C/N_0. For example, as it is shown in Figure 2-3, when the distance between spoofer antenna and user's antenna changes from 8 m to 100 m, the received C/N_0 reduces by 22 dB. It should be considered that all spoofing signals are usually transmitted from the same antenna and therefore, all experience the same propagation medium. As such, variations of all spoofing signals will be the same regardless of the receiver movement and multipath effects (Nielsen et al 2011).

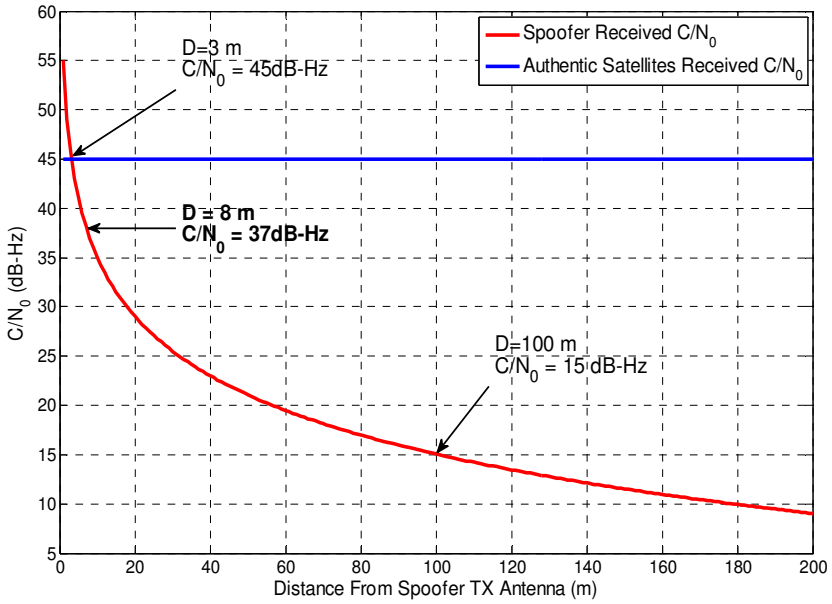


Figure 2-3 Variations of spoofing and authentic received C/N0 versus receiver's distance from spoofer transmitting antenna

This method is a low complexity spoofing discrimination technique that does not impose extensive hardware/software modifications to the GPS receiver. However, since the

receiver does not necessarily know the position of the spoofer antenna, there is no guarantee that the receiver movement considerably changes the spoofer's C/N_0. For instance, when both spoofing transmitter and GPS receiver are located on the same platform, the movement of the platform does not cause variation in the measure of spoofing signals' C/N_0. Another limitation of this technique is that it cannot be employed for the case of static receivers, e.g. static timing receivers. Therefore, the effectiveness of this spoofing discrimination technique is limited to a few spoofing scenarios.

2.5.1.3 Spoofing Detection based on Antenna Pattern Diversity

Spoofing sources are usually a terrestrial transmitter that simultaneously propagates several PRN signals. Contrary to this, authentic GNSS signals are propagated from spatially distributed sources, namely GNSS satellites. This difference between propagation models can be detected using different antennas with different reception patterns. Zhang et al (2013) and Trinkle et al (2012) have proposed a spoofing detection technique that takes advantage of a patch and a monopole antenna. These two antennas are assumed to have complementary reception patterns, i.e. the patch antenna has a maximum at the zenith while the monopole has a minimum at that angle. The signals of these two antennas are fed to different low-end GNSS receivers and then the standard deviation of C/N_0 differences of these two receivers is calculated. The statistical analyses results show that two distinct distributions are achieved for the case of spoofing and authentic signals and this can be used for detection of the presence of spoofing signals.

2.5.1.4 Different Frequencies Power Level Comparison

There is a predefined power level difference between GPS signals in different frequency bands and many receivers are capable of monitoring both L1 and L2 signals. However, a less complicated spoofer may only generate counterfeit signals at the L1 frequency. Therefore, a large difference between L1 and L2 power levels or the absence of L2 signals for some specific PRNs can reveal the presence of a spoofing signal (Wen et al 2005). This method can successfully detect a single frequency spoofer. However, most civilian GPS receivers do not have the ability to monitor both L1 and L2 frequency bands and this discrimination technique imposes additional hardware complexity on GPS receivers.

2.5.1.5 Multi-Antenna Spoofing Discrimination

Due to logistical limitations, spoofing transmitters usually transmit several counterfeit signals from the same antenna while the authentic signals are transmitted from different satellites with different directions. Therefore, a spatial processing technique can be employed to estimate the spatial signature of received signals and discriminate those signals that are spatially correlated (Montgomery et al 2009, Daneshmand et al 2012, McDowell 2007, Chang 2012, Meurer et al 2012, Hornbostel et al 2013, Konovaltsev et al 2013, Borio 2013).

Montgomery et al (2009) have proposed a spoofing detection technique that monitors the phase difference between two fixed GNSS antennas for around one hour. Knowing the orientation of the antenna array and the azimuth and elevation of each satellite, the theoretical phase differences can be calculated and compared to the practical phase

difference observed by the antenna array in order to discriminate the spoofing threat. The main drawback of this algorithm is that it takes a long time (about 1 hour) to discriminate against spoofing signals. In addition, this technique requires a calibrated antenna array with known array orientation in order to operate properly. Borio (2013) has taken advantage of phase only analysis of variance (PANOVA) method in order to detect the phase difference coherency of spoofed PRN signals for a double antenna receiver. He has developed a GLRT detection test that is able to discriminate the spoofed signal set from the authentic one during the tracking stage of a GNSS receiver.

McDowell (2007) has proposed an antenna array processing technique that is used to detect and mitigate spoofing signals based on their spatial correlation. The correlator output phase measurements for different PRN signals are mutually compared to identify the ones received from the same spatial sector. This technique can successfully detect spoofing signals and it does not need any array calibration or information regarding array orientation. It can effectively discriminate the spoofing scenarios that employ a single transmit antenna. In addition, multipath propagation has minor effects on the performance of this method since all of the spoofing signals experience the same propagation channel characteristics. However, this technique increases the hardware complexity of the GPS receiver as it necessitates the use of several antenna branches. Furthermore, applying this method increases the computational complexity of GPS receiver since the receiver needs to acquire and track both spoofing and authentic signals in order to be able to discriminate spoofing PRNs.

A multiple-antenna spoofer might be able to defeat the multiple-antenna spoofing discrimination techniques depending on the number of transmit antennas, the number of receiver antennas and the geometry of spoofer antennas with respect to the target receiver antennas. However, there are many practical limitations toward realizing such a sophisticated spoofing scenario.

2.5.1.6 Synthetic Array Spoofing Discrimination

Nielsen et al (2011), Broumandan et al (2012) and Nielsen et al (2010) have proposed a spoofing detection technique that employs a synthetic antenna array. As shown in Figure 2-4, their proposed technique employs a single antenna handheld GPS receiver moving along a random trajectory and forming a synthetic antenna array structure. The received signals' amplitude and phase corresponding to different PRN signals are continually compared to each other using a correlation coefficient metric (ς_{ij}). Therefore, after acquiring different PRN signals in the received signal set (both authentic and spoofing signals); spoofing signals are discriminated using the following normalized correlation coefficient:

$$\varsigma_{ij} = \left| \frac{E\left[(\mathbf{u})_i^H (\mathbf{u})_j \right]}{\sqrt{E\left[(\mathbf{u})_i^H (\mathbf{u})_i \right]} \sqrt{E\left[(\mathbf{u})_j^H (\mathbf{u})_j \right]}} \right|, \tag{2-5}$$

where $E[\bullet]$ represents the statistical expectation and the superscript H denotes the conjugate transpose. $(\mathbf{u})_i$ and $(\mathbf{u})_j$ represent the ith and jth columns of matrix $\mathbf{u}$ which is defined as follows:

$$\mathbf{u}=\begin{bmatrix} \left[\mathbf{u}^a[1],\mathbf{u}^s[1]\right] \\ \left[\mathbf{u}^a[2],\mathbf{u}^s[2]\right] \\ \vdots \\ \left[\mathbf{u}^a[M],\mathbf{u}^s[M]\right] \end{bmatrix}_{M\times L}, \tag{2-6}$$

$$\mathbf{u}^a[k]=\left[u_1^a(kNT_s),\cdots,u_{N_{Auth}}^a(kNT_s)\right],$$

$$\mathbf{u}^s[k]=\left[u_1^s(kNT_s),\cdots,u_{N_{Spoof}}^s(kNT_s)\right].$$

In (2-6), it is assumed that correlator outputs are monitored during M time instances and $\mathbf{u}$ is a $M\times L$ matrix where L is the total number of acquired GNSS signals ($L \leq N_{Auth}+N_{Spoof}$). $\mathbf{u}^a[k]$ is the set of correlator outputs for all acquired authentic signals at time instant kNT_s, whereas $\mathbf{u}^s[k]$ consists of all acquired spoofing peaks for that time instant. M is the number of equivalent spatial samples.

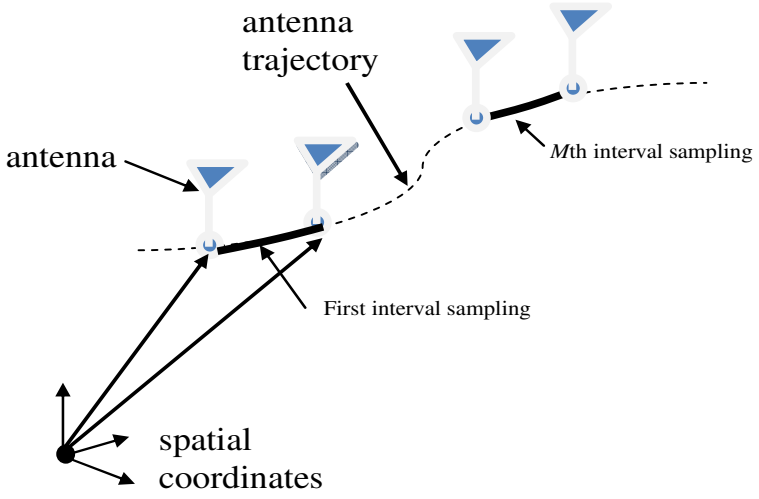


Figure 2-4 Spatial sampling for a moving handheld GPS receiver (modified from Nielsen et al 2011)

Figure 2-5 illustrates the normalized signal amplitude for acquired spoofing and authentic signals. During the data collection, the antenna was randomly moved. It is observed that the amplitude variations for spoofing signals are highly correlated (i.e. the plots representing the amplitudes of PRN-16, PRN-18, PRN-21 and PRN-29 are totally overlaid) while this correlation does not exist for the authentic signals (i.e. the amplitudes of PRN-22 and PRN-24 do not overlay).

This technique works effectively even in multipath environments because all the spoofing signals experience the same fading path and they are all similarly affected by multipath reflections. Furthermore, since this method does not employ several receive antennas, its hardware complexity is much lower as compared to the techniques proposed by Montgomery et al (2009) and McDowell (2007).

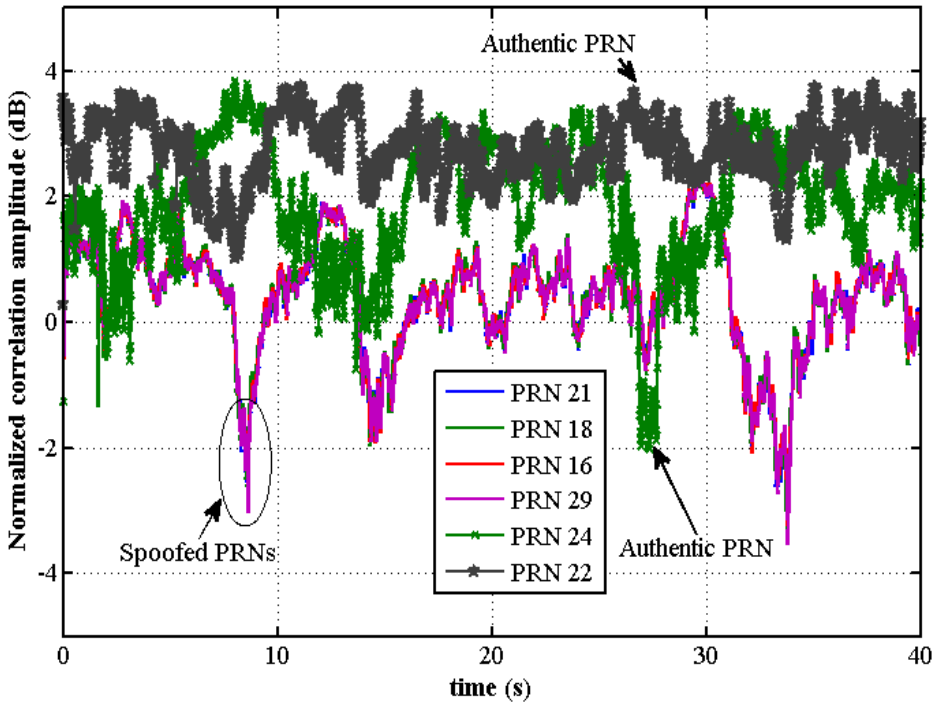


Figure 2-5 Correlation amplitude for spoofing and authentic PRN signals

2.5.1.7 Multiple Receiver Spoofing Detection

Spoofing signals can be detected by comparing the measurements coming from different receivers that are geographically separated (Swaszek et al 2013, Psiaki et al 2011, O'Hanlon et al 2012, and O'Hanlon et al 2010). Swaszek et al (2013) have proposed a Neyman Pearson spoofing detection test that compares the position solutions provided by two/three spatially separated GPS receivers in order to verify the authenticity of received signals. The relative positions of different receiver's antennas are assumed to be known and it is assumed that all the receivers are under spoofing attack when a spoofing signal exists. They have shown that in the presence of spoofing signals, all the receivers come up with similar position solutions while in presence of authentic signals, each receiver extracts a different position solution. This feature has been used for detecting the presence of spoofing threats.

Psiaki et al (2011) have proposed a civilian spoofing detection method based on cross correlating the received signals from a trusted GPS receiver to those of an under test GPS receiver. GPS signals are authenticated if there is a high correlation between military P(Y) codes of the received signals of both receivers otherwise, a spoofing attack will be declared. Herein, the civilian C/A codes are used to synchronize the data snapshots of the trusted and under test receivers. Although this technique can potentially detect many spoofing scenarios, it is vulnerable to the case that a GPS repeater is receiving and retransmitting both C/A and P(Y) GPS signals.

2.5.1.8 PRN Code and Data Bit Latency

In the case that the receiver based spoofer does not have any prior information about the navigation data bits, it should first decode the received GPS signals and extract the navigation data bit and accordingly generate a fake spoofing signal. Hence, an unavoidable delay exists between the spoofing data bit boundaries with respect to the authentic ones (Cho et al 2008). Therefore, if the data bit transition happens at time instants with a spacing other than 20 ms for GPS L1, then a spoofing attack might be underway.

This technique encounters some limitations because the data frame structure of GPS is already known and it consists of different parts with different update frequencies. The update frequency of most parts of the GPS frame is very low. Therefore, the spoofer can predict the majority of data bits if it has already acquired the GPS information before starting to transmit fake spoofing signals.

2.5.1.9 L1/L2 Signals Relative Delay

GPS satellites transmit encrypted P(Y) codes on both L1 and L2 frequencies. The signals received on these two frequencies have a relative delay/attenuation that is caused by the different frequency response of the ionosphere. Therefore, if a dual frequency GPS receiver correlates the L1 and L2 signals, it should observe only one correlation peak (Wen et al 2005). The propagation delay in L2 is larger than the L1 frequency; therefore, the approximate relative delay of correlation peaks is already known to the GPS receiver. The spoofer should be able to generate signals on both frequencies in order to defeat this countermeasure.

2.5.1.10 Signal Quality Monitoring (SQM)

SQM techniques have been previously employed to monitor the GPS correlation peak quality in multipath fading environments (Phelts 2001). Spoofing attacks on a tracking receiver can affect the correlator output in a way similar to that of multipath components (Shepard et al 2011). Therefore, Cavaleri et al (2010), Ledvina et al (2010), Wesson et al (2011) and Pini et al (2011) have extended the SQM techniques to detect spoofing attacks on tracking receivers that are working in line of sight (LOS) conditions. They have employed the *ratio* and *delta* SQM tests in order to detect any abnormal asymmetry and/or flatness of GPS correlation peaks that is imposed by the interaction between authentic and spoofing signals. It is assumed that the receiver has initially locked onto the authentic correlation peaks and a spoofing source tries to deceive the receiver toward tracking its fake correlation peaks.

The SQM anti-spoofing techniques are powerful methods toward detecting a spoofing attack especially in the LOS propagation environments. However, in the presence of multipath propagation and/or atmospheric instability, the SQM method might not be able to correctly detect spoofing signals.

2.5.1.11 Consistency Check with Other Navigation and Positioning Sensors

Augmenting data from auxiliary devices such as IMUs can help the target receiver to discriminate the spoofing threat (White et al 1998, Niedermeier et al 2010, Niedermeier et al 2012, and Gao & Bobye 2013). In addition, a GPS receiver can compare the solution extracted from received GPS signals to other position and navigation solutions obtained by mobile networks or WiFi access points. Therefore, if the confidence region of

different solutions does not have an intersection, there is a high likelihood of a spoofing attack.

Employing this spoofing detection technique can highly increase the reliability of position and timing solutions provided by GNSS receivers. Also, aiding from auxiliary sensors can considerably reduce the reaquisition time for a spoofed/jammed receiver (Gao & Bobye 2013). However, this approach increases the hardware and software complexity of the receivers. In addition, in case of consistency check with other wireless positioning techniques, it should be considered that there is a limited coverage of cellular and WiFi networks which, in turn, limits the applicability of this spoofing discrimination technique within specific operational environments.

2.5.1.12 Cryptographic Authentication

Authentication techniques can be employed to detect spoofing threats in both civilian and military applications. This capability is considered in the military version of GPS signals; however, cryptographic authentication procedures are not foreseen at this time for civilian GPS signals. Some articles have discussed possible approaches for cryptographic authentication of civilian GPS signals (Hein et al 2007, Xi-jun et al 2009, Schielin et al 2012, Humphreys 2013, Wesson et al 2011, Scott 2003, and Lo et al 2010). Scott (2003) has proposed cryptographic authentication techniques for modern GPS signals such as L2C and L5 and wide area augmentation system (WAAS) signals. Cryptographic authentication is potentially the most powerful approach for countermeasuring spoofing attacks on GNSS. However, most of the cryptographic authentication techniques require

some modifications in the GPS signal structure. Therefore, these methods do not seem to be readily applicable to the legacy GPS constellation.

2.5.1.13 Code and Phase Rates Consistency Check

In the case of authentic signals, the Doppler frequency and the code delay rate are consistent because they are both affected by the relative movement between GPS satellite and receiver (Misra & Enge 2006). Under stable ionospheric conditions, this consistency requires that

$$f_l^a = -f_{RF}\,\dot{\tau}_l^a, \tag{2-7}$$

where f_{RF} is the RF frequency of L1 GPS signals (f_{RF} = 1575.42 MHz) and $\dot{\tau}_l^a$ is the code delay rate for the lth authentic PRN signal. A low quality spoofer might not keep this consistency between Doppler frequency and code delay rate (Wen et al 2005). As such, a spoofing aware receiver can successfully detect this type of spoofing signals if the loop filter output of phase locked loop (PLL) and delay locked loop (DLL) are not consistent. The PLL and DLL loop filter outputs are estimates of the phase and delay rates respectively.

2.5.1.14 Received Ephemeris Consistency Check

The navigation message of each satellite contains some ephemeris information corresponding to the position of other GPS satellites. Any inconsistency among these ephemeris data can alert an unsynchronized spoofing attack.

2.5.1.15 GPS Clock Consistency Check

The navigation message of each PRN signal contains the GPS clock information. The GPS clock obtained from different satellites of GPS constellation should be consistent. However, the GPS time extracted from an unsynchronized spoofer might not be consistent with the GPS time extracted from other satellites and this can alert the presence of a spoofing attack.

Table 2-1 summarizes the performance of the previously discussed spoofing detection algorithms.

Table 2-1 Summary of spoofing detection techniques

Anti-Spoofing Method	Spoofing Feature	Complexity	Effectiveness	Receiver Required Capability	Spoofing Scenario Generality
RSS Monitoring	*Higher C/N_0*	*Low*	*Medium*	*C/N_0 Monitoring*	*Medium*
RSS Variation vs. Receiver Movement	*Higher Power Variations due to proximity*	*Low*	*Low*	*Antenna Movement / C/N_0 Monitoring*	*Low*
Antenna Pattern Diversity	*Low elevation angle*	*Medium*	*Medium*	*Specially Designed antennas*	*Medium*
L1/L2 Power Comparison	*No L2 Signal for Spoofer*	*Medium*	*Low*	*L2 Reception Capability*	*Medium*
Direction of Arrival Comparison	*Spoofing signals Coming from the Same Direction*	*High*	*High*	*Multiple Receiver Antennas*	*High*
Pairwise Correlation in Synthetic Array	*Spoofing signals Come from the Same Direction*	*Low*	*High*	*Measuring Correlation Coefficient*	*High*
TOA Discrimination	*Inevitable Delay of Spoofing Signal*	*Medium*	*Medium*	*TOA Analysis*	*Low*
Signal Quality Monitoring	*Deviated shape of Correlation Peak*	*Medium*	*Medium*	*Multiple Correlators*	*Low*
Consistency Check with other Solutions	*Inconsistency of Spoofing Solution*	*High*	*High*	*Different Navigation Sensors*	*High*
Cryptographic Authentication	*Not Authenticated*	*High*	*High*	*Authentication*	*High*
Code and Phase rate Consistency Check	*Mismatch between Spoofed Code and Phase rate*	*Low*	*Low*	---	*Low*
GPS Clock Consistency	*Spoofing/Authentic Clock Inconsistency*	*Low*	*Medium*	---	*Medium*
Multiple Receiver Spoofing Detection	*Same Solution for Different receivers/absence of valid spoofed P(Y)*	*Medium*	*High*	*Data link Between Receivers*	*High*

2.5.2 Spoofing Mitigation

2.5.2.1 Vestigial Signal Detection

In most cases, spoofer generates additional correlation peaks usually with a higher power in order to mislead the acquisition and tracking procedure of its target receiver(s). However, the authentic correlation peak still exists in the cross ambiguity function (CAF) and suppressing this peak is very hard for GPS spoofers because it requires precise knowledge of the victim's antenna phase centre position relative to spoofer's antenna phase centre. In most cases, after successful lift-off, a vestige of the authentic signal remains which can be used for spoofing detection and mitigation. Humphreys et al (2008) have proposed a vestigial detection technique where the receiver employs the following software-defined technique. First, the receiver copies the incoming digitized front-end data into a buffer memory. Second, the receiver selects one of the GPS signals being tracked and removes the locally regenerated version of this signal from the buffered input signal. Third, the receiver performs acquisition for the same PRN signal on the buffered data. This technique is very similar to the successive interference cancellation (SIC) used for removing strong signals in order to combat the near/far problem in direct sequence code division multiple access (DS-CDMA) networks (Moshavi 1996).

The implementation of the vestigial signal detection increases the processing complexity of the receivers because the technique requires additional tracking channels to track both authentic and spoofing signals. In addition, in the presence of high power spoofing signals and limited bit resolution of the receiver analog to digital converter (ADC), the

authentic vestige might not be easily detectable since it might have been fallen under the sensitivity level of the GPS receiver quantizer.

2.5.2.2 Multi-Antenna Beam-Forming and Null-Steering

A multi antenna receiver can employ array processing techniques in order to shape its beam. As such, this type of receiver can steer a null toward the spoofer source and suppress its harmful effect (Daneshmand et al 2011, Guo et al 2012, McDowell 2007, Daneshmand et al 2012, 2013). Considering equation (2-3), spoofing signals can be mitigated if the received signal is multiplied to a complex ($N\times 1$) weighting vector ($\mathbf{f}$) such that

$$\mathbf{f}^H\mathbf{b} = 0, \qquad \text{constraint: } \|\mathbf{f}\| = 1 . \tag{2-8}$$

The constraint avoids the trivial solution, which is $\mathbf{f} = \mathbf{0}$. Therefore, by applying this gain vector to the sampled signal of equation (2-3), the following output signal will be achieved:

$$\begin{aligned} s(nT_s) = \mathbf{f}^H\mathbf{r}(nT_s) = &\sum_{m=1}^{N_{Auth}} \mathbf{f}^H\mathbf{a}_m\sqrt{p_m^a}F_m^a\left(nT_s\right) \\ &+\underbrace{\mathbf{f}^H\mathbf{b}}_{=0}\sum_{q=1}^{N_{Spoof}}\sqrt{p_q^s}F_q^s\left(nT_s\right)+\mathbf{f}^H\boldsymbol{\eta}\left(nT_s\right). \end{aligned} \tag{2-9}$$

Consequently, the spoofing signal is removed after properly combining signals from different antenna branches (McDowel 2007, Daneshmand et al 2011, 2012).

Daneshmand et al (2011, 2012) have proposed low computational complexity multiple antenna spoofing mitigation methods that are able to spatially filter out the spoofing signals. These methods cross-correlate the received signals from different antennas in order to form a spatial correlation matrix and accordingly extract the spatial signature of spoofing signals based on their spatial power dominance. All these operations are performed on the raw samples before despreading the authentic and spoofing signals. Assuming that the spoofer module transmits several PRN signals each of which having a power level comparable to authentic ones, the steering vector corresponding to the spoofing signals (**b**) can be extracted since all spoofing signal energy is coming from the same spatial sector. Daneshmand et al (2013) have extended their previously proposed methods to the case when multiple resolvable reflections of spoofing signals are also received by the multi-antenna receiver. These methods require neither array calibration nor any prior information regarding the antenna array orientation and they can be employed as an in-line stand-alone antenna combining block that mitigate the spoofing signals at the input of conventional GPS receivers. This anti-spoofing method successfully mitigates the spoofing signals as long as the total spoofing power (TSP) is considerably higher than the average power of the authentic signals. Nevertheless, in some cases the application of these techniques might unintentionally reduce the power of some authentic signals that are located near the beam pattern nulls.

2.5.2.3 Receiver Autonomous Integrity Monitoring (RAIM)

Spoofing signals cause counterfeit measurements in GNSS receivers. These measurements might not be consistent and consequently, do not lead to a reasonable

position solution. Most of the GPS receivers perform measurements integrity monitoring in order to detect and reject the outlier observations; this technique is known as receiver autonomous integrity monitoring (RAIM). Ledvina et al (2010) proposed an extended RAIM technique which is able to detect and exclude the outlier measurements injected by the spoofing threat. RAIM can be employed as a useful anti-spoofing technique at the position solution level. However, this method is effective only in cases where only one or two spoofed measurements are present among several authentic pseudoranges.

Table 2-2 provides a summarized comparison among the previously discussed spoofing mitigation algorithms.

Table 2-2 Summary of spoofing mitigation techniques

Anti-Spoofing Method	Spoofing Feature	Complexity	Effectiveness	Receiver Required Capability	Spoofing Scenario Generality
Vestigial Signal Detection	*The Authentic Signal is still present and can be detected*	*High*	*Medium*	*Multiple Receive Channels*	*Medium*
Multi-Antenna Null Steering	*Spoofing signals Coming from the Same Direction*	*Medium*	*High*	*Multiple Receiver Antennas*	*High*
RAIM	*Higher Residuals for Spoofed Measurements*	*Medium*	*Medium*	---	*Medium*

2.5.3 Anti-Spoofing Techniques from a Multi-layer Perspective

From a multi-layer perspective, the previously discussed anti-spoofing techniques can be investigated at three different levels namely (i) the signal processing, (ii) data bit and (iii) position solution and navigation levels. Spoofing threat might be detected/mitigated at

any of the above mentioned levels. In other words, a successful spoofer should be able to overcome the anti-spoofing techniques implemented in different layers. In addition to previously discussed anti-spoofing methods, cross-layer techniques can be developed to incorporate measurements from different operational levels in order to combat the harmful effect of spoofing signals. Figure 2-6 shows some of the previously discussed anti-spoofing techniques in a multi-layer approach.

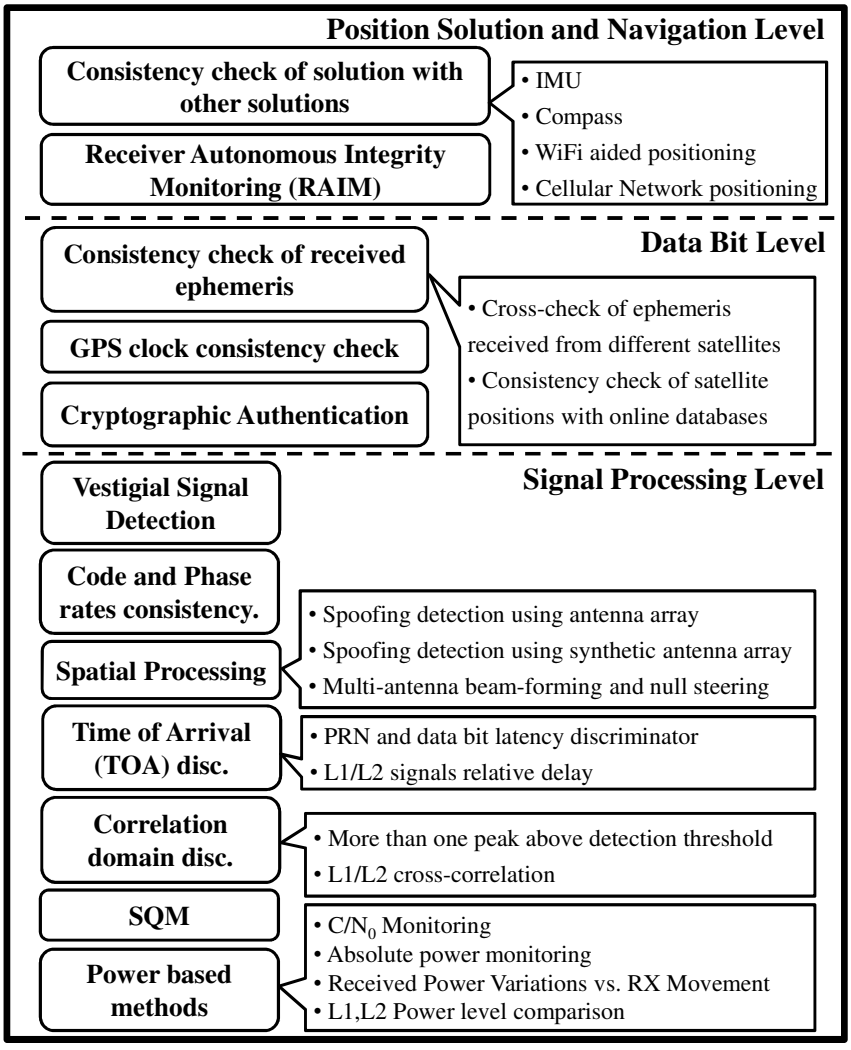


Figure 2-6 A multi-layer approach to anti-spoofing techniques

2.6 Spoofing/Anti-Spoofing Test Scenarios

Testing a spoofing/anti-spoofing system is challenging because the radio transmission regulations prohibit outdoor radio frequency (RF) power transmission in the GNSS frequency bands. Therefore, special considerations should be taken into account in order to test a spoofing/anti-spoofing system in the presence of authentic satellites' signals. This section presents some test scenarios that can be used for evaluating the performance of the anti-spoofing methods in real world spoofing scenarios.

2.6.1 Outdoor Signal Transmission with Limited Coverage

Although restricted, some papers report controlled outdoor signal transmission in specific areas. Konovaltsev et al (2013) have employed a GPS repeater mounted on a balloon for testing their proposed multi-antenna spoofing discrimination technique. The transmit power of spoofing signals are adjusted using a variable attenuator so that the target receiver is able to detect both authentic and spoofing PRN signals. Gao & Bobye (2013) have propagated multiple jamming and spoofing signals at iNAVFEST which is a military test site belonging to US Air Force. Shepard et al (2012) have also reported outdoor propagation of counterfeit civilian GPS signals at the white sands missile range (WSMR) in order to show the vulnerability of civilian unmanned aerial vehicles (UAVs) as well as smart grid's timing receivers to GPS spoofing attacks. They have employed a SDR based spoofer developed at the radio navigation laboratory (RNL) of University of Texas at Austin for generating counterfeit GPS signals.

2.6.2 GNSS Spoofing by Combining Recorded Digitized Data

In this scenario, no real RF transmission takes place; instead, the authentic intermediate frequency (IF) signal is digitized and stored on a hard disk; then, the recorded data is fed to a receiver based spoofer which tracks current GPS signals and generates spoofing signals accordingly. The output bit-stream is then combined with the original data by bit interleaving and the result of this process is fed to the target receiver (Humphreys et al 2008). Figure 2-7 depicts a block diagram of this test scenario.

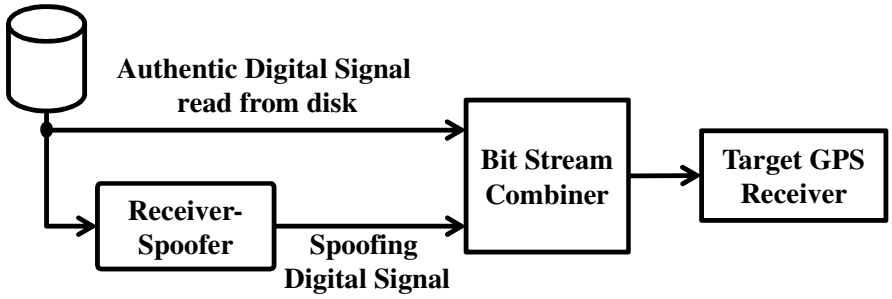


Figure 2-7 Spoofing test using recorded GPS data (modified from Humphreys et al 2008)

2.6.3 Employing RF Combiners to Combine Authentic and Spoofing Signals

Authentic GPS signals can be combined with locally generated spoofing signals using RF power combiners. Spoofing signal power can be adjusted using a cascaded setup of amplifiers and variable attenuators. Figure 2-8 shows the block diagram of this test setup for validating the proper performance of a multi-antenna anti-spoofing technique (Daneshmand et al 2012, 2013).

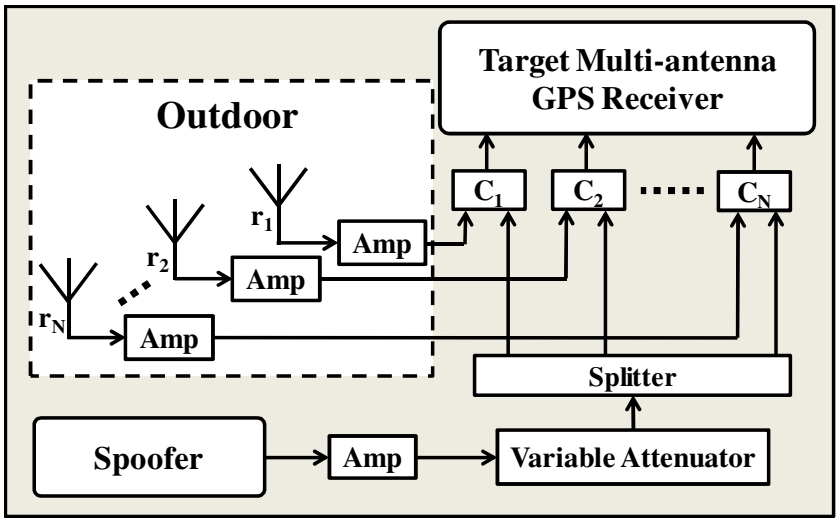


Figure 2-8 Spoofing test setup using RF combiners for a multi-antenna GPS receiver

2.7 Summary

Spoofing attack on GPS receivers is considered as a serious threat to various civilian applications. As discussed, design and implementation of spoofers is not prohibitively costly; furthermore, there is enough motivation for illicit application of spoofers. As such, many research activities are being conducted on increasing the security of civilian GPS receivers against spoofing and jamming attacks. In this chapter, an extensive literature review was provided on current spoofing scenarios and anti-spoofing techniques and the vulnerabilities of GPS that can potentially be exploited by a spoofer were discussed from a multilayer prospective.

It was shown that commercial GPS receivers are quite vulnerable to spoofing attacks generated by different spoofing scenarios. Nevertheless, by applying modest modifications, low complexity spoofing detection and mitigation techniques can be employed in order to increase the robustness of conventional GPS receivers against spoofing attacks. Countermeasures to spoofing signals can be introduced in any (or all) of

the processing levels of a GPS receiver. A powerful anti-spoofing technique should ideally be of low computational complexity and effectiveness for generic spoofing scenarios.

Chapter Three: Pre-Despreading Authenticity Verification of Received GNSS Signals

3.1 Introduction

The signal structure of spoofing signals is very similar to that of authentic GNSS signals as they are designed to misdirect their target receivers into generating incorrect time and/or position solutions. In order to be effective, a spoofer should transmit several counterfeit PRN signals whose related measurements converge to a position solution. The presence of these additional PRNs increases the power content of structural signals in the GNSS frequency band.

Detecting the presence of structural interference is very challenging in the digital domain and before de-spreading the received signals. Some previous research has proposed monitoring the AGC level to detect abnormal power content of GPS band signals (Akos 2012). This technique has shown to be very effective; however, it cannot be applied to the case when enough information regarding the AGC gain is not available and/or the receiver is only dealing with digital domain samples, e.g. the case of GNSS software receivers. Therefore, it is very beneficial if the receiver can verify the authenticity of its received signals based on digital domain samples only.

This chapter discusses a low computational complexity signal quality monitoring (SQM) technique that takes advantage of specific features of GPS signals in order to detect the presence of spoofing signals in the received signal set before being processed by a GPS receiver. The received raw signal samples are first filtered to a commensurate bandwidth and then multiplied by their delayed version in order to remove the effect of Doppler

frequency. It will be shown that due to the delay and multiply (DAM) property of gold codes, the resulting signal has a line spectrum. In the next stage, the signal and noise components are filtered by corresponding suitably designed comb filters. A detection test statistic is calculated based on the filter outputs and then it is compared to a threshold in order to differentiate between the presence and absence of spoofing signals.

This method can detect the presence of counterfeit PRN signals in the digital domain even if the receiver is equipped with an AGC that applies an unknown gain to the received signal set. Simulation results and real data processing demonstrate the effectiveness of the proposed anti-spoofing technique. This technique can be implemented as a pre-processing authenticity verification unit for commercial GPS receivers or it can be materialized as a small portable signal quality assurance device that informs the user whether or not a reliable position solution is provided by a GPS receiver. This method can be also utilized as a processing technique at a network based authenticity verification system [e.g. the system proposed by Chen et al (2012)]. Such a system can be designed so that each user captures several milliseconds of received GNSS signals and sends this data snapshot to an authenticity verification base station equipped with the proposed processing method. The base station can then analyse the received data snapshot and let the user know whether or not his/her received signal set is a genuine one.

The rest of this Chapter is organized as follows: Section 3.2 provides a simplified model for the received signal in the presence of spoofing interference on GPS L1 signals. Section 3.3 describes the proposed signal quality monitoring method. Section 3.4 discusses the simulation results and performance analysis of the proposed method. Data

collection and processing is discussed in Section 3.5. Section 3.6 provides an introduction to TEXBAT data sets and their processing results and finally, Section 3.7 provides concluding notes.

3.2 Problem Formulation

A spoofing source transmits several counterfeit PRN signals with the same or higher power level in GPS frequency band in order to misdirect its target receiver(s). Considering the GPS L1 C/A code, Equation 2.1 can be simplified so that the received sampled signal, consisting of all structural signals, can be written as

$$r(nT_s) = \underbrace{\sum_{m=1}^{M} \sqrt{p_m} h_m(nT_s - \tau_m) c_m(nT_s - \tau_m) e^{j\phi_m + j2\pi f_m nT_s}}_{S(nT_s)} + \eta(nT_s), \tag{3-1}$$

where T_s is the sampling interval and ϕ_m, f_m, p_m and τ_m are the carrier phase, Doppler frequency, signal power and code delay of the mth received structural signal, respectively. $h(nT_s)$ is the transmitted navigation data bit and $c(nT_s)$ is the PRN sequence corresponding to the authentic or spoofing signal set at time instant nT_s. $S(nT_s)$ represents the signal part of the received samples. $\eta(nT_s)$ is complex additive white Gaussian noise with variance σ^2 and j is the square root of -1. The subscript m corresponds to the mth received signal and M is the total number of authentic plus spoofing PRNs. Depending on the type of the spoofing attack, the number of spoofing PRNs can be the same or different from authentic ones. However, the power level of each spoofing signal should be comparable to that of the corresponding authentic ones and as a

consequence, the presence of spoofing signals increases the power content of the received signal set.

3.2.1 Spectral properties of GPS L1 signals

The civilian GPS L1 signals consist of PRN codes whose chip rate is 1.023 MHz. Each satellite transmits its specific PRN code which is repeated every 1ms and the navigation data is modulated at the rate of 50Hz. Therefore, the power spectral density (PSD) of GPS L1 signal is a line spectra whose spectral components are present at 1 KHz spacing (Shanmugam et al 2006). The spectral lines are shifted based on the Doppler frequency of each satellite's signal and the bandwidth of each line is 50 Hz, which is equal to the modulated data rate of the GPS signals.

3.2.2 Delay and Multiply (DAM) property of PRN Codes

The delay and multiply (DAM) property of a GPS PRN code originates from the DAM property of *m*-sequences. Based on this property, the multiplication of a PRN code with an integer chip delayed version of that code generates a new PRN code from the same set of Gold codes (Shanmugam 2008):

$$\hat{c}_m\left(nT_s-\hat{\tau}_m\right)=c_m\left(nT_s-\tau_m\right)c_m\left(nT_s-\tau_m-q\right),\quad q\in\left\{T_c,2T_c,\cdots\right\},\ q\neq N_cT_c \tag{3-2}$$

Herein, $\hat{c}_m$ represents a new Gold code that is generated by the multiplication of the *m*th PRN by its delayed version. $\hat{\tau}_m$ is the delay of the new generated Gold code ($\hat{c}_m$) and N_c is the number of chips per epoch of the PRN code.

3.3 Proposed Processing Method

The proposed processing method consists of several stages in order to detect the presence of undesired structural interference signals in the received signal samples. This approach takes advantage of the structure of GPS L1 signals toward the detection of spoofing threats and these features were briefly described in the previous section. The following sub-sections describe different stages of the proposed processing technique.

3.3.1 Differential Doppler Removal

As mentioned before, individual GPS L1 signals are periodic sequences that have line spectra with a 1 KHz frequency spacing that is shifted corresponding to the signal's Doppler frequencies. Several PRN signals are received by a GPS receiver simultaneously and each of them has its own Doppler shift that is generated based on its transmitter satellite motion, user dynamics and receiver internal frequency bias. Since each PRN is received from a different satellite at a different bearing, their corresponding Doppler frequencies are different from each other. Therefore, in order to concentrate all signal components to the same spectral lines, the Doppler shifts of the signals should be removed. Then, filtering should be performed along the spectral lines that contain signal components. To this end, the sampled baseband signal components are first multiplied to the complex conjugate of their one chip delayed version as

$$\begin{aligned} y(nT_s) &= \mathrm{Re}\left\{ r(nT_s) \times r^*(nT_s - T_c) \right\} \\ &\approx \underbrace{\sum_{m=1}^{M} p_m \hat{c}_m(nT_s - \hat{\tau}_m)}_{y_{ss}(nT_s)} + y_{ss}^{cc}(nT_s) + y_{s\eta}(nT_s) + y_{\eta\eta}(nT_s) \end{aligned} \tag{3-3}$$

where T_c is the chip duration which is almost equal to 1/1023 ms for GPS L1 signals. The term $y_{ss}(nT_s)$ represents the sum of products of individual PRN signals in their delayed conjugate version. Typical Doppler shifts for baseband GPS signals are between -5 KHz to +5 KHz; therefore, it can be written $f_m T_c << 1$. This operation removes the phase rotation due to the Doppler frequency of received GPS signals; both authentic and spoofed. It also removes the data bits that are modulated over each GPS signal. $\hat{c}_m(nT_s - \hat{\tau}_m)$ is the new Gold code that is achieved based on the DAM property of the Gold sequences and $\hat{\tau}_m$ is its corresponding delay value. The other terms can be written as follows

$$
\begin{aligned}
y_{ss}^{cc}(nT_s) &\approx \sum_{i=1}^{M}\sum_{\substack{q=1 \\ q\neq i}}^{M}\left\{\begin{array}{l}\sqrt{p_i}\sqrt{p_q}\,h_i(nT_s-\tau_i)\,h_q(nT_s-\tau_q-T_c)\,c_i(nT_s-\tau_i) \\ c_q(nT_s-\tau_q-T_c)\cos\left(2\pi f_i\,nT_s - 2\pi f_q\,(nT_s-T_c)+\phi_i-\phi_q\right)\end{array}\right\} \\
y_{s\eta}(nT_s) &= \mathrm{Re}\left\{S(nT_s)\eta^*(nT_s-T_c)+S^*(nT_s-T_c)\eta(nT_s)\right\} \\
y_{\eta\eta}(nT_s) &= \mathrm{Re}\left\{\eta(nT_s)\eta^*(nT_s-T_c)\right\}
\end{aligned}
\tag{3-4}
$$

where $y_{ss}^{cc}(nT_s)$ is the cross correlation of different PRN signals. Neglecting the effect of data bits, $y_{ss}^{cc}(nT_s)$ is also a periodic term since it is the multiplication of several periodic signals with the same period. $y_{s\eta}(nT_s)$ represents the signal and noise multiplication terms and $y_{\eta\eta}(nT_s)$ represents the real part of the product of the noise process into its delayed version. The last two terms are not periodic because the noise component is assumed to be uncorrelated in the receiver operational bandwidth.

3.3.2 Signal Filtering

The filtering process is performed on the signal spectral lines using their periodicity feature. This process adds each sample of $y(nT_s)$ to one epoch delayed version of this signal as

$$\begin{aligned} g_s(nT_s) &= \sum_{l=0}^{L-1} y(nT_s - lT_e) \\ &\approx \sum_{m=1}^{M} p_m \hat{c}_m(nT_s - \hat{\tau}_m) + y_{ss}^{cc}(nT_s) + \overline{y}_{s\eta}(nT_s) + \overline{y}_{\eta\eta}(nT_s) \end{aligned} \tag{3-5}$$

where T_e is the epoch length of the GPS L1 signals and L is the number of epochs added together during filtering operation. Using the properties of the Z transform, the frequency response of the above filter can be written as

$$H_s(z) = \frac{Z\{g_s(nT_s)\}}{Z\{y(nT_s)\}} = \sum_{l=0}^{L-1} z^{-l} = \frac{1-z^{-L}}{1-z^{-1}} \tag{3-6}$$

where $Z\{\bullet\}$ represents the Z-transform of its argument. Hence, considering $z = e^{j2\pi fT_e}$, the frequency response of the filter can be written as

$$H_s(f) = \frac{1-e^{-j2\pi LT_e f}}{1-e^{-j2\pi T_e f}} \tag{3-7}$$

The normalized frequency response of this filter is illustrated in Figure 3-1 for different values of L and in a frequency span of 3.5 KHz. It is observed that the frequency components that are located at multiples of $(1/T_e)$ pass through the filter while the other

parts of the spectra are considerably attenuated. Also, it is observed that as the number of filter stages (L) increases, the bandwidth of the filter decreases.

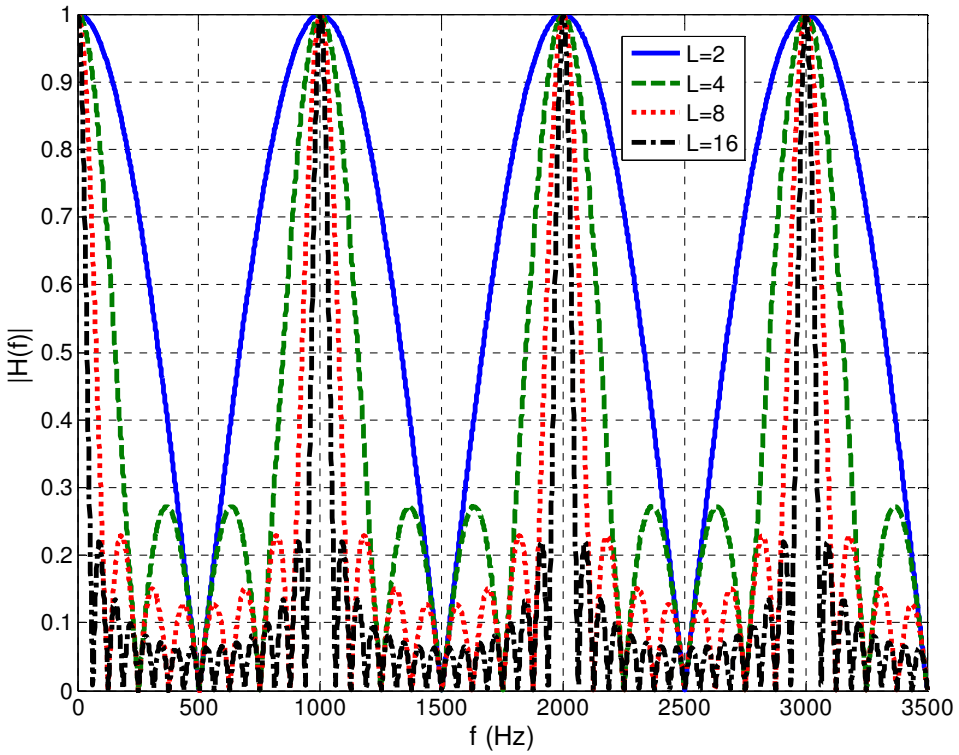


Figure 3-1 Normalized frequency response of the filter

This type of filtering can be used to extract the energy of periodic components of $y(nT_s)$ with period T_e. In other words, $g_s(nT_s)$ contains the energy of periodic parts of $y(nT_s)$ that are repeated every 1 ms.

3.3.3 Noise Filtering

A measure of noise energy can be extracted by filtering those parts of the spectrum that do not contain periodic signal components. In other words, this filtering process cancels out the periodic signal components and the only remaining component would be the filtered noise. The filtering process can be expressed as

$$g_n(nT_s)=\sum_{l=0}^{L-1}(-1)^l\, y(nT_s-lT_e)\approx \overline{y}_{s\eta}(nT_s)+\overline{y}_{\eta\eta}(nT_s) \tag{3-8}$$

The frequency response of the noise filter can also be derived directly using the Z-transform properties as mentioned in (3-6). Herein, $(-1)^l = e^{j2\pi(500)T_e l}$ represents a 500Hz frequency shifter before the filter of Equation (3-5). For the case that L is an even integer, the frequency response can be written as

$$H_n(f)=\frac{1-e^{-j2\pi LT_e f}}{1+e^{-j2\pi T_e f}} \tag{3-9}$$

Figure 3-2 illustrates the frequency responses of signal and noise filters for a filter length of L=16 ms. It is observed that the signal filter passes the periodic signal components

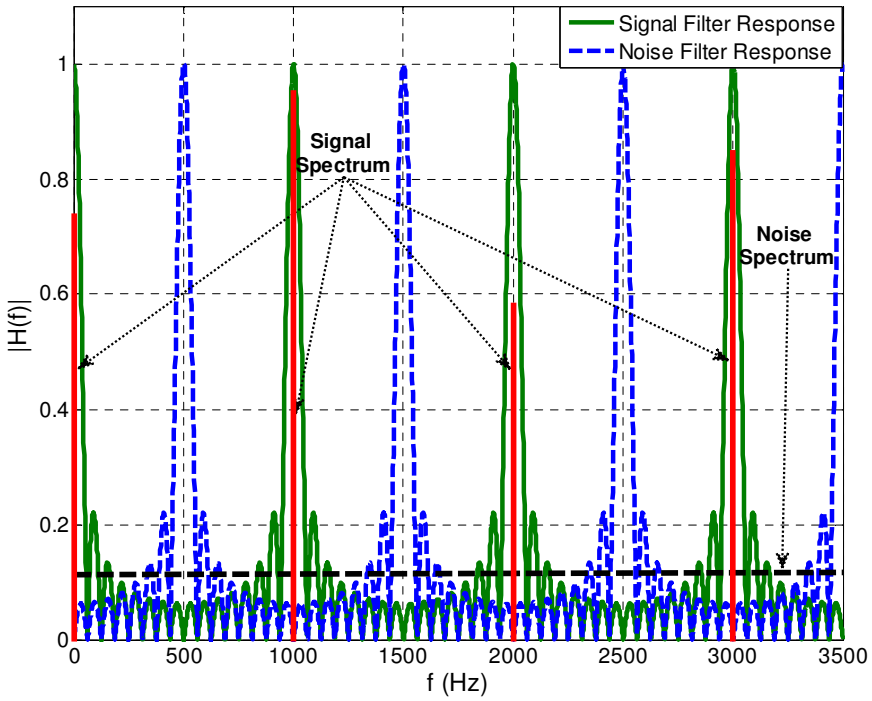


Figure 3-2 Frequency response of signal and noise filters for L=16 ms

while the noise filter only passes the noise component energy within an equivalent bandwidth of the noise spectrum. Therefore, the variance of the noise filter output can provide a measure of the noise power in an equivalent bandwidth of the received signal set.

3.3.4 Compensating the Effect of AGC

The presence of spoofing signals increases the power content of the received signal set. However, unlike other types of interference, spoofing signals are not easily detectable because they can be buried under the noise floor similar to the authentic signals. Herein, it is assumed that the receiver is equipped with an AGC system that changes the input amplifier gain in order to efficiently sample different signals with different power levels. The AGC gain is adjusted depending on the input signal power and it similarly affects both signal and noise filter outputs given in (3-6) and (3-8). This gain can be different in the presence and absence of spoofing signals. The signal and noise filter outputs both have approximately Gaussian distributions since they are the summation of *L* i.i.d random variables and *L* is usually a large number. Therefore, one can write

$$\begin{aligned} g_s\left(nT_s\right) &= \alpha\left(s\left(nT_s\right) + w\left(nT_s\right)\right) \\ g_\eta\left(nT_s\right) &= \alpha\, w\left(nT_s\right) \end{aligned} \tag{3-10}$$

where α contains the unknown AGC gain and $w\left(nT_s\right)$ represents a standard white Gaussian distributed signal with zero mean and unit variance. The noise components in $g_s\left(nT_s\right)$ and $g_\eta\left(nT_s\right)$ are not exactly the same however, their means and variances are approximately similar. $s\left(nT_s\right)$ gives the periodic parts of $y\left(nT_s\right)$, i.e. $y_{ss}\left(nT_s\right)$ and

$y_{ss}^{cc}(nT_s)$, that are passed through the signal filter. This signal also can be modeled by Gaussian distribution since it is generated by the summation of several independent PRN signals. Based on the central limit theorem, $s(nT_s)$ can be approximately modeled by a Gaussian distribution since it is generated by the summation of several independent PRN signals. Figure 3-3 shows the histogram of $s(nT_s)$ along with its Gaussian fit for the case of 10 simulated equal power GPS L1 C/A codes for L = 50 ms. It is observed that the Gaussian approximation is quite reasonable for this signal.

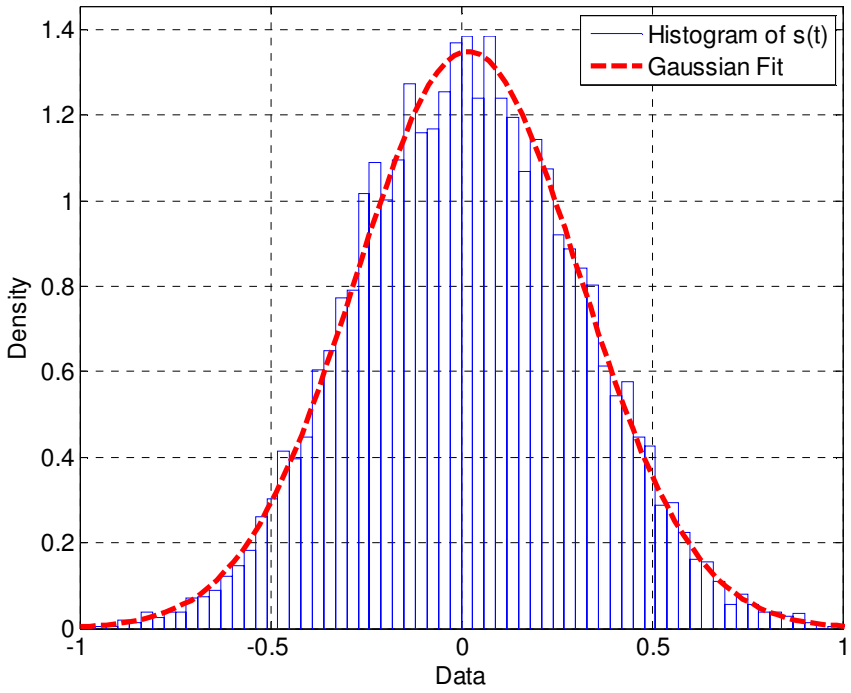


Figure 3-3 Histogram of s(nT$_s$) and its Gaussian approximation

The effect of unknown AGC gain can be removed from $g_s(nT_s)$ by normalizing it with the root mean square (RMS) of $g_\eta(nT_s)$ samples. Therefore, one can write

$$x(nT_s) = \frac{g_s(nT_s)}{\sqrt{E\left\{g_\eta(nT_s)^2\right\}}} = \frac{g_s(nT_s)}{\alpha} = s(nT_s) + w(nT_s) \tag{3-11}$$

3.3.5 Spoofing Detection

Herein, a detection test is designed so as to discriminate between the following two hypotheses based on the normalized signal filter output.

$$\begin{aligned} \mathbf{H}_0: &\quad x(nT_s) = s_a(nT_s) + w(nT_s) &&= w'(nT_s) \\ \mathbf{H}_1: &\quad x(nT_s) = s_s(nT_s) + s_a(nT_s) + w(nT_s) = s_s(nT_s) + w'(nT_s) \end{aligned} \tag{3-12}$$

where $s_a(nT_s)$ and $s_s(nT_s)$ refer to the authentic and spoofing signals, respectively. H_0 represents the hypothesis where only the authentic signals are present in the received signal set while H_1 represents the hypothesis where both spoofing and authentic signals are present. Based on the central limit theorem, since $s_a(nT_s)$ and $s_s(nT_s)$ are the summations of several asynchronous zero mean PRN sequences, their distribution can be approximated as zero mean Gaussian. As such, $w'(nT_s)$ is a Gaussian process which is the summation of normalized noise and $s_a(nT_s)$. The variance of $w'(nT_s)$ depends on several parameters such as the number of visible authentic satellites and their received power, the quality of receiver equipment, the length of the processing filter (L) and etc. This variance can be determined by a calibration process that can be performed on authentic GPS signals by the receiver manufacturer.

An effective spoofer should transmit several counterfeit PRN signals whose spectral and temporal features are very similar to those of authentic PRNs and their power level is

slightly higher than the authentic ones (Jafarnia et al 2012a, Shepard et al 2011). Therefore, the presence of $s_s(nT_s)$ increases the variance of $x(nT_s)$, which can reveal the $\mathbf{H}_1$ hypothesis. A GLRT detector can be designed in order to discriminate between the $\mathbf{H}_0$ and $\mathbf{H}_1$ hypotheses based on their variances:

$$\begin{aligned} &\mathrm{H}_0: \quad \sigma_x^2 = \sigma_{w'}^2 \\ &\mathrm{H}_1: \quad \sigma_x^2 > \sigma_{w'}^2 \end{aligned} \tag{3-13}$$

where σ_x^2 is the variance of $x(nT_s)$ and $\sigma_{w'}^2$ is the variance of $w'(nT_s)$, respectively. $\sigma_{w'}^2$ is supposed to be greater than 1 since $w(nT_s)$ has a normalized variance (see descriptions of equation 3.10). The GLRT selects $\mathbf{H}_1$ if (Kay 1998)

$$L_G(\mathbf{x}) = \frac{p(\mathbf{x}; \hat{\sigma}_1^2, \mathrm{H}_1)}{p(\mathbf{x}; \sigma_0^2, \mathrm{H}_0)} > \gamma \tag{3-14}$$

where $\mathbf{x} = \left[x(0), x(T_s), x(2T_s), ..., x\left((N-1)T_s\right) \right]^T$ is the vector of normalized samples for one epoch. σ_1^2 and σ_0^2 represent the variance of $x(nT_s)$ under the $\mathbf{H_1}$ and $\mathbf{H_0}$ hypotheses, respectively. $\hat{\sigma}_1^2$ is the estimate of the variance of $\mathbf{x}$ under the H_1 hypothesis. Therefore, the log likelihood ratio (LLR) can be written as

$$\begin{aligned} l(\mathbf{x}) &= \frac{N}{2} \ln\left(\frac{\sigma_0^2}{\hat{\sigma}_1^2}\right) - \frac{1}{2}\left(\frac{1}{\hat{\sigma}_1^2} - \frac{1}{\sigma_0^2}\right) \sum_{n=0}^{N-1} x(nT_s)^2 \\ &= \frac{N}{2} \ln\left(\sigma_0^2\right) - \frac{N}{2} \ln\left(\hat{\sigma}_1^2\right) - \frac{1}{2\hat{\sigma}_1^2} \sum_{n=0}^{N-1} x(nT_s)^2 + \frac{1}{2\sigma_0^2} \sum_{n=0}^{N-1} x(nT_s)^2 \end{aligned} \tag{3-15}$$

Hence, the GLRT selects H_1 if

$$T'(\mathbf{x}) = \frac{1}{N\sigma_0^2}\sum_{n=0}^{N-1} x(nT_s)^2 - \ln\left(\frac{1}{N}\sum_{n=0}^{N-1} x(nT_s)^2\right) > \gamma' \tag{3-16}$$

Since $T'(\mathbf{x})$ is a monotonic function of $\sum_{n=0}^{N-1} x(nT_s)^2$ for $x(nT_s) \geq 1$, Equation (3-15) can be simplified to (Kay 1998)

$$T(\mathbf{x}) = \frac{1}{N}\sum_{n=0}^{N-1} x^2(nT_s) > \gamma'' \tag{3-17}$$

which is an estimator of the variance of $x(nT_s)$.

Figure 3-4 shows a block diagram of the proposed signal authenticity verification technique. All the processing is performed on the raw signal samples and the proposed method is able to verify the authenticity of received signals without despreading individual GPS signals. This technique does not need any information regarding the AGC gain that is applied to the received signals before sampling. The proposed technique assumes that no information is available regarding the AGC gain and absolute received power. However, the presence of such types of information can highly increase the robustness of the proposed method against different types of spoofing scenarios. For example, in the case that a spoofer transmits a considerably higher power signal set over an elevated noise floor, the information regarding absolute received power can be very helpful toward detecting the presence of spoofing signals.

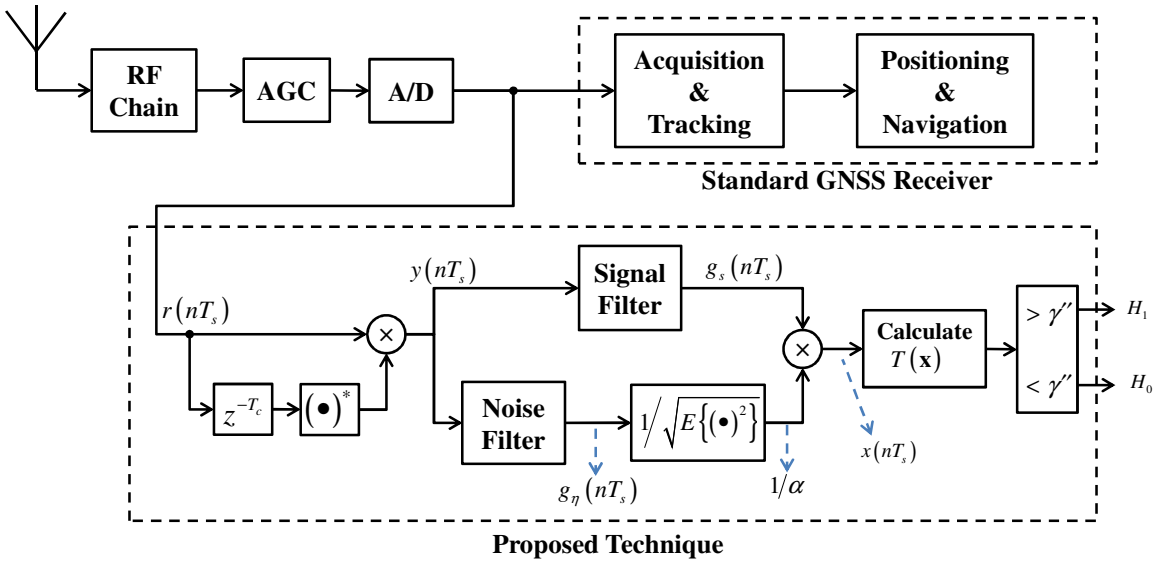


Figure 3-4 Block diagram of proposed signal quality monitoring technique

3.4 Simulation Results

Simulations have been performed to evaluate the performance of the proposed authenticity verification technique under different scenarios. Ten authentic PRNs as well as 10 spoofing PRNs have been considered at a sampling rate of 10Msps. The power level of each authentic PRN is assumed to be -157 dBW and the power of spoofing PRNs vary based on the simulation scenario and they are equal to each other. The Doppler shift of each PRN signal is randomly chosen between $-f_{max}$ and $+f_{max}$ where f_{max}=5 *kHz*. The code delay of each PRN is also randomly chosen and it is assumed that the PRNs are not chip synchronized. The additive Gaussian noise that is added to the signal is assumed to be white and its spectral density is assumed to be N_0=-204 dBW/Hz.

Figure 3-5 shows the receiver operating characteristics (ROC) curves of the proposed detector for different values of spoofing power. The filter length is assumed to be L=50 ms and the spoofing power varies from -160 dBW to -154 dBW in 1dB steps. Monte-

Carlo simulations have been performed for 1,000,000 epochs of the GPS signal when the code delay and Doppler frequency of each PRN set is changed randomly every 50 ms. It is observed that as the spoofing power increases, the detection performance of the proposed method increases as well. It is observed that once the power of spoofing signals exceeds the power level of authentic ones, the detection performance of the proposed method considerably increases and finally for a spoofing power of -154 dBW, an approximate ideal detection performance is achieved.

Figure 3-6 shows the detection performance of the proposed method in the presence of 10 equal power authentic signals each of which having -157 dBW. A variable number of spoofing PRNs has been assumed in the Monte Carlo simulations and their individual power is assumed to be 1 dB higher than that of the authentic signals. The number of spoofing PRNs is assumed to be 4, 6, 8, 10 and 12. It is observed that as the number of spoofing PRNs increases, the detection performance of the proposed technique also increases.

Figure 3-7 shows the detection performance of the proposed method for different values of filter length *L,* i.e. *L*=10, 20, 50, 100, 200 epochs. The number of authentic and spoofing PRN signals are the same and each equal to 10 PRNs and their signal power is also the same and equal to -157 dBW. It is observed that as the filter length increases, the detection performance also increases. However, when the filter length (*L*) increases from 100 ms to 200 ms, the detection performance does not improve considerably.

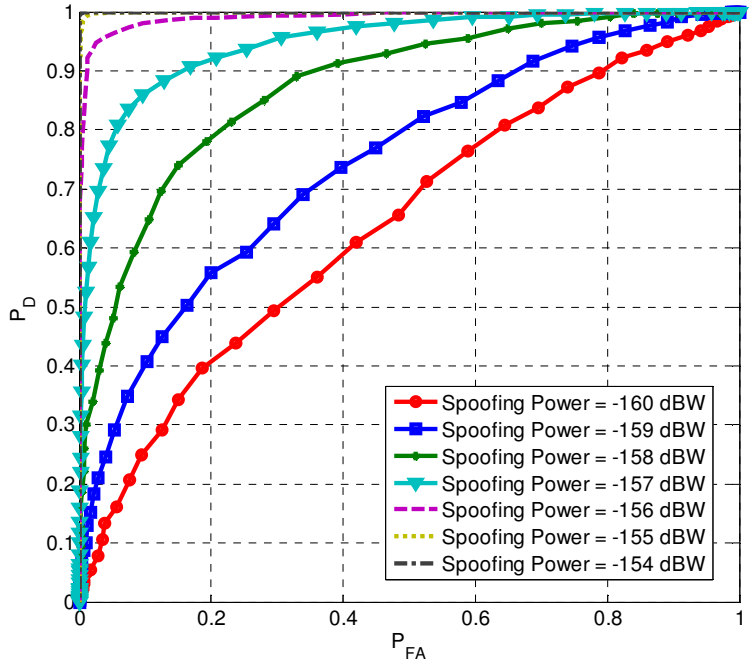


Figure 3-5 Spoofing detector ROC for 10 authentic and 10 spoofing PRNs (P_{auth}= -157 dBW)

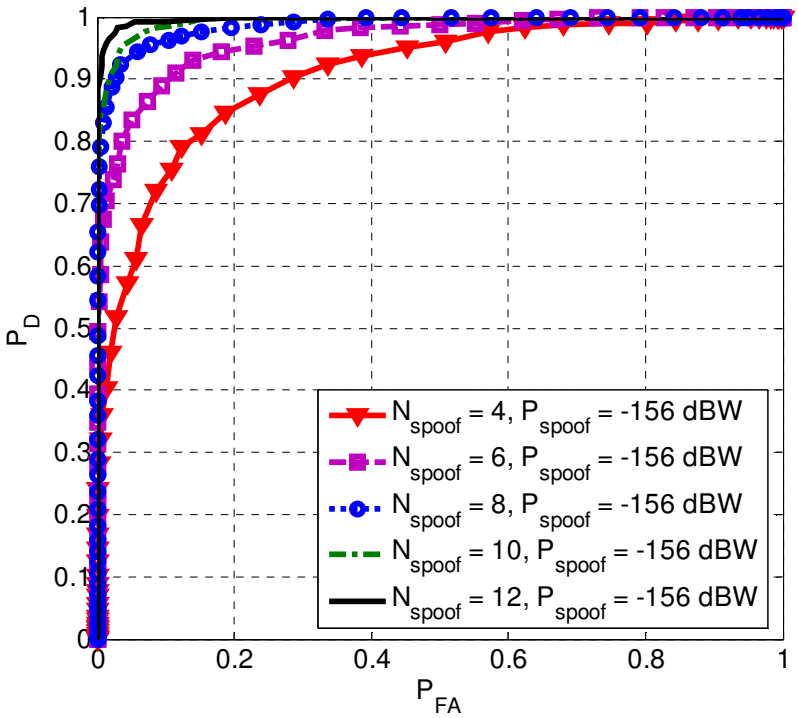


Figure 3-6 Spoofing detector ROC for 10 authentic PRNs and different numbers of spoofing PRNs (P_{auth}=-157 dBW, P_{spoof}=-156 dBW)

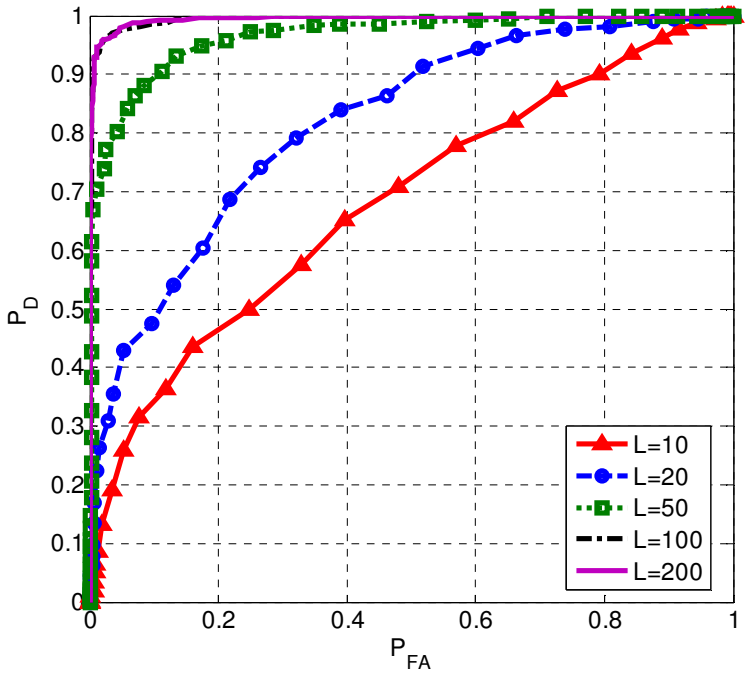


Figure 3-7 Detection performance of proposed technique for different values of filter length (P_{auth}= -157 dBW, P_{spoof} = -157 dBW)

Table 3-1 shows the threshold values corresponding to different probabilities of false alarm at different values of *L*. It should be noted that for longer filter lengths, e.g. *L*=200 ms or more, the receiver clock stability in terms of the sampling rate accuracy becomes more important. The reason is that the performance of the proposed technique is very dependent on the receiver interpretation of the PRN signal epoch length. In case that the epoch length of GPS signals on the receiver side is interpreted differently from its actual length, the line spectral components would not add coherently and this limits the performance of the proposed method.

Table 3-1 Probability of detection and threshold values corresponding to different probabilities of false alarm

	P_{FA}=0.1		P_{FA}=0.01		P_{FA}=0.001	
	P_D	γ''	P_D	γ''	P_D	γ''
***L*=10**	0.35	1.57	0.05	1.6	0.01	1.62
***L*=20**	0.47	1.62	0.14	1.66	0.05	1.69
***L*=50**	0.89	1.78	0.68	1.83	0.13	1.94
***L*=100**	0.98	2.06	0.93	2.14	0.66	2.26
***L*=200**	0.99	2.73	0.94	2.94	0.78	3.18

3.5 Real Data Collection and Processing

Several data sets have been collected to test the proposed method using real scenarios. For testing the proposed technique, fake GPS signals were generated using a hardware simulator and after controlled amplification, they are combined with real GPS signals that are received by an outdoor antenna. Controlled amplification is achieved by first amplifying the hardware simulator's signal and then attenuating the amplified signals using a variable attenuator. The combined signal is then fed to a NI PXIe-1065 RF sampling front-end. The block diagram of the proposed data collection method is illustrated in Figure 3-8.

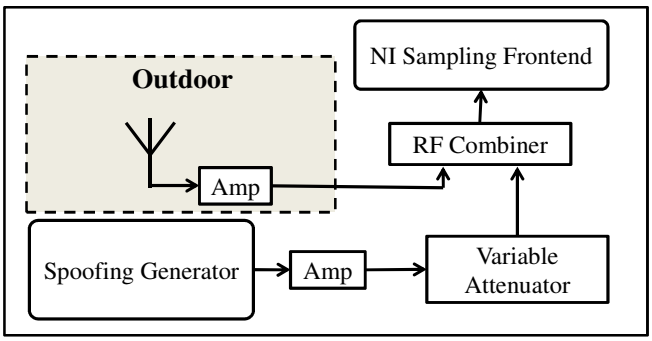


Figure 3-8 Data collection scenario schematic

Figure 3-9 illustrates the frequency response of $y(nT_s)$ for the case when an amplified version of the hardware simulator signal is combined with the received authentic GPS signals. In this case, the power level of spoofing signals is higher than the authentic ones. The spectral response of $y(nT_s)$ has been depicted in a 3 KHz frequency span from 16.2 KHz to 19.2 KHz. Furthermore, the frequency responses of signal filter and noise filter for L=32 ms have been also shown in green and red, respectively. It is observed that signal peaks appear at integer multiples of 1 KHz and these components pass through the signal filter. These peaks correspond to the periodic parts of the $y(nT_s)$ that are repeated every 1 ms. For the case of a noise filter, it is observed that no dominant signal component is present in the pass-band of the filter. Therefore, the noise filter only measures the power content of non-periodic parts of $y(nT_s)$.

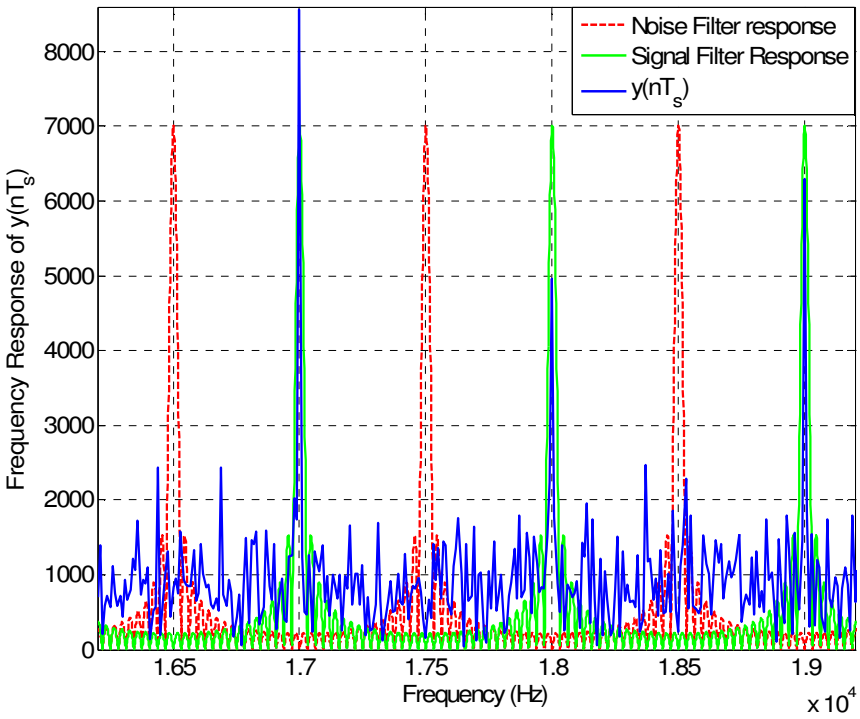


Figure 3-9 Frequency response of $y(nT_s)$ for real data along with the response of a filter with L=32 ms

Table 3-2 shows the position solution provided by the GSNRx^{TM} software receiver for different values of spoofing gain. GSNRx^{TM} is a GNSS software receiver developed by the PLAN Group of University of Calgary (Petovello et al 2008). The average power of spoofing signals with respect to the authentic ones has changed from -18 dB (equivalent to the absence of spoofing signal) to +18dB (spoofer completely overpowers the authentic signals) in 3 dB steps. The latitude, longitude and height errors of the spoofed position with respect to the authentic coordinates are 8873 m, 9338 m, and 118 m, respectively. There are 10 authentic and 11 spoofing PRNs present in the received signal samples.

Table 3-2 shows that the positioning capability of the receiver is interrupted as the spoofing signals' average power relative to the authentic ones exceeds -3 dB. For the case that the relative power is between -3dB to +3dB, the receiver cannot come up with a position fix. The reason is that in this case both spoofing and authentic PRNs are acquired and since the spoofed pseudorange measurements are not consistent with the authentic ones, the receiver is not able to come up with a position solution. However, when the relative average power of spoofed PRNs become more than 3dB stronger than the authentic ones, the spoofed PRN set becomes the dominant signal and forces the receiver to extract the spoofed position solution. In this table the authentic position errors are shown in green whereas the spoofed position errors are shown in red.

Table 3-2 Position solutions provided by the GSNRx™ software receiver for different values of spoofing-authentic relative power

Relative Spoofing-Authentic Power	**Latitude Error** (m)	**Longitude Error** (m)	**Height Error** (m)	**Time** (s)	**3D Position Error with respect to the true coordinates** (m)
G = -18 dB	**2**	**5**	**5**	**259536**	**7**
G = -15 dB	**1**	**5**	**7**	**259242**	**9**
G = -12 dB	**1**	**1**	**2**	**259030**	**2**
G = -9 dB	**6**	**5**	**1**	**258588**	**8**
G = -6 dB	**2**	**3**	**2**	**258288**	**4**
G = -3 dB	**No Fix**	**No Fix**	**No Fix**	**257137**	**N/A**
G = 0 dB	**No Fix**	**No Fix**	**No Fix**	**256842**	**N/A**
G = +3 dB	**No Fix**	**No Fix**	**No Fix**	**565995**	**N/A**
G = +6 dB	**8,880**	**9,331**	**117**	**566388**	**12882**
G = +9 dB	**8,870**	**9,341**	**116**	**566805**	**12882**
G = +12 dB	**8,870**	**9,335**	**116**	**569826**	**12878**
G = +15 dB	**8,870**	**9,332**	**116**	**569538**	**12875**
G = +18 dB	**8,870**	**9,340**	**116**	**570168**	**12881**

Figure 3-10shows the probability of spoofing detection as a function of the spoofing signal gain. The test statistic is compared to the predefined threshold values corresponding to P_{FA}=0.1, P_{FA}=0.01, P_{FA}=0.001 for the filter length of L=100 ms. It is observed that the presence of spoofing signals starts to be detected as soon as the value of spoofing signals average power with respect to the authentic signals exceeds -9 dB. As the spoofing power dominance over the authentic signals exceeds -6 dB, the probability of spoofing detection for all threshold values exceeds 95% and based on the information provided in Table 3-2, this is exactly the gain level above which the receiver operation is

interrupted by the spoofing signals. The probability of spoofing detection approaches to unity for the cases that the ratio of average power of spoofing signals over the authentic ones is higher than -3 dB.

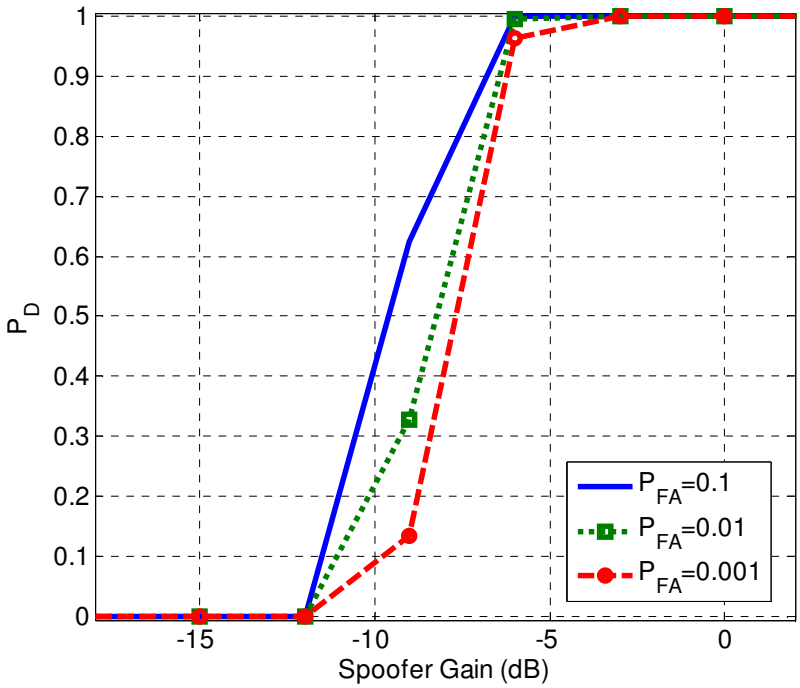


Figure 3-10 Probability of detection vs. spoofer gain for different values of false alarm rate

3.6 TEXBAT Data Processing

3.6.1 Introduction to TEXBAT Datasets

A spoofing test battery, TEXBAT, was recently developed by the Radio Navigation Laboratory (RNL) at the University of Texas at Austin, which is very useful for testing different spoofing countermeasure methods for GPS L1 C/A signals. Based on the discussions provided by Humphreys et al (2012), the TEXBAT datasets can be

considered as the data component of a potential spoofing resitance standard for civilian GPS receivers.

A receiver based spoofer was employed in the configuration illustrated in Figure 3-11 in order to generate TEXBAT datasets. In this setup, the spoofer can generate a synchronized spoofing attack having real-time information from the current GPS constellation and knowing the position of its target receiver. In addition to code phase alignment, the spoofer has aligned navigation data bit transitions by predicting the data bits sequence. For the case when the number of spoofing PRNs is low, additional noise is added to the spoofing signal set in order to prevent unexpected high C/N_0 values.

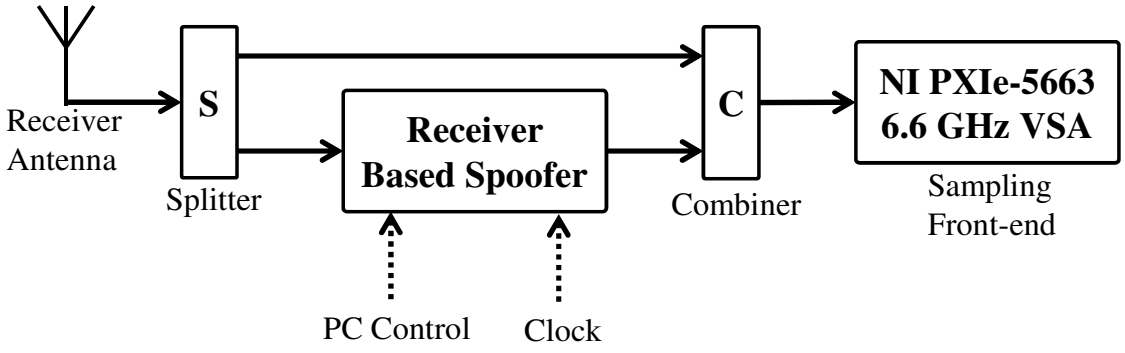


Figure 3-11 TEXBAT data collection setup

This spoofing "test battery" consists of six spoofing datasets plus two sets of unspoofed reference signals. Four spoofing scenarios correspond to static spoofing attack and two of them correspond to dynamic spoofing. Herein, only static spoofing scenarios have been considered for testing the proposed authenticity verification methods. The spoofed datasets are down-converted and sampled by a National Instrument (NI PXIe-5663) vector signal analyser (VSA) at 25 MSps where each sample consists of in-phase and

quadrature 16 bit baseband components. The spoofing attacks in different spoofing scenarios take place after around 100 s from the beginning of the data stream.

Data set #0 (S0) contains clean static data in which only authentic signals are present and no spoofing attack takes place. This dataset is the base of all static spoofing scenarios. Data set #1 (S1) represents a switched spoofing attack during which the authentic input signals are detached from the receiver and after that the receiver is directly fed by counterfeit signals. This case can represent a spoofing scenario in which the spoofer's operator has physical access to the target receiver and can disconnect the input authentic signals and directly feed the spoofing signals to the input antenna port of the receiver. Data set #2 (S2) represents the overpowered spoofing attack where the spoofing signals are added to the authentic signal ensemble. In this scenario the average power of spoofing signals is 10 dB higher than that of the authentic signals. In this case, the power of spoofing signals is much higher than the authentic ones and this power advantage prevents interaction between authentic and spoofing signal sets. This scenario can be easily detected by a GPS receiver since an abrupt C/N_0 variation can be observed for the spoofing PRNs. Data set #3 (S3) represents the matched power spoofing scenario where the mean power of spoofing PRNs is 1.3 dB higher than that of the authentic signals. Matched power spoofing attacks are potentially more difficult to detect by RSS based spoofing detection methods since considerable C/N_0 variations might not be detected for spoofed PRNs. Finally, data set #4 (S4) represents a matched power spoofing scenario where the power advantage of spoofing signals ensemble is further reduced compared to

the S3 scenario. In this case, the average power of spoofing signals is only 0.4 dB higher than that of the authentic signals.

3.6.2 TEXBAT Processing Results

Figure 3-12 illustrates the proposed test statistics for TEXBAT static datasets. The detection threshold for a false alarm probability of P_{FA} = 0.0001 is also shown in Figure 3-12. The detection thresholds are determined based on the test statistics in the clean data set. It is observed that the detection test can successfully detect the presence of spoofing signals in the S2, S3 and S4 scenarios. In all of these scenarios the spoofing signals are added to the present authentic signal set and therefore, the power content of structural signals is increased in the presence of a spoofing attack.

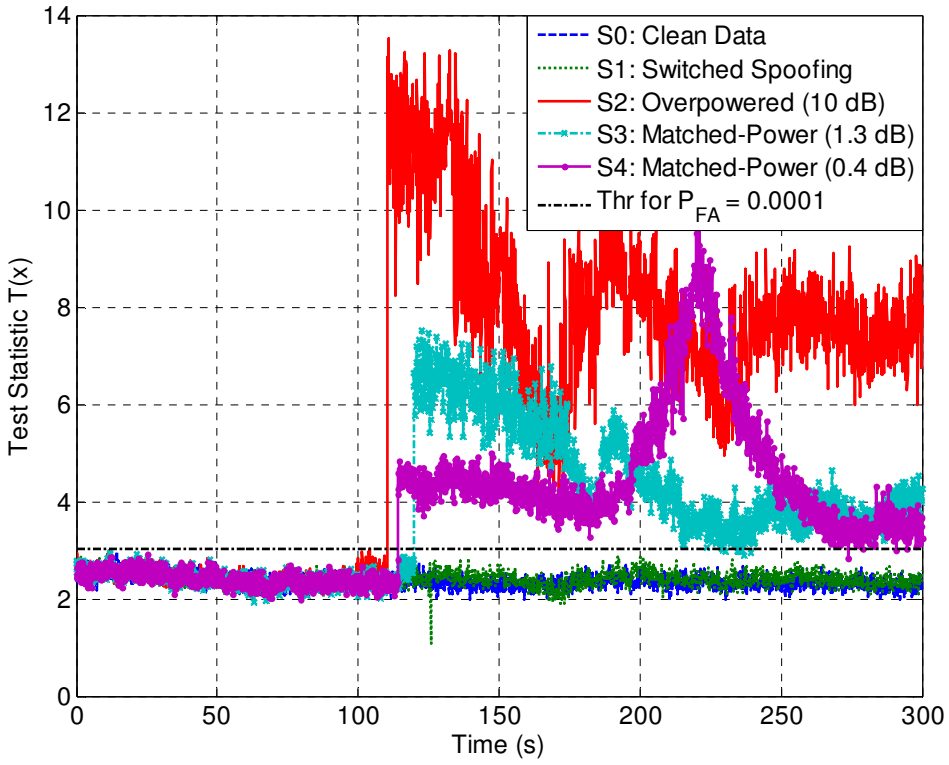


Figure 3-12 Spoofing detection for RNL datasets in different scenarios

As it is shown in Figure 3-12, even for the case that the average power of the spoofing signals is 0.4 dB higher than the authentic ones (scenario S4), the test statistic considerably exceeds all of the detection thresholds and this shows the applicability of the proposed processing method even for the case of matched power spoofing attacks. The proposed technique is not able to detect a switched spoofing attack (scenario S0) because in this scenario, the authentic signals are replaced by spoofing ones. As such, the structural signal power content is not increased during a spoofing attack and spoofing interference does not affect the proposed test statistic.

3.7 Summary

A pre-despreading scheme has been proposed in order to verify the authenticity of received GPS signals. The proposed method operates on raw GPS samples and detects the abnormal power content of GPS spectrum without relying on the knowledge of the AGC gain value. The proper performance of this technique is verified by several simulation scenarios as well as with some real data sets generated by a hardware simulator and the spoofing datasets provided by RNL. The real data processing results show that the proposed technique can successfully detect the presence of spoofing signals when these are powerful enough to interrupt the normal operation of user equipment. The computational complexity of the proposed technique is very low; therefore, it can be used as an integrated signal quality monitoring block in civilian GPS receivers or it can be materialized as a portable stand-alone GPS signal quality assurance system.

Chapter Four: Spoofing Analysis and Countermeasure during GPS Acquisition

4.1 Introduction

Spoofing sources can effectively disrupt a GPS receiver process during the acquisition stage by transmitting additional PRN signals which can lead to generation of fake correlation peaks at the output of the despreading process. Such deceptive correlation peaks can mislead the GPS receiver into acquiring the spoofer generated signals rather than the authentic signals. Furthermore, a higher power spoofer can increase the target receiver's noise floor due to the cross correlation of the counterfeit PRN signals. In this case, the presence of spoofing signals can bury the authentic signals under the noise floor and at the same time generate counterfeit correlation peaks with amplitudes commensurate with reasonable C/N_0 expectations.

During the acquisition procedure a generic GPS receiver correlates the received signal with a locally generated one to provide a rough estimate of the code delay and the Doppler frequency of each received PRN signal. Herein, it is assumed that the receiver searches over all Doppler and code delays in range and estimates the signal parameters corresponding to the highest power correlation peak that is above a predetermined detection threshold. The presence of spoofing signals can potentially misdirect the acquisition procedure by generating higher power PRN signals leading to higher power correlation peaks in the cross ambiguity function (CAF). Thus, the acquisition process of the receiver will be presented with seemingly legitimate correlation peaks from which a false navigation solution is generated. The spoofer can also generate a component of uncorrelated noise in the GPS band that can arbitrarily manipulate the noise floor

observed by the receiver. Additionally, as the counterfeit PRN codes are not orthogonal to locally generated PRN replicas, there is a mutual non-zero cross correlation caused by spoofing PRN codes that further increases the receiver's noise floor.

As mentioned in previous chapters, the maximum GPS signal strength at the receiver antenna is known approximately; therefore, a receiver can detect the presence of a spoofing source if its power is too large. In other words, a receiver has the effective means of detecting a spoofing source and hence can take the appropriate action. This may be that the receiver merely informs the user of a potential spoofing attack such that less reliability is placed on the eventual navigation solution. A more sophisticated response would be for the receiver to attempt to discriminate and sort the spoofer and authentic correlation peaks. By monitoring the power levels of the noise and correlation peaks it becomes much more difficult for the spoofer to be effective (Dehghanian et al 2012).

Hence, to be effective, a spoofer must present the receiver with an accurate signal power level within the vulnerability window of its target receiver. This is significantly further exasperated by multipath as the spoofing signal level is then essentially random. Also the distance between the spoofer and the receiver might not be known to the spoofer. As will be shown in this chapter, application of these simple power thresholds virtually assures the receiver that if the spoofer signal is strong enough to be effective then it is also detectable with a reasonable probability.

The main focus of this chapter is on the vulnerability assessment of the GPS receiver's acquisition procedure to the spoofing attack. The effectiveness of spoofing

countermeasure approaches based on SNR and absolute power analysis will be discussed and compared. As shown, while the SNR based discrimination of spoofing signals is of limited effectiveness, with a modest circuit modification, the receiver can measure the absolute power of each received PRN which is an effective means of detecting and discriminating spoofer sources and considerably reducing the vulnerability region of the target GPS receiver.

To this end, an analytical approach has been considered to investigate the effect of the spoofing signals on the receiver noise floor. It has been shown that the distribution of spoofing interference can be approximated by a circularly symmetric Gaussian distribution which is added to the ambient additive white Gaussian noise (AWGN). Acquisition performance of a typical GPS receiver has been analyzed as a function of the total spoofing power (TSP) metric. It is shown that the spoofing interference can decrease the effective SNR of the authentic signals, which results in the deterioration of receiver acquisition performance. On the contrary, the spoofing power increment increases the SNR of the spoofing PRN signals, which can mislead the receiver toward acquiring the spoofed correlation peaks.

The rest of this chapter is organized as follows: In Section 4.2 the received signal model is discussed. Section 4.3 discusses the acquisition procedure of a GPS receiver as a detection problem. Section 4.4 describes the noise floor estimation of a typical GPS receiver and then the effect of spoofing signals on increasing the noise floor estimate of a GPS receiver is discussed. Section 4.5 analyses the received SNR of authentic and spoofing signals. Section 4.6 analyses the vulnerability of acquisition process to spoofing

signals. Section 4.7 discusses two spoofing discrimination techniques namely SNR monitoring and absolute power monitoring for acquiring receivers. Real data processing and analysis results are presented in Section 4.8 and finally concluding notes are provided in Section 4.9.

4.2 System Model

Herein, it is assumed that the spoofing signals are transmitted from a single terrestrial antenna and is received at the target receiver's antenna as shown in Figure 4-1. It is assumed that the structure of the spoofing signals is similar to that of the authentic GPS signals; however the spoofer is not limited to generating signals at the same power level, code delay, Doppler frequency and even PRN set as currently available authentic signals.

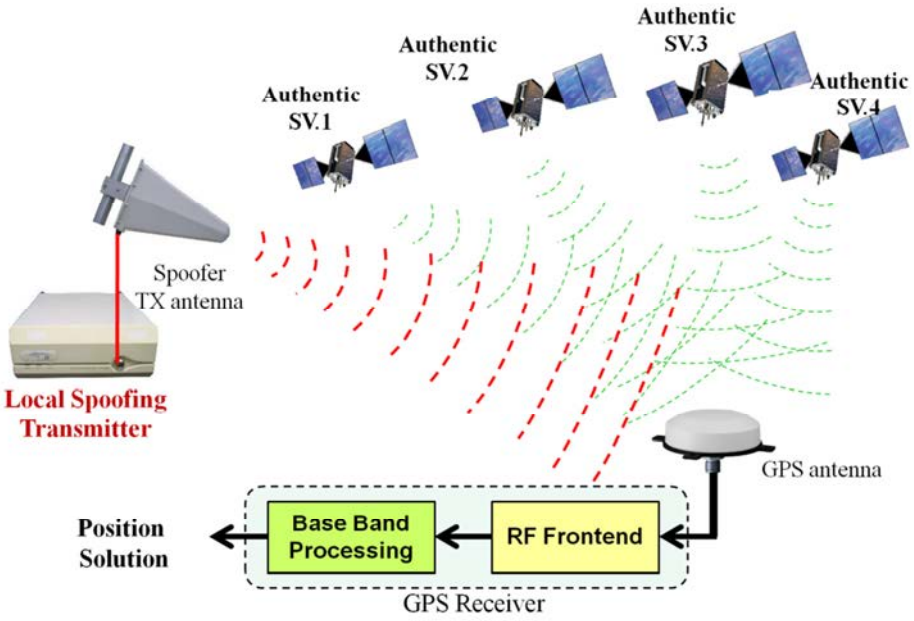


Figure 4-1 Spoofing Scenario Illustration

The target GPS receiver is assumed to operate in the acquisition stage and aim to correctly detect the presence of authentic signals and provide a rough estimate of the code

delay and Doppler frequency of each received PRN. Therefore, if the spoofing signal generates a totally aligned correlation peak with the authentic signal in terms of Doppler frequency and code delay, it does not mislead the acquisition procedure of the target receiver.

The baseband processing section of a generic GPS receiver consists of several complex correlators whose typical structure has been shown in Figure 4-2. This part of the receiver includes Doppler removal, signal de-spreading and low pass filtering.

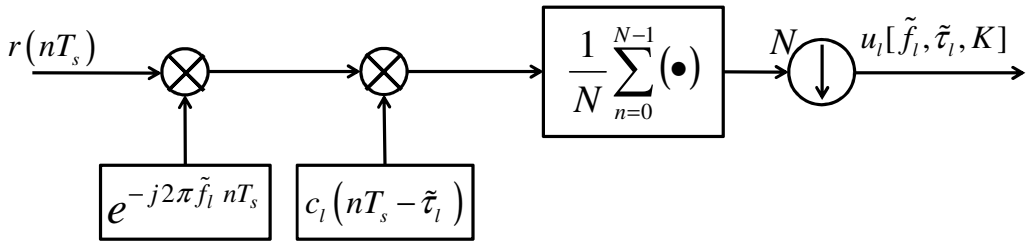


Figure 4-2 Correlator structure in the base-band section of the GPS receiver

In Figure 4-2 c_l is the *l*th locally generated spreading sequence, $\tilde{f}_l$and $\tilde{\tau}_l$ are the estimated Doppler and code delay of the locally generated signal, respectively. During the acquisition process the receiver correlates the received signal, defined in (2-1), with locally generated PRN codes with different delays that are modulated by different Doppler frequencies. Then, the resulting signal is integrated over *N* consecutive samples. When the Doppler frequency and the code delay of the locally generated signal match those of the received signal, a correlation peak will be observed at the output of the integrator. Herein, it is assumed that the phase of the locally generated carrier is not necessarily synchronized to the target PRN but that its Doppler frequency and spreading code delay are perfectly matched to the desired signal's parameters. Also, the integration

time has been considered to be much shorter than the data bit duration and as such, the effect of data bit transitions have been neglected in the following formulations. Therefore, the output signal from integrator and dump block can be written as follows (Van Dierendonck 2002):

$$u_l[\tilde{f}_l,\tilde{\tau}_l,k]=\underbrace{\sqrt{p_l^a}\,e^{j\varphi_l^a}}_{\text{I: Desired Signal}}+\underbrace{\sum_{\substack{m\in\mathbf{J}^a\\ m\neq l}}\sqrt{p_m^a}\,\psi_{ml}^a[\tilde{f}_l,\tilde{\tau}_l,k]}_{\text{II: Interference caused by other authentic PRNs}}+\underbrace{\sum_{q\in\mathbf{J}^s}\sqrt{p_q^s}\,\psi_{ql}^s[\tilde{f}_l,\tilde{\tau}_l,k]}_{\text{III: Interference caused by spoofer generated PRNs}}+\underbrace{\overline{\eta}[k]}_{\text{IV: Gaussian Noise}} \tag{4-1}$$

where

$$\begin{aligned}\psi_{ml}^a[\tilde{f}_l,\tilde{\tau}_l,k]&=\frac{1}{N}\sum_{n=(k-1)N+1}^{kN}F_m^a(nT_s)\,c_l\left(nT_s-\tilde{\tau}_l\right)e^{-j2\pi\tilde{f}_l\,nT_s}\\ \psi_{ql}^s[\tilde{f}_l,\tilde{\tau}_l,k]&=\frac{1}{N}\sum_{n=(k-1)N+1}^{kN}F_q^s(nT_s)\,c_l\left(nT_s-\tilde{\tau}_l\right)e^{-j2\pi\tilde{f}_l\,nT_s}\end{aligned} \tag{4-2}$$

where $F_m^a(nT_s)$ and $F_q^s(nT_s)$ are defined based on Equation (2-2). $u_l[\tilde{f}_l,\tilde{\tau}_l,k]$ is the correlator output corresponding to the *l*th locally generated PRN signal with the Doppler frequency of $\tilde{f}_l$ and code delay of $\tilde{\tau}_l$ at the *k*th integration interval. This signal is composed of four terms as follows: the first term, (I), is the desired signal which is the term of interest during acquisition process; the second term, (II), is the interference caused by other authentic PRNs; the third term, (III), is the interference caused by the spoofing PRNs. Term II and III are generated due to the cross correlation between

different Gold sequences with the locally generated signal replica ($c_l\left(nT_s-\tilde{\tau}_l\right)e^{-j2\pi\tilde{f}_l nT_s}$). $\bar{\eta}[k]$ is a circularly symmetric complex Gaussian noise process with co-variance matrix of $\bar{\sigma}^2\mathbf{I}_2=\left(\sigma^2/N\right)\mathbf{I}_2$ where $\sigma^2\mathbf{I}_2$ is the covariance matrix of the input ambient complex white Gaussian noise and $\mathbf{I}_2$ is a 2×2 identity matrix. Commercial GPS receivers consider all the last three terms as the noise term and perform the acquisition and tracking operations just on the first term.

4.3 GPS Signal Acquisition, a GLRT Detection Problem

The acquisition process of a GPS receiver can be considered as a generalized likelihood ratio test (GLRT) that detects the presence of a PRN signal if (Kay 1998)

$$L_G\left(u_l\right)=\frac{p_{u_l|\boldsymbol{\theta}_{l,1};\mathrm{H}_{l,1}}\left(u_l\,|\,\tilde{\boldsymbol{\theta}}_{l,1};\mathrm{H}_{l,1}\right)}{p_{u_l;\mathrm{H}_{l,0}}\left(u_l;\mathrm{H}_{l,0}\right)}>\gamma_{th} \tag{4-3}$$

where $\mathrm{H}_{l,0}$ represents the hypothesis of the absence of *l* th PRN and $\mathrm{H}_{l,1}$ represents the hypothesis of the presence of that PRN signal at the estimated Doppler shift and code delay. u_l is the output value of the correlator branch corresponding to the *l*th PRN. $\tilde{\boldsymbol{\theta}}_{l,1}=\left[\tilde{f}_l,\tilde{\tau}_l,\tilde{\Lambda}_l\right]$ represents the maximum likelihood estimate (MLE) of the parameters vector that consists of Doppler shift, code delay and received SNR for the *l*th PRN signal. γ_{th} is the threshold for detecting the $\mathrm{H}_{l,1}$ hypothesis. $p_{u_l|\boldsymbol{\theta}_{l,1};\mathrm{H}_{l,1}}$ and $p_{u_l;\mathrm{H}_{l,0}}$ represent the complex Gaussian distribution of correlator output under the $\mathrm{H}_{l,1}$ and $\mathrm{H}_{l,0}$ hypotheses, respectively. After simplification of Equation (4-3), sufficient statistic for GLRT

detection can be extracted as the squared value of correlator output ($D_l = u_l u_l^*$). $p_{D_l|\boldsymbol{\theta}_{l,1};\mathrm{H}_{l,1}}$ and $p_{D_l;\mathrm{H}_{l,0}}$ follow central and non-central chi-square distributions that can be written as

$$\begin{aligned} p_{D_l;\mathrm{H}_{l,0}}\left(D_l;\mathrm{H}_{l,0}\right) &= \frac{1}{2\bar{\sigma}^2} e^{\left(\frac{-D_l}{2\bar{\sigma}^2}\right)} \\ p_{D_l|\boldsymbol{\theta}_{l,1};\mathrm{H}_{l,1}}\left(D_l \mid \tilde{\boldsymbol{\theta}}_{l,1};\mathrm{H}_{l,1}\right) &= \frac{1}{2\bar{\sigma}^2} e^{\left(-\frac{D_l+p_l}{2\bar{\sigma}^2}\right)} I_0\left(\frac{\sqrt{D_l\, p_l}}{\bar{\sigma}^2}\right), \end{aligned} \tag{4-4}$$

where $I_0(\bullet)$ is the modified zero order Bessel function of the first kind. If the detection threshold is defined as D_{th}, then the probability of detection ($P_{D\text{-}cell}$) and probability of false alarm ($P_{FA\text{-}cell}$) for a given pair of $\tilde{f}_l$ and $\tilde{\tau}_l$can be defined as (Kaplan & Hegarty 2006)

$$\begin{aligned} P_{D-cell} &= \int_{D_{th}}^{\infty} \frac{1}{2\bar{\sigma}^2} e^{\left(-\frac{D_l+p_l}{2\bar{\sigma}^2}\right)} I_0\left(\frac{\sqrt{D_l\, p_l}}{\bar{\sigma}^2}\right) dD_l \\ P_{FA-cell} &= \int_{D_{th}}^{\infty} \frac{1}{2\bar{\sigma}^2} e^{\left(\frac{-D_l}{2\bar{\sigma}^2}\right)} dD_l \end{aligned} \tag{4-5}$$

GLRT suggests that the GPS receiver evaluates the correlator output corresponding to all possible range of Doppler and code delays and picks a cell with the highest squared amplitude. If the amplitude is above the threshold, the signal presence is flagged and the Doppler and code delay of the corresponding cell is reported as the rough estimate of detected signal parameters. Therefore, for the correct detection only one of the CAF cells should be above the detection threshold and the false alarm should not occur in any of the CAF cells. Therefore, considering the independent CAF cells, the false alarm probability of total CAF ($P_{FA-system}$) can be written as (Borio 2008)

$$P_{FA-system} = 1-\left(1-P_{FA-cell}\right)^{N_c} \tag{4-6}$$

where N_c represents the total number of cells in CAF search space and therefore

$$P_{FA-cell} = 1-\left(1-P_{FA-system}\right)^{\frac{1}{N_c}} \tag{4-7}$$

Considering (4-4), (4-5) and (4-7), the detection threshold can be defined as (Borio 2008)

$$D_{th} = -2\bar{\sigma}^2 \ln\left[P_{FA-cell}\right] = -2\bar{\sigma}^2 \ln\left[1-\left(1-P_{FA-system}\right)^{\frac{1}{Nc}}\right] \tag{4-8}$$

Equation (4-8) shows that the detection threshold depends on the noise floor variance of the receiver, the assumed probability of false alarm for the system and the number of CAF cells. Equation (4-8) can be modified to define a SNR detection threshold as

$$\Lambda_{th} = \frac{D_{th}}{2\bar{\sigma}^2} = -\ln\left[1-\left(1-P_{FA-system}\right)^{\frac{1}{N_c}}\right] \tag{4-9}$$

Based on (4-9), it can be deduced that for a given probability of false alarm, the acquisition procedure is able to detect those signals whose post correlation SNR is above the detection threshold, Λ_{th}.

4.4 Noise Floor Estimation

One of the methods for calculating received noise variance is correlating the received signal set with a normalized PRN signal, $c_\ell\left(nT_s-\tau_\ell\right)$, which is known to be absent in the received signal set. In this case, the correlator integration time is chosen the same as

the acquisition integration time; therefore, the variance of correlator output provides an estimate of the post correlation noise variance as

$$\hat{\sigma}^2 = \frac{1}{2N_s}\sum_{k=0}^{N_s-1}\left|u_\ell[f_\ell,\tau_\ell,k]\right|^2 = \frac{1}{2}\mathrm{var}\left[u_\ell[f_\ell,\tau_\ell,k]\right] \tag{4-10}$$

where N_s is the number of correlator outputs over which the noise variance has been calculated, and f_ℓ and τ_ℓ represent a randomly chosen code delay and Doppler shift for the fictitious PRN signal. The calculated variance is divided by two in order to measure the post correlation noise variance in either of the in-phase (I) or quadrature (Q) branches. The value of estimated noise variance ($\hat{\sigma}^2$) should be ideally equal to the post correlation ambient noise variance ($\bar{\sigma}^2$). However, as it will be discussed in the following section, this value can be considerably affected in presence of interference signals.

4.4.1 Effect of Spoofing Signal on Receiver Noise Floor Estimate

Consider the case where the spoofing signal received at the GPS receiver antenna is stronger than the authentic GPS signals. The interference caused by the spoofer can elevate the noise floor of the receiver processing due to the cross-correlation between spoofing PRN signals and the locally generated fictitious PRN signal. A detailed expression for Equation (4-10) can be written as

$$\hat{\sigma}^2 = \frac{1}{2}\mathrm{var}\left[\underbrace{\sum_{m\in \mathbf{J}^a} \sqrt{p_m^a}\,\psi_{m\ell}[f_\ell,\tau_\ell,k]}_{\text{II: Interference induced by authentic PRNs}} + \underbrace{\sum_{q\in \mathbf{J}^s} \sqrt{p_q^s}\,\psi_{q\ell}[f_\ell,\tau_\ell,k]}_{\text{III: Interference induced by spoofer generated PRNs}} + \underbrace{\bar{\eta}[k]}_{\text{IV: Post Corelation Gaussian Noise}} \right] \tag{4-11}$$

where it is assumed that the ℓ^{th} fictitious PRN is present in neither of the authentic nor the spoofing PRN sets. Therefore, the correlator output is made up of three major terms namely cross-correlation terms induced by authentic PRN signals, cross-correlation terms induced by the spoofing PRN signals and finally the post correlation Gaussian noise.

It is assumed that the delay and Doppler frequency of the authentic and spoofing PRNs are independent of each other and are randomly distributed. Therefore, (4-11) can be re-written as

$$\hat{\sigma}^2 = \frac{1}{2}\left[\underbrace{\sum_{m\in \mathbf{J}^a} p_m^a\,\mathrm{var}\left[\psi_{ma}[f_\ell,\tau_\ell,k]\right]}_{\text{II: Cross-correlation induced by authentic PRN signals}} + \underbrace{\sum_{q\in \mathbf{J}^s} p_q^s\,\mathrm{var}\left[\psi_{qa}[f_\ell,\tau_\ell,k]\right]}_{\text{III: Cross-correlation induced by spoofing PRN signals}} + \underbrace{\mathrm{var}\left[\bar{\eta}[k]\right]}_{\text{IV: Post Corelation Gaussian Noise}} \right] \tag{4-12}$$

The first and the second terms in (4-12) consist of $\mathrm{var}\left[\psi_{m\ell}[f_\ell,\tau_\ell,k]\right]$ and $\mathrm{var}\left[\psi_{q\ell}[f_\ell,\tau_\ell,k]\right]$. The former term corresponds to the cross correlation of the *m*th normalized authentic PRN and the ℓ th fictitious PRN and the latter corresponds to the cross correlation of the *q*th normalized spoofing PRN and the ℓ th fictitious PRN. The distribution of these cross-correlation terms have been calculated numerically and simulations show that they can be well approximated by a zero mean Gaussian

distribution in either of the I and Q branches. The simulations have been performed for normalized power spreading Gold codes and the cross correlation variance in either of in-phase or quadrature branches has been extracted to be $\bar{\sigma}_{\psi}^2 = 0.00033$. The expected value of the product of real and imaginary components of the correlator output can be written as

$$\begin{aligned}
&\mathrm{E}\left[\Re\{\psi_{q\ell}[f_\ell,\tau_\ell,k]\}\bullet\Im\{\psi_{q\ell}[f_\ell,\tau_\ell,k]\}\right]= \\
&=\frac{1}{N^2}\mathrm{E}\left[\begin{array}{l}\displaystyle\sum_{n=(K-1)N+1}^{KN} c_q\left(nT_s-\tau_q\right)c_\ell\left(nT_s-\tau_\ell\right)\cos\left(2\pi\Delta f_{q\ell}nT_s+\Delta\varphi_{q\ell}\right) \\ \times\displaystyle\sum_{m=(K-1)N+1}^{KN} c_q\left(mT_s-\tau_q\right)c_\ell\left(mT_s-\tau_\ell\right)\sin\left(2\pi\Delta f_{q\ell}nT_s+\Delta\varphi_{q\ell}\right)\end{array}\right] \\
&=\frac{1}{N^2}\sum_{n=(K-1)N+1}^{KN}\sum_{m=(K-1)N+1}^{KN}\left\{\begin{array}{l}\mathrm{E}\left[c_q\left(nT_s-\tau_q\right)c_\ell\left(nT_s-\tau_\ell\right)c_q\left(mT_s-\tau_q\right)c_\ell\left(mT_s-\tau_\ell\right)\right] \\ \times\cos\left(2\pi\Delta f_{q\ell}nT_s+\Delta\varphi_{q\ell}\right)\sin\left(2\pi\Delta f_{q\ell}nT_s+\Delta\varphi_{q\ell}\right)\end{array}\right\} \\
&\approx\frac{1}{2N^2}\sum_{n=(K-1)N+1}^{KN}\left\{\mathrm{E}\left[\left(c_q\left(nT_s-\tau_q\right)c_\ell\left(nT_s-\tau_\ell\right)\right)^2\right]\underbrace{\sin\left(2\left(2\pi\Delta f_{q\ell}nT_s+\Delta\varphi_{q\ell}\right)\right)}_{\substack{=0\\ \text{[High Frequency terms]}}}\right\}=0
\end{aligned} \tag{4-13}$$

where $\Re\{\bullet\}$ and $\Im\{\bullet\}$ represent the real and imaginary parts of their argument respectively. $\mathrm{E}\{\bullet\}$ represents the statistical expectation of its corresponding argument. Therefore, the distribution of the correlator output of the noise floor estimator can be written as

$$\psi_{q\ell}[f_\ell,\tau_\ell,k]\sim\mathrm{N}_c\left(\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}\bar{\sigma}_{\psi}^2 & 0\\ 0 & \bar{\sigma}_{\psi}^2\end{bmatrix}\right) \tag{4-14}$$

where the $\mathrm{N}_c(\mathbf{A},\mathbf{C})$ is the circularly symmetric complex Gaussian distribution with the mean vector of **A** and the covariance matrix of **C**. It should be noted that the statistical

properties of cross-correlation terms are similar for normalized authentic and spoofing signals, therefore, the distributions of $\psi_{q\ell}[f_\ell,\tau_\ell,k]$ and $\psi_{m\ell}[f_\ell,\tau_\ell,k]$ are similar. Considering Equation (4-14), the correlator output $u_\ell[f_\ell,\tau_\ell,k]$ is a complex Gaussian random variable that can be written in the form of the summation of complex Gaussian random variables with the following distribution:

$$u_\ell[f_\ell,\tau_\ell,k] \sim \mathrm{N}_c\left(\begin{bmatrix}0\\0\end{bmatrix}, \frac{N_0}{2NT_s}\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} + \left(\sum_{m\in\mathbf{J}^a} p_m^a + \sum_{q\in\mathbf{J}^s} p_q^s\right)\begin{bmatrix}\bar{\sigma}_\psi^2 & 0\\0 & \bar{\sigma}_\psi^2\end{bmatrix}\right) \tag{4-15}$$

Equation (4-16) shows that the variance of the cross correlation term is directly affected by the transmitted power of the authentic and spoofing PRNs. The transmit power of GPS signals is designed such that the cross-correlation level of authentic PRNs does not exceed the ambient noise floor (O'Driscoll 2007). However, spoofing signals can be much more powerful than the authentic GPS signals. Therefore, their corresponding cross-correlation interference level can overtake the ambient Gaussian noise floor and therefore decrease the authentic SNR at the correlator output of conventional GPS receivers. To investigate the effect of spoofing interference on the noise floor variance, the total received spoofing power (TSP) has been considered and is defined as

$$[TSP]_{dBW} = 10\log_{10}\left(\sum_{q\in\mathbf{J}^s} p_q^s\right) \tag{4-16}$$

In Figure 4-3 the estimated noise floor, $2\hat{\sigma}^2$, is depicted versus the TSP for different coherent integration times of T_c=1 ms, T_c= 2 ms, T_c= 4 ms and T_c= 8 ms.

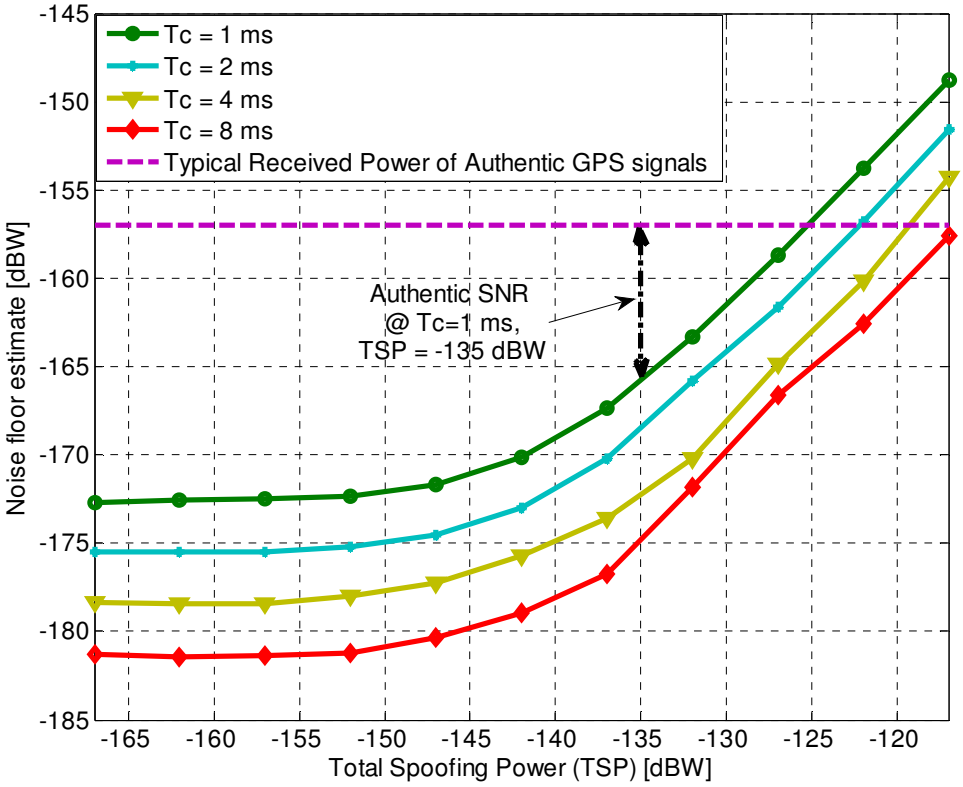


Figure 4-3 Noise Floor Estimate ($2\hat{\sigma}^2$) versus Total Spoofing Power (TSP)

It is observed that when TSP is very low, the ambient Gaussian noise is the dominant term that determines the noise floor. However, increasing the TSP will increase the noise floor and cause it to overtake the authentic satellites' received signal power. Figure 4-3 also shows that increasing the coherent integration time does not mitigate the cross-correlation effect of the higher power spoofing signals and it only causes a vertical shift to the estimated noise floor.

4.5 Received SNR analysis in the Presence of Spoofing Interference

Having the noise floor estimate of the received GPS signal set, the effective signal-to-noise ratio (SNR) of the *l*th authentic and spoofing signals (i.e. Λ_l^a and Λ_l^s) can be written as

$$\Lambda_l^a = \frac{p_l^a}{2\hat{\sigma}^2}$$
$$\Lambda_l^s = \frac{p_l^s}{2\hat{\sigma}^2} \quad (4\text{-}17)$$

In the following subsections of this chapter, all the SNR values are calculated based on 1 ms coherent integration time.

Figure 4-4 shows the authentic and spoofing SNR values versus the TSP for the case of 10 equal power authentic PRNs and 10, 20, 30 and 40 equal power spoofing PRNs. The power of each authentic PRN is -158 dBW and the integration time is T_c=1 ms. The SNR threshold has been calculated for $P_{FA}=10^{-3}$ as a typical probability of false alarm. The search space consists of 15 Doppler bins and 2046 code delay bins, therefore the size of search space is defined as $N_c=15\times2046=30690$. It is observed that SNR of the authentic signals decreases as the TSP increases while on the opposite, the SNR of spoofing PRNs increases up to a certain level as the TSP increases. The maximum spoofing SNR level depends on the number of transmitted spoofing PRNs and the distribution of TSP among them. The receiver noise floor estimate at 1 ms integration time has been also depicted on the right hand Y-axis in blue. This curve is useful for analyzing the noise floor increase at a certain TSP level.

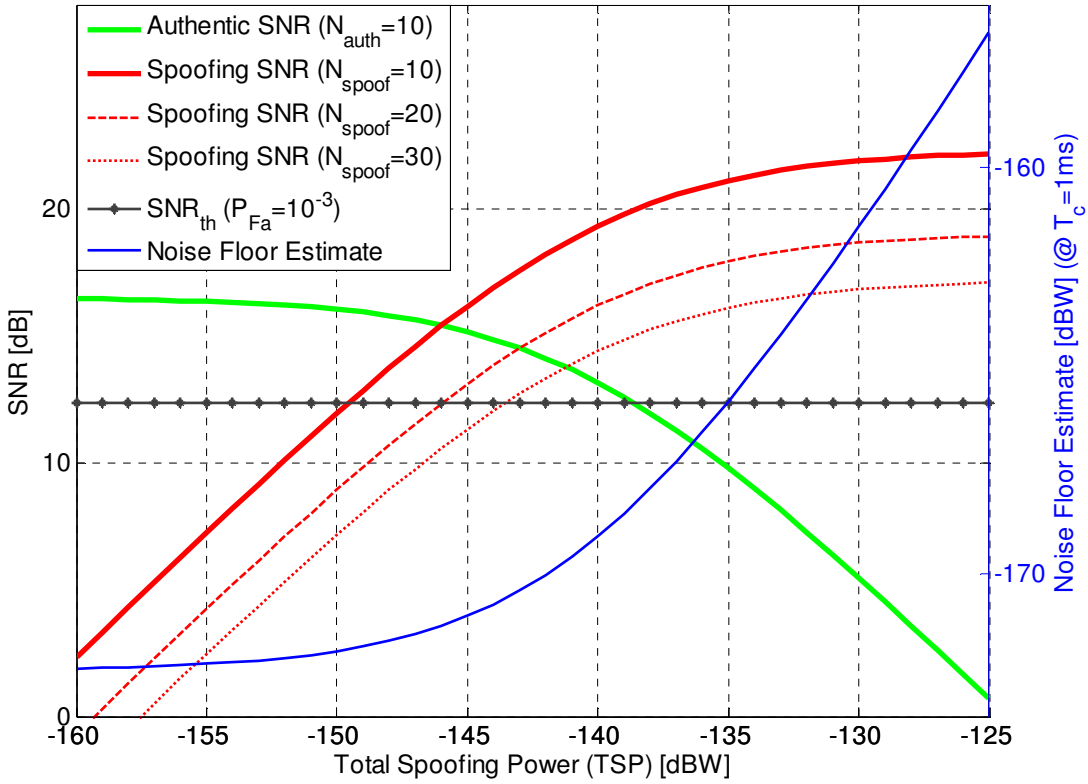


Figure 4-4 Received SNR versus TSP for authentic and spoofing correlation peaks

In Figure 4-4 it is also observable that if the number of PRNs among which the spoofer is dividing its transmit power increases, each individual PRN will receive a smaller portion of spoofing power which leads to a lower SNR at the same TSP value. For instance, for the case of 30 spoofing PRNs, it is observed that the maximum SNR is less than 19 dB.

4.5.1 Requirements for an Effective Spoofer

An effective spoofer should meet the following conditions in order to avoid detection:

- The power of spoofing generated PRN signals should be higher than that of the authentic PRN signals' power in order to mislead the previously discussed GLRT detector. However, this power should not be higher than the maximum authentic signal's power level anticipated by the receiver as it can be easily detected.

- The spoofing interference should not considerably increase the receiver noise floor, since it might be detected as unwanted interference by a spoofing-aware GPS receiver.
- The number of spoofing PRNs should be selected from a plausible list of visible SV's. Furthermore, the SNR of spoofing PRNs should not exceed the typical SNR level of the authentic signals, because unusual SNR levels might be detected by the receiver.
- If the spoofer knows the detection threshold of the receiver, it is better to choose a TSP bias point such that the authentic SNR falls under the detection threshold. In this case only the spoofing peak can be found above the detection threshold.

Based on the above conditions and the information provided, a possible TSP bias point can be TSP=-143 dBW for 10 equal power spoofing PRNs. In this case all the above first three conditions has been met while the absolute power of each spoofing PRN is around -153 dBW which is equal to the maximum possible power level of the L1 C/A GPS signals (IS-GPS-200E 2010). Also, the noise floor increase is around 2 dB, which is not considerable.

4.6 Vulnerability of GPS Acquisition to Spoofing Attack

The acquisition process of GPS receivers is aimed at detecting the correlation peaks corresponding to the authentic signals and estimating their approximate Doppler frequency and code delay. However, the interference caused by a spoofing signal can considerably increase the observed noise floor of a GPS receiver. In the presence of spoofing signals, the squared amplitude of the correlator output corresponding to the *l*th PRN CAF can be written under three different hypotheses, namely $H_{l,0}$ (Signal absent),

$\mathrm{H}_{l,1}$ (Authentic signal present) and $\mathrm{H}_{l,2}$ (Spoofing signal present) with the following distributions:

$$
\begin{aligned}
p_{D_l;\mathrm{H}_{l,0}}\left(D_l;\mathrm{H}_{l,0}\right) &= \frac{1}{2\hat{\sigma}^2}e^{\left(\frac{-D_l}{2\hat{\sigma}^2}\right)} \\
p_{D_l|\tilde{\boldsymbol{\theta}}_{l,1};\mathrm{H}_{l,1}}\left(D_l \mid \tilde{\boldsymbol{\theta}}_{l,1};\mathrm{H}_{l,1}\right) &= \frac{1}{2\hat{\sigma}_a^2}e^{\left(-\frac{D_l+p_l^a}{2\hat{\sigma}_a^2}\right)} I_0\left(\frac{\sqrt{D_l\ p_l^a}}{\hat{\sigma}_a^2}\right) \\
p_{D_l|\tilde{\boldsymbol{\theta}}_{l,2};\mathrm{H}_{l,2}}\left(D_l \mid \tilde{\boldsymbol{\theta}}_{l,2};\mathrm{H}_{l,2}\right) &= \frac{1}{2\hat{\sigma}_s^2}e^{\left(-\frac{D_l+p_l^s}{2\hat{\sigma}_s^2}\right)} I_0\left(\frac{\sqrt{D_l\ p_l^s}}{\hat{\sigma}_s^2}\right)
\end{aligned}
\tag{4-18}
$$

where $\tilde{\boldsymbol{\theta}}_{l,1}=\left[\tilde{f}_l^a,\tilde{\tau}_l^a,\tilde{\Lambda}_l^a\right]$ and $\tilde{\boldsymbol{\theta}}_{l,2}=\left[\tilde{f}_l^s,\tilde{\tau}_l^s,\tilde{\Lambda}_l^s\right]$ and

$$
\begin{aligned}
\hat{\sigma}^2 &= \frac{N_0}{2NT_s}+\bar{\sigma}_\psi^2\left(\sum_{m\in\mathbf{J}^a}p_m^a+\sum_{q\in\mathbf{J}^s}p_q^s\right) \\
\hat{\sigma}_a^2 &= \frac{N_0}{2NT_s}+\bar{\sigma}_\psi^2\left(\sum_{\substack{m\in\mathbf{J}^a\\ m\neq l}}p_m^a+\sum_{q\in\mathbf{J}^s}p_q^s\right) \\
\hat{\sigma}_s^2 &= \frac{N_0}{2NT_s}+\bar{\sigma}_\psi^2\left(\sum_{m\in\mathbf{J}^a}p_m^a+\sum_{\substack{q\in\mathbf{J}^s\\ q\neq l}}p_q^s\right)
\end{aligned}
\tag{4-19}
$$

In case that the number of authentic and spoofing PRN signals is large (around 10 or so), it can be assumed that the values of the three variances of (4-19) are approximately equal and it can be written that $\hat{\sigma}^2 \approx \hat{\sigma}_a^2 \approx \hat{\sigma}_s^2$. Figure 4-5 illustrates the three chi-square distributions of (4-19). In this illustration, the power of authentic correlation signal is assumed to be -157 dBW and the spoofing signal power is -155 dBW. Two detection thresholds that can be used for discrimination between these three hypotheses are also shown.

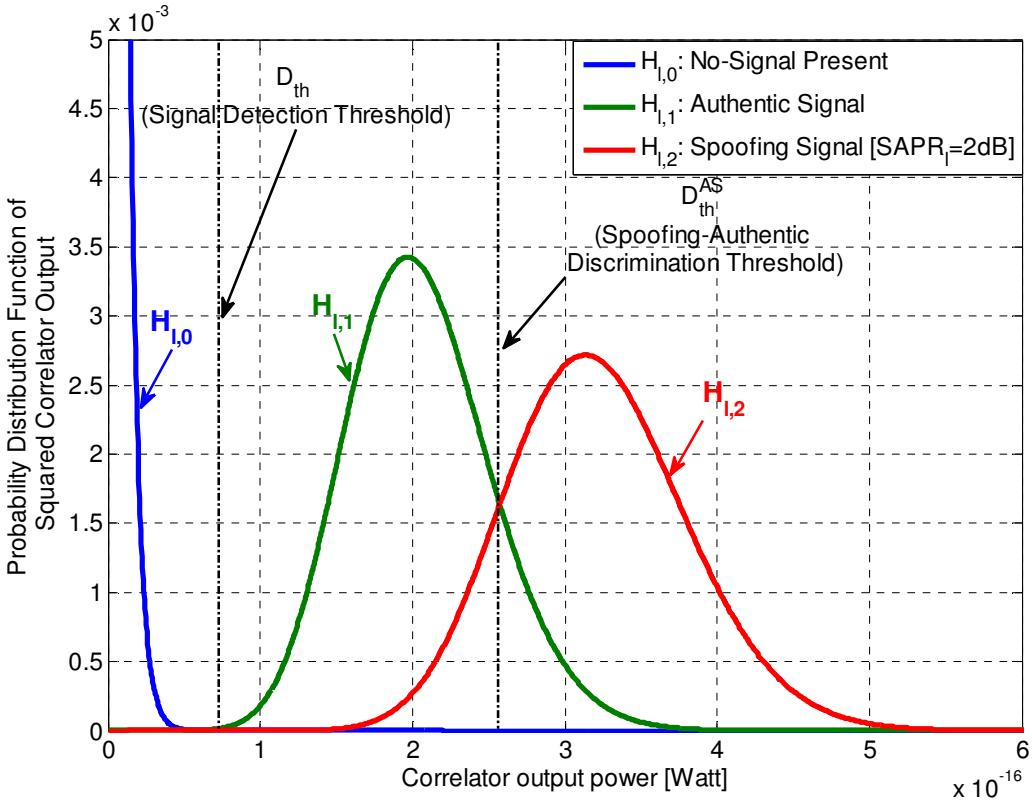


Figure 4-5 Correlator squared amplitude distributions for three hypotheses of $H_{l,0}$, $H_{l,1}$ and $H_{l,2}$

4.6.1 Acquisition Vulnerability Analysis for Uncommon Authentic/Spoofing PRNs

In this case it is assumed that the receiver is trying to acquire an authentic PRN signal which is common among authentic and spoofing PRN sets, i.e. $\mathbf{J}^a$ and $\mathbf{J}^s$. Therefore, as shown by the green line in Figure 4-4, the spoofing signal decreases the SNR of the authentic signal and finally makes it fall under the detection threshold (Λ_{th}). In this scenario, the spoofer performs more like wide-band interference that degrades the detection performance of the receiver by decreasing the received SNR through an increase in the noise plus interference floor. Receiver operating characteristic (ROC)

plots are a standard tool for evaluating the performance of a detection test. An ROC curve shows the probability of detection (P_D) as a function of probability of false alarm (P_{FA}). Figure 4-6 shows the ROC for different values of TSP where the average power of authentic PRNs is -157 dBW. It is observed that the detection performance of the receiver substantially decreases as the TSP increases.

The case of uncommon spoofing and authentic PRNs can also include the scenario where the receiver is acquiring a PRN signal which is only transmitted by the spoofer. In this case, as shown by the red curves in Figure 4-4, the receiver might acquire a spoofed correlation peak if the spoofing power is enough to overtake the detection threshold.

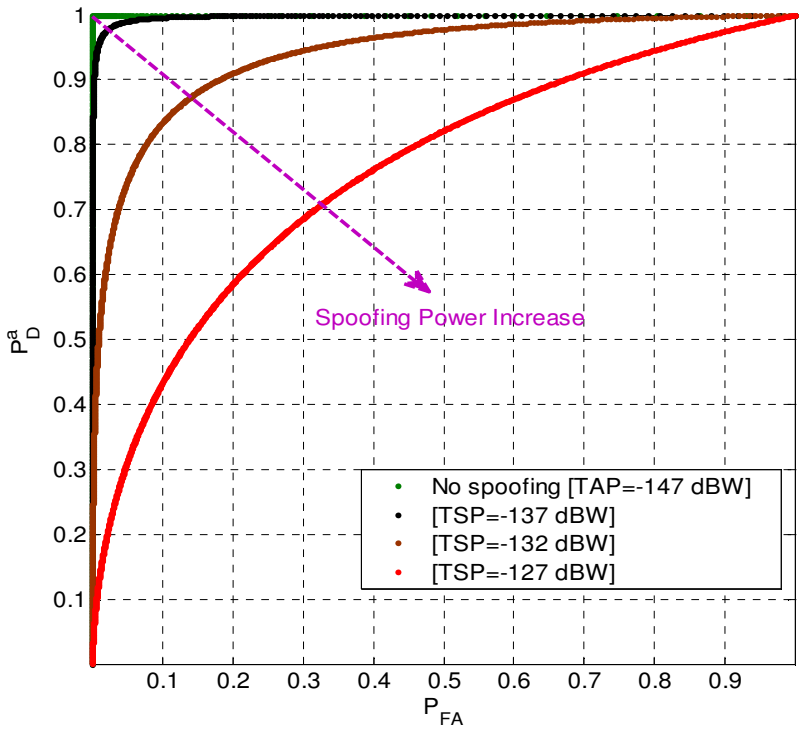


Figure 4-6 Receiver operating characteristics for the case of uncommon spoofing and authentic PRNs for different spoofing powers

4.6.2 Acquisition Vulnerability Analysis for Common Authentic/Spoofing PRNs

In this case, it is assumed that the receiver is acquiring a PRN signal that is common between authentic and spoofing signals. Therefore, both green and red curves in Figure 4-4 should be considered while analysing the receiver detection performance. Figure 4-7 shows a SNR variation curves as a function of TSP for the case of 10 equal power authentic PRNs and 10 equal power spoofing ones. Three different zones can be observed in where the first area ,(I) , corresponds to the case when the TSP is less than -150 dBW, therefore the spoofing SNR is under the detection threshold. Here, the only harmful effect of the spoofer is a slight reduction in the authentic signal SNR. In this case, the authentic correlation peak can be still acquired by the receiver.

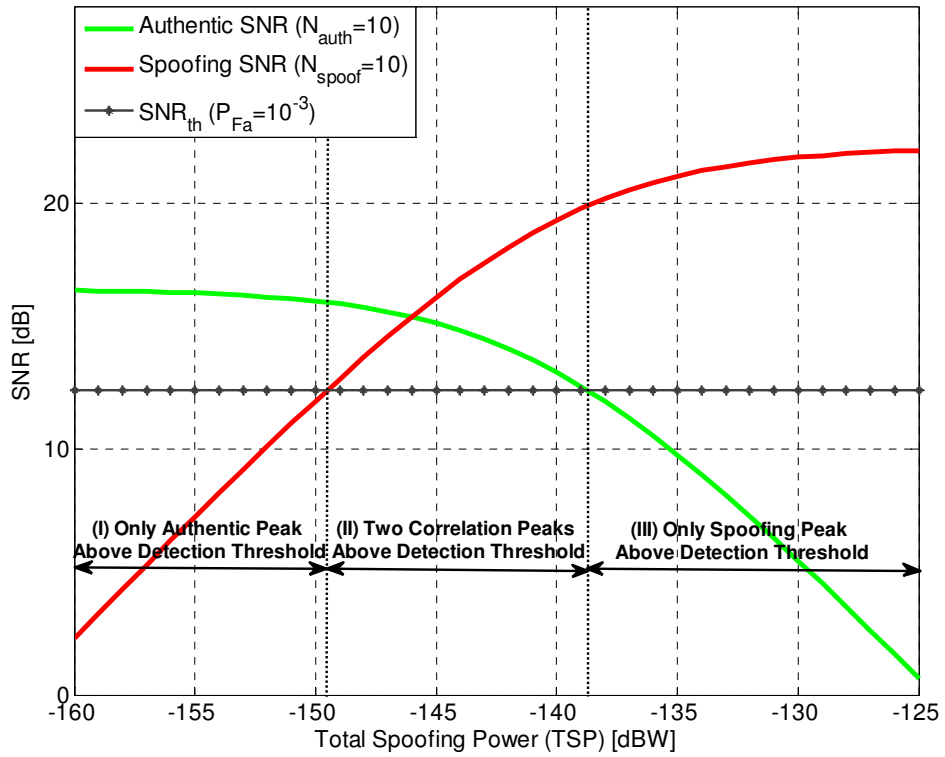


Figure 4-7 Acquisition in the presence of both authentic and spoofing correlation peaks

The second area, (II), happens when the TSP is higher than -150 dBW and lower than -139 dBW. In this case the SNR values of both authentic and spoofing signals are above the detection threshold, which implies the presence of two correlation peaks above the detection threshold. This scenario is illustrated in Figure 4-8. Hence, the receiver might mistakenly acquire the spoofing correlation peak when its SNR is higher than the authentic signal's SNR. In this area the spoofer does not considerably increase the receiver noise floor and within this TSP window the GPS receiver has maximum vulnerability to the spoofing attack.

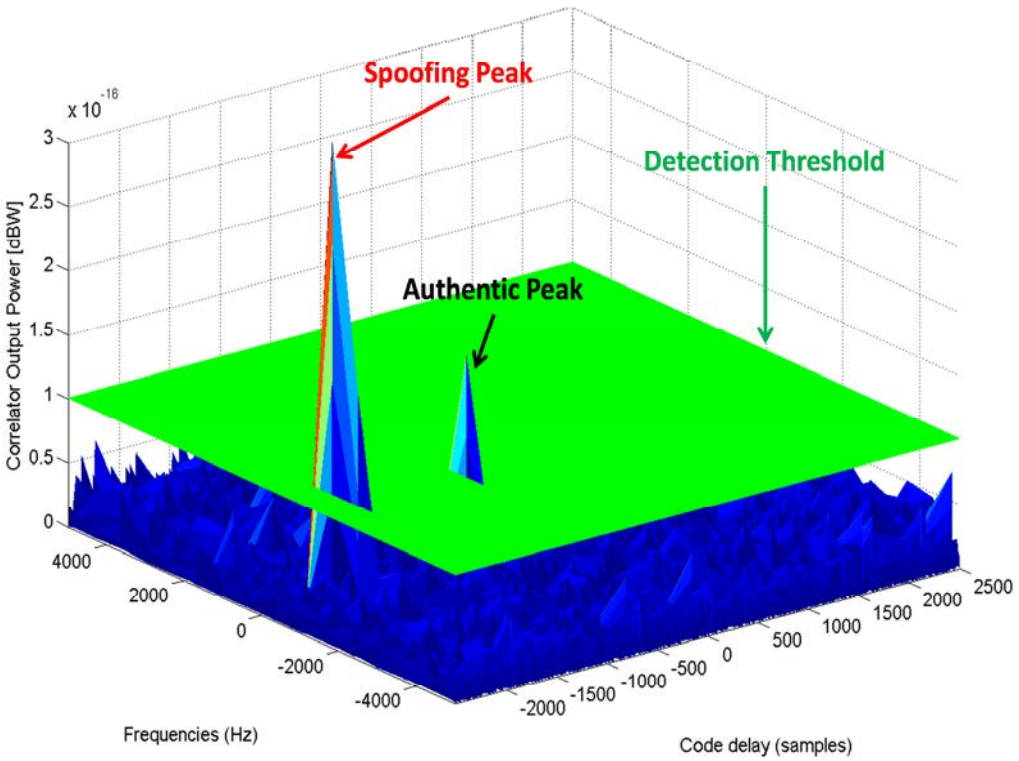


Figure 4-8 Spoofing signal generates higher power correlation peak above receiver's detection threshold

The third area, (III), belongs to the case of TSPs greater than -139 dBW where the authentic SNR falls under the detection SNR threshold and only the spoofing generated correlation peak can be detected by the acquisition procedure. In this case the spoofing interference has a major contribution on the receiver noise floor. As it is observed, at high TSP values, the SNR for spoofing PRNs reached an upper limit due to the fact that the cross correlation of spoofing signals become the dominant component in the receiver noise floor. In other words, at high TSP values, the spoofer is generating powerful correlation peaks over an elevated noise floor caused by the cross correlation between spoofing signals and local PRN replicas. In this case the ambient noise in negligible compared to the spoofing signals' cross correlation terms.

4.7 Spoofing Discrimination during Acquisition

Herein, two spoofing countermeasure techniques for an acquiring receiver have been considered i.e. "spoofing discrimination based on received SNR" and "spoofing discrimination based on absolute received power".

4.7.1 Spoofing Discrimination based on Received SNR

SNR based spoofing countermeasure techniques are designed to discriminate spoofed correlation peaks based on their unusual high SNR. Dehghanian et al (2012) have proposed a multiple hypothesis spoofing discrimination technique that sets two thresholds in order to discriminate among the three distributions discussed in (4-19). They have defined the first SNR threshold based on (4-9) in order to set the first detection threshold and discriminate $\mathrm{H}_{l,0}$ from $\mathrm{H}_{l,1}$ and $\mathrm{H}_{l,2}$. In the next step, a second threshold has been set in order to discriminate abnormal high SNR spoofing correlation peaks among all

correlation peaks that are above the first detection threshold. To this end, they have assumed a uniform distribution for authentic signals' SNR in order to come up with a marginal distribution for the authentic signals power as follows:

$$p_{D_l|\boldsymbol{\theta}'_{l,1};\mathrm{H}_{l,1}}\left(D_l \mid \boldsymbol{\theta}'_{l,1};\mathrm{H}_{l,1}\right)=\frac{1}{\Lambda_{\max}-\Lambda_{\min}}\int_{\Lambda_{\min}}^{\Lambda_{\max}} p_{D_l|\boldsymbol{\theta}_{l,1};\mathrm{H}_{l,1}}\left(D_l \mid \boldsymbol{\theta}_{l,1};\mathrm{H}_{l,1}\right)d\Lambda_l \tag{4-20}$$

where $\boldsymbol{\theta}'_{l,1}=\left[f_l^a,\tau_l^a\right]$ and $\Lambda_{\max}$ and $\Lambda_{\min}$ are the maximum and minimum possible SNR values for an authentic signal. Based on (4-21) and considering a probability of false alarm, a spoofing detection threshold has been defined as

$$P_{FA}^{AS}=\int_{\Lambda_{th}^{AS}}^{\infty} p_{D_l|\boldsymbol{\theta}'_{l,1};\mathrm{H}_{l,1}}\left(D_l \mid \boldsymbol{\theta}'_{l,1};\mathrm{H}_{l,1}\right)dD_l \tag{4-21}$$

where P_{FA}^{AS} is the probability of false alarm for the spoofing discrimination test and Λ_{th}^{AS} is the spoofing discrimination SNR threshold. Figure 4-9 illustrates the performance of this spoofing countermeasure technique. Based on this technique, a correlation peak is declared as an authentic one if it is located between two detection thresholds. Although SNR based spoofing discrimination methods are one of the most well-known spoofing countermeasure techniques, their effectiveness is limited in cases when spoofing signals elevate the noise floor of the receiver. For instance, as it is shown in Figure 4-4, a spoofer can set up its TSP such that the SNR of individual spoofing signals does not exceed the spoofing detection threshold (Λ_{th}^{AS}).

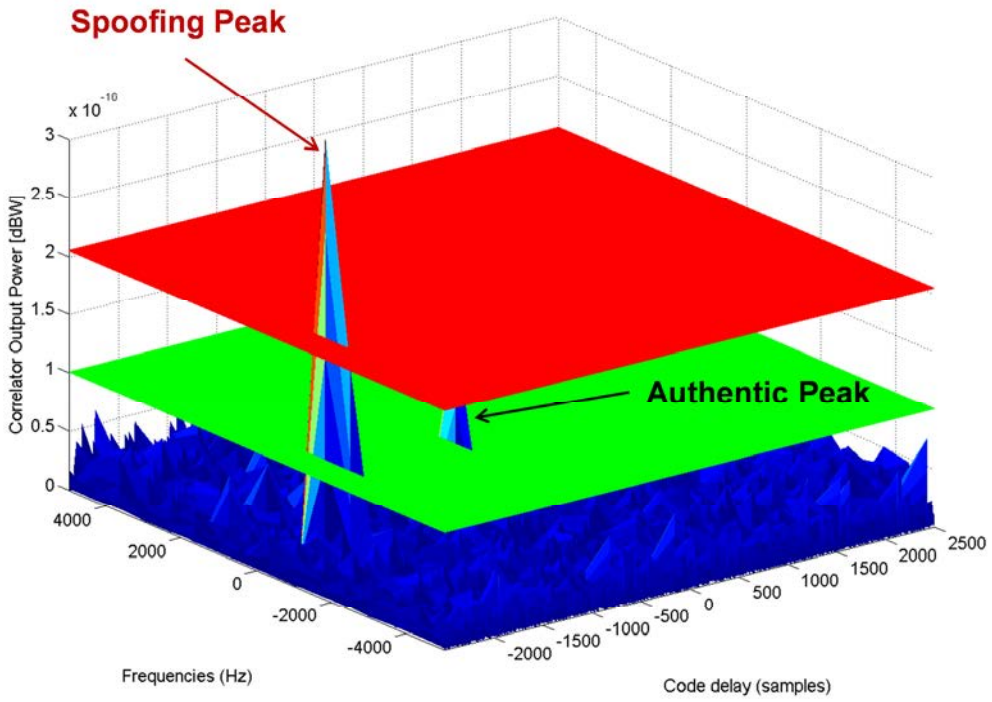


Figure 4-9 Spoofing discrimination based on received SNR

4.7.2 Spoofing discrimination based on absolute received power

In the case when the receiver is capable to analyze the absolute received power only within a certain accuracy level, the receiver vulnerability against the spoofing attack will be reduced significantly. A spoofing aware receiver should be able to monitor the noise floor in order to detect any unusual noise level increase due to spoofing interference. In addition, the ability of the receiver to monitor the absolute received power of each individual PRN increases its resistance to spoofing PRNs whose power is considerably higher than the typical power level of the authentic GPS PRNs. Since this type of receiver does directly deals with the absolute received power of spoofing and authentic signals, it is not vulnerable to the noise floor increase caused by the cross correlation of spoofing PRNs.

The incremental receiver hardware required to facilitate an absolute power measurement within an uncertainty of about 2 dB is trivial especially in the context of monolithic application specific integrated circuit (ASIC) integration. However, an additional factory calibration step would be required. Based on this, it is very reasonable to consider absolute power measurements as a readily available spoofer countermeasure.

Figure 4-10 compares the spoofing vulnerability region for a SNR monitoring spoofing countermeasure versus an absolute power monitoring receiver. In this illustrative example it has been assumed that the absolute power monitoring receiver is able to discriminate the elevated noise floor as well as higher power PRNs within a 2 dB accuracy range. In other words, this receiver is able to discriminate those PRNs whose absolute power is at least 2 dB higher than the maximum possible received power of GPS L1 C/A signals, which is -153dBW (IS-GPS-200 2010). Also, this receiver is capable of detecting a 2 dB increase in noise floor from its desired value. However, the SNR monitoring receiver can only discriminate the signals whose SNR is higher than the maximum possible SINR of the GPS L1 C/A signal (This value is assumed to be 21.8 dB for T_c=1 ms and temperature=$300^\circ K$).

Therefore, the SNR monitoring receiver accepts those signals whose received SNR is higher than the detection threshold and lower than the acceptable maximum SNR level of the authentic GPS signals (Λ_{th}^{AS}). The vulnerability region of this receiver is depicted in Figure 4-10. It is shown that for a spoofer whose TSP is equally divided among 16 PRNs, the SNR monitoring is vulnerable to TSPs higher than -145 dBW. However, the

vulnerability region of the absolute power monitoring receiver is limited to those signals whose absolute power is above the detection threshold and below the maximum allowable GPS L1 power level. In this case, the vulnerability region is limited to the TSP value above which the receiver noise floor increases by more than 2 dB.

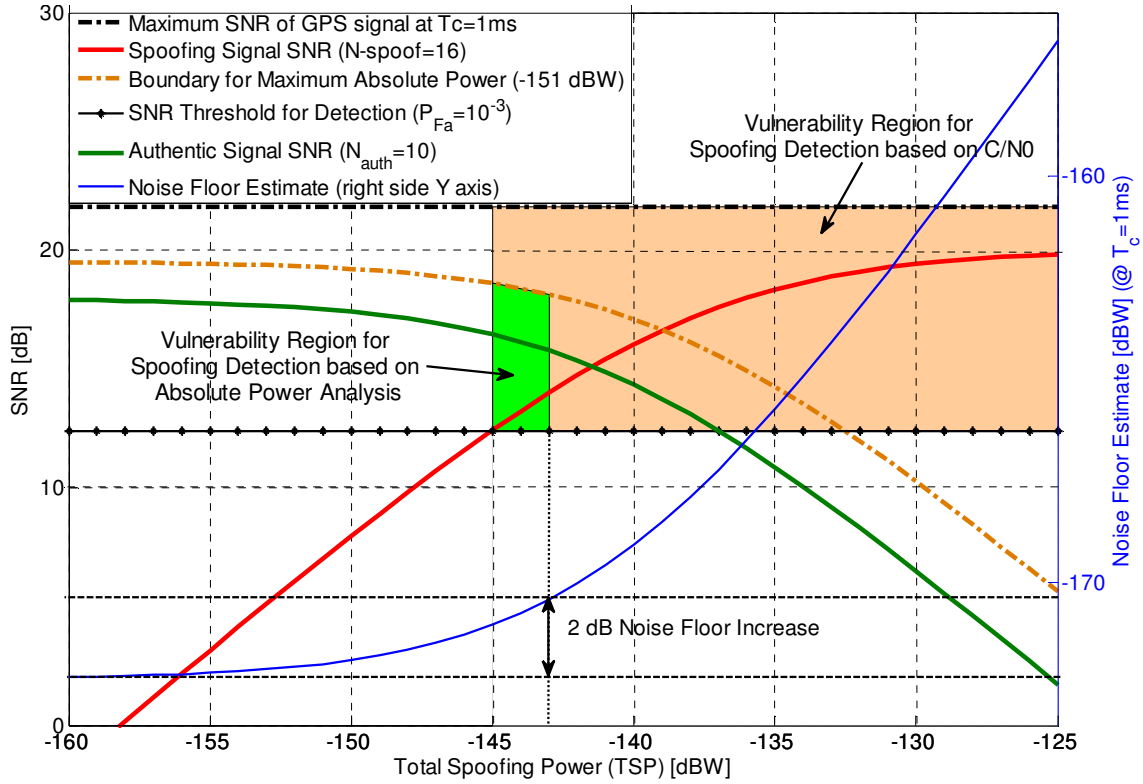


Figure 4-10 Vulnerability region comparison of SNR vs. absolute power monitoring techniques

Hence, as depicted in Figure 4-10, the vulnerability region of the absolute power monitoring receiver is much smaller than the vulnerability region of SNR monitoring receiver. Furthermore, if the receiver is able to detect the absolute receiver power more accurately, it can considerably reduce the size of its vulnerability window in the presence of spoofing attacks.

4.8 Real Data Analysis

Real data has been collected and processed in order to analyse the effect of spoofing attacks on the acquisition procedure of a GPS receiver. The data collection scenario is the same as that of Section 3.5 in which simulated GPS signals are amplified and then combined with real GPS signals using an RF power combiner (see Figure 3-8).

Figure 4-11 shows the receiver noise floor elevation with respect to the un-spoofed noise floor as a function of average spoofing to authentic power ratio (SAPR). The standard deviation of noise floor estimate has been also shown in these plots.

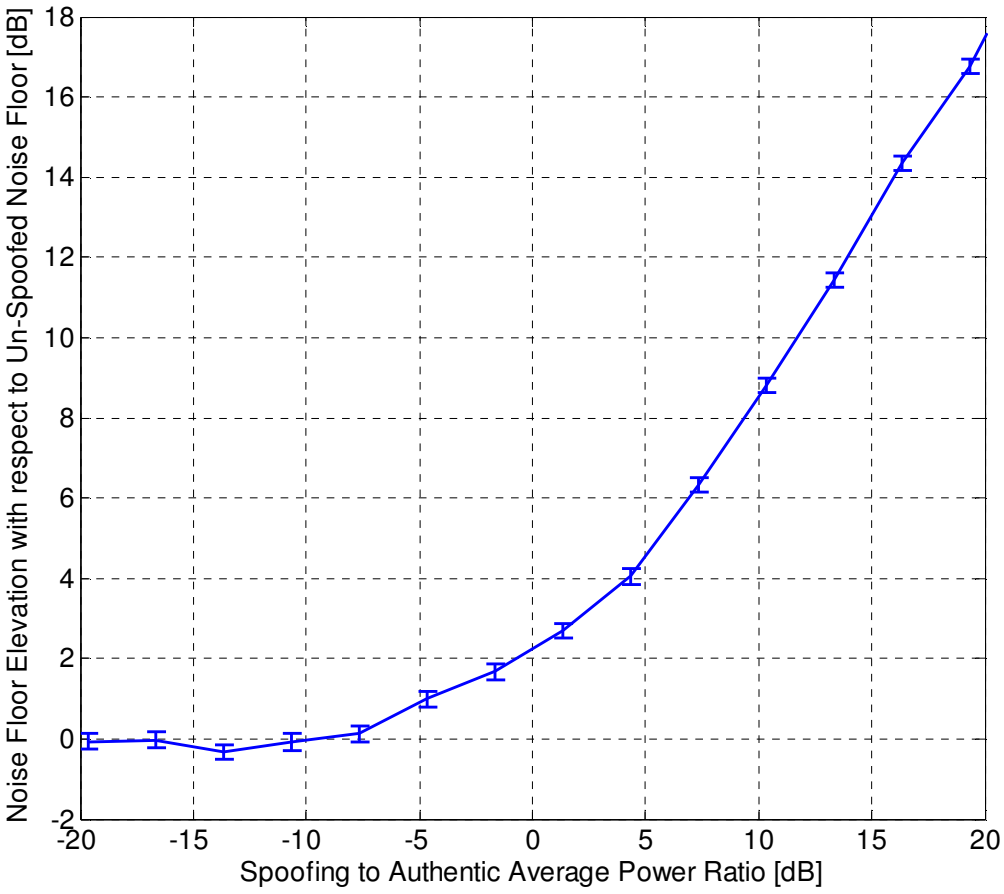


Figure 4-11 Noise floor elevation versus spoofing to authentic average power ratio

It is observed that once SAPR exceeds -6 dB, the estimated noise floor of the target receiver starts to increase. For higher SAPR values, the noise floor almost increases linearly as a function of SAPR and this can cause severe SNR reduction for authentic GPS signals.

Table 4-1 tabulates SNR and absolute power variations of authentic and spoofing signals as a function of average SAPR for PRN-29. In the collected data set, PRN-29 is common among spoofing and authentic PRN sets. The average SAPR has changed from -6 dB to +6 dB in 3 dB steps. The first two rows of Table 4-1 show the SNR variations of authentic and spoofed correlation peaks corresponding to PRN-29. It is observed that the SNR of authentic signals, $\Lambda^{a}_{l=29}$, increases as the SAPR increases and on the contrary, the spoofing peak's SNR, $\Lambda^{s}_{l=29}$, increases as a function of SAPR increment. This trend of SNR variations completely conforms to the previous discussions of this chapter.

The second two rows of Table 4-1 correspond to absolute power variations of authentic and spoofing correlation peaks, i.e. $\underline{p}^{a}_{l=29}$ and $\underline{p}^{s}_{l=29}$, as a function of average SAPR values. The absolute power values have been divided by un-spoofed noise floor in order provide comparable numbers to SNR measurements of the first two rows of this table. It is observed that $\underline{p}^{a}_{l=29}$ does not considerably change once the SAPR changes. However, the values of spoofing power, $\underline{p}^{s}_{l=29}$, considerably increase with an increment of SAPR.

Table 4-1 SNR and absolute power variations of authentic and spoofing signals as a function of average SAPR

	SAPR = -6 dB	SAPR = -3 dB	SAPR = 0 dB	SAPR = +3 dB	SAPR = +6 dB
$\Lambda^{a}_{l=29}$ [dB]	16.9	15.5	14.7	13.7	11.6
$\Lambda^{s}_{l=29}$ [dB]	12.6	13.7	16.0	17.7	18.9
$\underline{p}^{a}_{l=29}$ [dB]	17.9	17.2	17.4	17.5	17.6
$\underline{p}^{s}_{l=29}$ [dB]	13.6	15.3	18.7	21.6	24.9

The underlined numbers in Table 4-1 show the possible synchronization options for a SNR monitoring receiver versus an absolute power monitoring receiver. Assuming a spoofing detection threshold of 20 dB for both of these receivers, it can be observed that a SNR monitoring receiver is much more susceptible to spoofing signals than an absolute power monitoring receiver.

4.8.1 TEXBAT Data Processing

The spoofing data sets provided by RNL at University of Texas at Austin (Humphreys et al 2012) have been processed in order to monitor noise variance variations of a GPS receiver under a spoofing attack. Descriptions regarding different data sets and their corresponding spoofing scenario have been previously provided in Section 3.6.1 where it was mentioned that the first 100 seconds of the received data sets are not spoofed. In order to perform a fair comparison among all spoofing scenarios, the signals of S0 (clean

authentic data) has been scaled in order to conform to the same noise floor as the other datasets during their un-spoofed interval.

Figure 4-12 provides a comparison of receiver's noise floor variations with respect to un-spoofed noise floor as a function of time. It is observed that the estimated noise floor of all spoofing scenarios conforms before the start of a spoofing attack (i.e. before Time = 100 s). For the case S0 which belongs to an un-spoofed authentic dataset, the noise floor remains the same during the entire observation interval. However, for the S1 scenario involving a switched spoofing attack, it is observed that the noise floor estimate suddenly decreases as spoofing signals replace the authentic GPS signals. The reason is that the spoofing signals have been designed to provide the same SNR level as the authentic signals however; they are considerably less powerful than the original authentic signals. Spoofing scenario S2 represents an overpowered spoofing attack where the presence of spoofing signals considerably increases the estimated noise floor of the GPS receiver. For the case of matched power spoofing attacks (i.e. S3 and S4 scenarios), it is observed that the presence of spoofing signals slightly increases the receiver's noise floor estimate. However, this slight increment might not provide considerable discrimination between authentic and spoofing signal sets. The information provided in Figure 3-10 and Figure 4-12 can clearly reveal the presence of spoofing attack in different scenarios of TEXBAT data sets.

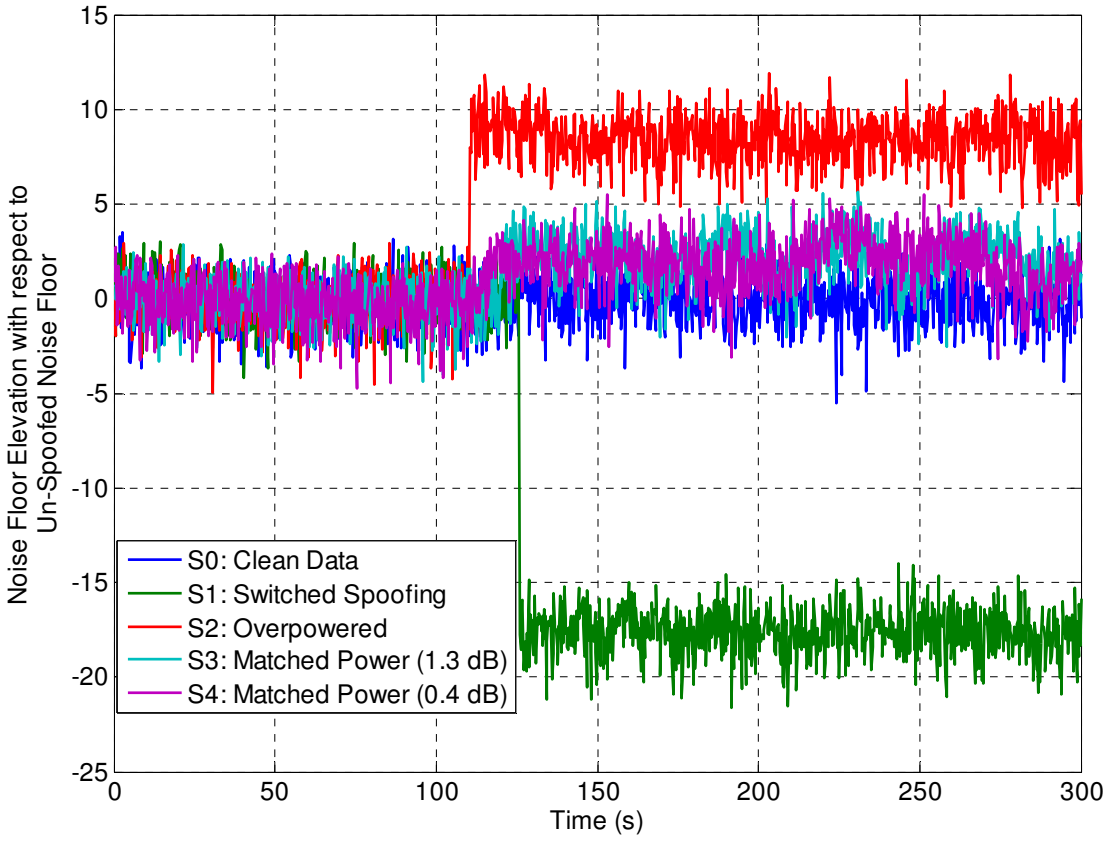


Figure 4-12 Noise floor elevation with respect to un-spoofed noise floor for TEXBAT data set (dB scale)

4.9 Summary

A GPS receiver vulnerability analysis to spoofing attacks during the acquisition process has been presented. It was shown that spoofing signals can degrade or mislead the conventional acquisition process of a GPS receiver. Spoofing signals can transmit multiple higher power PRN signals that elevate the noise floor estimate of a GPS receiver and as a consequence decrease the SNR of authentic correlation peaks. Another sinister effect of spoofing signals is the generation of additional fake correlation peaks at the cross ambiguity function (CAF). These counterfeit correlation peaks can also misdirect the acquisition procedure of GPS receivers.

The performance of two RSS based spoofing countermeasure techniques namely, SNR monitoring and absolute power monitoring, have been investigated. It has been shown that the SNR measurements alone are not sufficiently effective means of spoofing discrimination. In this case, due to the noise floor increase, SNR of the authentic signals reduces and leads to a deterioration of the receiver detection performance. On the contrary, it was shown that absolute power monitoring provides GPS receivers with the capability to analyze the noise floor as well as absolute strength of correlation peaks. As a consequence, any abnormal variation of noise floor as well as acquired correlation peaks could be monitored in order to detect the presence of spoofing signals. This approach can considerably reduce the vulnerability of GPS receivers to spoofing signals.

Chapter Five: Spoofing Analysis and Countermeasure during the Signal Tracking Stage

5.1 Introduction

Spoofing signals can be designed to mislead the tracking procedure of GPS receivers by generating synchronized PRN codes leading to counterfeit correlation peaks. These fake correlation peaks can overlay with the authentic ones and gradually misdirect the tracking procedure of the target receiver. Detection and mitigation of spoofing attacks on tracking GNSS receivers is becoming one of the important anti-spoofing topics (Ledvina et al 2010, Cavaleri et al 2011, Shepard et al 2011, Parro-Jimenez et al 2012). Shepard et al (2011) showed that the interaction between the authentic and spoofing correlation peaks is very similar to the case of direct and multipath signal component interaction. Therefore, multipath detection and mitigation techniques can be generalized to the case of spoofing countermeasure. Signal quality monitoring (SQM) techniques, previously designed to check the quality of correlation peaks in the presence of multipath and interference (Phelts 2001), have been adopted to detect the spoofing attack on tracking receivers (Ledvina et al 2010, Pini et al 2011, Wesson et al 2011).

This chapter focuses on the analysis of the effects of spoofing attack on a tracking receiver and detecting the presence of counterfeit signals. Herein, it is assumed that the receiver is operating under calm ionospheric situations and has initially locked to the authentic signals while a spoofing attack tries to deceive this receiver toward tracking fake GNSS signals. Correlator outputs are mathematically analyzed during interaction of spoofing and authentic signals. Based on this analysis, two spoofing detection approaches

are proposed to detect different types of spoofing attack on tracking receivers. The first technique employs a GLRT detection scheme that continually monitors the carrier Doppler frequency and code rate of tracked PRN signals and flags the presence of a spoofing attack upon observing any inconsistency between these two parameters. The second detection technique continuously checks the amplitude of correlator outputs and looks for any abnormality in the correlator output distribution. If this distribution considerably deviates from the expected distribution for authentic signals, a spoofing attack is flagged. The proposed anti–spoofing technique has been tested under different spoofing scenarios implemented by a Spirent hardware simulator. Two approaches have been considered for modeling spoofing attacks on a tracking receiver. Furthermore, spoofing datasets available from the Radio Navigation Lab (RNL) at The University of Texas at Austin have been also analyzed. It is shown that the theoretical analyses conform to practical observations and the proposed countermeasure techniques can detect the presence of spoofing attack in various real world scenarios.

The rest of this chapter is organized as follows. Section 5.2 introduces different spoofing scenarios that can be designed to misdirect a tracking receiver. Section 5.3 provides the problem formulations and analyses for the interaction between spoofing-authentic signals in different spoofing scenarios. Section 5.4 proposes spoofing detection methods based on consistency check between Doppler and code rate of received signals as well as correlator output amplitude fluctuations. Real data collection scenarios and setups are discussed in Section 5.5 and the processing results are presented in Section 5.6. Concluding notes are finally provided in Section 5.7.

5.2 Spoofing Attacks on a Tracking Receiver

When a GPS receiver focuses on tracking an authentic correlation peak, it does not consider other regions of CAF and therefore, even a higher power spoofing signal might not affect the receiver's tracking procedure if their delays or Doppler frequencies are not aligned. Therefore, to mislead a tracking receiver without imposing loss of lock, a spoofer should first align the delay and Doppler shift of its signal to those of the authentic signal and then lift-off the tracking point of the receiver by gradually deviating from the authentic correlation peak. For a successful lift-off, the spoofing correlation peak should obtain a higher power level compared to the authentic one during its interaction with the authentic signal.

5.2.1 Synchronous versus Asynchronous Spoofing Attack

Figure 5-1 illustrates two scenarios of synchronous and asynchronous spoofing attacks on a tracking receiver. Herein, the counterfeit correlation peaks are shown in dashed red lines while the authentic ones are shown in solid black. The red circles show the prompt correlator output while the green ones illustrate the early (E), late (L) correlator outputs. The yellow circles illustrate very early (VE) and very late (VL) correlator outputs. In the synchronous spoofing scenario, a very low power phase aligned spoofing correlation peak is generated at the same Doppler and code delay as the authentic peak ($\mathbf{T_1}$). Spoofing power gradually increases and finally exceeds the authentic signal's power level ($\mathbf{T_2}$). After that, the higher power spoofing peak gradually moves away from the authentic correlation peak ($\mathbf{T_3}$) and finally the spoofing power level comes back to the normal power level of the authentic signals ($\mathbf{T_4}$). This procedure can effectively mislead

the tracking point of a GPS receiver. However, the spoofer needs to know the three dimensional (3D) pointing vector from its transmit antenna toward the target receiver's antenna within accuracy of a few centimetres in order to align its carrier phase to that of the authentic signal and generate a synchronous attack (Montgomery et al 2009). In addition, the spoofer should be aware of the authentic signal power at its target receiver and the propagation channel condition between the spoofer antenna and the target receiver's antenna in order to accurately adjust its transmit power. These conditions are very difficult to achieve and in many cases implementation of synchronous spoofing attack is not practical in real world scenarios.

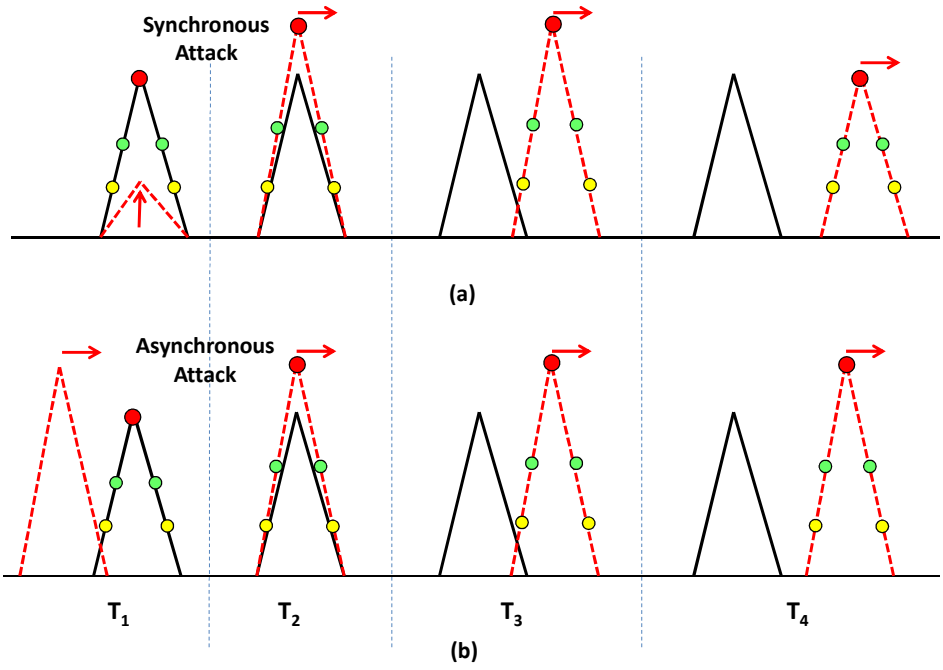


Figure 5-1 Two spoofing attack scenarios on a tracking receiver (a) Synchronous attack (b) Asynchronous attack

In the case of an asynchronous spoofing attack, the spoofer roughly knows the position of its target receiver's antenna and the channel condition between the spoofer's transmit

antenna and the target receiver's antenna. Therefore, a higher power spoofing correlation peak is generated which gradually moves toward the authentic correlation peak and tries to grab the tracking point of the target receiver. Figure 5-1 (b) illustrates an asynchronous spoofing attack in which a counterfeit correlation peak is trying to misdirect the tracking point of the target receiver. An asynchronous spoofing attack is still difficult to implement but it is a more realistic spoofing scenario compared to synchronous attack.

5.2.2 Locked Doppler versus Consistent Doppler Spoofing Attack

Based on the discussion provided by Humphreys et al (2012), a spoofing attack on a tracking receiver might take place in two different modes i.e. consistent Doppler or locked Doppler. In the former case, the spoofer keeps the consistency between code delay rate and Doppler frequency. These two parameters are also consistent for the authentic GPS signals since they are both generated based on the relative motion between GPS satellites and user equipment. However, as will be discussed in Section 5.3, the interaction between authentic and spoofing signals in a consistent Doppler spoofing attack can cause rapid fluctuations in the correlator output amplitude which may reveal the presence of spoofing signals. To prevent these amplitude fluctuations, a spoofer can generate locked Doppler attack in which the Doppler frequency of spoofing signal stays the same as that of the authentic signal during the interaction between authentic and spoofing correlation peaks. Therefore, the target receiver is less likely to lose lock or detect spoofing signals due to correlator amplitude fluctuations. However, as it will be discussed in Section 5.4.1, code rate and Doppler consistency check methods can reveal the presence of such a spoofing attack.

5.3 Problem Formulation

Assuming line of sight propagation, a simplified model for sampled IF GPS L1 C/A signals in the presence of spoofing signals can be written as (See 2-1 and 2-2)

$$\begin{aligned} r(nT_s) = & \sum_{m \in \mathbf{J}^a} \sqrt{p_m^a}\, h_m^a\left(nT_s - \tau_m^a\right) c_m^a\left(nT_s - \tau_m^a\right) e^{j\phi_m^a + j2\pi f_m^a nT_s} \\ & + \sum_{q \in \mathbf{J}^s} \sqrt{p_q^s}\, h_q^s\left(nT_s - \tau_q^s\right) c_q^s\left(nT_s - \tau_q^s\right) e^{j\phi_q^s + j2\pi f_q^s nT_s} + \eta(nT_s), \end{aligned} \tag{5-1}$$

where T_s is the sampling interval and ϕ_m^a, f_m^a, p_m^a and τ_m^a are the carrier phase, Doppler frequency, received signal power and code delay of the mth authentic signal, respectively. ϕ_q^s, f_q^s, p_q^s and τ_q^s are the carrier phase, Doppler frequency, received signal power and code delay of the qth spoofing signal, respectively. $c(nT_s)$ is the PRN sequence corresponding to the authentic or spoofing signal set at time instant nT_s. $\eta(nT_s)$ is complex additive white Gaussian noise with variance σ^2 and j is the square root of -1. $h_m^a\left(nT_s - \tau_m^a\right)$ and $h_q^s\left(nT_s - \tau_q^s\right)$ represent the navigation data bits for m th authentic and q th spoofing PRN signals, respectively. The subscripts m and q correspond to the m th and q th received authentic and spoofing PRN signals, respectively. During the despreading process of a tracking receiver, GPS receiver correlates the received signal with a locally generated synchronized replica and then performs low pass filtering. The correlator complex output, $u_l[k]$, can be written as

$$u_l[k] = \frac{1}{N} \sum_{n=(k-1)N}^{kN-1} r(nT_s)\, c_l\left(nT_s - \tilde{\tau}_l^L\right) e^{-j2\pi \tilde{f}_l^L nT_s} \tag{5-2}$$

where N determines the coherent integration interval and k is a short representation of kNT_s which is the time instant at which the correlator output is updated. Assume that the PRN number l is present at both spoofing and the authentic signal sets also assume that the code delay and Doppler frequency of the spoofing and the authentic signals are very close to those of the local replica ($\tilde{\tau}_l^L$ and $\tilde{f}_l^L$). This is the scenario that may happen during the spoofing attack on a tracking receiver. Therefore, the correlator output can be approximately written as (see appendix A)

$$\begin{aligned} u_l[k] = & \left(\sqrt{p_l^a} h_l^a[k] R\left(\Delta\tau_l^{a,L}\right) \frac{\sin\left(\pi\Delta f_l^{a,L} N T_s\right)}{N \sin\left(\pi\Delta f_l^{a,L} T_s\right)} e^{j\pi\Delta f_l^{a,L}\left[(2k-1)N-1\right]T_s + j\Delta\phi_{l,0}^{a,L}} \right) \\ & + \left(\sqrt{p_l^s} h_l^s[k] R\left(\Delta\tau_l^{s,L}\right) \frac{\sin\left(\pi\Delta f_l^{s,L} N T_s\right)}{N \sin\left(\pi\Delta f_l^{s,L} T_s\right)} e^{j\pi\Delta f_l^{s,L}\left[(2k-1)N-1\right]T_s + j\Delta\phi_{l,0}^{s,L}} \right) + \bar{\eta}_l[k] \end{aligned} \tag{5-3}$$

where $h_l^a[k]$ and $h_l^s[k]$ represent authentic and spoofing data bits at the kth integration interval. $\bar{\eta}[k]$ represents the low pass filtered Gaussian noise component at the output of correlator branch. $\Delta\tau_l^{a,L}$, $\Delta f_l^{a,L}$ and $\Delta\varphi_{l,0}^{a,L}$ represent the differences between code delays, Doppler frequencies and initial carrier phases of the authentic l-th PRN signal and those of the locally generated replica, respectively. These are the parameters of interest for the tracking loop which is following the authentic signal's dynamics. $\Delta\tau_l^{s,L}$, $\Delta f_l^{s,L}$ and $\Delta\varphi_{l,0}^{s,L}$ represent the difference between code delays, Doppler frequencies and initial carrier phases of spoofing signals and those of the locally generated replica, respectively. $\bar{\eta}_l[k]$ is complex additive white Gaussian noise with variance $\bar{\sigma}^2$ at the output of the lth PRN correlator. $R(\bullet)$ is the correlation function which is closely related to the choice of

subcarrier in GNSS signal. This function is a triangle with normalized height and two chips base width for the GPS L1 C/A subcarrier.

Assuming a coherent tracking receiver which is initially locked into the *l*-th authentic PRN Doppler frequency, carrier phase and code delay ($\Delta f_l^{a,L} \simeq 0$, $\Delta \varphi_{l,0}^{a,L} = 0$, $\Delta \tau_l^{a,L} \simeq 0$), (5-3) can be simplified as follows

$$u_l[k] = \sqrt{p_l^a}\, h_l^a[k] + \begin{pmatrix} \sqrt{p_l^s}\, h_l^s[k] R\left(\Delta \tau_l^{a,s}[k]\right) \dfrac{\sin\left(\pi \Delta f_l^{a,s}[k] N T_s\right)}{N \sin\left(\pi \Delta f_l^{a,s}[k] T_s\right)} \\ e^{j\pi \Delta f_l^{a,s}[k]((2k-1)N-1)T_s + j\Delta \varphi_{l,0}^{a,s}} \end{pmatrix} + \bar{\eta}_l[k] \tag{5-4}$$

where $\Delta \tau_l^{a,s}[k]$ and $\Delta f_l^{a,s}[k]$ are the differences between code delays and Doppler frequencies of the received authentic and spoofing signals at time instant kNT_s, respectively. It is assumed that the spoofer smoothly changes the code delay and the Doppler frequency of its signal in order to gradually lift-off the tracking point of its target receiver without causing it to lose lock. Also, it is assumed the spoofing signal parameters change so that at a certain moment, the delay and Doppler difference of spoofing and authentic signals become negligible and after that moment, spoofing peak starts to move away from the authentic peak. For a successful lift-off, the amplitude of the spoofing signal should be higher than that of the authentic signal.

In most GPS applications a third-order dynamic model is assumed for relative user-satellite motion (Kaplan & Hegarty 2006). Therefore, assuming that both spoofing and authentic signals follow the same dynamic model, the following equations can be written

for the temporal variations of their code delay difference and Doppler frequency difference:

$$\begin{aligned}\Delta\tau_l^{a,s}\left[k\right] &= \Delta\tau_{l,0}^{a,s} + kNT_s\,\Delta\dot{\tau}_{l,0}^{a,s} + \frac{1}{2}\left(kNT_s\right)^2\Delta\ddot{\tau}_l^{a,s} \\ \Delta f_l^{a,s}\left[k\right] &= \Delta f_{l,0}^{a,s} + kNT_s\,\Delta\dot{f}_l^{a,s}\end{aligned} \tag{5-5}$$

where $\Delta\tau_{l,0}^{a,s}$, $\Delta\dot{\tau}_{l,0}^{a,s}$ and $\Delta\ddot{\tau}_l^{a,s}$ are the initial code delay difference, initial delay rate difference and the second time derivative of spoofing authentic relative delays corresponding to the *l*'th PRN signal, respectively. $\Delta f_{l,0}^{a,s}$ and $\Delta\dot{f}_l^{a,s}$ are initial Doppler frequency difference and Doppler rate difference between authentic and spoofing signals, respectively. In general, $\Delta\ddot{\tau}_l^{a,s}$ and $\Delta\dot{f}_l^{a,s}$ can be a slowly varying functions of time; however, for simplicity herein they are assumed to be constant. Without loss of generality, it can be assumed that the time reference (*k=0*) is the moment when the spoofing and authentic correlation peaks are aligned, i.e. $\Delta\tau_{l,0}^{a,s} \approx 0$, $\Delta f_{l,0}^{a,s} \approx 0$. Herein, it is assumed that the spoofer has not phase aligned its carrier to that of authentic signal since in real world scenarios spoofing phase alignment is very difficult to achieve if not impractical (Humphreys et al 2012). The following two sub-sections provide a problem formulation for locked Doppler and consistent Doppler spoofing attacks.

5.3.1 Locked Doppler Spoofing Attack

For the case of locked Doppler spoofing attack, the Doppler frequency of spoofing signals remain the same as the authentic signal's Doppler while their relative code delay

is changing. Therefore, substituting $\Delta f_l^{a,s}[k] \simeq 0$ and $\Delta \tau_l^{a,s}[k] \neq 0$ in (5-4), this equation can be simplified to

$$u_l[k] = \sqrt{p_l^a}\, h_l^a[k] + \left(\sqrt{p_l^s}\, h_l^s[k] R\left(\Delta \tau_l^{a,s}[k]\right) e^{j\Delta\phi_{l,0}^{a,s}}\right) + \overline{\eta}_l[k] \tag{5-6}$$

In this case, the carrier phase difference between authentic and spoofing signals is constant and can be written as

$$\Delta\varphi_l^{a,s}[k] = \Delta\phi_{l,0}^{a,s} \tag{5-7}$$

Therefore, there is no relative carrier phase variation between authentic and spoofing signals and consequently no amplitude fluctuations happen due to authentic and spoofing signal interaction.

5.3.2 Consistent Doppler Spoofing Attack

For the case of a consistent Doppler spoofing attack, the Doppler frequency and code delay rates of spoofing signals are consistent. This consistency requires that (Misra & Enge 2006)

$$\begin{aligned} \Delta f_l^{a,s}[k] &= -f_{RF}\, \Delta \dot{\tau}_l^{a,s}[k] \\ \Delta \dot{f}_l^{a,s} &= -f_{RF}\, \Delta \ddot{\tau}_l^{a,s} \end{aligned} \tag{5-8}$$

where f_{RF} is the carrier frequency of GNSS signals (e.g. $f_{RF} = 1575.42\,\text{MHz}$ for the GPS L1 signals). Therefore, considering the initial alignment of the authentic and spoofing correlation peaks and assuming a third order dynamic model for both authentic and

spoofing signals, $\Delta\ddot{\tau}_l^{a,s}$ (equivalently $\Delta\dot{f}_l^{a,s}$) is the only parameter that can actually lead the gradual separation of authentic and spoofing correlation peaks. Based on the above discussion and Equation (5-8), (5-4) can be approximated as

$$u_l[k] = \sqrt{p_l^a}\,h_l^a[k] + \left(\sqrt{p_l^s}\,h_l^s[k]\,R\left(-\frac{\Delta\dot{f}_l^{a,s}}{2f_{RF}}(kNT_s)^2\right)e^{j\Delta\varphi_l^{a,s}[k]}\right) + \overline{\eta}_l[k] \tag{5-9}$$

In Equation (5-9), the ratio of two sinusoidal terms has been approximated by unity as spoofing and authentic peaks have been assumed very close to each other in terms of their Doppler frequencies. Considering Equations (5-4), (5-5) and (5-8), the phase difference between spoofing peak and the authentic signal at the *k*th integration interval can be written as

$$\begin{aligned}\Delta\varphi_l^{a,s}[k] &= \left(\pi kNT_s^2\left(N(2k-1)-1\right)\right)\Delta\dot{f}_l^{a,s} + \Delta\phi_{l,0}^{a,s} \\ &= \left(2\pi N^2T_s^2\Delta\dot{f}_l^{a,s}\right)k^2 - \left(N+1\right)\left(\pi NT_s^2\Delta\dot{f}_l^{a,s}\right)k + \Delta\phi_{l,0}^{a,s}\end{aligned} \tag{5-10}$$

It is observed that $\Delta\varphi_l^{a,s}[k]$ is a second order function of time and its variation depends on the value of $\Delta\dot{f}_l^{a,s}$. Since data modulation imposes random variations on the correlator output signals, it is more convenient to work with the squared amplitude of correlator outputs wherein the effect of data bits has been removed. Therefore, the squared amplitude of correlator output, $D_l[k] = u_l[k]u_l^*[k]$, can be written as

$$\begin{aligned}D_l[k] &= p_l^a + p_l^sR^2\left(-\frac{\Delta\dot{f}_l^{a,s}}{2f_{RF}}(kNT_s)^2\right) \\ &\quad +2\sqrt{p_l^a\,p_l^s}\,R\left(-\frac{\Delta\dot{f}_l^{a,s}}{2f_{RF}}(kNT_s)^2\right)\cos\left(\Delta\varphi_l^{a,s}[k]\right) + \tilde{\eta}_l[k]\end{aligned} \tag{5-11}$$

Herein it is assumed that the spoofing source has synchronized its data bits with those of authentic signals, therefore $h_l^a[k]h_l^s[k]=1$; $\tilde{\eta}_l[k]$ represents the noise component.

Based on (5-11) it can be stated that the interaction between the authentic and spoofing signals causes rapid fluctuations in the correlator output amplitude. These fluctuations which depend on the relative power of spoofing and authentic signals and their relative Doppler rate variation, deviates the correlator output distribution from its expected chi squared distribution. Figure 5-2 shows the simulated early, late and prompt correlator outputs during spoofing and authentic signals interaction. For this simulation, authentic and spoofing signal powers are assumed to be the same and equal to -158 dBW. Also, noise power has been assumed to be -173 dBW for a 1 ms integration time. Relative spoofing-authentic Doppler rate has been assumed to be $\Delta\dot{f}_l^{a,s}=0.78\,(\text{rad/s}^2)$. As such the temporal derivative of the code delay rate is $\Delta\ddot{\tau}_l^{a,s}=-0.5\,(\text{ns/s}^2)$. It is observed that rapid fluctuations occur in the correlator output amplitude as the spoofing correlation peak is deviating from the authentic one. Figure 5-2 (b) provides a closer view of the authentic and spoofing correlation peaks interaction when the noise component is removed.

When only an authentic signal plus noise is present in the correlator output, the distribution of squared amplitude of correlator output follows a non-central Chi-Squared (χ^2) distribution with two degrees of freedom because it is the sum of squared value of two Gaussian random variables. However, during the spoofing and authentic signals interaction, due to the amplitude fluctuations, the correlator output would not follow a χ^2

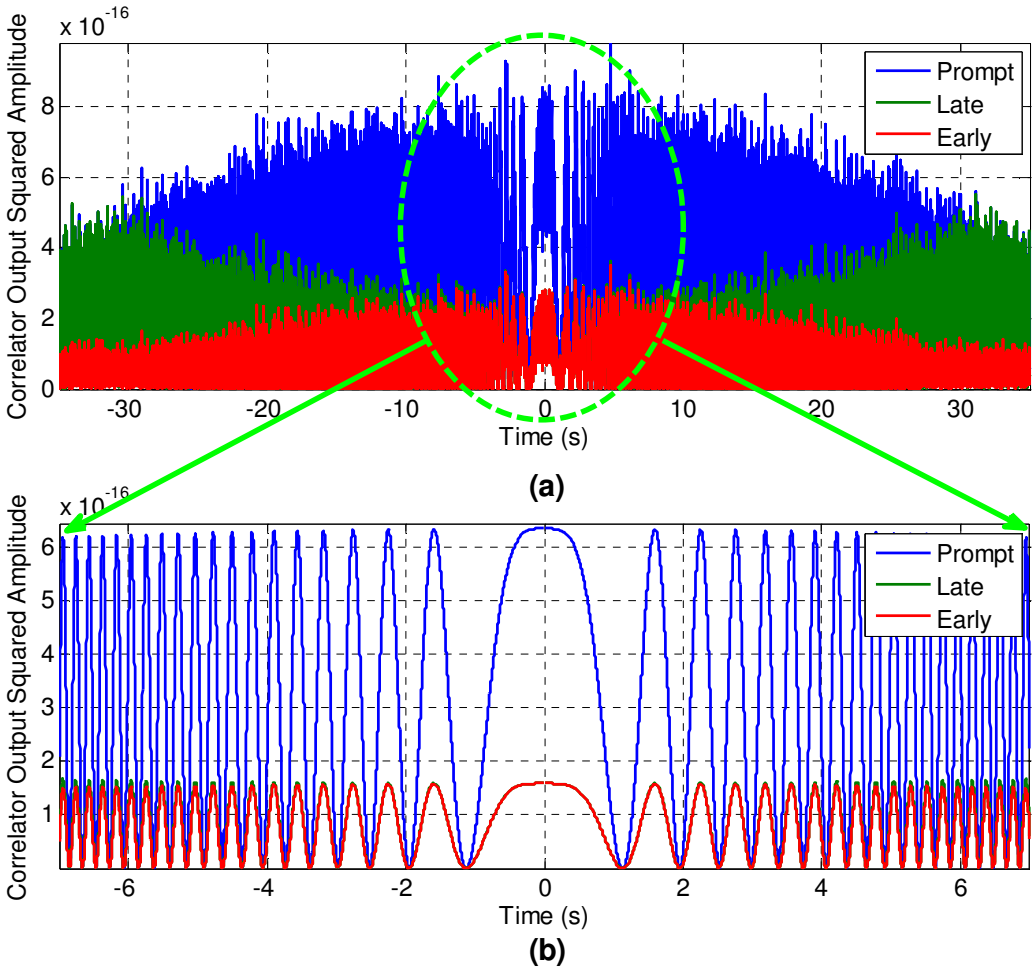


Figure 5-2 Simulation results for spoofing-authentic peaks interaction (a) squared amplitude of early, late and prompt correlators (b) closer view of correlator output near spoofing-authentic peaks alignment (noise component removed)

distribution anymore. Figure 5-3 compares the distribution of the prompt correlator output in the absence and presence of spoofing signals.

The distributions have been shown for different relative power levels of spoofing and authentic signals. It is observed that in the presence of the spoofing-authentic interaction, the correlator output distribution is completely different from a χ^2 distribution. This

feature also exists for the output of other correlator branches and it can be utilized for spoofing detection.

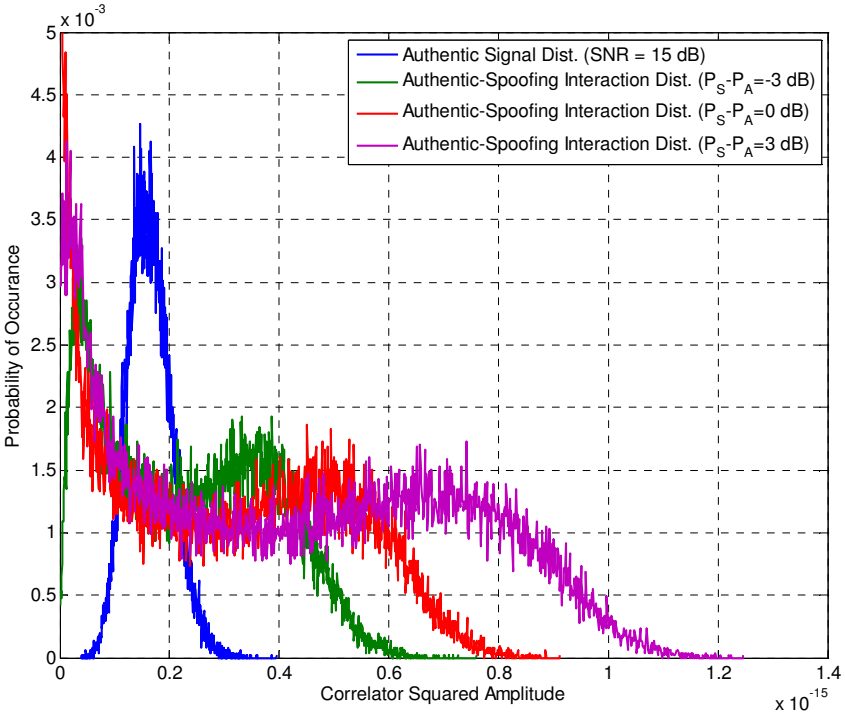


Figure 5-3 Prompt correlator output distribution for authentic signals and authentic-spoofing interaction for different spoofing powers

5.4 Proposed Spoofing Detection Techniques

Two detection schemes have been proposed to detect the presence of locked Doppler and consistent Doppler spoofing attacks on a tracking receiver. For the case of a locked Doppler spoofing attack, the consistency between Doppler frequency and code rate of the receiver signals is checked while for the case of a consistent Doppler spoofing attack, a chi-square test has been designed to detect the abnormal distribution of correlation peaks during the interaction of authentic and spoofing signals.

5.4.1 Doppler and Code rate Consistency Check

As mentioned before, in calm ionospheric situations, code rate and Doppler frequency should be consistent because they are both generated due to the relative motion of satellite and user. In GNSS receivers, the PLL loop filter output is actually a measure of Doppler frequency while the loop filter output of DLL is reflecting the code rate estimate of the received PRN signal. Since the carrier tracking loop jitter is orders of magnitude less noisy that the code loop jitter (Kaplan & Hegarty 2006), many GPS receivers take advantage of a scaled version of the Doppler estimate in order to aid the code tracking process. The scale factor can be calculated as

$$\beta_s = -\frac{R_c}{f_{RF}} = -\frac{1.023\times10^6}{1575.42\times10^6} = -\frac{1}{1540} \tag{5-12}$$

where R_c is the code chip rate and f_{RF} is the carrier frequency of GPS L1 signals. Based on the analyses provided by Crosta & Alenia (2009) and assuming the steady state operation of PLL and DLL at high C/N_0 and considering a coherent DLL discriminator, it can be assumed that the difference between the DLL loop filter output and the scaled version of PLL loop filter output, $x[k] = s_{DLL}[k] - \beta_s\, s_{PLL}[k]$, conforms to an approximate Gaussian distribution. Herein, $s_{DLL}[k]$ and $s_{PLL}[k]$ represent the loop filter outputs for DLL and PLL, respectively. Therefore, the following detection hypotheses can discriminate the presence of spoofing signals:

$$\begin{aligned} \mathrm{H}_0 &: \quad x[k] = w[k] \\ \mathrm{H}_1 &: \quad x[k] = A[k] + w[k] \end{aligned} \tag{5-13}$$

where H_0 and H_1 represent the hypotheses in the absence and presence of code rate and Doppler estimates inconsistency, respectively. The H_1 hypothesis can reveal the presence of locked Doppler spoofing attacks on a tracking receiver. $w[k]$ represents a zero mean white noise component with variance of $\sigma_{DLL}^2 + \left(\sigma_{PLL}/1540\right)^2$, where σ_{DLL}^2 and σ_{PLL}^2 represent the variances of DLL and PLL loop filter outputs, respectively. The whiteness of this process has been verified through real data analysis for 1 ms coherent integration time during the steady state operation of PLL and DLL tracking loops. In (5-13), $A[k] \neq 0$ represents a non-zero bias to account for the inconsistency between code rate and Doppler estimates. Therefore, assuming a short term constant value for $A[k]$ and unknown values for σ_{DLL}^2 and σ_{PLL}^2, a GLRT detector would decide H_1 if (Kay 1998)

$$L_G(\mathbf{x}) = \frac{p\left(\mathbf{x}; \hat{A}, \hat{\sigma}_1^2, \mathrm{H}_1\right)}{p\left(\mathbf{x}; \hat{\sigma}_0^2, \mathrm{H}_0\right)} > \gamma \tag{5-14}$$

where $\hat{\sigma}_0^2$ and $\hat{\sigma}_1^2$ represent the estimates of distribution variance assuming H_0 and H_1 hypotheses, respectively. $\hat{A}$ represents the estimate of DC bias for the H_1 hypothesis and γ is the detection threshold. $\mathbf{x} = \left[x[1], x[2], \cdots, x[K]\right]$ is a vector of input samples over which the detection problem is being defined. Now consider the MLE estimates of unknown parameters as follows (Kay 1993):

$$\hat{A} = \frac{1}{K}\sum_{k=0}^{K-1} x[k]$$
$$\hat{\sigma}_1^2 = \frac{1}{K}\sum_{k=0}^{K-1}\left(x[k]-\hat{A}\right)^2 \tag{5-15}$$
$$\hat{\sigma}_0^2 = \frac{1}{K}\sum_{k=0}^{K-1}\left(x[k]\right)^2$$

The detection test of (5-14) can be written as (Kay 1998)

$$T(\mathbf{x}) = K\ln\left(1+\frac{\hat{A}^2}{\hat{\sigma}_1^2}\right) > \gamma' \tag{5-16}$$

where $\ln(\bullet)$ represents the natural logarithm of its input argument and $T(\mathbf{x})$ is the detection test statistic. γ' is the modified detection threshold. Based on Theorem 9.1 in Kay (1998), the detection performance of this detector can be written as

$$P_{FA} = Q_{F_{1,K-1}}(\gamma')$$
$$P_D = Q_{F'_{1,K-1}(\lambda)}(\gamma') \tag{5-17}$$

where P_{FA} and P_D represent probability of false alarm and probability of detection of spoofing attack, respectively. $Q_{F_{r,p}}$ and $Q_{F'_{r,p}(\lambda)}$ represent the cumulative density functions (CDF) of central and non-central *F* distributions with *r* numerator degrees of freedom and *p* denominator degrees of freedom, respectively. Herein, the non-centrality parameter λ can be defined as.

$$\lambda = \frac{KA^2}{\sigma_{DLL}^2 + \left(\frac{\sigma_{PLL}}{1540}\right)^2} \tag{5-18}$$

In (5-18), the detection threshold , γ', can be extracted using the inverse CDF of the $F_{1,K-1}$ distribution. Figure 5-4 illustrates the PLL and DLL structure for a GPS receiver with the proposed spoofing detection shown.

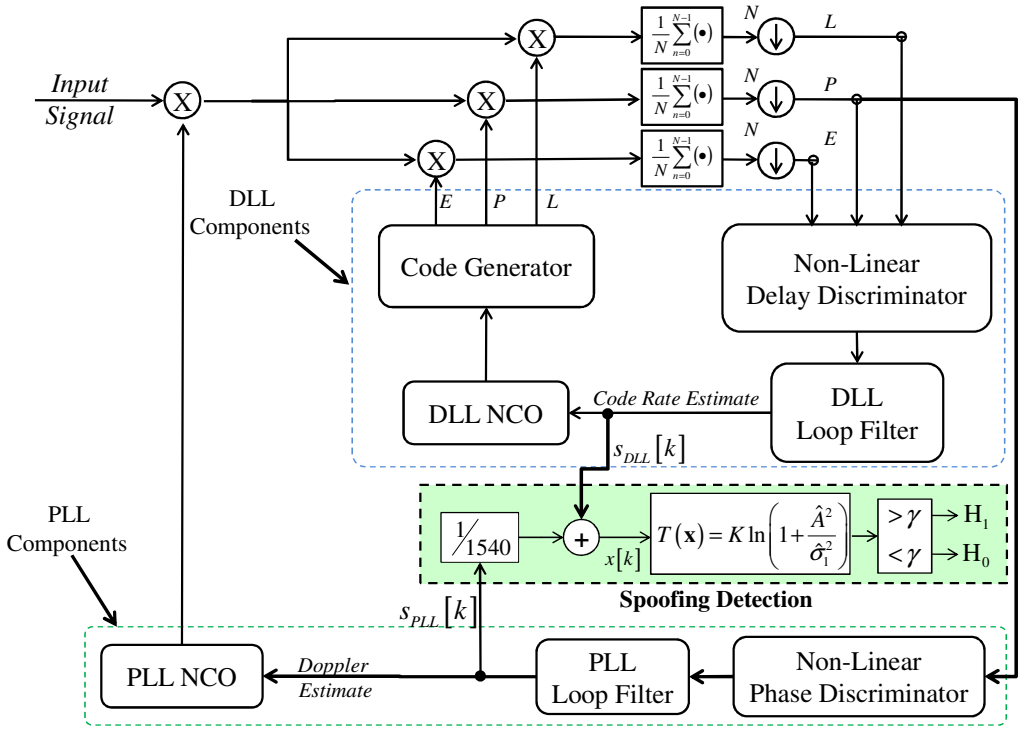


Figure 5-4 Code rate and Doppler consistency check for the tracking loops of a GNSS receiver

5.4.2 Testing the Goodness of Fit for Correlator Output

Based on the discussions provided in 5.3.2, consistent Doppler spoofing attack imposes rapid fluctuations on the correlator outputs. Figure 5-3 showed that these fluctuations deviate the correlator outputs from their desired chi-square distribution and this feature can be used to detect the presence of spoofing attack. Herein a spoofing countermeasure technique is proposed that is aimed to detect abnormalities in the distribution of different correlator branches. Five correlator branches namely very early (VE), early (E), prompt

(P), late (L) and very late (VL) are considered for this purpose. It is assumed that the tracking procedure in the receiver only relies on the E, L and P correlator outputs and other correlator branches have been used for advance detection of the spoofing correlation peaks that are approaching to or moving away from the authentic correlation peak. As it was discussed in the previous section, in the absence of the spoofing-authentic signals interaction, the squared amplitude of the correlator outputs follows a χ^2 distribution. However, when a spoofing correlation peak is interfering with an authentic one, the distribution of the authentic correlator outputs will be considerably affected and this can reveal the presence of a spoofing attack.

Here, two hypotheses have been considered for the correlator output. The null hypothesis (H_0) corresponds to the case where the authentic correlation peak is being tracked by the receiver. The alternative hypothesis (H_1) refers to the case where the null hypothesis is not true. H_1 happens in different cases including when spoofing-authentic peaks interact, higher power spoofing peak is tracked and when the receiver has lost lock.

It is assumed that the receiver is working in a line-of-sight condition and it is already locked onto tracking the authentic correlation peak. Therefore, correlator output statistics are extracted for different correlator branches i.e. VE, E, P, L, VL. Several histogram bins have been defined based on the means and standard deviations of the authentic correlator outputs and then a Chi-squared test statistic (Papoulis 2002) is formed for each branch on an observed set of correlator outputs for several milliseconds. The chi square test statistic on the prompt correlator branch can be written as

$$\kappa_P = \sum_{m=1}^{M} \left[\frac{\left(O_P(m) - E_P(m)\right)^2}{E_P(m)} \right] \tag{5-19}$$

where M is the number of bins. $O_P(m)$ and $E_P(m)$ are the number of observations and the expected number of observations for the mth bin, respectively. κ_P follows a chi square distribution with $M-1$ degrees of freedom. Additional test statistics such as κ_E, κ_L, κ_{VE}, κ_{VL} can be defined for other correlator outputs. As such, the H_0 hypothesis will be rejected if any of the test statistics exceeds the previously determined critical value.

The critical value of a chi square goodness of fit test is determined based on a previously assumed significance level. Two critical values namely $\xi_{\alpha_{\text{det}}}$ and $\xi_{\alpha_{\text{rel}}}$ have been defined based on α_{det} and α_{rel} significance levels. α_{det} is the level of significance for rejecting the H_0 hypothesis when this hypothesis is valid. α_{rel} is the significance level for re-accepting the H_0 hypothesis after it is rejected due to amplitude abnormalities. The relation between α and ξ_α can be written as

$$\alpha = \int_{v=\xi_\alpha}^{\infty} \chi^2_{M-1}(v)\, dv \tag{5-20}$$

where χ^2_{M-1} represents the probability density function for a chi square distribution of $M-1$degrees of freedom. Assuming that the receiver is initially working under the H_0 hypothesis, spoofing attacks will be detected if any of the previously proposed chi-square test statistics exceeds $\xi_{\alpha_{\text{det}}}$. After that, the spoofing attack will be refuted if all of the detection test statistics fall under the spoofing release threshold ($\xi_{\alpha_{\text{rel}}}$).

Figure 5-5 illustrates the performance of the proposed spoofing detection tests for a simulated data set. The parameter settings are the same as those in the previous section. Significance level values for spoofing detection and release have been considered as $\alpha_{\text{det}} = 0.01$ and $\alpha_{\text{rel}} = 0.90$. As such, critical values for $M = 10$ will be defined as $\xi_{\alpha_{\text{det}}} = 21.7$ and $\xi_{\alpha_{\text{rel}}} = 4.17$.

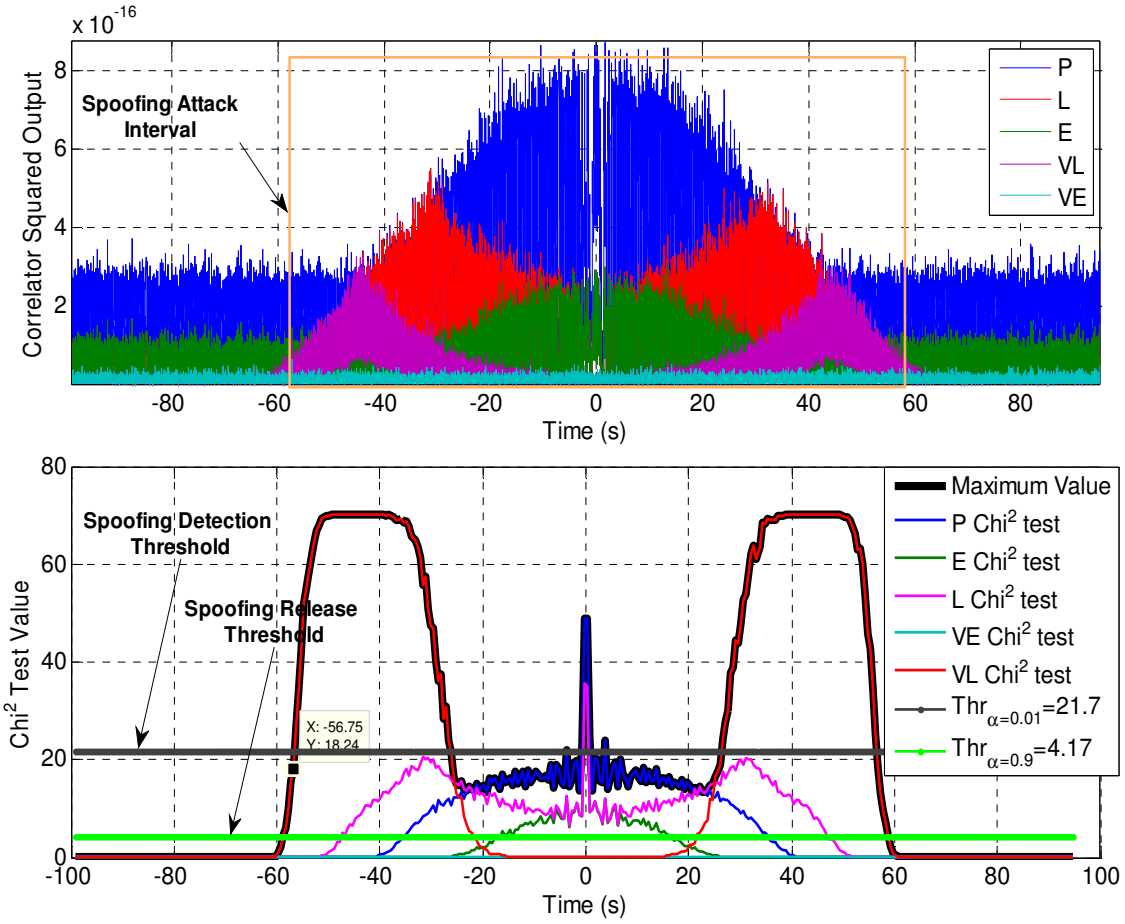


Figure 5-5 Chi square test results for a simulated spoofing attack on a tracking receiver

The number of correlator output samples that have been considered for calculating the test statistics is 500. It is observed that the spoofing attack is detected as the spoofing

correlation peak approaches the authentic one (χ^2_{VE} exceeds the spoofing detection threshold). Finally, at *T=58* s the spoofing threat is refuted as all test statistics fall under a lower detection threshold.

5.5 Real Data Collection

This section considers the use of a GPS hardware simulator in order to simulate spoofing attacks on a tracking receiver without any indoor/outdoor signal propagation. The performance of proposed spoofing detection and mitigation techniques have been investigated on synchronous and asynchronous spoofing attacks simulated with a Spirent G7700 GPS hardware simulator.

5.5.1 Asynchronous Spoofing Attack using Hardware Simulator

The Spirent hardware simulator is able to generate multipath components on each PRN. The relative delay and signal strength of direct and multipath PRN signals can be modified as a function of time using a fifth order polynomial. Relative Doppler frequency of authentic and multipath signals is automatically defined based on their relative code delay variations. Asynchronous spoofing attacks have been simulated by using modified multipath components whose delay and strength are varying temporally. As such, a low power multipath component is designed that gradually approaches the main correlation peak. It then increases its amplitude after full alignment to the authentic peak and tries to misdirect the tracking point of the target receiver.

Figure 5-6 shows a possible configuration for the relative delay and attenuation of multipath component with respect to the main authentic correlation peak. It is observed

that the multipath signal starts from 9 dB lower power compared to the authentic peak and gradually increase its power to exceed the power level of authentic signal at t=112 s. Similar to the simulations of Section 5.3.2, it is assumed that the relative spoofing-authentic Doppler rate is $\Delta\dot{f}_l^{a,s} = 0.78\,(\text{rad/s}^2)$ and the temporal derivative of the code delay rate is $\Delta\ddot{\tau}_l^{a,s} = -0.5\,(\text{ns/s}^2)$.

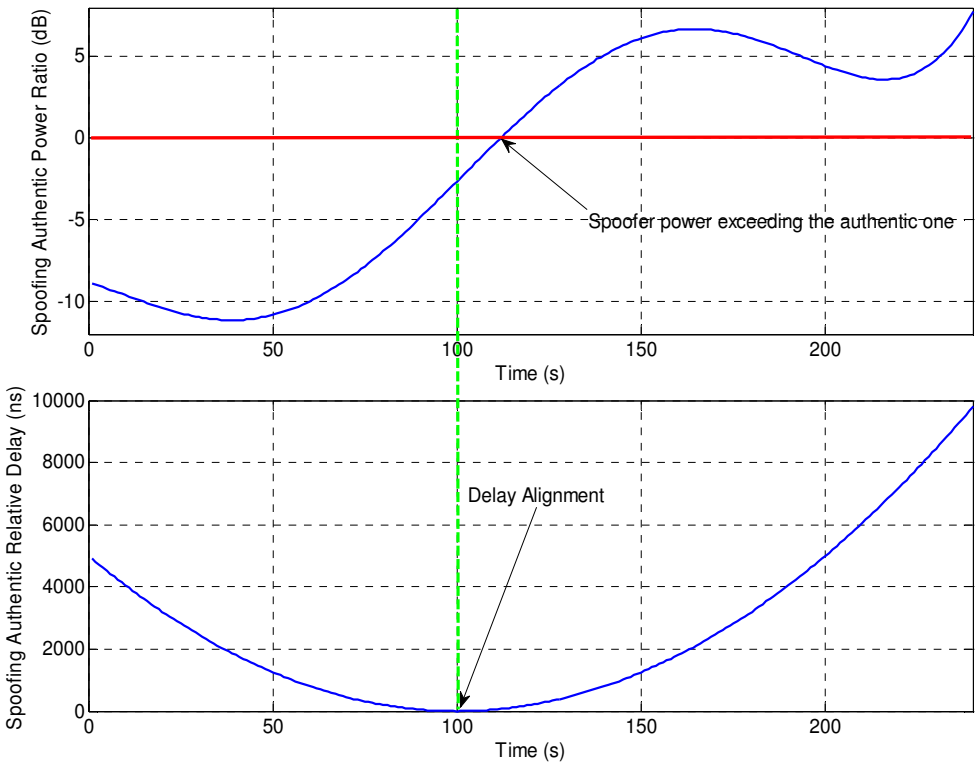


Figure 5-6 Relative delay and Doppler frequency of authentic and spoofing correlation peaks

The delay of multipath component starts from 5000 ns and gradually decreases to completely align with the authentic signal at t=100 s. After that, the multipath delay gradually increases to finally move away the tracking point of PLL/DLL and mislead its

corresponding pseudorange measurement. This scenario simulates a consistent Doppler spoofing attack in which the Doppler and code rate of spoofing signals conform.

5.5.2 Synchronous Spoofing Attack using Hardware Simulator

Another configuration has been considered with the Spirent hardware simulator in order to simulate a synchronous spoofing attack on a tracking receiver. This scenario considers two vehicles that start their movement from the same location and with the same dynamics and after sometime, their corresponding trajectories start to deviate from each other. One of the trajectories is considered as the authentic trajectory and the other one is considered as the spoofing one. Both vehicles incorporate the same PRN set and their corresponding correlation peaks are perfectly aligned before trajectory separation. The RF signals corresponding to the authentic and spoofing trajectories are fed to different output channels of the simulator and then combined together using a RF combiner (see Figure 5-7). Before combining, the power of the spoofing signal is adjusted using a cascaded amplifier-variable attenuator system. It should be noted that the signals of both outputs of the hardware simulator should experience almost the same delay before being fed to the RF combiner. In this scenario the power of spoofing signals is increased before separation of spoofing-authentic signals in order to be able to misdirect the tracking procedure of the target receiver.

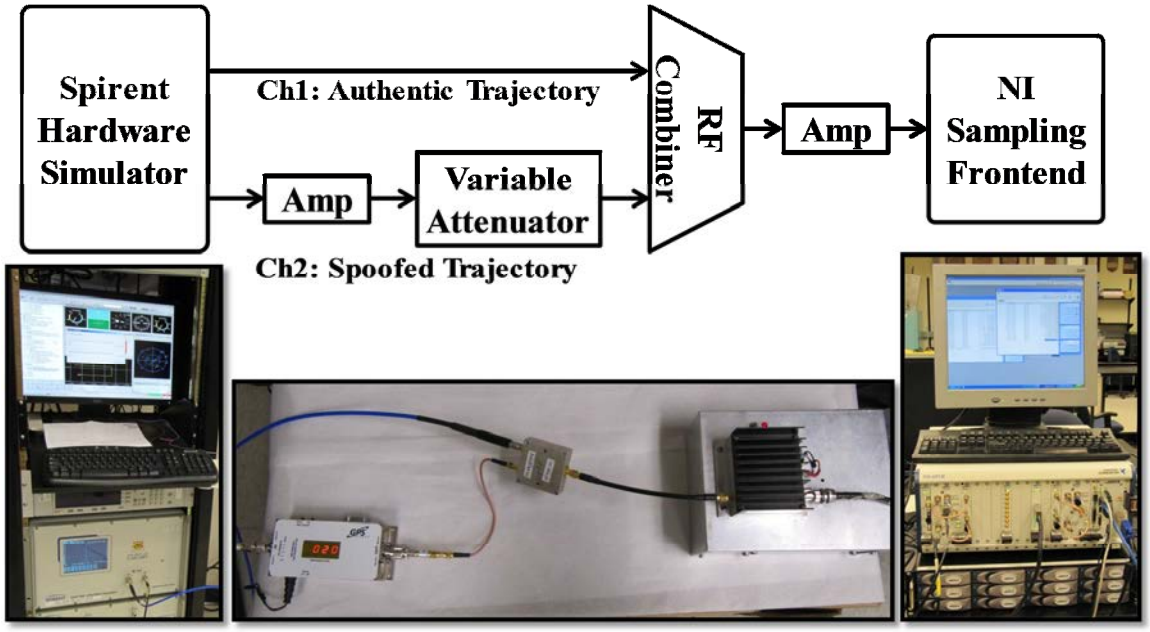


Figure 5-7 Data collection setup using a two-channel hardware simulator configuration

Figure 5-8 shows authentic and spoofing trajectories corresponding to this spoofing simulation scenario. The authentic trajectory has been depicted in green while the spoofed one is depicted in red. Vehicles motion starts from the top left corner and the trajectories deviate from each other after 65 seconds.

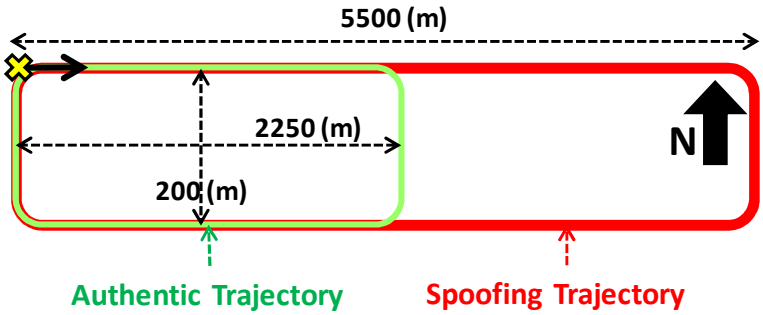


Figure 5-8 Spoofing and authentic trajectories

Table 5-1 lists the parameters settings of the authentic and spoofing trajectories and spoofing detection thresholds used for data processing.

Table 5-1 Parameter settings for data collection and processing

Parameter	Value
Start GPS Time (s)	162000
Spoofing Path Length (m)	5500
Authentic Path Length (m)	2250
Separation Time (s)	162065
Maximum Speed (km/h)	120
Speed at Corners (km/h)	10
Sampling Rate (Msps)	10
Significance Level for Rejecting H_0	1%
Significance Level for re-accepting H_0	90%
Spoofing Detection Threshold	21.7
Spoofing Release Threshold	4.17

5.6 Data Processing Results

Spoofing detection tests have been performed on correlator outputs for different PRNs under spoofing attack. Five correlator branches have been employed and their chip spacing is ½ chips between each two adjacent correlator branches. Coherent integration time is 1 ms and the spoofing detection tests are done on squared output amplitude of each correlator branch. Significance level values for spoofing detection and release have been considered as $\alpha_{\text{det}} = 0.01$ and $\alpha_{\text{rel}} = 0.90$, and spoofing detection and release thresholds have been set accordingly. Each test statistic has been calculated over 250 correlator output samples.

Figure 5-9 shows the spoofing detection test statistics for the asynchronous spoofing attack on PRN-09.

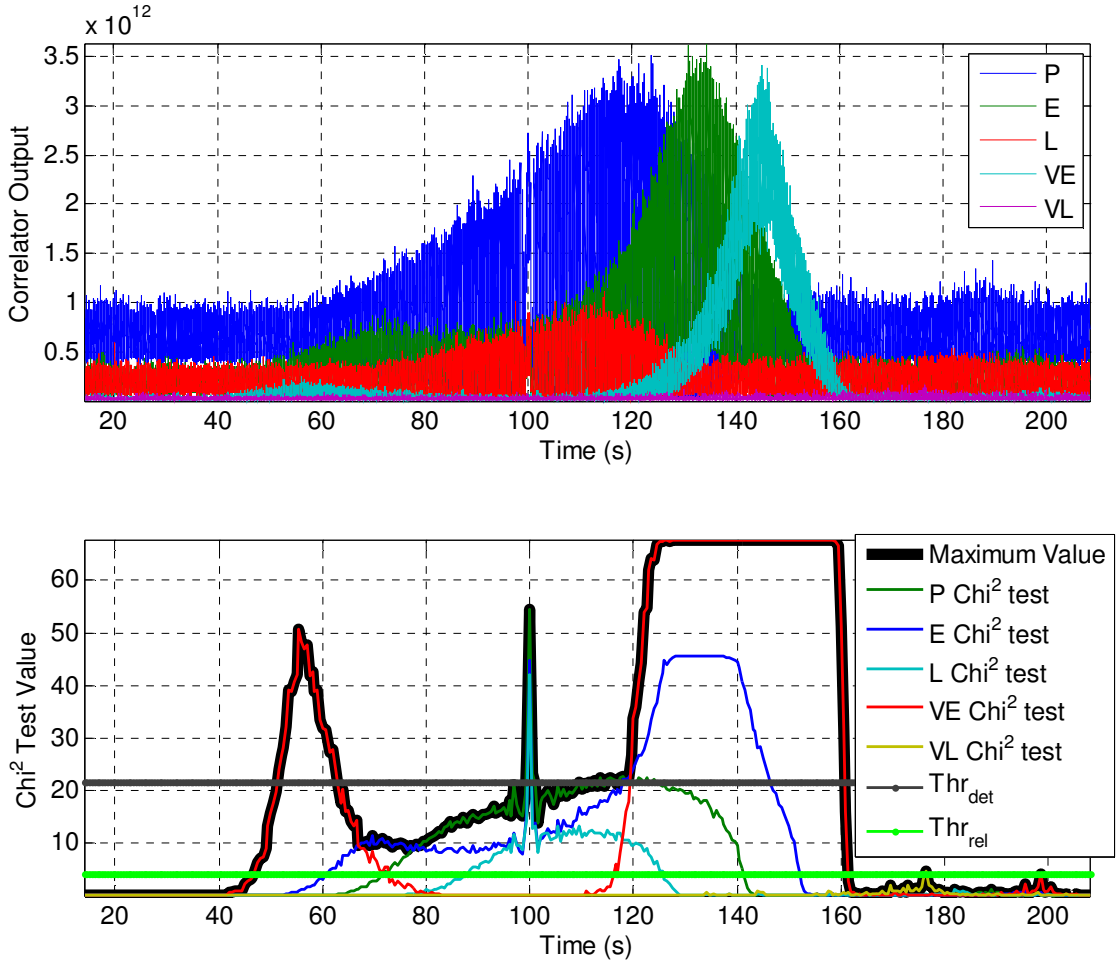


Figure 5-9 Detection tests for asynchronous spoofing attack on PRN-09

In this scenario the spoofing signal power increases to exceed the power level of the authentic signal and then gradually separates from authentic peak and tries to grab the tracking point of the receiver. It is observed that the spoofing attack is successfully detected as the detection test for very early correlator branch exceeds the spoofing detection threshold. It is shown that spoofing attack is refuted when all of the test

statistics fall under the spoofing release threshold. Figure 5-10 depicts a closer view of spoofing and authentic peaks interaction before and after their code alignment. It is observed that output amplitude of different correlator branches adopt sinusoidal variations before and after complete alignment of their corresponding code delays.

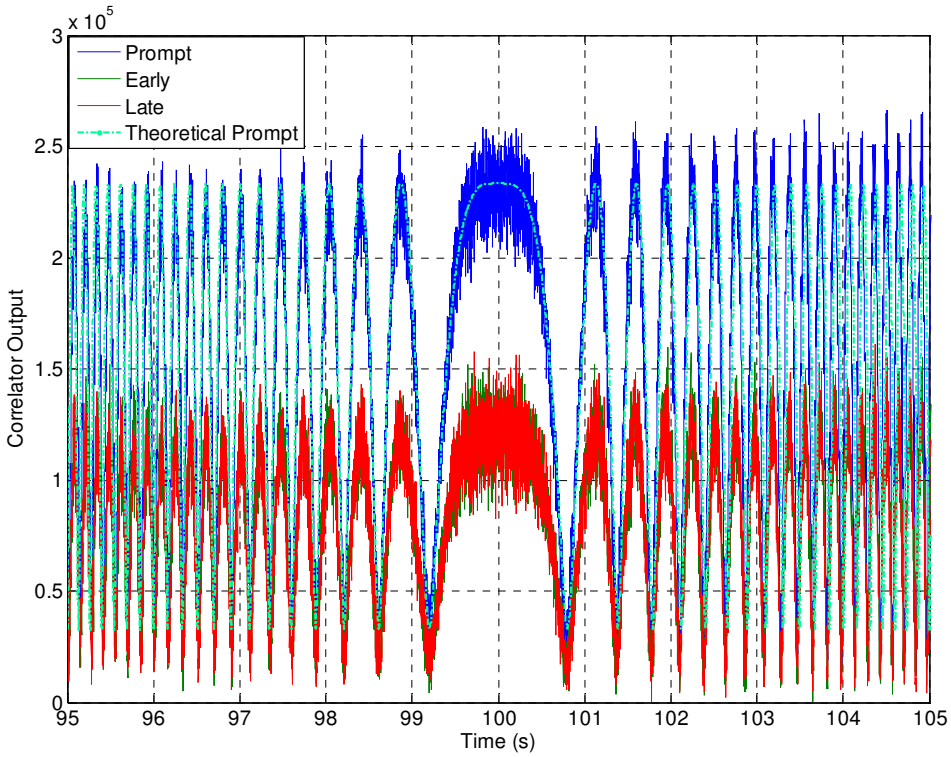


Figure 5-10 Correlator amplitude variations before and after alignment of spoofing and authentic peaks

The green dashed plot in Figure 5-10 illustrates the theoretical variations of prompt correlator output extracted from (5-11) for $\Delta\dot{f}_l^{a,s} = 0.78\,(\text{rad/s}^2)$. It is observed that the theoretical and practical amplitude variation results are completely consistent.

5.6.1 TEXBAT Data Processing

The spoofing datasets provided by RNL (University of Texas at Austin) implement synchronized spoofing attacks on GPS L1 signals wherein the spoofing signal is first aligned to the authentic correlation peak, then starts to increase its power and after that gradually break away from the authentic correlation peak. Dataset S0 corresponds to an unspoofed scenario wherein only authentic signals are present. Dataset S1 corresponds to a switched spoofing attack in which spoofing signals replace the authentic ones. Dataset S2 corresponds to a synchronized consistent Doppler spoofing attack in which the power of the spoofing PRNs is 10 dB higher than the authentic ones. Dataset S3 and S4 corresponds to synchronized locked Doppler spoofing attacks in which the power of spoofing PRNs is slightly higher than the authentic ones. In the S2, S3 and S4 scenarios, the spoofing attack starts with a higher power spoofing signal whose code delay is aligned with the authentic one. After several seconds, the higher power spoofing peak starts to move away from the authentic one and mislead the tracking procedure of its target receiver. For the case of a locked Doppler spoofing attack, the Doppler frequency of spoofing signal stays the same as its corresponding authentic signal while its code delay is changing.

Figure 5-11 illustrates the absolute value of prompt correlator outputs for PRN-19 and PRN-10 for the spoofing scenario S2. The received signals are tracked by a second order DLL and a third order PLL operating at 1 ms integration time. Figure 5-11 (a) shows that the emergence of higher power spoofing signals at T=110 s considerably affects the amplitude of the prompt correlator. The spoofing correlation peak starts to deviate from

the authentic one after 23 seconds. Since S2 scenario corresponds to a consistent Doppler spoofing attack, the separation of authentic and spoofing PRNs imposes increasing frequency fluctuations in the correlator output amplitude, which is clearly observable in Figure 5-11b.

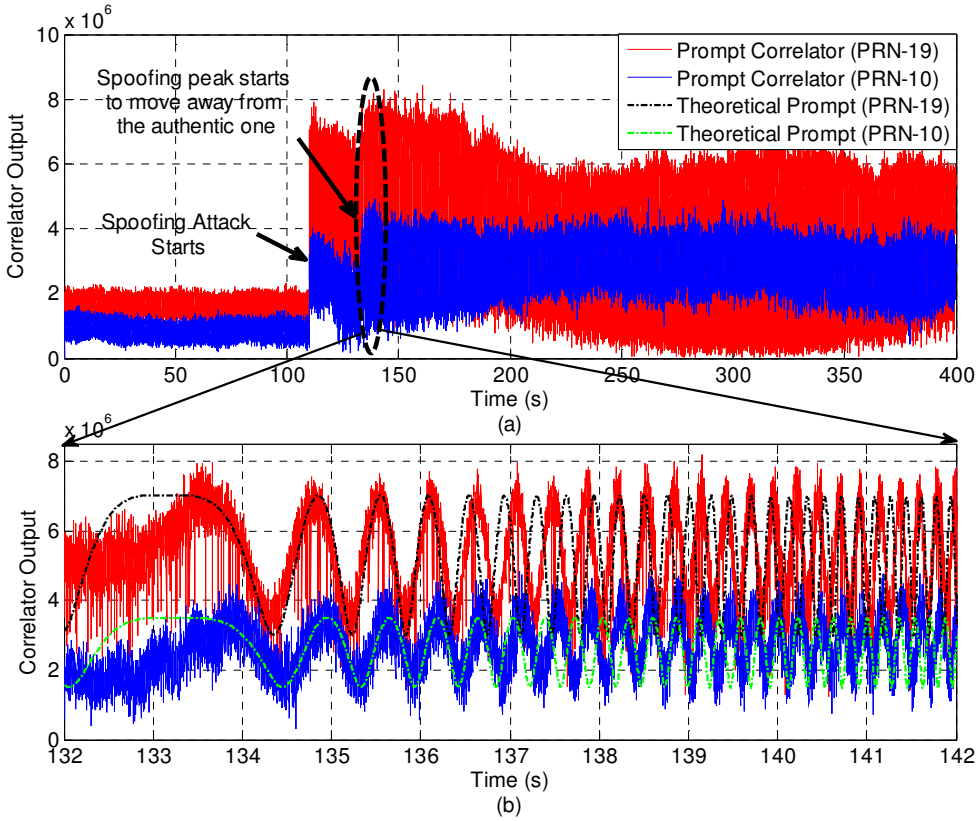


Figure 5-11 Amplitude variations of prompt correlator branches for PRN-10 and PRN-19 of TEXBAT data for a consistent Doppler spoofing scenario (S2)

These rapid amplitude variations considerably affect the correlator output distribution and reveal the presence of spoofing attack. In Figure 5-11 b, it is also observed that amplitude fluctuations do not completely conform with theoretical plots extracted from (5-11) and this might be due to the time-variant Doppler rate variations in TEXBAT datasets.

Figure 5-12 illustrates the detection test statistic of (5-18) for different spoofing scenarios in TEXBAT datasets. It is assumed that the integration time is 1 ms and K=1000. Three detection thresholds have been also shown in this figure that correspond to different false alarm probabilities of $P_{FA}=10^{-4}$, $P_{FA}=10^{-3}$ and $P_{FA}=10^{-2}$.

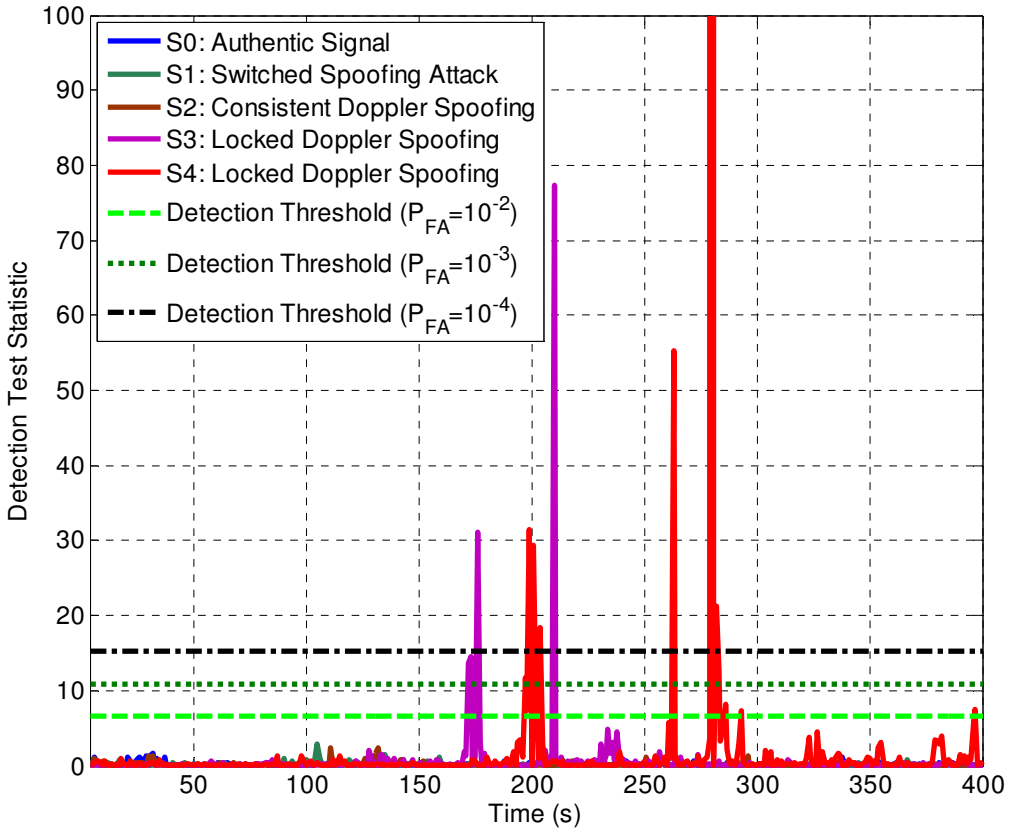


Figure 5-12 Detection test statistics for Doppler and code rate consistency check for different TEXBAT spoofing scenarios (PRN-10)

The cases of S1 (switched spoofing attack) and S2 (overpower spoofing attack) are consistent Doppler spoofing scenarios. Therefore, the code rate and Doppler frequency of these signals agree and these scenarios do not raise any spoofing detection flag. S3 and S4 spoofing scenarios correspond to locked Doppler spoofing attacks wherein the Doppler frequencies of spoofing signals remain the same as authentic ones and separation

of authentic and spoofing correlation peaks does not cause rapid fluctuations in correlator output amplitudes. For this case, it is observed that the detection test statistics of Figure 5-12 exceed the detection thresholds at several instances and this reveals the presence of spoofing signals with inconsistent Doppler and code rates.

5.7 Summary

The interaction between spoofing and authentic signals for a tracking receiver has been analyzed for different cases of spoofing attacks. It was shown that the interaction of consistent Doppler spoofing signals causes rapid fluctuations on the amplitude of correlator outputs and this feature can be used to reveal the presence counterfeit GNSS signals. A spoofing detection technique based on the correlator amplitude analysis was proposed. For this purpose, Chi-squared tests continuously analyze the correlator output distributions for different correlator branches; spoofing attack is flagged if the correlator output distribution significantly deviates from that of the authentic signal. The spoofing attack is refuted if all the test statistics fall under the spoofing release threshold. In some scenarios spoofing signals try to avoid rapid amplitude fluctuations by keeping their Doppler frequency the same as that of their corresponding authentic signal. In this case, it is shown that the inconsistency between code rate and Doppler frequency of spoofing signals can reveal the presence of these signals. To this end, a spoofing detection test that compares the Doppler and code rate estimates of a tracking receiver and detects spoofing attack based on the inconsistency of these two parameters was proposed. Synchronous and asynchronous spoofing attacks have been simulated using a hardware simulator. Real

measurement results further verify the effectiveness of the proposed spoofing countermeasure techniques in real world spoofing scenarios.

Chapter Six: Position Layer PVT Authenticity Verification in the Presence of Relative Motion between Spoofer and the Target Receiver

6.1 Introduction

Spoofing and meaconing signals try to mimic different features of authentic GNSS signals with potentially damaging effects. As discussed in Chapter 2, spoofing transmitters can be divided into three main categories, namely GNSS signal generators, receiver-based spoofers and multi-antenna receiver-based spoofers. The first two categories take advantage of a single transmit antenna in order to propagate counterfeit GNSS signals while the third category employs a plurality of synchronized transmit antennas. The latter type of spoofers is of such complexity that its practical implementation for civilian applications is questionable. Therefore, it can be assumed that spoofing signals are typically transmitted from a single terrestrial antenna while the authentic GNSS signals are transmitted from different satellites at different directions.

Nielsen et al (2010, 2011) and Broumandan et al (2012) have taken advantage of this feature of spoofing signals and proposed a spoofing detection technique for a moving GNSS receiver. This approach is based on taking pairwise correlation between received signals from different satellites during the acquisition and tracking stages. This technique is effective in both line of sight (LOS) and multipath propagation environments; however, it requires the receiver's ability to separate the effect of Doppler and local clock variations from those variations caused by receiver movement. Psiaki et al (2013) have considered a rapidly spatially oscillating GNSS antenna in order to detect the presence of a spoofing transmitter based on the coherent phase variations of spoofing PRNs. They

have modelled the effect of antenna oscillation on the phase variation of the received signals and then detected the spoofed PRNs based on the similar trends of their phase variations.

This chapter focuses on detecting the presence of spoofed PVT solutions based on the position level observables of a moving receiver. One of the features of spoofing signals that makes them different from other types of GNSS interference is that spoofers transmit ranging signals similar to genuine GNSS signals. Therefore, unlike other jamming categories, a spoofer can be detected (and/or even localized) based on the pseudorange measurements extracted from its own PRN signals. In a single-antenna spoofing scenario, all fake PRNs are transmitted from the same antenna and hence, they all experience a common delay that is due to the propagation distance between spoofer antenna and the target receiver's antenna. Herein, it is shown that a relative position variation between the spoofer and receiver imposes a variable bias in the clock state of the receiver and this bias can be utilized to reveal the presence of a spoofed PVT solution. To this end, a generic analysis on pseudorange observables of different types of spoofer is first provided and then a PVT authentication technique based on the clock state variation analysis of the moving receiver is discussed. Since all spoofer generated PRN signals experience the same propagation channel, the proposed method is able to reveal the presence of counterfeit PVT solutions even in multipath propagation environments.

The proposed technique is based on the correlation of the clock bias variations with the receiver motion. Five motion scenarios have been considered that can be listed as known arbitrary, circular, random walk, constant speed linear and completely unknown motion.

For the case of the first three motion scenarios the receiver is able to authenticate PVT solutions without any prior knowledge of receiver clock parameters. However, for the case of the two latter motion scenarios the receiver needs to first estimate the clock model parameters during a static learning phase and then start its movement in order to detect the authenticity of its PVT solution. In this case the presence of a spoofer can be detected if the PVT solution clock state deviates considerably from its prediction. The detection performance varies depending on the level of the receiver's knowledge of its movement trajectory, clock stability and accuracy of the clock model parameter estimates. Several simulations have been performed to compare receiver operating characteristics (ROC) for different levels of knowledge of the receiver trajectory and also different clock types. Real data collection and processing results show the acceptable performance of the proposed spoofing detection technique for different motion scenarios and clock qualities.

The rest of this chapter is organized as follows; Section 6.2 provides an analysis on the system model and pseudoranges for aligned and non-aligned spoofing attacks. Section 6.3 focuses on spoofing detection for a moving receiver under different trajectory motions. Simulation results are provided in Section 6.4 and real data collection and processing are discussed in Section 6.5. The concluding notes are finally provided in Section 6.6.

6.2 Problem Formulation

A successful spoofer must be able to simultaneously synthesize several consistent GNSS signals in order to mislead its target receiver(s). In other words, the pseudorange observations extracted from the spoofing signals should be consistent and lead to a

plausible PVT solution. A simplified model for the *i*'th spoofed pseudorange observation at time *t* at the target receiver can be written as

$$\hat{P}R_i(t) = \underbrace{\hat{\rho}_i(t) + c.d\hat{t}_i(t)}_{\text{Specific to } PRN_i} + \underbrace{c.dT_u(t) + \rho_{su}(t) - c.dT_s(t)}_{\hat{C}(t):\text{ Common among all PRNs}} + \hat{\eta}_i(t) \tag{6-1}$$

where $\hat{\rho}_i(t)$ is the fake range between the spoofer generated fake position and the *i*th counterfeit GNSS satellite at time *t*. $d\hat{t}_i(t)$ is the timing error corresponding to the *i*th counterfeit satellite at time *t*. $dT_u(t)$ and $\rho_{su}(t)$ are the user clock bias and physical range between the spoofer transmit antenna and target receiver's antenna, respectively; $dT_s(t)$ represents a deliberate time advance that might be added to the spoofer's transmit signal in order to compensate for the propagation delay between spoofer antenna and the target receiver's antenna. This term must be either constant or follow a predefined clock state model in order to be consistent with the expected features of the GNSS receiver clock variations. *c* is the speed of light in the vacuum and $\hat{\eta}_i(t)$ represents the other error sources such as ambient noise and multipath.

An approximate model for the pseudorange measurement derived for the *i*th authentic PRN can be written as

$$PR_i(t) = \underbrace{\rho_i(t) + cdt_i(t)}_{\text{Specific to } PRN_i} + \underbrace{c\,dT_u(t)}_{C(t):\text{ Common among all PRNs}} + \eta_i(t) \tag{6-2}$$

where ρ_i is the range between the user antenna and the *i*th GNSS satellite; dt_i and dT_u are the *i*th satellite clock bias and receiver clock bias, respectively; $\eta_i(t)$ represents the other error sources such as ambient noise and multipath.

6.2.1 Non-aligned Spoofing Attack

For the case of a simplistic spoofing attack via an unsynchronized GNSS signal simulator, the counterfeit correlation peaks are not aligned with the authentic ones. Therefore, distinct correlation peaks corresponding to authentic and spoofing signals may appear in the cross ambiguity function (CAF). In this case, the spoofer tries to mislead acquiring receivers into tracking its higher power correlation peaks; however, as discussed in Chapter 5, the GNSS receivers that are operating in tracking mode are not highly vulnerable to this type of spoofing attack. This type of spoofer might take advantage of an omni-directional antenna to mislead several receivers within its coverage area.

6.2.2 Aligned Spoofing Attack

Aligned spoofing attacks can be generated by receiver-based spoofers. As discussed in Chapter 2, this type of spoofer consists of two main parts namely "GPS receiver" and "spoofing generator" (Humphreys et al 2008). In this case, the information regarding the current GPS constellation and the authentic signal parameters are extracted by the GPS receiver measurements and then these parameters are used to generate counterfeit signals to mislead a specific target GPS receiver. Aligned spoofing attack intends to mislead a tracking receiver by first generating correlation peaks at similar code delays and Doppler

frequencies as currently available authentic signals received by the target receiver; and then, gradually moving away their fake correlation peaks in order to misdirect the tracking process of the target receiver. It is assumed that the spoofer knows the approximate position of the target receiver's antenna. Therefore, the spoofer is able to align its counterfeit correlation peaks with the authentic ones received by the target receiver.

In order to align the authentic and spoofing correlation peaks, the deterministic parts of the pseudorange observations in (6-1) and (6-2) should be the same and as such the following equality should be satisfied at the lift-off moment, t_l:

$$\underbrace{\hat{\rho}_i(t_l) + c.d\hat{t}_i(t_l)}_{PRN_i\ specific} + \underbrace{c.dT_u(t_l) + \rho_{su}(t_l) - c.dT_s(t_l)}_{Common\ among\ all\ PRNs} = \underbrace{\rho_i(t_l) + c.dt_i(t_l)}_{PRN\ specific} + \underbrace{c.dT_u(t_l)}_{Common\ among\ all\ PRNs} \tag{6-3}$$

As shown in (6-3), each side of the equation consists of two parts where one of them is PRN specific and the other one is common among all PRNs. After a successful lift-off, the spoofer can gradually change the term $\hat{\rho}_i$ and dT_s in order to bias the PVT solution of the receiver from the genuine solution.

A receiver-based spoofer may employ a directional antenna to cover a specific spatial sector within which its target receiver is located. In addition, this type of spoofer can still affect many acquiring GNSS receivers inside its coverage area because, for the receivers other than the target receiver, the spoofing and authentic correlation peaks are not aligned.

6.3 Spoofing Detection using a Moving Receiver

Relative motion between a spoofing source and its target receiver changes their relative range. Considering (6-1), the movement of target receiver can cause variations in $\rho_{su}(t)$ that are common among all spoofed pseudorange measurements. As such, this distance variation shows up in the clock state of the receiver's PVT solutions. Since short term clock variations of a GNSS receiver can be modeled as a linear function of time, any abnormal deviations from this model can indicate the presence of a spoofed PVT solution. For example, it will be shown that the circular motion of a receiver antenna can impose sinusoidal variations in the clock state of a spoofed PVT solution and consequently reveal the presence of malicious signals.

The discrete time first order expansion of short term clock variations of a GNSS can be written as

$$c.\upsilon[n] = c.\upsilon_{u,0} + c.\dot{\upsilon}_{u,0}\, n + \eta[n] \tag{6-4}$$

where the $\upsilon_{u,0}$ and $\dot{\upsilon}_{u,0}$ represent the initial clock bias and the clock drift of the receiver, respectively. $\eta[n]$ is the additive Gaussian noise process at time instant *n* whose spectral density is determined by the oscillator characteristics. It is assumed that the spoofing signals also follow the clock state model of the authentic signals since they need to mimic the authentic signal features as much as possible in order to avoid being detected by the target receiver. It is also assumed that the spoofer is not aware of the receiver motion; therefore, it does not adaptively change its signals' clock state model with respect to the

receiver movement. Spoofing detection can be accomplished by monitoring the clock state of the PVT solution of a moving receiver. To this end, spoofing detection tests for several motion scenarios of a GNSS receiver are proposed in the following subsections.

6.3.1 Detection test development

The spoofing detection problem can be defined as follows

$$\begin{aligned} \mathrm{H}_0: &\quad x[n] = c.\upsilon_{u,0} + c.\dot{\upsilon}_{u,0}\, n + \eta[n] \\ \mathrm{H}_1: &\quad x[n] = \Delta\rho_{su}[n] + c.\upsilon_{u,0} + c.\dot{\upsilon}_{u,0}\, n + \eta[n] \end{aligned} \tag{6-5}$$

for $n=1,2,\ldots,N$. H_0 and H_1 represent the hypotheses of the absence and presence of a spoofing signal, respectively. N is the number of samples used for hypothesis testing. It is assumed that the intentional time advance added by the spoofer, $c.dT_s[n]$ in (6-1), also follows the clock state variations model for the user local clock and therefore, the overall short term clock variations. Consequently, the only term that discriminates between the H_0 and H_1 hypotheses is the uncompensated range variation between the spoofer and the target receiver, which can be written as

$$\begin{aligned} \Delta\rho_{su}[n] &= \rho_{su}[0] - \rho_{su}[n] \\ &= \left\|\mathbf{P}_u[0] - \mathbf{P}_s[0]\right\| - \left\|\mathbf{P}_u[n] - \mathbf{P}_s[n]\right\|, \end{aligned} \tag{6-6}$$

where $\mathbf{P}_u[n]$ and $\mathbf{P}_s[n]$ are the target receiver's three dimensional positions at time n and $\|\bullet\|$ represents the norm of its argument vector [see Figure 6-1]. In the following subsections it is assumed that the spoofer is a stationary transmitter whose movement is negligible with respect to the target receiver's movement, therefore, $\mathbf{P_s}[n] \approx \mathbf{P_s}[0]$ for $n=1,2,\ldots N$.

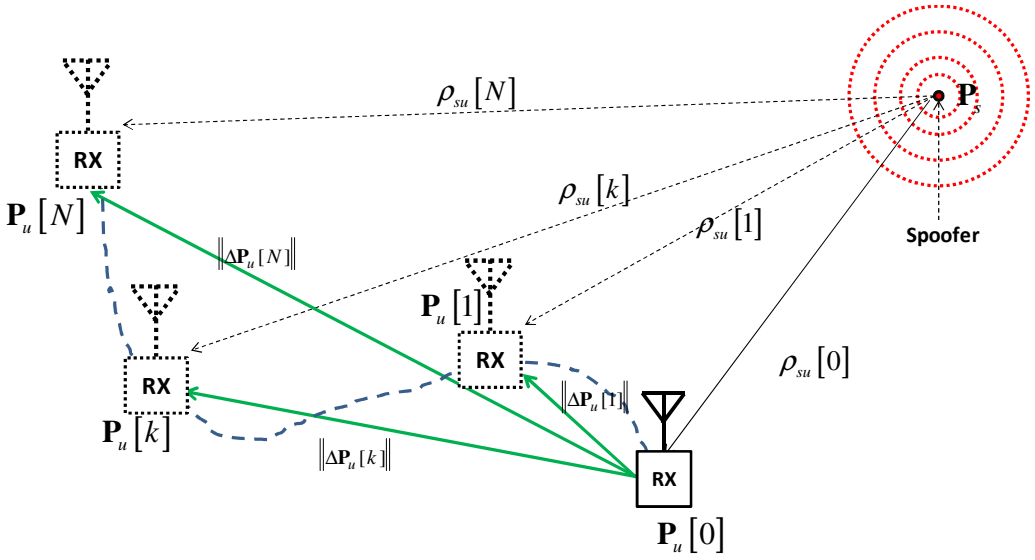


Figure 6-1 Spoofing detection scenario for a known arbitrary trajectory

6.3.2 Known Arbitrary Trajectory

In this case it is assumed that the short term variations of receiver trajectory ($\Delta\mathbf{P}_u[n]$) is known and the user-spoofer distance is much larger than the user position variations. Therefore, equation (6-6) can be re-written as

$$\Delta\rho_{su}[n] = \underbrace{\|\mathbf{P}_u[0]-\mathbf{P}_u[n]\|}_{\|\Delta\mathbf{P}_u[n]\|}\cos(\varphi_u[n]-\varphi_s)\cos(\theta_u[n]-\theta_s) \tag{6-7}$$

where $\varphi_u[n]$ and φ_s represent the azimuth angle of the user motion vector at time n and the azimuth angle of the spoofing source with respect to the initial position of user, respectively. $\theta_u[n]$ and θ_s represent the elevation angle of the user motion at time n and the elevation angle of the spoofing source with respect to the initial position of user, respectively. Herein, the detection test of (6-5) can be written in the form of a classical linear model as (Kay 1998)

$$\mathbf{x} = \mathbf{H}\boldsymbol{\theta} + \mathbf{w} \qquad \begin{cases} \mathrm{H}_0 : \ \mathbf{A}\boldsymbol{\theta} = \mathbf{b} \\ \mathrm{H}_1 : \ \mathbf{A}\boldsymbol{\theta} \neq \mathbf{b} \end{cases} \tag{6-8}$$

where $\mathbf{H}$ is a *N*-by-*6* design matrix whose *n*, *p*th element, $[\mathbf{H}]_{n,p}$, can be written as

$$\begin{aligned} [\mathbf{H}]_{n,1} &= \|\Delta\mathbf{P}_u[n]\| \cos(\varphi_u[n]) \cos(\theta_u[n]) \\ [\mathbf{H}]_{n,2} &= \|\Delta\mathbf{P}_u[n]\| \cos(\varphi_u[n]) \sin(\theta_u[n]) \\ [\mathbf{H}]_{n,3} &= \|\Delta\mathbf{P}_u[n]\| \sin(\varphi_u[n]) \cos(\theta_u[n]) \\ [\mathbf{H}]_{n,4} &= \|\Delta\mathbf{P}_u[n]\| \sin(\varphi_u[n]) \sin(\theta_u[n]) \\ [\mathbf{H}]_{n,5} &= 1 \\ [\mathbf{H}]_{n,6} &= n \end{aligned} \tag{6-9}$$

The other parameters of equation (6-8) can be written as

$$\begin{aligned} \boldsymbol{\theta} &= \begin{bmatrix} \cos(\varphi_s)\cos(\theta_s) \\ \cos(\varphi_s)\sin(\theta_s) \\ \sin(\varphi_s)\cos(\theta_s) \\ \sin(\varphi_s)\sin(\theta_s) \\ c.\upsilon_u \\ c.\dot{\upsilon}_u \end{bmatrix}, \mathbf{b} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \mathbf{w} = \begin{bmatrix} \eta[1] \\ \eta[2] \\ \vdots \\ \eta[N] \end{bmatrix} \\ \mathbf{A} &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \ \mathbf{x} = \begin{bmatrix} x[1] \\ x[2] \\ \vdots \\ x[N] \end{bmatrix} \end{aligned} \tag{6-10}$$

Therefore, a GLRT detector will select H_1 if (Kay 1998)

$$T(\mathbf{x}) = \frac{\left(\mathbf{A}\hat{\boldsymbol{\theta}}_1 - \mathbf{b}\right)^T \left[\mathbf{A}\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{A}^T\right]^{-1} \left(\mathbf{A}\hat{\boldsymbol{\theta}}_1 - \mathbf{b}\right)}{\sigma^2} > \gamma \tag{6-11}$$

where

$$\hat{\boldsymbol{\theta}}_1 = \left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{x} \tag{6-12}$$

is the maximum likelihood estimate (MLE) of $\boldsymbol{\theta}$ under H_1 and γ is the detection threshold. σ^2 is the variance of the noise process vector which is assumed to be constant during the observation interval. The asymptotic detection performance of this detector can be written as

$$P_D = Q_{\chi_q'^2(\lambda)}\left(Q_{\chi_q^2}^{-1}\left(P_{FA}\right)\right) \tag{6-13}$$

Eqation 6-13 is an approximation where P_D is the probability of detection and P_{FA} is the probability of false alarm. $Q_{\chi_q'^2(\lambda)}(\bullet)$ is the tail probability of the non-central chi-squared distribution with non-centrality parameter of (λ) and q degrees of freedom. $Q_{\chi_q^2}^{-1}(\bullet)$ represents the inverse of the tail probability of a central chi-squared distribution with q degrees of freedom. Herein, q=4 which is equal to the number of rows in matrix **A**. The non-centrality parameter can be written as (Kay 1998)

$$\lambda = \frac{\left(\mathbf{A}\boldsymbol{\theta}_1 - \mathbf{b}\right)^T\left[\mathbf{A}\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{A}^T\right]^{-1}\left(\mathbf{A}\boldsymbol{\theta}_1 - \mathbf{b}\right)}{\sigma^2} \tag{6-14}$$

where $\boldsymbol{\theta}_1$ is the exact value of the parameters under H_1 hypothesis.

6.3.3 Circular Trajectory

This scenario considers a receiver moving at a constant speed along a circular trajectory. The radius of the circle, *r,* is unknown and the angular velocity of the receiver, ω_0, is

assumed to be known. The initial angle of user with respect to the line connecting the spoofer to the centre of the motion circle (φ_0) is unknown. Figure 6-2 illustrates the scenario of the circular trajectory. In this case, equation (6-6) can be approximately written as

$$\Delta\rho_{su}[n] \approx r\cos(\Delta\theta_s)\left(\cos(\omega_0 n+\varphi_0)-\cos(\varphi_0)\right) \tag{6-15}$$

where $\Delta\theta_s$ is the elevation angle of the spoofing source with respect to receiver movement plane.

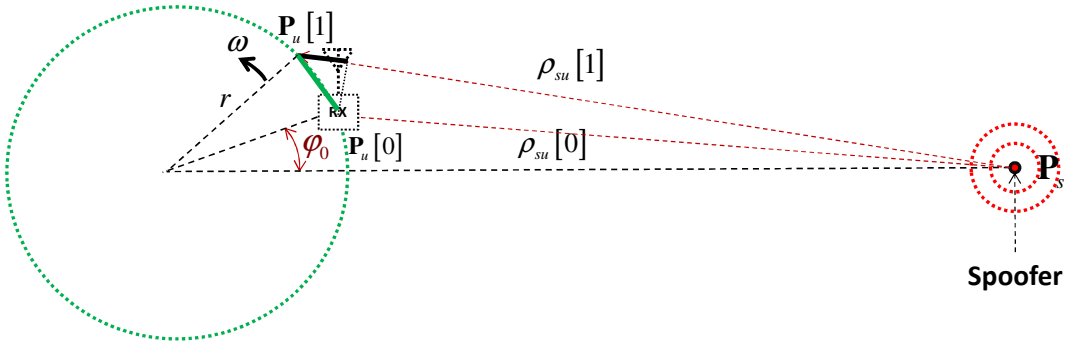


Figure 6-2 Receiver circular motion

Herein, the definitions of **x** and **w** of the detection model of (6-8) are the same as (6-10). After some mathematical simplifications the parameters of detection model (6-8) can be written as

$$\mathbf{H}=\begin{bmatrix} \cos(\omega_0) & \sin(\omega_0) & 1 & 1 \\ \cos(2\omega_0) & \sin(2\omega_0) & 1 & 2 \\ \vdots & \vdots & \vdots & \vdots \\ \cos(N\omega_0) & \sin(N\omega_0) & 1 & N \end{bmatrix}, \quad \mathbf{b}=\begin{bmatrix} 0 \\ 0 \end{bmatrix}$$
$$\boldsymbol{\theta}=\begin{bmatrix} r\cos(\Delta\theta_s)\cos(\varphi_0) \\ -r\cos(\Delta\theta_s)\sin(\varphi_0) \\ c.\upsilon_u - r\cos(\Delta\theta_s)\cos(\varphi_0) \\ c.\dot{\upsilon}_u \end{bmatrix}, \mathbf{A}=\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \tag{6-16}$$

The detection performance of this system can be provided by (6-13) where q=2. In case that the angular velocity of the user (ω_0) is unknown, the detector should choose the maximum value of the detection test statistic evaluated for different angular velocities and then compare this value with a detection threshold. Therefore, the detection test can be written as

$$\max_{\omega_0}\{T(\mathbf{x};\omega_0)\} > \gamma' \tag{6-17}$$

where $T(\mathbf{x};\omega_0)$ is the detection test statistic of (6-11) assuming that the angular velocity is known and γ' is the modified detection threshold. The operator $\max_{\omega_0}\{\bullet\}$ chooses the maximum value of its argument over different values of ω_0. It is assumed that the value of ω_0 is in the interval $[0,\pi]$ and this value is not very close to the interval borders.

6.3.4 Random Walk Motion

In this scenario it is assumed that the receiver adopts an unknown random walk motion around its initial position. Hence, the detection problem can be written in vector format as

$$\mathbf{x}=\mathbf{H}\boldsymbol{\theta}+\mathbf{w}\ \begin{cases}\mathrm{H}_0:\mathbf{w}=\left[\eta[1],\eta[2],...,\eta[N]\right]^T\\ \mathrm{H}_1:\mathbf{w}=\left[\Delta\rho_{su}[1]+\eta[1],...,\Delta\rho_{su}[N]+\eta[N]\right]^T\end{cases} \tag{6-18}$$

where the definition of $\mathbf{x}$ is the same as (6-10). $\mathbf{H}$ and $\boldsymbol{\theta}$ are defined as

$$\mathbf{H}=\begin{bmatrix}1 & 1\\ 1 & 2\\ \vdots & \vdots\\ 1 & N\end{bmatrix},\quad \boldsymbol{\theta}=\begin{bmatrix}c.\upsilon_u\\ c.\dot{\upsilon}_u\end{bmatrix} \tag{6-19}$$

Therefore, the clock state parameters should be first estimated before detecting the presence of a spoofing signal. The estimate of clock state parameters can be written as (6-12). Since in this scenario no deterministic model has been considered for the receiver movement, the detection test selects H_1 if

$$T(\mathbf{x})=\frac{1}{\sigma^2}\left(\mathbf{x}-\mathbf{H}\hat{\boldsymbol{\theta}}\right)^T\left(\mathbf{x}-\mathbf{H}\hat{\boldsymbol{\theta}}\right)>\gamma \tag{6-20}$$

where $T(\mathbf{x})$ is the test statistic and γ is the detection threshold.

6.3.5 Linear Trajectory

In this scenario it is assumed that the receiver is moving along a linear trajectory having a constant speed *v* with unknown direction with respect to the spoofing source as shown in Figure 6-3. Also, it is assumed that $\Delta\rho_{su}[n]\ll\rho_{su}[n]$ for *n=1,2,…,N.* Therefore, there is an approximately constant angle ($\Delta\varphi_s$) between the movement direction of the receiver and the incident plane wave of the spoofing signal. Hence, (6-6) can be updated as

$$\Delta\rho_{su}[n] = \rho_{su}[0] - \rho_{su}[n] = vnT \times \cos(\Delta\varphi_s) \tag{6-21}$$

where T is the time interval between consecutive samples of clock state differences. This scenario is applicable to the case of a vehicle traveling along a straight trajectory.

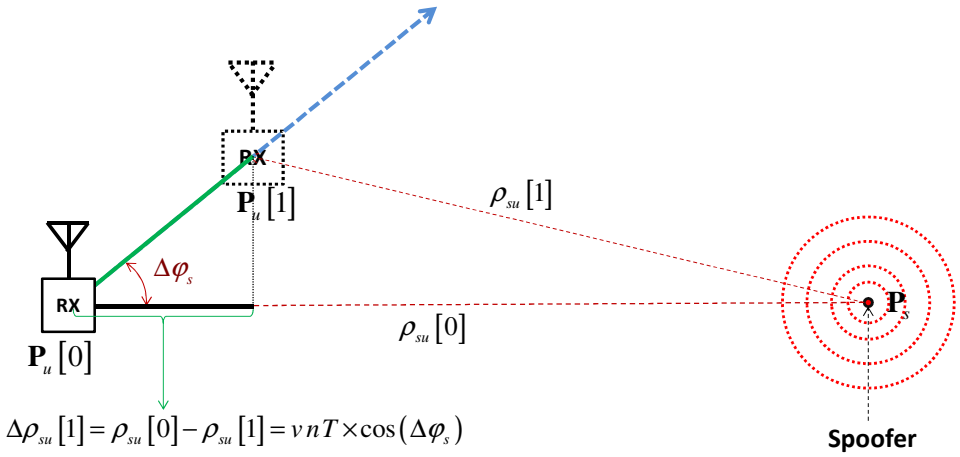


Figure 6-3 Linear motion in unknown direction

For this type of user movement, the spoofer-user range variations ($\Delta\rho_{su}[n]$) is a linear function of time; therefore, it should be separated from clock bias variations of the user which is also a linear function of time. To this end, spoofing detection should take place in the following two steps:

- **Learning phase:** in this phase the receiver stays stationary and extracts the PVT solution. Based on the clock state observations, the receiver is able to estimate the clock bias ($\hat{\upsilon}_{u,0}$) and clock drift ($\hat{\dot{\upsilon}}_{u,0}$) so as to predict the clock state variations during

its movement. It is assumed that the receiver is using a sufficiently stable oscillator whose short-term model is a linear function of time.

- **Moving phase:** the receiver starts to move from its initial position and the clock state deviation from its predicted value is continually monitored for the purpose of spoofing detection.

Since a linear motion has been considered for the receiver, a GLRT detector using a classical linear model can still be adopted to detect the presence of a spoofer in this scenario. Herein, the classical linear model parameters of Equation (6-8) can be defined as

$$\mathbf{H}=\begin{bmatrix}1 & 1\\ 1 & 2\\ \vdots & \vdots\\ 1 & N\end{bmatrix},\ \boldsymbol{\theta}=\begin{bmatrix}c.\upsilon_u\\ c.\dot{\upsilon}_u\end{bmatrix},\ \mathbf{A}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\ \mathbf{b}=\begin{bmatrix}c.\hat{\upsilon}_{u,0}\\ c.\hat{\dot{\upsilon}}_{u,0}\end{bmatrix} \tag{6-22}$$

The detection test statistic can be written as (6-11) and the performance of this detector can be calculated based on (6-13).

6.3.6 Completely Unknown Trajectory

In this scenario no assumptions have been considered for the receiver trajectory. Similar to the case of linear motion, spoofing detection requires two operational phases namely "Learning phase" and "Moving phase". The difference between this scenario and the random walk scenario is that, herein the receiver does not require moving around its initial position. The detection test chooses the H_1 hypothesis if

$$T(\mathbf{x}) = \frac{1}{\sigma^2}\left(\mathbf{x}-\mathbf{Hb}\right)^T\left(\mathbf{x}-\mathbf{Hb}\right) > \gamma \tag{6-23}$$

The performance of this detector is dependents on the accuracy of the clock and its modeling and it can be degraded in the presence of even a small error in the clock parameter estimates.

6.4 Simulation results

Monte-Carlo simulations were performed to evaluate the performance of the proposed PVT authentication techniques. It is assumed that the spoofer is a far away static transmitter located at the relative ENU position of $\mathbf{P}_s$= [10 km 10 km 0] with respect to the initial position of the target receiver and the receiver is locked onto tracking spoofing signals and providing PVT solution based on spoofed pseudorange observables. Herein, it is assumed that the short term variation in the receiver clock state is a first order function of time. The initial clock bias and clock drift of the user are assumed to be 100 m and 0.5 m/s, respectively. Three motion scenarios namely "*random walk motion*", "*linear motion*" and "*circular motion*" have been considered here. The user clock information is updated at 1 s intervals. For the case of "*random walk motion*", at each step, the user moves 1.5 m along an arbitrary 3D trajectory while for the case of "*linear motion*", all the user movements are along the same line with an arbitrary angle. The rotation frequency of user during "*circular motion*" is considered as $\omega_0 = 0.62$ rad/s. The clock bias noise process is considered a zero mean Gaussian process with a standard deviation of σ = 3 m. Monte-Carlo simulations were performed for 10000 runs, with 100 s of user clock information is processed in each run.

Figure 6-4 shows the receiver operating characteristics (ROC) plot for detectors of types (i), (iii) and (v) in the presence of random walk motion. For the case of type (v) detector that requires prior knowledge regarding user clock state parameters, it is assumed that the receiver first comes up with an estimate of the clock state parameters during a stationary interval of 30 s.

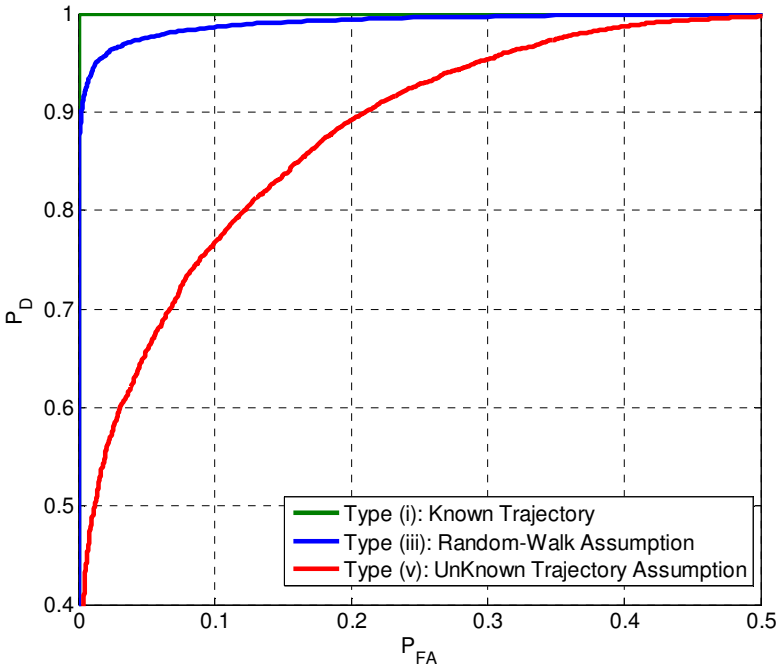


Figure 6-4 ROC for detectors (i), (iii) and (v) for the case of random walk motion

It is observed that the known trajectory detector (detector type i) achieves the best detection performance among the other detectors. The performance of the random walk trajectory detector (detector type iii) achieves the second rank. This detector is designed based on the assumption that the user moves randomly around its initial position and it does not rely on any other information regarding user motion. Finally, the unknown

trajectory detector that works based on 30 s of stationary learning achieves the least detection performance.

Figure 6-5 compares the ROC of detectors of type (iv) and type (v) for the case of a linear trajectory in an unknown direction. The ROC curves have been shown for different lengths of learning intervals, namely 10s, 30s, 60s and 100s. It is observed that as the length of the learning interval increases the detection performance of these detectors also increases and this is due to a more accurate estimation of the clock model parameters during longer learning intervals. It is observed that for short learning intervals the performance of both detectors are almost the same, however in the presence of more accurate parameter estimation, the linear detector (type iv) outperforms the unknown trajectory detector (type v).

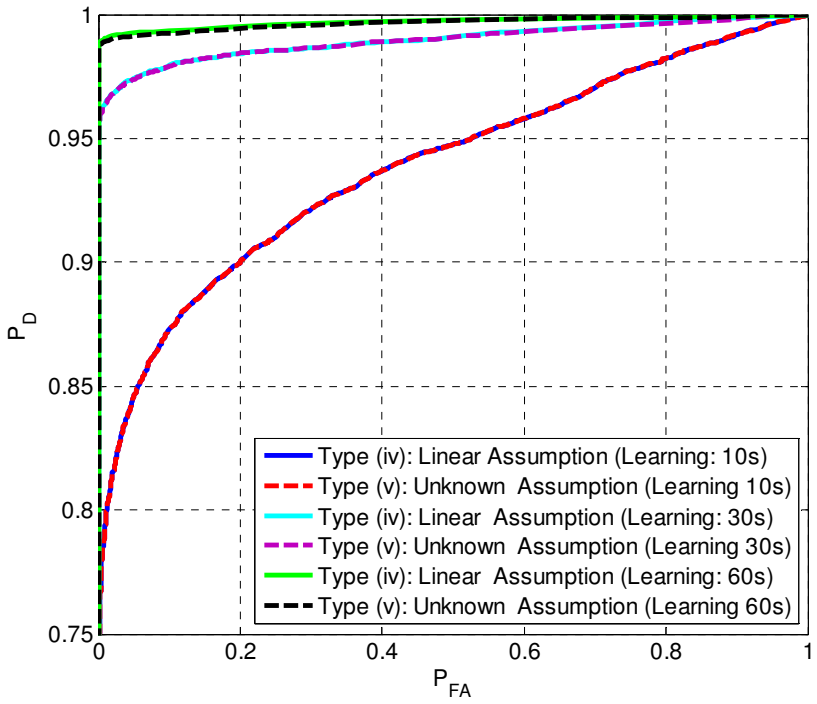


Figure 6-5 ROC for detectors (iv) and (v) for the case of linear motion

Figure 6-6 shows the ROC plots for detector types (i), (ii) and (iii) when the receiver is moving along a circular trajectory with r=1 m. It is observed that the detector type (i) achieves the best performance. The detection performance of detector (ii) is almost the same as that of type (i) when the rotation frequency is known, however for the case of an unknown rotation frequency, the detection performance degrades. The theoretical performance of detector type (ii), based on (6-13), has also been shown in dashed green lines which is in agreement with the simulation results. As observed in Figure 6-6, the detector type (iii) can also detect the presence of the spoofing source (although with a lower performance) because the circular motion takes place around the initial position of the receiver and this is a required assumption for a random walk trajectory.

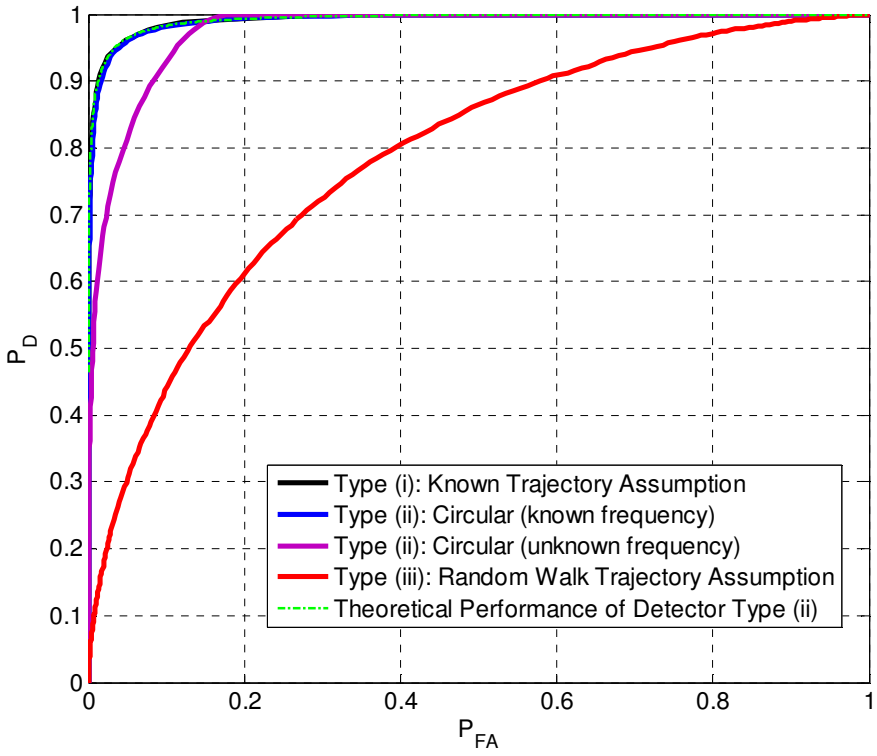


Figure 6-6 ROC for detectors (i), (ii) and (iii) for the case of circular motion (r=1m)

Figure 6-7 shows the ROC curves for a circular trajectory detector type (ii) in the presence of different values for the receiver circular motion radius. The standard deviation of the receiver clock state is the same as in previous cases, namely σ=3 *m*. It is observed that as the circle radius increases, the detection performance of the receiver also increases and, for the case of r=1.5 m, the receiver can almost perfectly detect the presence of spoofing source. In all cases, the lack of knowledge for the receiver rotation frequency lowers the detection performance.

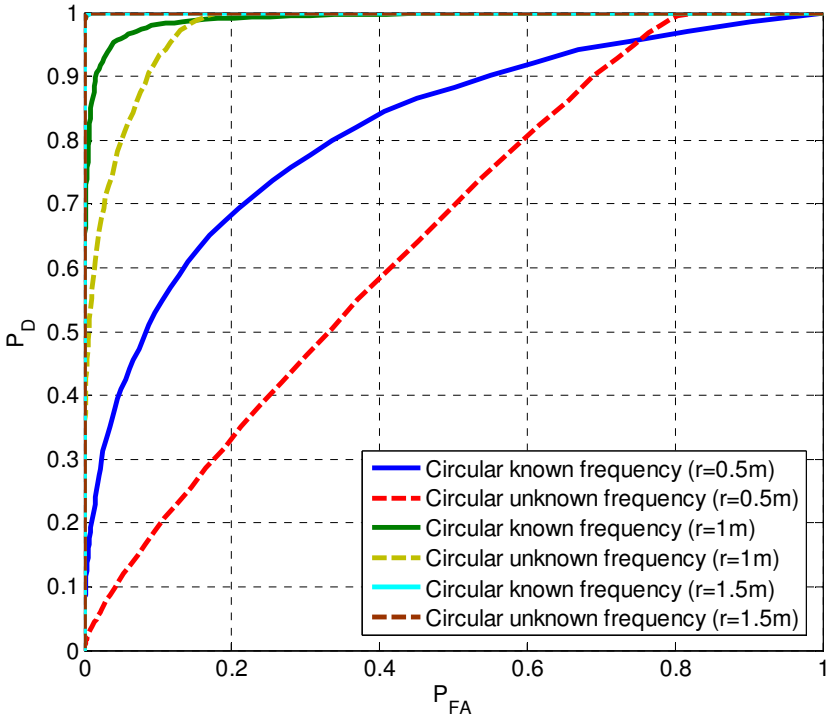


Figure 6-7 ROC for a circular trajectory detector at different motion radius values

6.5 Real Data Collection and Processing

A real data collection was performed to verify the proper operation of the proposed PVT authentication method. Due to frequency regulations, signal transmission in the GPS band is prohibited. Therefore, an indoor transmission and reception scenario was

considered in order to simulate the range variations between spoofing source and the user. The setup is shown in Figure 6-8 where the received authentic GPS signals have been amplified and then retransmitted inside a navigation laboratory. The retransmitted signals were received through a NovAtel 702 GG antenna connected to a NI (National Instruments) PXIe-1065 RF sampling front-end. The sampling frequency is 5 Msps and the data was processed with GSNRx^{TM} (Petovello et al 2008). As shown in Figure 6-8 another version of rooftop signal was directly fed to the NI front-end in order to enable a comparison between static and moving antenna signals. The NI front-end was fed by an external clock source provided by a Morion MV-89 A03 OCXO oscillator whose short term frequency stability is on the order of 2×10^{-12} at 1 s.

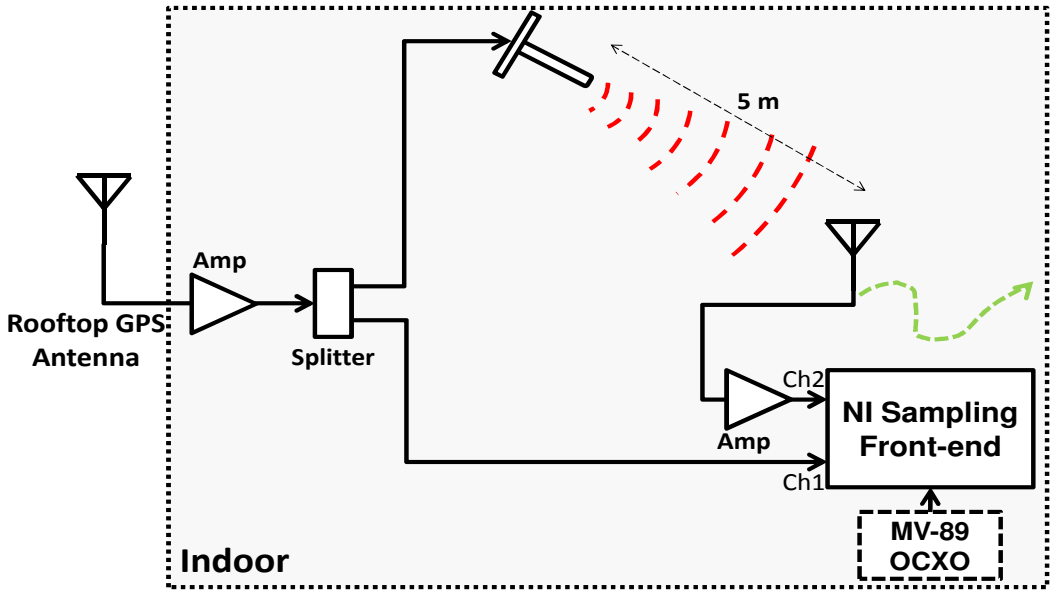


Figure 6-8 Data collection setup

Data collections were performed for different motion scenarios experienced by the indoor GPS antenna. It should be noted that the clock source of the receiver did not move in any

of the test scenarios and the antenna orientation has been constant with respect to the spoofing source in order to avoid antenna phase wrap-up due its motion. Three motion scenarios was considered as "*circular table motion*", "*circular handheld motion*" and "*arbitrary motion*". The first scenario takes advantage of a circular motion table that rotates the receiver antenna at the constant rate of ω_0=0.62 rad/s. The radius of the circle was 108 cm. The second scenario, which is more realistic, considers a semi-circular motion performed by a user. The radius of this motion was 30 cm and the approximate rotation rate ω_0=1.6 rad/s. Figure 6-9 illustrates the circular handheld motion of the receiver's antenna for this data collection scenario. Finally, the third motion scenario is an arbitrary movement which consists of different motion types such as circular motion with different frequencies and radiuses and also a random walk movement. For all of the above discussed motion scenarios, the receiver stays static during the first minute and then moves for two minutes. The static interval is used to extract the clock model parameters for linear and unknown trajectory detectors. However, for the case of circular and random walk trajectory detectors, the information of static phase was not used.

Figure 6-10 shows the receiver clock bias deviation from its linear short term model for the case of a static receiver as well as a receiver rotating on the circular motion table. It is observed that the receiver circular motion causes sinusoidal variations in the clock bias, which is different from its expected linear model. Table 6-1 compares the values of different detection tests for this type of motion. Since the order of the test statistics is

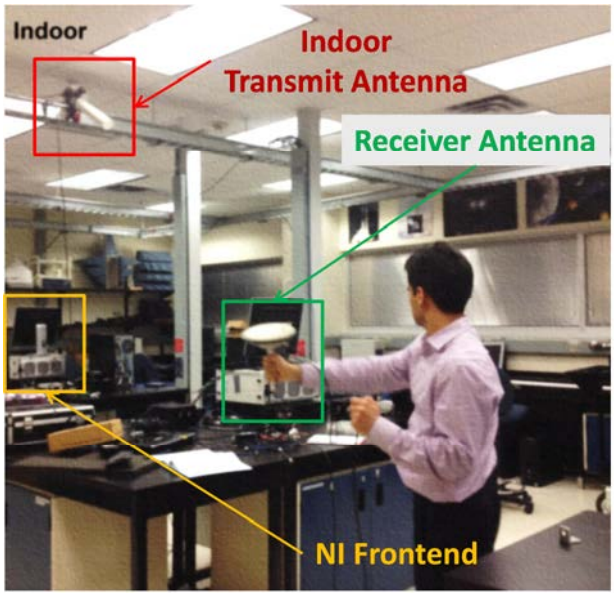


Figure 6-9 Circular handheld motion of the receiver antenna

different for different tests, the ratio of $T(\mathbf{x}|H_1)/T(\mathbf{x}|H_0)$ was compared. Herein, $T(\mathbf{x}|H_0)$ is calculated based on the observations from Channel 1 of NI frontend that belongs to the rooftop authentic signals set. As expected the detector type (ii) has the best performance among other detectors. After that, the random walk trajectory detector, type (iii), provides the second best discrimination. It is observed that neither detector type (iv) nor detector type (v) can provide an acceptable detection performance since their estimate of clock bias is not accurate enough.

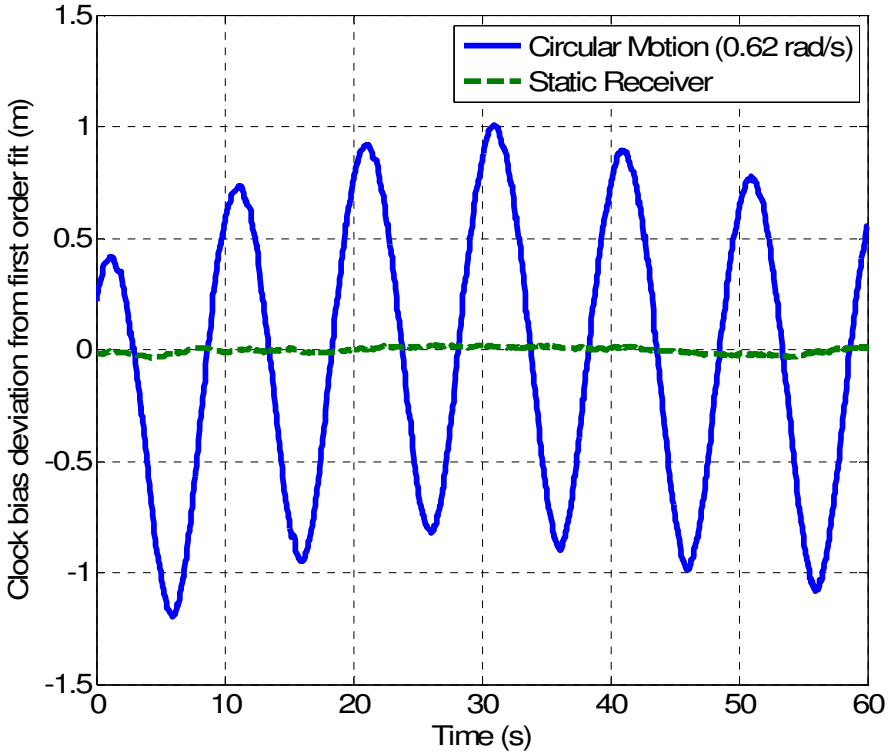


Figure 6-10 Clock bias deviation from its linear model for a static and circularly rotating receiver antenna using a circular motion table

Table 6-1 Comparison of T(x|H1)/T(x|H0) ratio for different receiver motion scenarios

	Circular Motion Detector Type (ii)	Random Walk Motion Detector Type(iii)	Linear Motion Detector Type(iv)	Unknown Motion Detector Type (v)
Circular Table	3.75×10^{4}	2.4×10^{3}	1.21	1.21
Circular Handheld	8.23×10^{3}	44.4	5.8	6.03
Random Trajectory	5.39	11.8	0.45	0.55

Figure 6-11 compares the clock bias deviation from its linear model for a handheld circularly rotating antenna in the presence of indoor spoofing signals and outdoor authentic signals. It is observed that for the case of a spoofed receiver the clock state of the PVT solution shows clearly observable sinusoidal deviation from its linear model due to the circular motion of the antenna. However, in the presence of an authentic position solution, the deviation of clock state from its linear model is negligible. As shown in Table 6-1, the detector type (ii) still achieves the best discrimination among all other detectors.

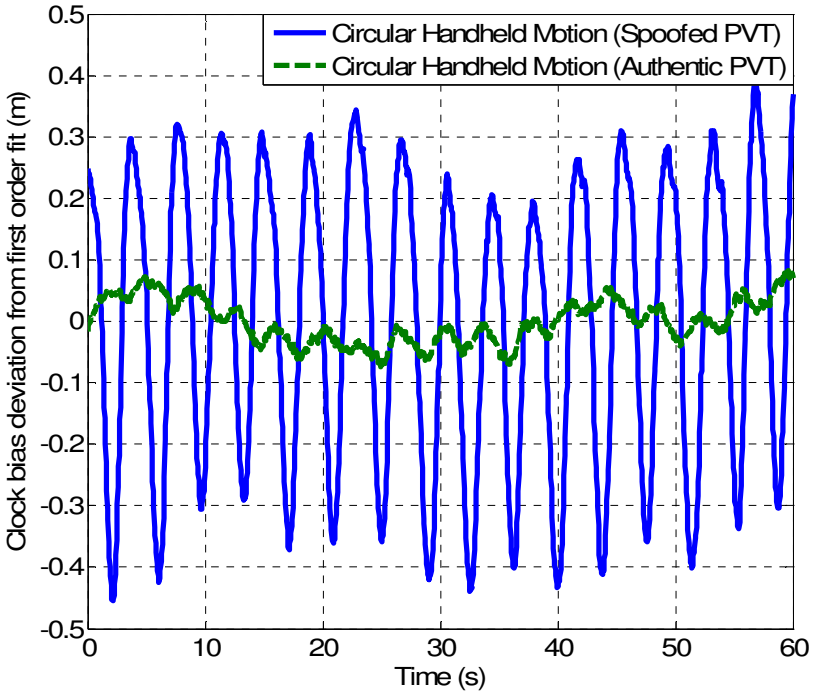


Figure 6-11 Clock bias deviation from its linear model for a handheld circularly rotating receiver antenna in presence of spoofing and authentic GPS signals

Figure 6-12 shows the clock state deviation from its linear model for the both cases of a randomly moving receiver antenna and a static antenna. Herein, the reference clock is the

internal oscillator of the NI front-end. The green plot shows that the receiver's clock fluctuates for ±0.2 m around its expected model under H_0 hypothesis.

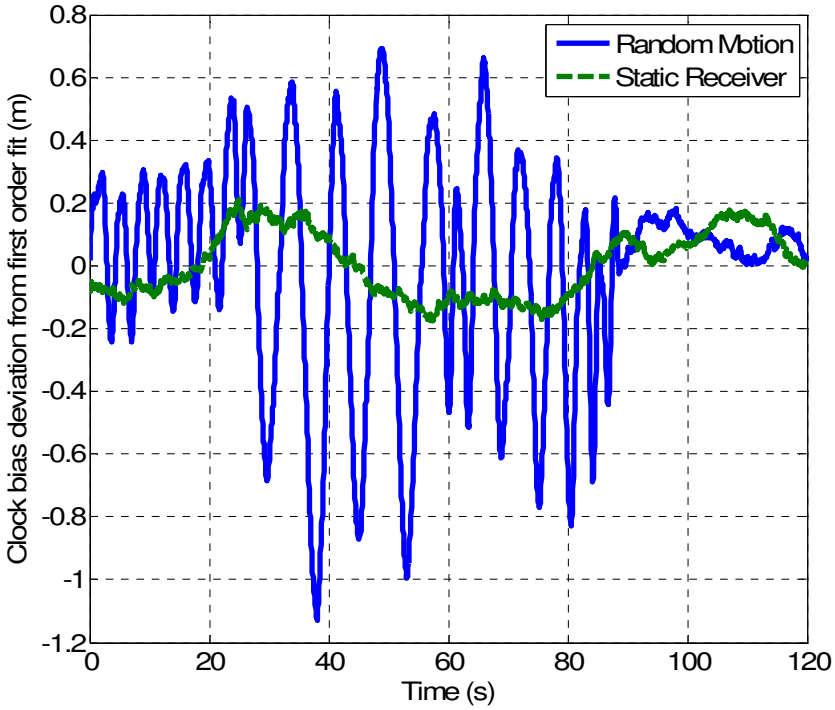


Figure 6-12 Clock bias deviation from its linear model for a static and randomly moving receiver antenna

It is observed that the clock bias deviation from its linear model is much more considerable for the case of randomly moving receiver compared to the static receiver. Based on the information provided in Table 6-1, it is observed that the detector type (iii) achieves the best detection performance among all the other detectors. Due to the presence of some sinusoidal variations in the receiver clock state, the detector type (ii) also is able to detect the existence of the counterfeit PVT solution.

Figure 6-13 shows the clock bias deviation from its linear model for three types of oscillators in the presence of a handheld circular motion. The dashed blue plot belongs to

the DFA S1-LHZ 10.000 MHz B0.5 TCXO whose stability is much lower than that of the Morion MV-89 A03 OCXO shown in solid green. The red dotted line corresponds to the internal oscillator of the SiGe V3 front-end, which is a low-end sampling equipment whose internal oscillator is of comparable quality to those of handheld GPS receivers. It is observed that although the MV-89 OCXO provides a much higher stability compared to that of the other two oscillators, noticeable sinusoidal fluctuations due to the circular motion of the antenna are modulated on the receiver clock state variations as seen in Figure 6-13. Therefore, the detector type (ii) is still able to detect the presence of sinusoidal variations in the clock state.

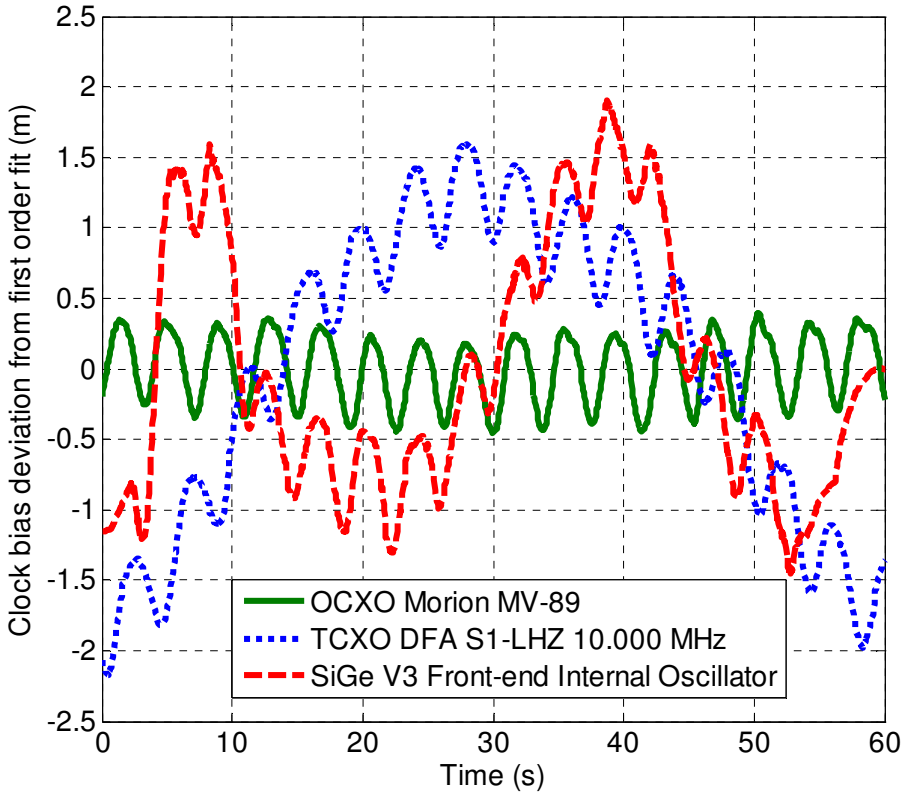


Figure 6-13 Clock bias deviation from its linear model for a circularly rotating handheld antenna in the presence of different oscillators

Table 6-2 provides a comparison of the ratio $T(\mathbf{x}|H_1)/T(\mathbf{x}|H_0)$ for a handheld circularly rotating antenna in the presence of different clock sources. Herein, the $T(\mathbf{x}|H_1)$ refers to the case where the antenna is moving and $T(\mathbf{x}|H_0)$ refers to the case of a static receiver antenna. This table also shows information regarding the short term stability of the clocks (i.e. Allan deviation at 1s) which is reported in the oscillator datasheets. It is observed that in the presence of high quality OCXO clocks, the detection performance of the detector type (ii) is much higher than its performance with TCXOs. In other words, the ratio of $T(\mathbf{x}|H_1)/T(\mathbf{x}|H_0)$ is highly dependent on the short term stability of the clock and a more stable clock leads to a higher detection performance. However, as it is observed in this table, for the case of less stable clocks such as TCXOs or the SiGe internal oscillator, the detection performance is still acceptable. For instance, for the case of the SiGe portable front-end, the test statistic under the H_1 hypothesis is 12 times larger than the value of this parameter under the H_0 hypothesis.

Table 6-2 Comparison of $T(\mathbf{x}|H_1)/T(\mathbf{x}|H_0)$ ratio for different oscillators for the handheld circular motion scenario

Oscillator Type	Short Term Frequency Stability @ 1s	$T(\mathbf{x}\|H_1)/T(\mathbf{x}\|H_0)$
OCXO MV89 - A03 E	2×10^{-12}	8.23×10^{3}
OCXO VS - AV5	$< 5 \times 10^{-10}$	1.45×10^{3}
OCXO 8626 - AV5S	$< 5 \times 10^{-11}$	2.24×10^{3}
OCXO 8712 - ASH	$< 5 \times 10^{-11}$	4.73×10^{3}
TCXO DFA S1 – LHZ	Not Available	211
SiGe V3 internal Osc.	Not Available	12

6.6 Summary

A position layer PVT authentication technique was proposed based on the analysis of the clock state variations of a moving receiver in order to verify solution validity. This technique is based on the fact that most spoofing generators transmit counterfeit signals from a single source transmitter whereas authentic PRNs are received from different satellites. Several detection tests have been proposed for different motion scenarios. Some of the proposed test methods simultaneously estimate the clock model parameters and authenticate the PVT solution based on the assumption of circular or random walk motion of the receiver. The other proposed techniques rely on the initial estimate of the receiver clock model parameters and require a static learning phase before moving the receiver. The simulation and real data processing results show that the proposed method can effectively detect the presence of counterfeit position solution. The performance of the proposed techniques has been verified by several practical tests in the presence of different oscillators with different stability features. The proposed methods can be employed as low-cost feasible solution as and at the same time very effective authentication techniques for handheld GNSS receivers without requiring any hardware modifications to legacy GNSS receivers.

Chapter Seven: Conclusions and Recommendations

Considering the different analyses and detection approaches described in this thesis, it can be concluded that conventional GPS receivers are quite vulnerable to structural interference signals such as spoofing and meaconing. The effect of spoofing signals at different processing stages of a GPS receiver has been analysed and it was shown that a GPS receiver can be easily misled by malicious spoofing signals. However, based on the theoretical and practical analyses provided in different chapters of this thesis, it was shown that with modest modifications of the firmware or software of commercial GPS receivers, their vulnerability to structural interference signals can be substantially reduced.

This chapter provides some concluding remarks as well as recommendations for further research in the field of spoofing countermeasure. Based on the material previously proposed in this thesis, Section 7-1 provides a possible structure for a spoofing aware GPS receiver in which the authenticity of received signals is verified in different processing stages. Section 7-2 presents some possibilities and recommendations for future research toward structural interference counter-measures.

7.1 Spoofing Aware GPS Receiver

Summing up the discussions provided in previous chapters of this thesis, this section provides a potential structure for a spoofing aware stand-alone GPS receiver which takes advantage of previously proposed spoofing countermeasure techniques in order to check the authenticity of received signals at different processing stages. The proposed

authenticity verification techniques operate on digital domain samples; therefore, they are compatible with different hardware configurations of conventional GPS receivers. It is assumed that this receiver does not benefit from additional positioning/navigation sensors and its GNSS signal reception capability is limited to GPS L1 C/A signals. Figure 7-1 illustrates a simplified block diagram of this receiver wherein different stages of received signal authenticity verification have been shown in green rectangles. The stages are described in the figure.

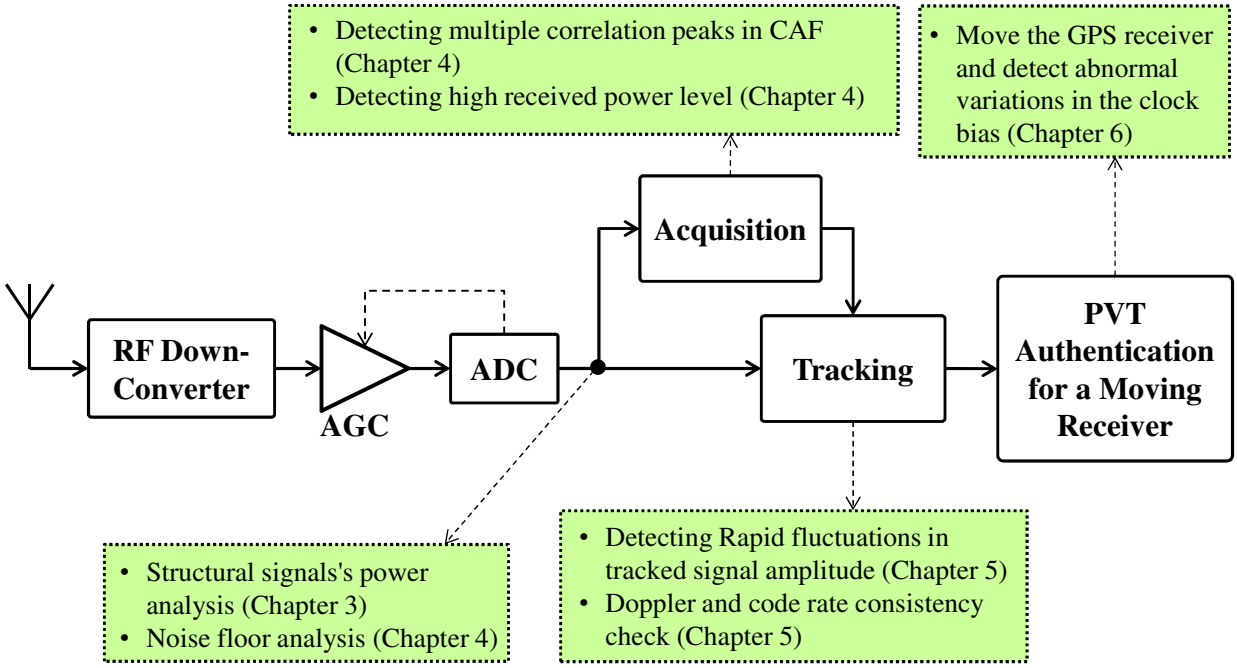


Figure 7-1 Possible structure for a spoofing aware GPS receiver

7.1.1 Pre-despreading Authenticity Verification

Spoofing signals increase the power content of structural signals in GNSS frequency bands. As such, some signal quality measurement methods can be applied to the received GNSS signals to verify their authenticity before the de-spreading process. Two methods have been proposed in this dissertation, namely

- **Structural signals' power analysis:** Based on the discussions provided in Chapter 3, a spoofing aware receiver can detect the presence of the additional power injected by counterfeit GNSS signals by taking advantage of their cyclostationary feature. The proposed method operates on received digital samples and does not require additional knowledge of the AGC gain. The computational complexity of this technique is very low since it does not require acquisition/tracking of individual GPS PRN signals. This technique can effectively discriminate a spoofing attack especially when the total spoofing power (TSP) is comparable to total power of authentic signals.

- **Noise floor Analysis:** Based on the analyses provided in Chapter 4, the presence of higher power spoofing signals can elevate the target receiver's noise floor due to the cross-correlation of spoofing PRN signals with locally generated PRNs. Therefore, a spoofing aware GNSS receiver can continually monitor the received noise floor and flag any abnormal noise floor increase as a sign of the presence of spoofing signals. The application of this method becomes limited for the case that the input AGC block changes the received signal gain in order to maximize the bit efficiency of receiver's quantizer. In this case, an unknown AGC gain is applied to the input signals and directly affects the noise floor estimate.

7.1.2 Acquisition Stage Authenticity Verification

A spoofing aware GNSS receiver can detect the presence of counterfeit signals during the signal acquisition stage. Based on the material presented in Chapter 4, a receiver can

apply the following techniques toward detecting the presence of spoofing signals during acquisition:

- **Detecting the presence of multiple correlation peaks in CAF:** As discussed in Chapter 4, spoofing signals might lead to the generation of additional correlation peaks in the search space during acquisition. As such, a spoofing aware GPS receiver should search over the entire CAF in order to find all of the correlation peaks above the detection threshold. The presence of multiple correlation peaks corresponding to the same PRN index can reveal the presence of a spoofing attack. These correlation peaks can be classified as authentic or spoofing in further processing stages of the receiver.
- **Detecting the presence of an abnormally high received power level:** As discussed in Chapter 4, it is very difficult for a spoofer to present its target receiver with an accurate power level which is slightly higher than that of the authentic signals, in order to effectively mislead the receiver and at the same time avoid being detected by power monitoring techniques. Therefore, based on the analyses provided in Chapter 4, a spoofing aware GPS receiver should discard a signal whose SNR (or absolute received power) is considerably higher than that of a typical authentic GPS signal. Compared to the SNR based spoofing discrimination techniques, absolute power monitoring methods considerably reduces the vulnerability region of that receiver against spoofing signals. However, the application of this technique might require some modifications in the hardware structure of commercial GNSS receivers.

7.1.3 Tracking Stage Authenticity Verification

An accurately designed spoofing attack can target a GNSS receiver which is already locked into tracking the authentic signals. Such a spoofing attack can be detected using the following techniques:

- **Detecting the presence of rapid fluctuations in the received signal amplitude:** A spoofing signal whose Doppler and code rate are consistent can target the tracking process of a GNSS receiver by aligning its code delay and Doppler frequency to those of the authentic GNSS signal. In this case the spoofing signals do not generate multiple correlation peaks in the CAF; however, as analyzed in Chapter 5, the interaction between authentic and spoofing signals can lead to rapid fluctuations of the correlator output. A spoofing aware GPS receiver can continuously monitor the distribution of correlator output and detect abnormal amplitude distributions due to the interaction between authentic and spoofing signals.

- **Detecting an inconsistency between the estimated Doppler and code rate:** To avoid the previously discussed signal amplitude fluctuations, a spoofer might change its code delay while it has locked its Doppler signal to that of the authentic signal. In this case the Doppler and code rate of spoofing signals are no longer consistent. Therefore, based on the discussions of Chapter 5, a spoofing aware GPS receiver can continuously check the consistency between code rate and Doppler frequency of received signals and detect the presence of a spoofing attack upon observing an inconsistency between these two parameters.

7.1.4 Position Level Authenticity Verification for a Moving Receiver

The relative motion between target receiver and the spoofing source can equally change the propagation distance for different spoofing PRNs. Based on the discussions provided in Chapter 6, this common distance variation appears in the clock state of receiver's PVT solution and can reveal the presence of a spoofed position/timing solution. A moving receiver is able to authenticate its PVT solution based on monitoring the clock bias deviation from its expected model. Although the performance of this detection technique depends on the clock stability and the accuracy of the receiver motion modeling, it can be employed as a powerful authenticity verification technique for spoofing aware handheld GNSS receivers.

7.1.5 Analysis of TEXBAT Datasets

Using the above discussed spoofing aware receiver structure, TEXBAT datasets have been processed as a case study in order to show the effectiveness of proposed multi-stage authenticity verification approach. The detection results have been shown in Table 7-1. Herein, the "S1: switched spoofing", "S2: static overpowered", "S3: Static matched power (1.3 dB spoofing power advantage)" and "S4: static matched power (0.4 dB spoofing power advantage)" represent different spoofing scenarios previously introduced in Chapter 3. The word "Yes" indicates the ability of corresponding spoofing detection technique to discriminate the presence of spoofing signals while "No" indicates that the corresponding technique is not able to discriminate spoofing signals. "N/A" shows that the corresponding spoofing detection technique is not applicable to that dataset.

Table 7-1 Performance of proposed spoofing aware GPS receiver on TEXBAT data

	Detection Technique	S1	S2	S3	S4
Pre-Despreading	Structural signals power analysis	No	Yes	Yes	Yes
	Noise floor analysis	Yes	Yes	No	No
Acquisition	Detecting multiple correlation peaks	No	No	Yes[1]	Yes[1]
	Detecting high received power level	No	Yes	No	No
Tracking	Rapid fluctuations in tracked signal amplitude	No	Yes	No	No
	Doppler and code rate consistency check	No	No	Yes	Yes
	Position level authenticity verification	N/A	N/A	N/A	N/A

[1] The CAF has been evaluated once spoofing and authentic peaks have separated from each other

Based on the information provided in Table 7-1, it can be observed that the presence of a spoofing attack can be detected by one or several of the proposed authenticity verification techniques. More specifically, it can be mentioned that the "Structural signals power analysis" method is able to discriminate those spoofing scenarios in which the spoofing signal's power is added to the existing authentic signal's power. However, for the case of switched spoofing attack, this technique is not very helpful since in this scenario, the spoofing signals replace the authentic ones. The "Noise floor analysis" method is only able to detect those spoofing scenarios in which the variance of the input signal is highly affected. For example, for the case of a switched spoofing attack, the noise floor estimate

suddenly decreases because the authentic signals are replaced by low noise spoofing signals while for the case of an overpowered spoofing attack, the noise estimate experiences a sudden increase because the higher power spoofing signals are added to the current authentic signal set.

Those spoofing scenarios that generate distinct fake correlation peaks in the CAF can be detected using the acquisition level authenticity verification techniques. For example, the S3 and S4 scenarios are detectable once spoofing and authentic correlation peaks have been separated. The switched spoofing attack (S1) is not detectable because the authentic signals have been removed. The overpowered spoofing attack (S2) can be detected by the "received power analysis" technique which is looking for abnormally higher power correlation peaks in the CAF.

Tracking level spoofing detection methods are able to detect different types of interaction between authentic and spoofing signals during a spoofing attack. It is observed that the spoofing attacks with consistent Doppler and code rate, namely Scenario S2, are detected based on the fluctuations in the correlator output amplitude. However, the locked Doppler methods are detectable using the consistency check between Doppler and code rate of each PRN.

The position level authenticity verification method is not applicable to TEXBAT spoofing scenarios, since this technique requires receiver motion under a single antenna spoofing attack.

7.2 Recommendations

This section discusses some recommendations that can be considered for the future research in the field of spoofing and meaconing countermeasure.

7.2.1 Spoofing Mitigation

The main focus of this thesis was on the vulnerability assessment of GNSS receivers to structural interference signals and the authenticity verification of received GNSS signals. The next step of research could concentrate on neutralizing the harmful effect of spoofing/meaconing signals once they are detected by the previously proposed methods. Using spoofing mitigation techniques, a GPS receiver can retrieve its positioning capability even in presence of counterfeit spoofing signals. Two possible approaches for spoofing mitigation can be listed as vestigial signal detection and spatial null steering toward spoofing source using antenna array processing techniques.

7.2.2 Spoofing Countermeasure in Multipath Environments

Most of the analyses performed in this research focused on line of sight reception models for spoofing and authentic signals. However, in real-world scenarios, GNSS receivers are usually subject to multipath reflections that should be taken into account in the design and development of spoofing countermeasure techniques. Future research could focus on the statistical analysis of structural interference signals in multipath environments toward the design and development of multipath-aware spoofing countermeasure techniques. The proposed methods should be able to discriminate between additional correlation peaks generated by spoofing signals from those caused by multipath reflections. Furthermore, for the case of position level countermeasure techniques it should be noted that multipath

reflections in urban canyons can cause rapid fluctuations in the pseudorange observables that might highly affect the accuracy and precision of the extracted PVT solution.

7.2.3 Spoofing Countermeasure at Higher Integration Times

Most of the analyses and countermeasure methods provided in this thesis was based on 1 ms coherent integration time. However, future research could focus on analysis and development of spoofing detection and mitigation techniques at higher integration times. Increasing the integration time can decrease the level of cross correlation terms caused by higher power spoofing PRNs and this can increase the chance of detecting the authentic correlation peaks that might be buried under the noise floor. In addition, a higher coherent integration time can reduce the bandwidth of receiver tracking loops that consequently reduces the vulnerability region of a tracking receiver against malicious spoofing and meaconing signals.

7.2.4 Multi-Constellation/Multi-Frequency Authenticity Verification

The analyses provided in this thesis were limited to the case of GPS L1 C/A signals only. However, since many of the commercially available GNSS receivers are capable of receiving multiple GNSS signals from different constellations and frequencies, future research can take advantage of the features of different GNSS signals for spoofing/meaconing countermeasures. This approach could be very effective since generating a consistent spoofing attack for multiple GNSS signals at different frequency bands imposes much more complexity on the spoofing source and this might not be affordable for low cost spoofers.

7.2.5 Multi Sensor Consistency Analysis

This research has been considering a stand-alone GPS L1 receiver which does not have access to any external aiding from other sensors. Future research could be extended to take advantage of other navigation sensors that are now commercially available at a very low cost. For example, a typical smart phone, in addition to a high sensitivity GPS receiver, is equipped with several sensors such as 3D accelerometers, gyroscopes, barometers and digital compass; these sensors are not affected by RF spoofing. Therefore, the authenticity of the position/navigation solution of their on-board GPS receiver can be cross-checked with the information coming from other sensors. In addition, a GPS receiver can cross-check its PVT solution with other solutions provided by Wi-Fi access points or cellular base stations. Although these solutions are not very accurate, they can be still used to reveal large position biases generated by a spoofing source.

7.2.6 Antenna Array Processing

Spoofing signals try to simulate different temporal and spectral features of authentic GNSS signals. However, due to logistical limitations, a spoofer usually employs a single antenna to transmit several counterfeit PRN signals. As such, spatial processing in the form of antenna array processing can be considered as one of the most powerful spoofing countermeasure approaches that can detect the spatial coherency of spoofing PRN signals. A well designed antenna array can detect the spatial signature of a spoofing source and spatially null out these signals and reduce or eliminate the elevated noise floor caused by their cross correlation effect. Furthermore, a calibrated antenna array can

enhance the received power of authentic signals after spatially discarding the spoofing signals.

7.2.7 Network Based Authenticity Verification

A spoofer is a terrestrial wireless transmitter which can potentially misdirect many GNSS receivers within its coverage area. As such, a network based approach can be considered to verify the authenticity of received GNSS signals within a certain region. In this approach, different communication enabled GNSS receivers can transmit some of their local measurements such as received PRN numbers and their corresponding C/N_0, GPS time, position solution, the auxiliary sensors' measurements, or even a short snapshot of raw samples to a central base station and inquire about the authenticity of their received signal. The base station can put together several observations and take advantage of different processing methods in order to find-out whether or not a user's observation is authentic. For example, based on the analyses provided in Chapter 6, all of the receivers inside the coverage zone of a single antenna spoofing source extract the same position solution since they receive the same counterfeit GNSS signal set with different delays. Therefore, once the base station observes that many receivers extract the same position solution at the same time, it would suspect to the presence of a spoofing source.

The concept of network based authenticity verification can turn into a standard validation procedure for future communication enabled GNSS receivers such as those in cell phones. This technique does not impose the implementation of any spoofing countermeasure techniques on a GNSS receiver. It only requires the ability of transmitting and receiving a limited amount of data to/from a central processing unit, this

data transfer feature being now available for many GNSS equipped systems such as cell phone, vehicles, etc.

References

Akos, D. M. (2012) "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)," in *Jounral of Navigation*, vol. 59, No. 4, Winter, Institute of Navigation, pp. 281-290

Borio, D. (2008) *A Statistical Theory for GNSS Signal Acquisition*, Doctoral Thesis, Dipartimento di Elettronica, Politecnico di Torino, Italy.

Borio, D. (2013) "PANOVA Tests and their Application to GNSS Spoofing Detection," in *IEEE Transactions on Aerospace and Electronic Systems,* vol. 49, no. 1, January, pp. 381-394

Borio, D., S. Savasta, and L. Lo Presti (2006) "On the DVB-T coexistence with Galileo and GPS systems," in *Proceedings of the 3rd ESA Workshop on Satellite Navigation User Equipment Technologies (NAVITEC'06)*, Dec. 11-13, Noordwijk, Netherlands

Broumandan, A., A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen, and G. Lachapelle (2012) "GNSS Spoofing Detection in Handheld Receivers Based on Signal Spatial Correlation," in *Proceedings of IEEE/ION PLANS 2012*, April 24-26, Myrtle Beach, South Carolina , pp. 479-487

Cavaleri, A., B. Motella, M. Pini, and M. Fantino (2010) "Detection of Spoofed GPS Signals at Code and Carrier Tracking Level," in *Proceedings of Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Dec 8-10, Noordwijk, Netherlands, pp.1-6

Chen, X., C. Harpes, G. Lenzini, M. Martins, S. Mauw, and J. Pang (2012) "Implementation and validation of a Localisation Assurance service provider," in *6th ESA Workshop on Satellite Navigation Technologies and GNSS Signals and Signal Processing (NAVITEC)*, Dec. 5-7, Noordwijk, Netherlands, pp. 1-8

Crosta, P., and T. Alenia (2009) "A Novel Approach to the Performance Evaluation of an Arctangent Discriminator for Phase Locked Loop and application to the carrier tracking of the Ionospheric Scintillation,"in *Proceedings of European Navigation Conference - GNSS 2009*, 3 - 6 May, Naples, Italy, 10 pages

Daneshmand, S. (2013) *GNSS Interference Mitigation Using Antenna Array Processing*, PhD Thesis, Report No. 20376, Department of Geomatics Engineering, University of Calgary

Daneshmand, S., A. Broumandan and G. Lachapelle (2011b) "GNSS Interference and Multipath Suppression Using Array Antenna," *in Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011)*, 20-23 September, Portland, OR, pp. 1183-1192

Daneshmand, S., A. Jafarnia-Jahromi, A. Broumandan and G. Lachapelle (2012) "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array" *in Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, 17-21 September, Nashville TN, 11 pages

Daneshmand, S., A. Jafarnia-Jahromi, A. Broumandan and G. Lachapelle (2011a) "A Low Complexity GNSS Spoofing Mitigation Technique Using a Double Antenna Array" *GPS World magazine*, December, vol 22, no 12, pp. 44-46

Dehghanian, V., J. Nielsen, and G. Lachapelle (2012) "GNSS Spoofing Detection Based on Receiver C/No Estimates," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, September 17-21, Nashville, TN, pp. 2878-2884

Dehghanian, V., J. Nielsen, and G. Lachapelle (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)*, September 17-21, Nashville, TN, pp. 2878 – 2884

Grabowski, J. C. (2012) "Personal Privacy Jammers," in *GPS World*, April, pp. 28-37

Guo, Y., M. Fan, and M. Kong (2012) "Spoofing interference suppression using space-time process for GNSS receiver," in *5th International Congress on Image and Signal Processing (CISP),*Oct 16-18, Sichuan, China, pp. 1537-1541

Hartman, R. G. (1996) "Spoofing Detection System for a Satellite Positioning System" US Patent 5557284, 13 pages

Hein, G.W., F. Kneissl, J.A. Avila-Rodriguez, and S. Wallner (2007) "Authenticating GNSS Proofs against Spoofs [Part-2]," in *Inside GNSS journal*, Sept./Oct., pp. 71-78

Hornbostel, A., M. Cuntz, A. Konovaltsev, G. Kappen, C. Hättich, C. A. Mendes da Costa, and M. Meurer (2013) "Detection and suppression of PPD-jammers and spoofers with a GNSS multi-antenna receiver Experimental analysis" in *Proceedings of the European Navigation Conference* (*ENC2013),* Apr 23-25, Vienna, Austria

Humphreys, T. E., B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner (2008) "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer,"in *Proceedings of ION GNSS 21st. International Technical Meeting of the Satellite Division*, September 16-19, Savannah, GA, pp. 2314-2325

Humphreys, T. E., J. Bhatti, D. Shepard, K. Wesson (2012) "The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, September 17-21, Nashville, TN, pp. 3569-3583

IS-GPS-200G (2012) *Global Positioning System Directorate, Systems Enginerring & Integration, Interface Specification*, Navstar GPS Space Segment/Navigation User Interfaces Rev G

IS-GPS-200G (2012) *Global Positioning System Directorate, Systems Enginerring & Integration, Interface Specification*, Navstar GPS Space Segment L5 Interfaces, Rev C

Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen and G. Lachapelle (2012c) "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques" in the

International Journal of Navigation and Observation, Hindawi Publishing Corporation, vol 2012, 16 pages

Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen and G. Lachapelle (2012a) "GPS Spoofer Countermeasure Effectiveness based on Using Signal Strength, Noise Power and C/N0 Observables" in *International Journal of Satellite Communications and Networking*, July, vol 30, no 4, pp. 181–191

Jafarnia-Jahromi, A., T. Lin, A. Broumandan, J. Nielsen and G. Lachapelle (2012b) "Detection and Mitigation of Spoofing Attacks on a Vector Based Tracking GPS Receiver," *Proceedings of International Technical Meeting of the Institute of Navigation (ION ITM 2012)*, 30 January-1 February, Newport Beach, CA, pp. 790-800

Juang, J. C. (2009) "Analysis of global navigation satellite system position deviation under spoofing," in *IET Radar, Sonar & Navigation* vol.3, No. 1, February, pp. 1-7

Jun, C. X., C. K. Jin, X. J. Ningand, and L. Bao (2009) "Analysis on Forgery Patterns for GPS Civil Spoofing Signals," in *Proceedings of 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*, Nov. 24-26, Seoul, Korea, pp. 353–356

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

Kay, S. (1993) *Fundamentals of Statistical Signal Processing Vol. I Estimation Theory*, Prentice Hall signal processing series.

Kay, S. (1998) *Fundamentals of Statistical Signal Processing Vol. II Detection Theory*, Pearson Education.

Kim, T. H., C. S. Sin, and S. Lee (2012) "Analysis of effect of spoofing signal in GPS receiver," in *12th International Conference on Control, Automation and Systems (ICCAS),* Oct. 17-21, Jeju, Korea, pp. 2083-2087.

Konovaltsev, A., M. Cuntz, C. Haettich, and M. Meurer (2013) "Performance Analysis of Joint Multi-Antenna Spoofing Detection and Attitude Estimation," in *Proceedings of the 2013 International Technical Meeting of The Institute of Navigation*, Jan. 29 – 27, San Diego, CA, pp. 864-872

Ledvina, B. M., W. J. Bencze, B. Galusha, and I. Miller (2010) "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers," in *Proceedings of the 2010 International Technical Meeting of The Institute of Navigation*, January 25 - 27, San Diego, CA, 2010, pp. 698-712

Lo, S.C., and P.K. Enge (2010) "Authenticating Aviation Augmentation System Broadcasts," in *Proceedings of Position Location and Navigation Symposium (PLANS)*, May 4-6, Indian Wells, CA, pp.708-717

Lo, S.C., D.D. Lorenzo, P. Enge, D. Akos, and P. Bradley (2009) "Signal Authentication: A secure Civil GNSS for Today," in *Inside GNSS journal*, Sept./Oct, pp. 30–39

McDowell, C.E. (2007) "GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling" US Patent 7250903 B1, 7 pages

Meurer, M., A. Konovaltsev, M. Cuntz, C. Hättich (2012) "Robust Joint Multi-Antenna Spoofing Detection and Attitude Estimation using Direction Assisted Multiple Hypotheses RAIM," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, September 17-21, Nashville, TN, pp. 3007-3016

Misra, P., and P. Enge (2006) *Global Positioning System: Signals, Measurments, and Performance*, Ganga-Jamuna Press, 2nd Edition

Mitch, R. H., R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, B. W. Bhatti, and T. E. Humphreys (2011) "Signal characteristics of civil GPS jammers," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION/GNSS)*, September 20-23, Portland, OR, pp. 1907-1919

Montgomery, P.Y., T.E. Humphreys, and B.M. Ledvina (2009) "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil GPS Spoofer" in *Proceedings of ION ITM 2009*, Jan 26-28, Anaheim, CA, pp. 124-130

Moshavi, S. (1996) "Multi-user detection for DS-CDMA communications," in *IEEE Communications Magazine*, vol.34, no.10, October, pp.124-136

Motella, B., M. Pini, M. Fantino, P. Mulassano, M. Nicola, J. Fortuny-Guasch, M. Wildemeersch, and D. Symeonidis (2010) "Performance assessment of low cost GPS receivers under civilian spoofing attacks," in *5th ESA Workshop on Satellite Navigation*

Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Dec 8-10, Noordwijk, Netherlands , pp. 1-8

Niedermeier, H., H. Beckmann, and B. Eissfeller (2012) "Robust, Secure and Precise Vehicle Navigation System for Harsh GNSS Signal Conditions," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, September 17-21, Nashville, TN, pp. 1589-1600

Niedermeier, H., H. Beckmann, B. Eissfeller, O. Pozzobon, R. Grzeszczyk, and T. Przybyla (2010) "Detection and Mitigation of GNSS Deception by Combination of Odometric Dead Reckoning and GNSS Observations for Vehicles," in *Proceedings of the 23rd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2010)*, September 21-24, Portland, OR, pp. 1145-1156

Nielsen, J., A. Broumandan, and G. Lachapelle (2011) "GNSS Spoofing Detection for Single Antenna Handheld Receivers" in *Journal of Navigation*, vol 58, no 4, Winter, pp. 335-344

Nielsen, J., G. Lachapelle, and A. Broumandan (2010) Method and System for Detecting GNSS Spoofing Signals. U.S. Patent No. 7,952,519 B1

Nielsen, J., V. Dehghanian and G. Lachapelle (2012) "Effectiveness of GNSS Spoofing Countermeasure based on Receiver CNR Measurements" in *International Journal of Navigation and Observations*, vol. 2012, Article ID 501679, 9 pages.

Nighswander, T., B. Ledvina, J. Diamond, R. Brumley, D. Brumley (2012) "GPS Software Attacks" in *Proceedings of the 2012 ACM conference on computer and communications security (CCS 12)*, Oct 16-18, New York, NY, pp. 450-461.

O' Hanlon, B.W., M. L. Psiaki, T. E. Humphreys, and J. A. Bhatti (2010) "Real-Time Spoofing Detection in a Narrow-Band Civil GPS Receiver," in *Proceedings of the 23rd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2010)*, September 21-24, Portland, OR, pp. 2211-2220

O' Hanlon, B. W., M. L. Psiaki, T. E. Humphreys, and J. A. Bhatti (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)*, September 17-21, Nashville, TN, pp. 3584-3590

O'Driscoll, C. (2007), *Performance Analysis of the Parallel Acquisition of Weak GPS Signals,* Ph.D. Thesis, Department of Electrical and Electronic Engineering, National University of Ireland, Cork, Ireland.

Papoulis, A. and S. U. Pillai (2002) *Probability, Random Variables and Stochastic Process* 4th Edition, McGraw-Hill Higher Education.

Parro-Jimenez, J. M., R. T. Ioannides, M. Crisci, and J. A. Lopez-Salcedo (2012) "Detection and mitigation of non-authentic GNSS signals: Preliminary sensitivity analysis of receiver tracking loops," in *6th ESA Workshop on Satellite Navigation Technologies and GNSS Signals and Signal Processing (NAVITEC),* Dec. 5-7, Noordwijk, Netherlands, pp. 1-9

Petovello, M., C. O'Driscoll, G. Lachapelle, D. Borio, and H. Murtaza (2008) "Architecture and Benefits of an Advanced GNSS Software Receiver," *Journal of Global Positioning Systems*, vol. 7, No. 2: pp. 156-168 www.gnss.com.au/JoGPS/v7n2/JoGPS_v7n2p156-168.pdf.

Phelts, R. E. (2001) *Multicorrelator techniques for robust mitigation of threats to GPS signal quality,* Ph.D. dissertation, Department of Mechanical Engineering, Standford University, Palo Alto, CA

Psiaki, M. L., S. P. Powell, and B. W. O'Hanlon (2013) "GNSS Spoofing Detection: Correlating Carrier Phase with Rapid Antenna Motion" in *GPS World Magazine,* vol. 24, no. 6, June, pp. 53-58

Savasta, S., L. Presti, F. Dovis, and D. Margaria (2009) "Trustworthiness GNSS Signal Validation by a Time-Frequency Approach," in *Proceedings of the 22nd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2009)*, September 22 - 25, Savannah, GA, pp. 66-75

Schielin, E., A. Allien, C. Taillandier, M. Jeannot, and D. Brocard (2012) "On the Foundation of GNSS Authentication Mechanisms," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, September 17-21, Nashville, TN, pp. 1194-1207

Scott, L. (2003) "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems" in Proceedings of ION GPS/GNSS 2003, Sept. 9-12, Portland, OR, pp. 1543-1552

Shanmugam, S. K. (2008) *New Enhanced Sensitivity Detection Techniques for GPS L1 C/A and Modernized Signal Acquisition*, Ph.D. thesis, published as Report No. 20264, Department of Geomatics Engineering, University of Calgary, Canada

Shanmugam, S. K., J. Nielsen, G. Lachapelle, and R. Watson (2006) "Pre-Correlation Noise and Interference Suppression for Use in Direct-Sequence Spread Spectrum Systems With Periodic PRN Codes," in *Proceedings of the 19th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2006)* , September 26-29, Fort Worth, TX, pp. 1297-1308

Shepard, D., and T. E. Humphreys (2011) "Characterization of Receiver Response to a Spoofing Attack," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, September 20-23, Portland, OR, pp. 2608-2618

Shepard, D., P. Bhatti, A. Jahshan, T.E. Humphreys, and A. A. Fansler (2012) "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks,"in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, September 17-21, Nashville, TN, pp. 3591-3605

Swaszek, P. F., R. J. Hartnett, M. V. Kempe, and G. W. Johnson (2013) "Analysis of a Simple, Multi-Receiver GPS Spoof Detector," in *Proceedings of the 2013 International Technical Meeting of The Institute of Navigation*, Jan. 29 – 27, San Diego, CA, pp. 884-892

Tippenhauer, N. O., C. Pöpper, K. B. Rasmussen, and S. Capkun (2011) "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*, Oct. 17-21, Chicago, IL, pp. 75-86

Trinkle, M., Z. Zhang, H. Li, and A. Dimitrovski (2012) "GPS Anti-Spoofing Techniques for Smart Grid Applications," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, September 17-21, Nashville, TN, pp. 1270-1278

Van Dierendonck, A. J. (2002) "Determination of C/A Code Self-Interference Using Cross-Correlation Simulations and Receiver Bench Tests" in *15th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2002)*, 24-27 September, Portland OR, pp. 630-642

Wen, H., P. Y. Huang, J. Dyer, A. Archinal, and J. Fagan (2005) "Countermeasures for GPS Signal Spoofing," in *Proceedings of ION GNSS 18th International Technical Meeting of the Satellite Division*, September 13 - 16, Long Beach, CA, pp. 1285- 1295

Wesson, K. D., D. P. Shepard, J. A. Bhatti, and T. E. Humphreys (2011) "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, September 20-23, Portland, OR, pp. 2646-2656

White, N.A., P. S. Maybeck, and S. L. Devilbiss (1998) "Detection of Interference/Jamming and Spoofing in a DGPS-Aided Inertial System" in *IEEE Transactions on Aerospace and Electronic Systems*, vol.34, no.4, Oct., pp.1208-1217

Wildemeersch, M., E. Cano Pons, A. Rabbachin, and J. Fortuny Guasch (2010) *Impact Study of Unintentional Interference on GNSS Receivers,* Technical report No. EUR 24742 EN, European Commission Joint Research Centre Security Technology Assessment Unit, 94 pages

Wullems, C. J. (2012) "A Spoofing Detection Method for Civilian L1 GPS and the E1-B Galileo Safety of Life Service," in *IEEE Transactions on Aerospace and Electronic Systems,* vol. 48, no. 4, October, pp. 2849-2864

Xi-jun, C., X. Jiang-ning, C. Ke-jin, and W. JieAn (2009) "Authenticity Verification Scheme Based on Hidden Messages for Current Civilian GPS Signals," in *Proceedings of Fourth International Conference on Computer Sciences and Convergence Information Technology*, Nov. 24-26, Seuol, Korea, pp.345-352

Zhang, Z., M.Trinkle, L. Qian, and H. Li (2012) "Quickest detection of GPS spoofing attack," in *2012 IEEE Military Communications Conference,* Oct 29- Nov 1, Orlando, FL, pp. 1-6.

APPENDIX A: CORRELATOR OUTPUT FOR A TRACKING RECEIVER

The following equation shows the formulation for the correlator output at time instant kNT_s when only authentic signal l is present in the received signal set

$$\begin{aligned} u_l[k] &= \frac{1}{N}\sum_{n=(k-1)N}^{kN-1} r(nT_s)\, c_l\left(nT_s-\tilde{\tau}_l\right) e^{-j2\pi\tilde{f}_l\, nT_s} = \\ &= \frac{1}{N}\sum_{n=(k-1)N}^{kN-1}\left(\left[\sqrt{p_l^a}\, c_l^a\left(nT_s-\tau_l^a\right)e^{j\phi_l^a+j2\pi f_l^a nT_s}+\eta(nT_s)\right] c_l\left(nT_s-\tilde{\tau}_l\right)e^{-j2\pi\tilde{f}_l\, nT_s}\right) \\ &= \frac{1}{N}\sum_{n=(k-1)N}^{kN-1}\left(\sqrt{p_l^a}\, c_l^a\left(nT_s-\tau_l^a\right) c_l\left(nT_s-\tilde{\tau}_l\right)e^{j\phi_l^a+j2\pi\Delta f_l^a nT_s}\right)+\overline{\eta}(nT_s) \end{aligned} \tag{A-1}$$

A non-coherent tracking receiver is assumed which is correlating the received authentic signal with a locally generated replica whose Doppler and code delay is close to the authentic signal. Therefore, assuming that the code delay of the locally generated replica is almost the same as that of the authentic signal, $\tau_l^a \approx \tilde{\tau}_l$, it can be written

$$\begin{aligned} &\frac{1}{N}\sum_{n=(k-1)N}^{kN-1}\left(\sqrt{p_l^a}\, c_l^a\left(nT_s-\tau_l^a\right) c_l\left(nT_s-\tilde{\tau}_l\right)e^{j\phi_l^{a,L}+j2\pi\Delta f_l^{a,L} nT_s}\right) \\ &\quad\simeq \sqrt{p_l^a}\, e^{j\phi_l^{a,L}}\,\frac{1}{N}\sum_{n=(k-1)N}^{kN-1} e^{j2\pi\Delta f_l^{a,L} nT_s} \\ &\quad= \sqrt{p_l^a}\, e^{j\phi_l^{a,L}}\,\frac{e^{j2\pi\Delta f_l^{a,L}(k-1)NT_s}-e^{j2\pi\Delta f_l^{a,L} kNT_s}}{N\left(1-e^{j2\pi\Delta f_l^{a,L}T_s}\right)} \\ &\quad= \sqrt{p_l^a}\,\frac{e^{-j\pi\Delta f_l^{a,L}NT_s}-e^{j\pi\Delta f_l^{a,L}NT_s}}{N\left(e^{-j\pi\Delta f_l^{a,L}T_s}-e^{j\pi\Delta f_l^{a,L}T_s}\right)} e^{j\pi\Delta f_l^{a,L}\left[(2k-1)N-1\right]T_s+j\phi_l^{a,L}} \\ &\quad= \sqrt{p_l^a}\,\frac{\sin\left(\pi\Delta f_l^{a,L}NT_s\right)}{N\sin\left(\pi\Delta f_l^{a,L}T_s\right)} e^{j\pi\Delta f_l^{a,L}\left[(2k-1)N-1\right]T_s+j\phi_l^{a,L}} \end{aligned} \tag{A-2}$$

Assuming that the Doppler frequency of the locally generated replica is almost the same as that of the received authentic signal, A1-1 can be approximated by the following equation

$$\begin{aligned}
&\frac{1}{N}\sum_{n=(k-1)N}^{kN-1}\sqrt{p_l^a}\,c_l^a\left(nT_s-\tau_l^a\right)c_l\left(nT_s-\tilde{\tau}_l^L\right)e^{j\phi_l^{a,L}+j2\pi\Delta f_l^{a,L}nT_s}\\
&\quad\simeq\frac{1}{N}\sqrt{p_l^a}e^{j\phi_l^{a,L}}\sum_{n=(k-1)N}^{kN-1}c_l^a\left(nT_s-\tau_l^a\right)c_l\left(nT_s-\tilde{\tau}_l^L\right)\\
&\quad=\frac{1}{N}\sqrt{p_l^a}e^{j\phi_l^{a,L}}R\left(\Delta\tau_l^{a,L}\right)
\end{aligned}\tag{A-3}$$

where $R(\bullet)$ is the correlation function which is closely related to the choice of subcarrier in GNSS signal. Therefore, combining A1 .2 and A1 .3, the output for a non-coherent correlator can be approximately written as

$$u_l[k]\simeq\frac{1}{N}\sqrt{p_l^a}R\left(\Delta\tau_l^{a,L}\right)\frac{\sin\left(\pi\Delta f_l^{a,L}NT_s\right)}{N\sin\left(\pi\Delta f_l^{a,L}T_s\right)}e^{j\pi\Delta f_l^{a,L}\left[(2k-1)N-1\right]T_s+j\phi_l^{a,L}}+\bar{\eta}\left[kNT_s\right]\tag{A-4}$$