GLOBAL POSITIONING SYSTEM SPOOFING AND DETECTION TECHNIQUES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

MEHMET BUĞRAHAN ÜSTÜNDAĞ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
ELECTRICAL AND ELECTRONIC ENGINEERING

JANUARY 2023

Approval of the thesis:

GLOBAL POSITIONING SYSTEM SPOOFING AND DETECTION TECHNIQUES

submitted by **MEHMET BUĞRAHAN ÜSTÜNDAĞ** in partial fulfillment of the requirements for the degree of **Master of Science** i**n Electrical and Electronic Engineering, Middle East Technical University** by,

Prof. Dr. Halil Kalıpçılar
Dean, Graduate School of Natural and Applied Sciences _____

Prof. Dr. İlkay Ulusoy
Head of the Department, Electrical and Electronics Engineering _____

Prof. Dr. Şimşek Demir
Supervisor, Electrical and Electronics Engineering, METU _____

Examining Committee Members:

Prof. Dr. Gönül Turhan Sayan
Electrical and Electronics Engineering, METU _____

Prof. Dr. Şimşek Demir
Electrical and Electronics Engineering, METU _____

Prof. Dr. Sencer Koç
Electrical and Electronics Engineering, METU _____

Prof. Dr. T. Engin Tuncer
Electrical and Electronics Engineering, METU _____

Prof. Dr. Asım Egemen Yılmaz
Electrical and Electronics Engineering, Ankara University _____

Date: 23.01.2023

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name Last name : Mehmet Buğrahan Üstündağ

Signature :

ABSTRACT

GLOBAL POSITIONING SYSTEM SPOOFING AND DETECTION TECHNIQUES

Üstündağ, Mehmet Buğrahan
Master of Science, Electrical and Electronic Engineering
Supervisor: Prof. Dr. Şimşek Demir

January 2023, 110 pages

As the number of applications relying on global navigation satellite systems increases, GNSS becomes to play a bigger role in the daily life. But recent studies and incidents prove how vulnerable GNSS can be against the intentional spoofing and jamming attacks. Due to ever-growing threat caused by spoofing attacks, reliability and security of the GNSS signals become a major concern that must be dealt with and it has become necessary to develop effective detection algorithms.

This thesis study examines a growing concern in modern navigation systems. The thesis investigates methodologies of spoofing along with detection techniques. To detect intentional interference attacks to ensure reliability of the global positioning systems, high-end solutions can be utilized. But these solutions lead to reduce accessibility of the GNSS receivers. To preserve approachability of the GNSS receivers high, low-cost and low-profile solutions must be developed. These solutions can be realized by using low-cost commercial off-the-shelf receivers and open-source GNSS receivers. Therefore, the thesis investigates low-cost solutions against spoofing attacks using highly accessible commercial off-the-shelf receivers and open-source software defined receivers.

The thesis implements spoofing attack scenarios created by an open-source GPS signal simulator. Scenarios are simulated in both software and hardware domains.

Attacks are created and received by using software defined radios and commercial off-the-shelf GPS receivers. In software domain an open-source GPS simulator is used along with an open-source GNSS receiver. Furthermore, an open-source test battery is used to examine effects of more sophisticated GPS spoofing attacks. For detection algorithms, the study focuses on pre-correlation techniques employing power-related metrics and signal quality monitoring techniques employing correlator values. The thesis examines effects of different types of spoofing attacks to victim receiver and tries to specify detection methods for each spoofing type.

Keywords: GPS spoofing detection, software defined radio, power monitoring methods, automatic gain control, signal quality monitoring

ÖZ

KÜRESEL KONUMLAMA SİSTEMİ ALDATMA VE TESPİT ETME YÖNTEMLERİ

Üstündağ, Mehmet Buğrahan
Yüksek Lisans, Elektrik ve Elektronik Mühendisliği
Tez Yöneticisi: Prof. Dr. Şimşek Demir

Ocak 2023, 110 sayfa

Küresel konum sistemlerini kullanan uygulamaların sayısı arttıkça, KKS gündelik yaşamda giderek artan bir role sahip olmakta. Ancak, konu üzerindeki son çalışmalar ve hadiseler küresel konum belirleme sistemlerinin, aldatma saldırılarına karşı ne kadar savunmasız olduğunu ispatlamakta. Bu sistemlerin güvenilirliği ve güvenliği hakkında büyük bir endişe kaynağı ve bunlara karşı testpit etme algoritmalarının gerekliliği oluşmakta.

Söz konusu tez aldatma ve bunları tespit etme yöntemlerini araştırmakta. Kasıtlı karıştırma saldırılarını tespit etmek ve KKS'nin güvenilirliğini sağlamak için pahalı çözümler geliştirilebilir. Ancak bu çözümler KKS alıcılarının ulaşılabilirliğini azaltmaktadır. Bu ulaşılabilirliği korumak için düşük maliyetli ve küçük alan kaplayan çözümler geliştirilmelidir. Bunlar, düşük maliyetli hazır KKS alıcıları ve açık-kaynak KKS alıcıları kullanılarak gerçekleştirilebilir. Bundan dolayı, bu çalışma yüksek ulaşılabilirliğe sahip hazır KKS alıcıları ve açık-kaynak yazılım tabanlı alıcıları incelemektedir.

Bu çalışma, aldatma saldırı senaryolarını açık-kaynak bir KKS sinyal üretecinden oluşturmaktadır. Senaryolar hem donanım hem de yazılım alanlarında

oynatılmaktadır. Saldırılar, yazılım tabanlı radyolar tarafından oluşturulup hazır KKS alıcıları tarafından alınmaktadır. Ayrıca, daha karmaşık aldtma sinyallerini inceleme amacıyla açık-kaynak bir deneme veri tabanı kullanılmaktadır. Tespit etme algoritmaları için korelasyon öncesi yöntemlere ve işaret kalitesi görüntüleme yöntemlerine odaklanılmaktadır. Bu çalışma, farklı tür aldatma sinyallerinin mağdur alıcılar üstündeki etkilerini incelemekte ve her biri için tespit etme yöntemlerini belirlemeye çalışmaktadır.

Anahtar Kelimeler: küresel konumlama sistemi aldatma tespiti, yazılım tabanlı radyo, güç görüntüleme yöntemleri, özdevinimli kazanç kontrolü, işaret kalitesi görüntüleme

To My Family…

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisor Prof. Dr. Şimşek Demir for his encouragements and advices through the thesis work and through my Master of Science program.

I would like to thank Dr. Bora Dikmen for his guidance and teachings about microwaves and engineering.

I would like to thank Dr. Hakan Tuna for helping to solve technical difficulties during my thesis work.

I would also like to thank METEKSAN Savunma for providing laboratory equipment to implement test setups on the thesis.

Last but not least, I would like to share my deepest gratitude to my family, my friends and my love who endlessly support and care about me. I would not achieve anything without their support and kindness.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

ABBREVIATIONS

ABSP Absolute Power Monitoring

ADC Analog to Digital Converter

AGC Automatic Gain Control

AoA Angle of Arrival

BPSK Binary Phase Shift Keying

CDMA Code Division Multiple Access

COTS Commercial off-the-self

DoA Direction of Arrival

DLL Delay Lock Loop

ECEF Earth-Centered Earth-Fixed Coordinate System

FSPL Free Space Path Loss

GB Gain Block

GPS Global Positioning System

GNSS Global Navigation Satellite System

IoT Internet of Things

IVGA Input Variable Gain Amplifier

LNA Low Noise Amplifier

NGEN Noise Generator

NMEA National Marine Electronics Association

OCXO Oven-Controlled Crystal Oscillator

OVGA Output Variable Gain Amplifier

PFA Probability of False Alarm

PLL Phase Locked Loop

PRN Pseudo Random Noise

RINEX Receiver Independent Exchange Format

RF Radio Frequency

SAW Surface Acoustic Wave

SDR Software Defined Radio

SQM Signal Quality Monitoring

VGA Variable Gain Amplifier

TCXO Temperature-Controlled Crystal Oscillator

CHAPTER 1

INTRODUCTION

From the early ages of the humankind, navigation is an essential necessity for transportation, agriculture, exploration and merchandise. Knowledge of time and location have assisted to transport through villages and countries. Explorers could not set foot into new continents without the knowledge of the location, merchandisers could not have carried loads across the continents and civilizations could not have interacted, hence the humankind we know would be much more undeveloped than it is today.

There have been many different navigation techniques over the years. But most of them lacks precision which has been offered by the satellite technology. With development of satellite systems in the late 1950s, it became possible to communicate through great distances on earth. This property of the satellite communication systems helped to construct satellite navigation systems providing spatial positioning information of an object across the earth.

Satellite-based navigation begun in 1970s in United States of America to help naval operations of the military. The GPS program started in 1973 and the first satellite was launched in 1978. By the 1990s GPS had 24 satellites in the orbit and they were ready to operate [1]. Ever since GPS became operational, its application areas have increased dramatically. Along with its foundation objective, which is providing a navigation solution for the military, now the GPS is used for civil transportation, amateur radio, astronomy, cellular telephony, clock synchronization, fleet and aircraft tracking, tectonics, robotics, IoT, sports and many more applications.

1.1 Fundamentals of GPS

Instantaneous position of a user can be determined by the virtue of the signals transmitted from the satellites. To find a position, trilateration method is used. Navigation is a real time process and to retrieve the specific information regarding to user in trilateration method, certain equations must be solved. But the equations required to solve the user position are nonlinear simultaneous equations. Also, in practical cases, inaccuracies occur due to sources of errors like user clock and these errors are included to these equations which emerges requiring one more satellite to calculate the error. Equations mentioned above can be solved using linearization methods. The outcome results are in Cartesian coordinate system and they are converted into a spherical system. But since the earth is not an ideal sphere, the real shape of the earth must be considered after calculation. Finally, by using at least four satellites user position is determined and converted into earth-based coordinate system.

1.1.1 GPS Segments

GPS is separated into three segments which are the control segment, the space segment and the user segment [2]. Space segment comprises of constellation of the satellites providing to users the required information to calculate their certain measurements. The satellites transmit navigation data and the ranging codes. Frequency allocation for each satellite is same, to discriminate signals between the satellites PRN codes are used. As of February 2019, there are GPS 31 satellites in the constellation. 27 of them are used actively and 4 of them are allocated as stand-by. In the constellation, there are six orbital planes separated by 60 degrees with four satellites each. Furthermore, each orbit makes a 55-degree angle with equator described as inclination angle [2].

The control segment consists of five control stations which are widely separated around the world. The main goal of the stations is monitoring the operation of the GPS satellites. But control stations also create and upload the navigation data to the satellites and synchronize the atomic clocks to sustain performance standards. The last segment is the user segment which is composed of all recipients benefiting from the information provided by the satellites [1].

1.1.2 GPS Antennas

GPS receivers use right-hand circularly polarized antennas. Selection of this kind of antenna is not arbitrary. In GPS applications, a major problem called as multipath occurs due to nearby reflectors to the GPS antenna. This phenomenon creates two or more links between antenna and the receiver. To mitigate this effect, antennas having RHCP pattern are employed. At first reflection, polarization flips to left-hand circular polarization. An RHCP antenna suppresses the LHCP reflection thus minimizing the error. A second reflection can occur but, in each reflection waves attenuate. Therefore, RHCP antennas successfully minimize the effects of the multipath [3]. Furthermore, the pattern of the antenna is hemispherical generally allowing tracking of the satellites from zenith to the horizon [4]. Also, phased array antennas can be used for multipath rejection. Phased array antennas are used in military applications helping to add nulling toward the direction of the jamming signals [4].

RHCP antennas are generally implemented with ceramic patch antennas which are favored over other antenna types since their compact and low profiles. Furthermore, patch antennas offer high gain towards zenith providing a suitable beam for satellite applications. They are economical to manufacture and easy to tune after fabrication.

Size of the ground plane placed beneath the antenna determines the center frequency and gain of the ceramic patch antenna. For example, while a 25mm x 25mm patch

antenna has a 5dBi gain at its highest point, a 15mm x 15mm patch antenna has a gain of 1dBi.

Aside from passive antennas, active antennas incorporating LNA circuitries can be used. But this can complicate the design since a need for bias-tee arises. Bias-tees are used for supplying current for the active antennas. It has three ports one of the ports injects the DC voltage and the other injects RF signal. At the third port, both DC and RF power are present [3].

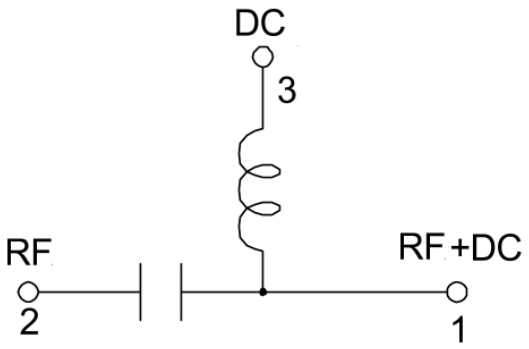

Figure 1.1. Bias-tee for active antennas

1.1.3 GPS Receiver Architecture

Process of the GPS signal begins with transmitted signal from the GPS satellites. As propagating through the atmosphere this signal attenuates, reflects from objects and eventually is received by an antenna. Due to imperfect polarization match the signal attenuates and LNAs populated in the receiver system amplifies the highly weakened signal. While propagating through the space and circuit of the receiver system GPS signal is combined with noise. Sources of the noise can be unintentional or intentional interference, noise caused by electronic devices and insertion loss due to mismatch losses or passive elements. At the end, received GPS signal power is around -130 dBm before its amplification at the RF front-end [3]. Maximum received GPS signal power can be up to -123 dBm [5]. This link budget will be discussed more broadly and analytically in Chapter 3 but if noise floor of a system having

bandwidth of 2 MHz is calculated, the result yields -111 dBm noise power. This quick calculation reveals an important property for RF front-end circuitries designed for GPS applications. Since GPS has a negative SNR level and this cannot be increased by an RF circuit, rather than taking account received signal level of GPS, RF front-end receivers are designed based on level of the thermal noise floor [3]. By doing that it is intended to add lowest noise possible, caused by noise figure of the electronic components. If this is achieved, SNR degradation will be small giving opportunity to increasing SNR by processing gain of the GPS signals.

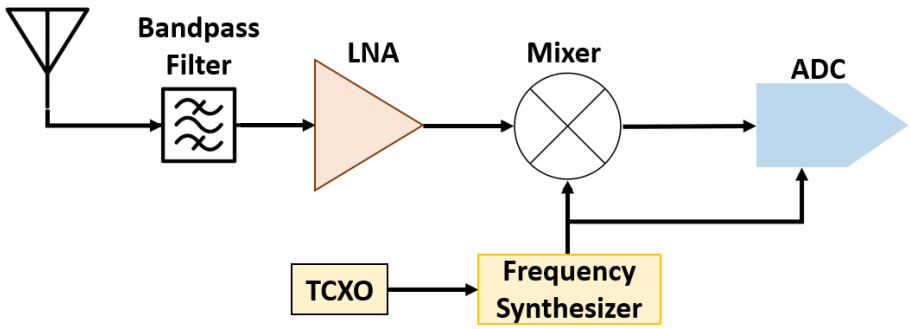

Figure 1.2. Basic diagram of an RF front-end design for a GPS receiver

Since the signal has low power, out-of-band interference must be suppressed. Filtering operation is often implemented with SAW filters because of their sharp cutoff frequency response. Furthermore, insertion loss of the filter must be as low as possible to minimize increase of overall noise figure and attenuation at stop band must be high to obtain good frequency selectivity preventing out of band interference.

After filtering, amplification must be employed. In hard-limiting architecture having 1-bit ADCs amplification is straightforward and there is no necessity for an AGC but for multibit receivers, AGC must be employed. Gain of the LNAs must be high enough to raise exceedingly low signal to a level that can be processed by an ADC.

Also, it is important to have low noise figure LNAs to not to include additional noise causing SNR to drop.

There are multiple choices of topologies to implement a GPS receiver which are zero-IF, downconversion to an IF frequency or a direct digitization. Down-conversion can be realized in single or multiple stages [4]. Also, without down converting the signal to an IF frequency, direct conversion to baseband signal can be used for the receiver topology. Direct digitization from the radio frequency can be a third option for a receiver design but it can be more expensive than the other options and need for amount of amplification can be tremendous. In this case, all required gain must be implemented at the same frequency causing possible oscillations due to very high gain at a single frequency [1].

After digitization, the signal is sent to signal processing blocks. First, acquisition block determines visible satellites by correlating local code replica with the incoming signal. Coarse estimations of code phase and carrier frequency are performed. Then tracking block refines the parameters. Tracking block will be examined thoroughly in Chapter 3.

1.1.4 GPS Reference Clock Properties

Crystal oscillators are used for reference frequency sources in receiver topologies. A highly sensitive application as GPS needs a highly stable clock in terms of its frequency stability. To successfully detect and demodulate the carrier frequencies, it is an essential necessity to include stable oscillators to GPS receivers.

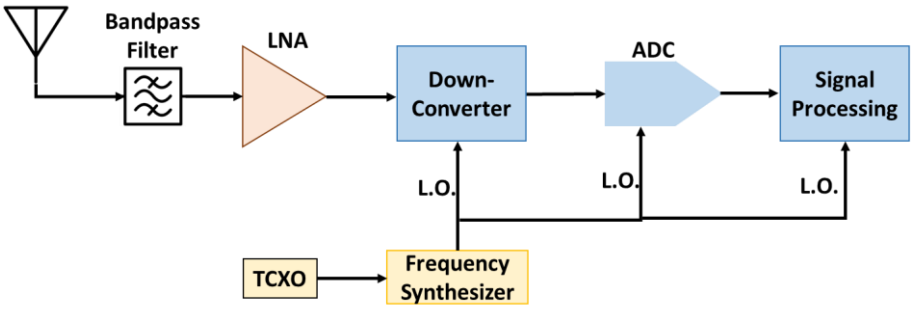

Figure 1.3. GPS Receiver blocks using the reference clock

As can be seen from Figure 1.3, reference clock is used in lots of blocks of the GPS receiver topology. Phase of the incoming signal is influenced by the phase noise during analog to digital conversion phase [6]. Therefore, an error is introduced to the initial phase by the reference clock. Furthermore, the NCO of the PLL is fed by the reference oscillator creating an additional error on estimated phase. Along with phase noise, frequency stability of the oscillator creates error and ambiguities. Frequency stability affects doppler measurements. As a result, it is important to choose the correct oscillator to minimize the source of errors.

There are various types of crystal oscillator which are temperature compensated crystal oscillator (TCXO), oven-controlled crystal oscillator (OCXO), voltage-controlled oscillator (VCXO) and voltage controlled TCXO (VCTCXO). In OCXO, temperature is controlled by a mini oven maintaining a consistent temperature which makes the output frequency of the oscillator more stable. Alternatively, in TCXO, ambient temperature is sensed and with a help of feedback circuit suitable correction is carried out [7]. Because of their superiority respect to frequency stability, generally TCXO and OCXO are used for GPS applications.

Table 1.1 Crystal oscillator types [7]

Type	Available Frequency Temperature Stability	Comparable Price
VCXO	±5 ppm to ±50 ppm	Low
TCXO	±0.1 ppm to ±5 ppm	Medium
VCTCXO	±0.5 ppm to ±5 ppm	Medium
OCXO	±0.1 ppb to ±10 ppb	Highest
VCOCXO	±1 ppb to ±0.25 ppb	High

There are various output waveforms that can be provided by the crystal oscillators which are TTL (transistor-transistor logic), CMOS, HCMOS, PECL (positive referenced ECL), ECL (emitter coupled logic), LVPECL (low voltage PECL), LVDS (low voltage differential signaling), CML (current mode logic), sinewave and clipped sinewave [7]. The most popular waveforms are CMOS, sinewave and clipped sinewave. Especially in TCXOs, clipped sinewave waveform is a de facto standard due to its very low power consumption. In CMOS type of signals, amplitude of the output wave form is determined by the supply voltage of the oscillator as can be shown from below.

While the type of the crystal oscillator having major impact of frequency stability, type of the waveform affects mostly the phase noise of the oscillator.

Table 1.2 Phase noise ranges respect to output waveform types [7]

Type	Phase Noise Range (dBc/Hz)
LVDS	-140 to -145
Clipped sinewave	-150 to -160
Sinewave	-180 or lower
CMOS	-65 to -170

1.1.5 GPS Receiver Conditions

GPS receivers which presently do not track the satellites, it must perform acquisition algorithm to find satellite signal in the visible sky. Before assigning a channel to GPS satellite, the receiver must know PRN numbers of the visible satellites. After tracking the satellites and acquiring the navigation data, GPS receiver can calculate a position solution.

This start-up can occur into different scenarios [3]. Generally, they are classified into three specific conditions.

Cold Start

The receiver has no prior information about ephemeris and almanac data. Consequently, the receiver requires to search each of the available C/A codes along with a frequency range caused by Doppler shift. Therefore, this is the scenario which the receiver consumes the highest power. This process can take up from 30 seconds to several minutes respect to performance of the receiver.

Warm Start

In this scenario, the receiver has almanac data but has no ephemeris data or stored ephemeris data become outdated. The current time is known by the receiver and the location of the receiver is within 100 km radius when the last fix has occurred. By using the prior information, the receiver can forecast which satellites are overhead but it must download present ephemeris data. This process usually takes around 45 seconds, some of the newer receivers can perform this in shorter periods of time.

Hot Start

The receiver has both accurate almanac and ephemeris data. Along with conditions in warm start scenario, additional conditions must be met to perform a start-up in hot start mode. A fix must have been founded within the last two hours and accurate

ephemeris data for at least five satellites must have been stored. Time to first fix in the hot start mode usually takes a few seconds.

1.1.6 GPS Applications

The initial purpose of the global satellite navigation systems was military. But as GNSS technologies enhance their efficiency, cost has decreased and availability has increased greatly. Now, they are used in mapping, surveying, space applications, military, autonomous systems, maritime, science, location-based services and timing applications.

Augmented reality, requesting information regarding to the nearest business or service such as a restaurant or transportation hub and alerting traffic jam can be examples for location-based services that uses GNSS technologies. Also, GNSS are used for civil applications such as fleet management and vehicle tracking, traffic management, tolling, en-route and approach navigation of air traffic, signaling in railroads, package and container tracking, mining and precision agriculture. Furthermore, GNSS are used for space applications which can be classified as precise orbit determination, satellite real-time navigation and satellite formation flying which helps operations like docking and trailing. Along with applications above, GNSS are used in earth sciences such as geodesy and geodynamics, ocean surface altimetry, ionospheric and troposphere monitoring. Last but not least, GNSS are used for precise timing applications such as frequency control, synchronization of multiple reference clocks, network synchronization and telecommunication synchronization [8].

1.2 Motivation and Problem Definition

As the number of applications using global navigation satellite systems increases, GNSS becomes to play a bigger role in the daily life. As mentioned in the previous chapter, GNSS have a wide area of usage and certainly makes our lives easier. But recent reports and journal papers mentioned in Chapter 2 show how vulnerable GNSS is against the intentional spoofing and jamming attacks. Since GNSS is used in the most of the modern life applications and it seems that GNSS cannot be replaced by any other system, it must be ensured that obtain reliable information from the global navigation satellite systems. Reliability and security of the GNSS signals become a major concern that must be dealt with. To overcome problems created by spoofing and jamming attacks military systems using GNSS can build complex architectures and algorithms which are not cost-efficient. Civil GNSS receivers must overcome this issue by producing low-cost solutions to ensure to keep availability of GNSS technology remains high. Therefore, the thesis investigates low-cost solutions against spoofing and jamming attacks using by highly accessible COTS receivers and open-source software defined receivers.

1.3 Structure of the Thesis

First chapter of the thesis introduces the basic concepts of the global navigation satellite systems. The chapter emphasizes the vital need for reliable GNSS and it examines current threats against GNSS along with problems caused by these threats.

Second chapter of the thesis gives a broad literature review about current threats against global positioning systems and counter measurement methods against them. Furthermore, it classifies threats respect to their sophistication levels and refers each of their detection methods. The chapter also shares survey papers and their research methodologies on the subject.

Third chapter of the thesis gives a comprehensive theoretical background about spoofing and interference detection techniques which are received power monitoring, automatic gain control data coupled with C/N_0 values and signal quality monitoring. The chapter determines nominal values of the metrics and tries to set threshold values analytically and statistically. To determine these values, the chapter examines link budget of the global positioning system and interprets effects of interference to AGC and C/N_0 values. Also, tracking topology of the receivers are examined to investigate effects to SQM metrics. These data are provided by low-level commercial off the shelf GPS receivers and software defined receivers. It is intended to evaluate performances of low-cost solutions against GNSS spoofing by selecting COTS and software defined receivers.

In Chapter 4, the thesis proposes both hardware and software test techniques to assess effectiveness of the interference detection methods. The chapter employs SDRs to generate spoofing signals and compares SDRs and reference clocks to select the most suitable one to generate GPS signals. Chapter 4 also emphasizes the LO leakage problem created by zero-IF topology of the SDRs. It proposes a solution regarding to the problem. Furthermore, numerous test setups are demonstrated to investigate vulnerabilities of receivers operating in cold-start and tracking scenarios and the thesis proposed detection techniques for each of them. In Chapter 5, thesis concludes the work and specifies possible enhancements for future research.

CHAPTER 2

LITERATURE REVIEW OF SPOOFING AND DETECTION TECHNIQUES

As awareness against solemnity of threats against GPS has been increasing, research in this matter have accelerated greatly in recent years. Research have been mainly focused on detection techniques but also GPS spoofing techniques is a highly researched area to determine vulnerabilities of GPS receivers. By determining the vulnerabilities, systems having more robust navigation solutions can be designed. There are numerous survey papers regarding to this issue. In [9], the authors acknowledge the readers about the latest spoofing incidents and emphasize the dangers of spoofing, then classifies the spoofing attack methods respect to technologies employed and in possible scenarios that they might be used. Furthermore, the paper categorizes spoofing detection methods and discusses their effectiveness against various methods of the attack. Detection methods introduced in the paper are given in both navigation level, encryption level and pre-correlation level. The paper briefly shares analytical background of the mentioned detection methods. Finally, the paper examines recovery methods if the spoofing attack affects the receiver system, by introducing steps of recovery and verification of authentic signals aftermath of the spoofing. Another survey paper [10] authors draw attention to solemnity of the situation by firstly sharing spoofing incidents that are reported. The paper classifies spoofing generation techniques into three sub-categories and draws a clear frame between the generation techniques and briefly introduces possible countermeasure methods against each of them. The paper also categorizes vulnerabilities of the GPS against the spoofing attacks which are vulnerability in navigation and position level, data bit level and signal processing level. This classification makes categorization of the detection methods easier since signal

processing level vulnerability can be avoided by using suitable signal processing techniques and vulnerability in navigation solution level can be avoided by using consistency checks and so on. Before classifying anti-spoofing techniques, the paper derives analytical received signal model on the presence of spoofing and then introduces main two categories of the anti-spoofing techniques which are detection and mitigation. Authors define ten main categories for spoofing detection techniques and give broad information by again introducing subcategories for each of them respect to their use of different information gathered from the receiver. Furthermore, the paper investigates and classifies detection techniques respect to their complexity levels, effectiveness and coverage levels against different spoofing scenarios. The authors categorize mitigation techniques into three groups and investigates in a same manner. Finally, the paper introduces spoofing and anti-spoofing test scenarios and underlines the rules strictly prohibiting that transmission of the GPS signals at the outdoor. Therefore, demonstrations must be carried out carefully. In [11] the author shares possible motivations behind spoofing attacks and classifies spoofing attacks and detection methods different from other surveys. The paper introduces three different scenarios regarding the situation of the receiver. They are classified as cold-start, reacquisition, and tracking modes. In cold-start mode, the receiver has no prior knowledge about its location, time, ephemeris and almanac which is stated as giving the largest independence to the spoofer meaning that easier to be spoofed. In reacquisition mode, spoofing begins before acquisition but the receiver has a prior knowledge. This scenario occurs when there is a presence of a jammer before spoofing operation. The last scenario is stated as the most challenging situation for the spoofer. Other different classification made by this paper is about injecting spoofing signals to the receiver. In non-coherent superposition injection method, the paper states that authentic signals can be kept under the noise and in coherent superposition method, the spoofer must know the exact position of the receiver. The paper investigates effectiveness of each method introduced.

In a recently published paper [12] authors claim that previously surveys on this topic are outmoded and do not fully cover recent progress. The paper is mainly focused on

spoofing threats against aerial vehicles and briefly mentions threats against land platforms. Unlike previous surveys, the paper examines practical real-life concerns more than analytical background of the topic. Threats are categorized as spoofing and jamming. Spoofing attacks are classified as time and location spoofing, also names of the SDRs demonstrating attacks for each paper are given. Taxonomy of the spoofing attacks are interpreted by placement of the spoofing transmitter respect to receiver and stealthiness. According to paper, stealthiness of the spoofing attacks are comprised of two categories which are overt attack and covert attack. In overt attacks, the spoofer does not make an attempt to obscure the attack. Furthermore, the paper examines challenges against successful spoofing attacks and concludes the paper by discussing unsolved issues on this topic and future research directions.

2.1 Threats Against Global Positioning System

The importance of the GPS is undisputable therefore, its safety and reliability draw attention as number of reports and journal papers regarding to intentional spoofing and jamming operations increases greatly. For instance, a report on [13] shows successful spoofing attacks affected number of ships in the Black Sea in 2017. Furthermore, numerous periodicals like [14, 15, 16, 17] have been published successful cases of spoofing attacks demonstrating capturing the control of a yacht and an unmanned aerial vehicle.

2.2 Classification of Spoofing Generation Techniques

Spoofing generation can be split up into three categories as mentioned in [9, 10, 18, 19].

2.2.1 GPS Signal Simulator

This can be regarded as the most basic spoofing generator method. A GPS signal simulator concatenated with an RF transmitter circuitry can mislead commercial GPS receivers by transmitting higher power than authentic GPS signal power levels which generally correspond to -130dBm in a 2 GHz bandwidth [1, 2] This can be implemented with an expensive simulator [20] or an open-source software and an SDR. Latest RINEX files and a trajectory file comprising desired latitudes and longitudes in ECEF format must be provided to open-source software to perform successful spoofing attack [21].

Spoofing signals created with this method without knowing position of the victim will look like noise for a victim receiver running in the tracking mode. Since spoofer does not match the spoofing signal code and carrier phase to authentic GPS signals at the receiver, to implement this method successfully, victim receiver operating in tracking mode may need to be jammed to break the connection between the receiver and GPS satellites [9]. Therefore, an auxiliary jamming hardware could be required which is discussed more on Chapter 3. Jammed GPS receivers do not have the knowledge of its current position, velocity and the time. Also, there is no visibility of the GPS satellites from the receiver. This status is named as cold start [22]. Thus, it is easier to spoof the victim receiver when it is in cold start mode.

Furthermore, if signal power level of the spoofing signal is high enough, it can jam the receiver. Patent in [23] depicts a spoof signal whose center frequency is at 1.575GHz with power levels from -65dBm to -75dBm. Research in the patent shows the spoofing signal can serve together as a jamming source and a spoofing source [23].

Detection of this kind of attacks is examined on Chapter 2.2.

2.2.2 Receiver-Based Spoofing Attacks

Receiver-based spoofing attacks requiring RF receiver and transmitter circuitries creating the ability to perform more sophisticated spoofing attacks. This type of attacks can be classified into two subcategories. Main advantage of these two methods over GPS signal simulator method is the ability of transmitting the legacy P(Y) code since the P(Y) code is encrypted and cannot be created by the simulators [9].

First method is simply recording the GPS signals and replaying them without changing its properties. This process can be implemented by using a commercial SDR [24]. Second method is named as meaconing which is a more advanced one. Meaconing method records the authentic GPS signals and repeats the signals through a transmitter circuitry with sufficient gain and suitable delay [25]. If the spoofer wants to take over the victim GPS receiver without raising flags caused by major amplitude differences compared to authentic GPS signals, spoofer must know current location of the victim receiver and calculate the free space path loss to adjust its output power of its transmitter. Furthermore, spoofing signals at the victim receiver must be at correct signal delay [15].

This type of attacks can be detected by using inconsistencies created by the clock of transmitter circuitry of the spoofer or by an angle of arrival algorithm. More details about detection strategies are examined on Chapter 2.2.

2.2.3 Sophisticated Receiver-Based Spoofing Attacks

This can be considered as the most complex and effective method of spoofing. To execute this type of attack, the spoofer must know exact position of the victim receiver within an accuracy of centimeters [26]. This information is a necessity to perfect alignment of phase of the code and the carrier of the spoofing signal to authentic signal at the receiver. To eliminate angle of arrival detection method, spoofer also designs an array multifarious that is consistent with the array manifold

of the genuine GPS signals. This type of spoofing is harder to implement since phase alignment and array synchronization might be accomplished in only a small zone. Furthermore, additional difficulties might occur due to physical placements of the antennas [10].

2.3 Classification of Spoofing Detection Techniques

Spoofing detection can be performed at different stages of the receiver chain of the GPS. At precorrelation, tracking and navigation solution levels, receiver can gather required data to detect presence of spoofing. These methods can be classified as shown below.

2.3.1 Signal Power Monitoring Methods

Absolute Power Monitoring

Presence of a spoofing or a jamming signal within the bandwidth can elevate the noise floor. Elevated noise floor can be noticed by utilizing absolute power monitoring circuitries. But since GPS signal levels are already low, even overpowered attacks against authentic signals elevate noise floor in terms of a subtle increase. Therefore, the circuitry requires received power within a certain accuracy level [10].

C/N_0 Monitoring

Ionospheric variations can gradually change received C/N_0 values by the receiver. Furthermore, received C/N_0 levels may change due to atmospheric conditions, multipath environments so on. If a receiver successfully models the C/N_0 variations,

it can set a threshold to indicate spoofing signals, since spoofing signals cause sudden changes in C/N_0 values [10].

Automatic Gain Control Data Monitoring

GPS receivers employ automatic gain control circuitries because of the numerous reasons that are discussed at Chapter 3. AGC circuitries effectively monitor the received noise power within a desired bandwidth and respect to received band power, they change gain values of their amplifiers. Most of the receivers share instant gain values which can help to monitor presence of additional signals within the desired band. In [27, 28, 29, 30] authors employ AGC data of the receivers to investigate received noise power levels in 2 MHz bandwidth. They try to monitor transients and classify them. Authors do not approach the classification problem with statistical methods like ROC analysis. Instead of that, they try to model behavior of the AGC data under spoofing and nominal conditions.

Comparison Between Received Band Power of L1 and L2 Bands

Power difference between L1 and L2 signals are predefined by the specifications of the Global Positioning System. Spoofers having simple architectures can only transmit L1 frequency band. Therefore, band power difference between L1 and L2 frequency bands might differ due to presence of spoofing attacks indicating possible spoofing attacks [10].

Received Power Variations Respect to Movement of the Receiver

GPS satellites are in the orbit of 20000 kilometers away from the surface. Received band power of the GPS signals do not vary significantly by changing location of the receiver under clean sky conditions. But a spoofer employing single antenna located at the surface of the earth cannot make such an effect. Therefore, movement of the

receiver can substantially change C/N_0 levels measured by the receiver since, spoofing power will decrease by following the FSPL equation. Thus, if received C/N_0 levels change respect to changing location, there might indicate presence of a spoofing signals [10].

2.3.2 Direction of Arrival Discrimination

A receiver utilizing antenna array can determine direction of incoming signals. If the spoofer comprises single antenna, satellite signals created by the spoofer come from a single direction. But for nominal case, the authentic signals come from various angles. Each satellite has different elevation angles at a certain time. Therefore, if a receiver incorporates DoA algorithm, it can detect spoofing signals [9].

A drawback for this detection algorithm is its complexity. Since it needs an array calibration process due to mutual coupling between the antennas. In [31] authors claim that by employing spatial energy of the spoofing signal without need for a calibration phase, spoofing signals can be detected. Another paper [32] designs and utilizes miniature antenna arrays to detect direction of spoofing transmitter having single antenna.

2.3.3 Signal Quality Monitoring

Signal quality monitoring techniques are powerful toward detecting spoofing attacks. They utilize changes caused by interaction between authentic and spoofing signals. In the literature numerous signal quality monitoring metrics are investigated which are computed from correlator values [33, 34, 35, 36, 37, 38]. SQM is discussed broadly in Chapter 3.

2.3.4 Time Difference of Arrival Discrimination

PRN code latency and relative delay between L1 and L2 signals can be a potential discriminator between authentic and spoofing signals. For example, the propagation delay in L2 band is larger than delay in L1 band. Relative delay caused by distance between satellites to receiver is known by the receiver. If spoofer cannot create the same exact delay, it can be discriminated by the receiver [10].

There are numerous TDOA algorithms in literature for both single emitter and multiple emitter geo-location. One of the widely used technique is maximum likelihood TDOA estimation [39].

2.3.5 Consistency Check Methods

GPS clock and navigation data levels consistency checks can be performed to detect any unusual jump in mentioned data [10]. In navigation data, the arrangement of the changes and signature of the navigation message can be monitored [11].

2.3.6 Consistency Check with Other Navigation Methods

The vehicle employing a GPS receiver can also utilize inertial navigation systems or inertial measurement unit to discriminate between authentic and spoofing signals. Main goal behind fusing these two systems together is constantly checking their consistency. If a disagreement between the systems occurs, it might indicate a possible spoofing attack [9]. But coupling of these two systems can be tricky and adds additional computational complexity. In [18] and [40] they perform spoofing detection algorithm using IMU measurements. [41] and [42] uses INS coupling for spoofing detection.

2.4 Spoofing and Detection Test Scenarios

Spoofing signals whether recorded and being ready to be replayed or generated by a GPS signal simulator can be combined with authentic signals on software and hardware platforms. Hence, various scenarios can be created on both platforms.

2.4.1 Software Domain Test Scenarios

GPS signals can be generated by using open-source GPS simulators [21]. Another way to create GPS signals in software domain is recording and storing the IF signal [10]. After generation, combining two GPS signals can be performed by using MATLAB of GNU Radio. By using software defined receivers [43] post correlation and pre correlation GPS spoofing detection techniques can be implemented.

2.4.2 Hardware Domain Test Scenarios

Test setups performing RF signal transmission must be careful to avoid broadcasting the GPS signals. Because it is strictly prohibited broadcasting in protected navigation RF bands [9]. In each country, there are regulatory institutions to standardize the emission levels within certain bandwidths. For example, in [44] restricted bands are determined and only spurious emissions are permitted in any of the frequency bands listed as restricted.

Therefore, to realize spoofing scenarios conducted RF transmission must be implemented. This configuration for the test setups is legal since the spoofer never broadcasts the signal through the air.

CHAPTER 3

GPS SPOOFING DEMONSTRATION AND DETECTION METHODS

3.1 Generating Spoofing Signals using Direct Conversion Topology

One of the most popular topologies for transmitter circuitries is direct conversion topology which translates baseband spectrum to RF spectrum. Especially, this topology is popular among software defined radios. Since direct conversion transmitters provide simple topology requiring lesser number of components than other transmitter architectures. Along with its compactness, output of the transmitter is cleaner than other topology choices. The output spectra of the topologies include the desired signal around the carrier frequency and its harmonics but the spectra do not suffer from spurious components.

Direct conversion or namely zero-IF topology having zero intermediate frequency employs a mixer and a local oscillator to perform up-conversion from the baseband. Frequency of the local oscillator is same with desired RF frequency.

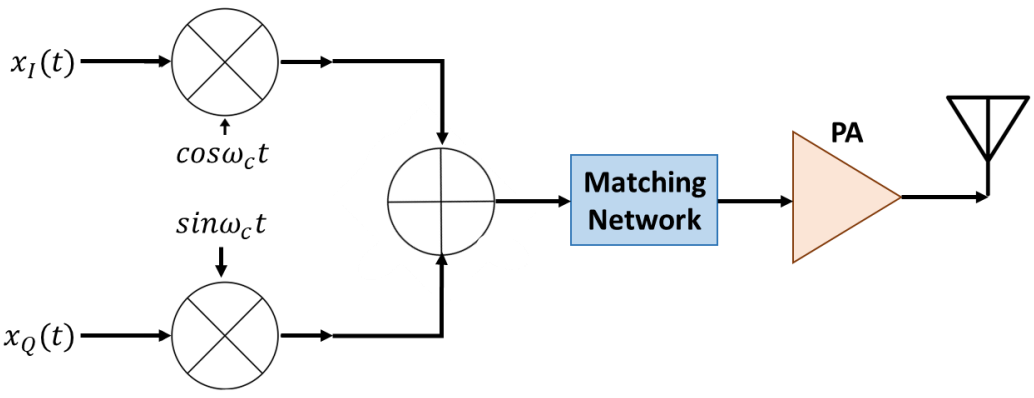

Figure 3.1. Direct conversion topology

Along with many perks provided by the topology, it creates a problem that must be tackled down which is named as LO leakage. Since LO and RF is at the same frequency, LO presents at the center of the desired RF signal.

This originates from imperfectness of the mixer. Non-ideal isolation between LO and RF ports causes leakage from LO port to RF port as can be seen from figure shown below.

LO leakage problem which is shown in Figure 3.2 can be omitted by ensuring amplitude of the baseband signal is sufficiently large. But this can create linearity problems in up conversion mixers. Therefore, amplitude must be carefully adjusted [45].

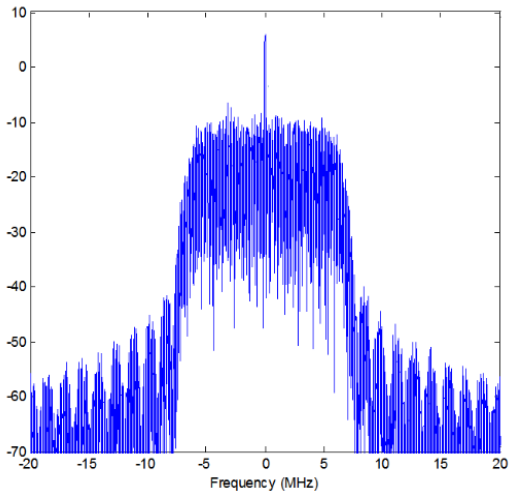

Figure 3.2. LO leakage due to non-ideal mixer [46]

Other problems faced in zero-IF transmitters are linearity of the mixer and unwanted coupling from output of the transmitter to LO circuitry [45]. These two problems occur when high output powers are introduced at the output of the transmitter circuitry but since GPS simulators need relatively low power at their output, this will not be concern. Just providing sufficient gain to raise desired signal above unwanted spurs would be adequate.

3.2 Power Monitoring Methods

Power monitoring methods are useful to detect unusual signals present within a certain bandwidth. If link budget of a certain system is known, then by simply monitoring received noise and signal power in a bandwidth can give a clue about intentional interference. One of the widely used methods among power monitoring techniques is absolute power monitoring method which can be used in both transmitter and receiver chains for power measurement and power control. To perform absolute power measurements, couplers or voltage dividers can be used to sample the RF signal [47]. After obtaining small portion of the signal, RF power level can be measured by using RF power detectors.

To ensure low insertion loss through receiver or transmitter paths, suitable coupler topologies must be selected. Hybrid couplers like rat-race couplers and Lange couplers [48] are not suitable for absolute power monitoring since they split incident RF power equally between two output ports. Directional couplers having higher coupling ratios like Wiggly couplers [49] and sawtooth couplers can be used. As coupling ratio increases, insertion loss of the coupler decreases. Therefore, it is crucial to select coupling ratio of the coupler as high as possible. But note that, as coupling ratio of the coupler increases, power that must be read from the RF power detector decreases. Since RF power detectors have a limited dynamic range, they cannot detect RF signal power below than a certain level. For COTS RF power detectors, regardless type of their technology, minimum detectable RF power levels are approximately -70 dBm.

Table 3.1 Dynamic Range Comparison of Selected RF Power Detectors

Part Number	*Dynamic Range (dB)*	*Minimum Detectable Signal (dBm)*
LT5537	83	-76
ADL5513	80	-70
HMC1120	72	-60
HMC1030	67	-55
AD8318	65	-60

As it will be discussed comprehensively on following chapters, a GPS spoofing attack can be demonstrated around power levels of authentic GPS signals. Since received GPS signals at the antenna have negative SNR levels, even amplitude of an overpowered attack having 15 dB advantage over GPS signals can be lower than noise floor. But this type of attack can raise noise floor because of summation of the noise, spoofing signal and the genuine signal. Consequently, it would be useful to monitor power levels of the noise and GPS signal in a certain bandwidth to detect intentional attacks against GPS signals.

But minimum detectable signal levels of the RF power detectors do not allow to measure RF power levels around noise floor. Therefore, it is important to provide enough gain to amplify noise floor to be able to be monitored by the RF power detectors. Alternatively, power related metrics like C/N_o and AGC data can be utilized. These two metrics are provided by data stream of the COTS GPS receivers allowing to implementing power monitoring techniques by only using a COTS GPS receiver. This opportunity eases the hardware design for GPS receivers having capability of spoofing detection.

3.2.1 Power Monitoring Methods for Interference Detection

Interference attacks can be classified as jamming and spoofing attacks. As mentioned in Chapter 2, spoofing attacks can be performed by applying higher signal levels to input of the victim receiver. These overpowered spoofing attacks increase received power level by the receiver significantly. Another threat for a GPS receiver is a jamming attack. Just like overpowered spoofing attacks, jamming attacks increase received power level by the receiver. To detect and discriminate between these attacks, C/N_o monitoring can be used. While spoofing attacks increase the C/N_o metric of the received signal, jamming attacks decrease the value of the metric.

The received GPS signal power on the surface of the Earth by a traditional RHCP antenna is lower than thermal noise floor power. Thermal noise power can be determined with equation shown below where k is Boltzmann's constant, T_A is the effective antenna temperature and BW is the bandwidth of the system.

$$P_N = kT_ABW \tag{3.1}$$

While for a system having 2 MHz bandwidth, noise floor becomes -110.92dBm, it increases to -108.37dBm and -103.93dBm with 3.6 MHz and 8 MHz bandwidth values respectively. Figure 3.3 shows change of the noise power respect to bandwidth of the system.

As it is stated in [3] first null bandwidth of the GPS L1 C/A signal is approximately 2 MHz but if it is desired to capture side lobes of the BPSK signal, bandwidth of the receiver can be adjusted up to 20 MHz.

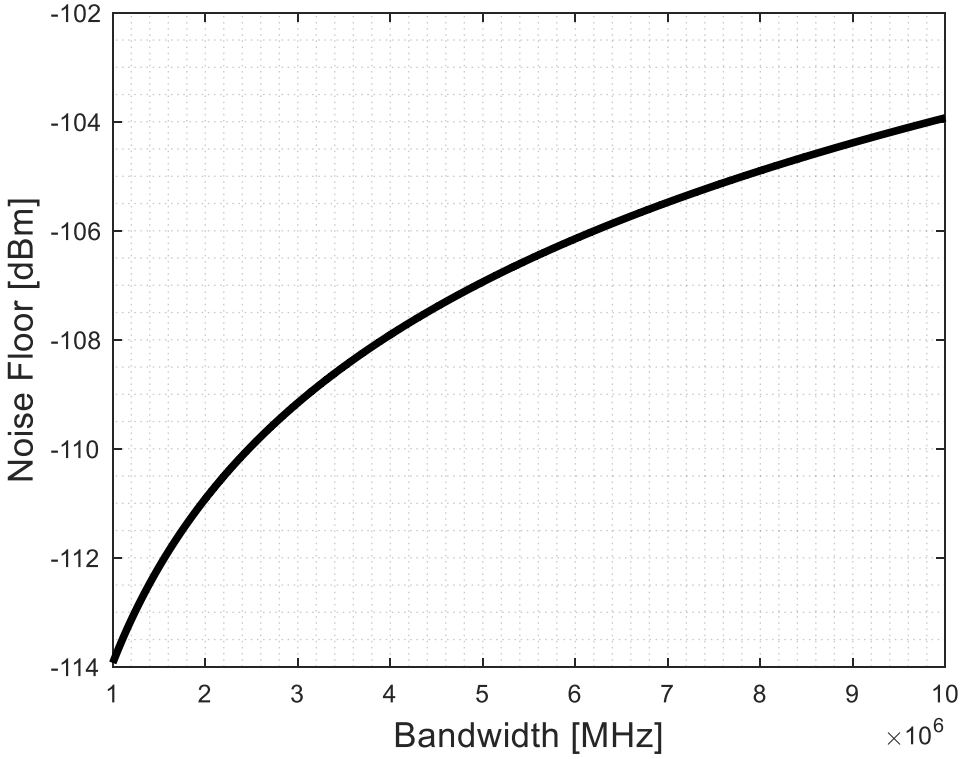

Figure 3.3. Noise floor respect to bandwidth of the system

To calculate received GPS power transmitted by the satellites over the horizon, link budget of the system can be examined.

Minimum transmitted power of the GPS satellites is 26.8dBW which corresponds to 57dBm approximately [4]. Free-space loss (FSPL) between the satellites and the ground can be calculated as shown below [50].

$$\mathrm{FSPL} = \left(\frac{\lambda}{4\pi \mathrm{R}}\right)^2 \tag{3.2}$$

where λ is the carrier wavelength corresponding to 0.19m at 1575.42 MHz and R is the distance between the receiver and the satellites. If the receiver is located at the sea level, R can be taken as $2 \times 10^7 \mathrm{m}$. Therefore, free space path loss becomes

182.4dB. Accounting atmospheric attenuation (ATT) as 2dB gives the following equation [4].

$$\text{Min received power} = \text{Min transmitted power} - \text{FSPL} - \text{ATT} \qquad (3.3)$$

Equation (3.6) gives the received GPS signal power from a single satellite as approximately -130dBm. Received GPS signals produced by a single satellite lies below the noise floor.

It is clear that the noise is the dominant factor over a GPS receiver. This phenomenon also entails that the design of the RF front-end is established on the thermal noise floor rather than the received GPS signal level itself.

Table 3.2 Carrier Link Budget of GPS L1 C/A Signal

Parameter	Gain+ / Loss-	Absolute Value
Power at the satellite transmitter		43.4 dBm
Satellite antenna gain	+13.4 dB	
Radiate power EIRP		56.8 dBm
Loss due to polarization mismatch	-3.4 dB	
Free space loss	-184.4 dB	
Atmospheric loss	-2 dB	
Gain from reception antenna	+3 dB	
Power at the receiver input		-130 dBm

SNR of the signal at the receiver input can be calculated as shown below.

$$\text{SNR (dB)} = \text{Signal power at receiver input} - \text{Noise power} \tag{3.4}$$

$$\text{SNR (dB)} \cong -130 - (-111) = -19 \text{ dB} \tag{3.5}$$

After input of the receiver, thermal noise power is coupled with receiver system and with noise figure of the system, total noise power seen by the ADC can be calculated.

$$P_{N_{total}} = k(T_A + T_R)BW \tag{3.6}$$

T_R is the cascaded receiver noise temperature which can be calculated by Equation (3.7) and Equation (3.8) derived from Friis equation [51].

$$F = F_1 + \frac{F_2 - 1}{G_1} + \frac{F_3 - 1}{G_1 G_2} + \cdots \tag{3.7}$$

$$NF = 10 \log_{10} F \text{ dB} \tag{3.8}$$

Due to noise figure of the GPS receiver, SNR of the signal is degraded. It is crucial to keep noise figure of the receiver as small as possible since the received signal levels are already below the thermal noise floor.

Noise figure of commercial GPS receivers vary from 3 dB to 10 dB. For instance, total noise figure of the NEO-6M GPS receiver is 3 dB [52] and ZED-F9P has a noise figure of 9.5 dB [53]. Furthermore, these two receivers need an active antenna as it is stated in their datasheets. While NEO-6M needs an active antenna whose gain must be between 15 dB to 50 dB, ZED-F9P needs an antenna having a gain which can takes values from 17 dB to 50 dB. Also, maximum noise figure of the active antennas must be less than 1.5 dB.

After front-end amplification, filtering and performing analog to digital conversion, GPS signal down converted at the baseband. With digital signal processing techniques namely despreading (i.e., correlation) SNR of the signal can be increased at the baseband. As it is discussed before, precorrelation SNR of the signal is negative but after the correlation with local replica of the code, SNR increases and signal becomes over the noise level. Despreading techniques are discussed more thoroughly in Chapter 1.1.2.

After the correlation, the signal is despread and becomes occupying the bandwidth of the navigation data which is 50 Hz. Recalling the Equation (3.1) and Equation (3.4), we obtain the following values.

$$P_N = kT_A BW \cong -156 \text{ dBm} \tag{3.9}$$

$$\text{SNR (dB)} \cong -130 - (-156) = 26 \text{ dB} \tag{3.10}$$

The theoretical increase in the SNR is approximately to 45 dB. Apparently, in practical circuits the increase in the SNR is below than 45 dB since front-end components add noise respect to their noise figure values. If the noise figure of the front-end is not atrocious, the signal is raised above the noise floor after correlation.

The SNR of spread-spectrum signals is a value depending to a certain bandwidth in the receiver under concern. Normalizing SNR values to a 1-Hz bandwidth achieves a bandwidth independent ratio between the signal and the noise. Also, this can be considered as a density giving a name as “carrier-to-noise density” ratio to the metric. Carrier to noise density ratio (C/N_o) can be calculated as shown below.

$$C/N_0 = \text{SNR} \times \text{BW [ratio} - \text{Hz]} \tag{3.11}$$

$$C/N_0 = 10 \log_{10}(\text{SNR} \times \text{BW}) \text{ [dB} - \text{Hz]} \tag{3.12}$$

Typical C/N_o value for a GPS receiver can be calculated as shown below.

$$C/N_0 = 10\log_{10}(-19 \times BW)\ [dB - Hz] \quad (3.13)$$

SNR in a 2 MHz bandwidth is -19dB and SNR in 50 Hz bandwidth is 26dB as calculated above corresponding to 0.0126 and 389 in linear scale respectively giving nominal C/N_o value approximately as 43dB-Hz. While calculating C/N_o, it would be more correct if one takes bandwidth for noise power as 50 Hz. Because the correct noise power bandwidth is one that is tantamount to the digitally modulated carrier's symbol rate.

Note that, as it is discussed before, received noise power and received signal strength vary due to user antenna gain, RF front-end gain, satellite elevation angle, satellite age and the noise figure of the receiver. Therefore, GPS receivers can observe C/N_0 values ranging from 35 dB-Hz to 50 dB-Hz [4].

Additionally, since it is hard to directly calculate the C/N_0 values, there are algorithms estimating C/N_0 values in GPS receivers [54].

To successfully deceive a GPS receiver at least four satellite signals must be generated by the spoofer. As it is stated before, received signal power level in a 2 MHz bandwidth transmitted by a single satellite approximately equals to -130 dBm. Since the spoofer needs at least 4 satellites to deceive the victim receiver, its output power increases by 6 dB. Therefore, output power of the spoofer needs to be adjusted accordingly. If the spoofer wants a 10 dB advantage over the GPS signals, output power of the spoofer can be calculated as shown below.

$$\text{Output power} = -\text{FSPL} + 10\log_{10}(\text{NS}) + (-130) + 10 \quad (3.14)$$

where FSPL is the free space path loss between the spoofer and the victim receiver and NS is number of the satellites simulated.

Since GPS is a CDMA system, increasing number of channels will increase the total power transmitted at the output of the spoofer but each channel will look like noise to each other, therefore although output power of the spoofer increases, C/N_0 values will decrease by adding each satellite. This property can be useful to adjust C/N_o values of the attacks. Figure 3.4 shows contribution of each receiver to band power.

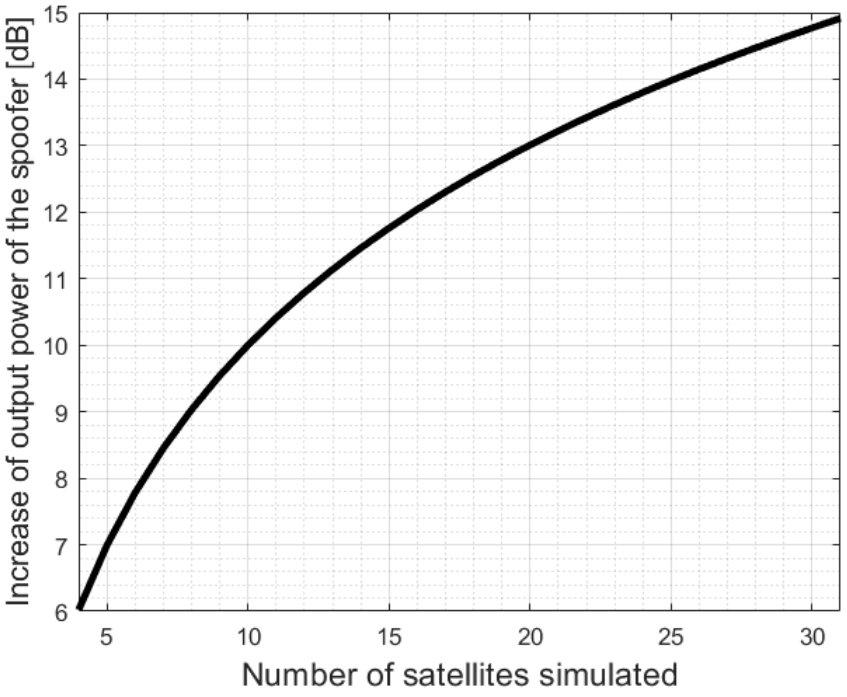

Figure 3.4. Increase of the output power of the spoofer respect number of satellites

To deceive a victim GPS receiver without raising any flags regarding to power changes at the input of the receiver is hard to implement since a transmitter having wide dynamic range must be implemented. While for a static scenario, dynamic range of 10 dB can be enough, for a dynamic scenario this can be more extreme.

Furthermore, to adjust output power of the transmitter located at spoofer, the spoofer needs to know the precise position of the victim receiver and monitor the skyline to know amount of visible satellites which complicates the design of the spoofer. Also,

if the path loss between the spoofer and the victim receiver is exceedingly inconsistent, determining required transmitter power becomes highly variable. It is obvious that implementing a transmitter having these properties is arduous. Therefore, power monitoring methods coupled with C/N_o monitoring provides simple yet effective solutions against spoofing and interference detection.

A problem toward this kind of spoofing detection can be created by man-made signals other than GNSS can deteriorate performance of the metrics if the signals lie in the spectrum of the GNSS signals which will increase the measured noise levels.

In [55], noise floor measurements in both rural and urban areas are investigated.

With RF front-end designed for measuring noise power and GPS signal levels shows that both in rural and urban areas percentage of man-made signals is very low in GPS L1 band in [55]. The band can be considered as pristine and quiet. Therefore, if the power monitoring techniques raise a flag, its probability caused by an intentional interference or a spoofing attack is high. Furthermore, consistency between urban and rural areas gives a chance of a unified threshold for the power monitoring metrics. The spoofing detection metrics do not require to be modified for each specific area.

As it is discussed before, power monitoring can be implemented by using a COTS receiver by utilizing its AGC and C/N_o data. But AGC data may not provide sensitive measurement around noise floor levels which makes receiver vulnerable to GPS spoofing attacks around noise floor levels. A more precise measurement can be implemented by using RF power detectors providing analog measurement of the noise power levels. This can be realized at both IF and RF domains as can be seen on Figure 3.5 and Figure 3.6. But it must be noted that absolute power monitoring needs additional hardware making the system design more complex.

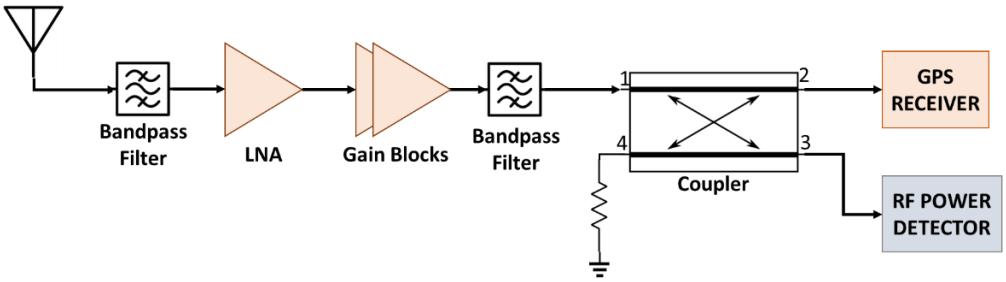

Figure 3.5. RF Front-End with analog absolute power monitoring at RF

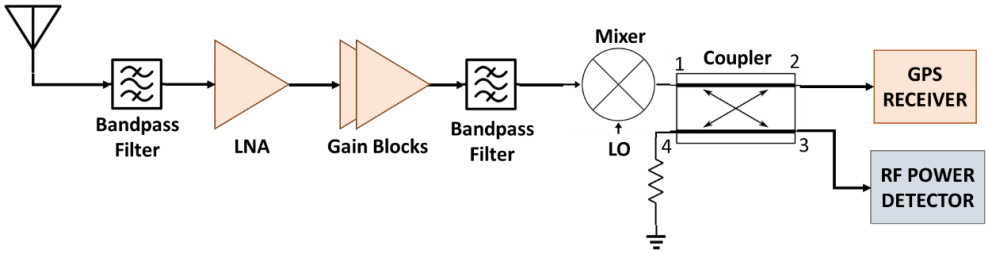

Figure 3.6. RF Front-End with analog absolute power monitoring at IF

Since COTS GPS receivers provide enough data to monitor noise level of the GPS band, it would be more practical to obtain data from COTS GPS receivers for the systems who has already employed COTS receivers in their receiver chain.

3.3 Automatic Gain Control

Automatic gain control is an essential property in many modern systems where incident signals having high dynamic range must be administered. AGC circuitry automatically adjusts gain of the receiver chain to set output signal level in a desired value. Since Analog-to-digital converters have a certain dynamic range, incident power level to ADC is neither too high to saturate the ADC nor falls below a noise level.

Dynamic range of an ADC is correlated with its number of bits. Dynamic range of an ADC is six times the number of bits in decibels. For example, dynamic range of a 10-bit ADC is 60 dB [56]. ADCs are one of the most power consuming components in a chain. ADCs having higher dynamic ranges have more complex topologies leading more power consumption. Therefore, it is important to have AGC circuitries in a receiver chain regulating incoming signal strength and increasing dynamic range of the ADCs. Automatic gain control circuitries can be implemented at RF, at IF or at baseband section of the receiver.

There are two different topologies to implement AGC circuitries which are feedforward loops and feedback loops. If input of the variable gain amplifier is employed for detection, topology is defined as feedforward loop, if the output of the amplifier is sensed then AGC is defined as feedback loop. Second topology is preferred in the GPS receivers and can be seen in Figure 3.7. Furthermore, feedback loop is more popular since it provides higher linearity and demands narrower dynamic range [56].

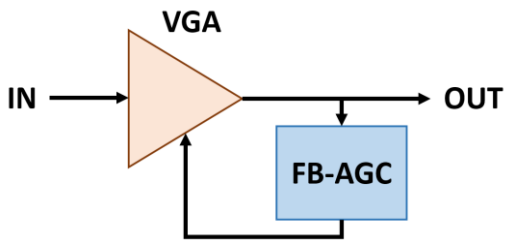

Figure 3.7. AGC architecture popular among GPS receivers

3.3.1 Why AGC is Used in GPS Receivers?

There are three primary reasons why automatic gain control circuitries are used in GPS receivers. These are increasing dynamic range, quantization level control and pulse interference suppression [57]. First two goals are adapting to varying levels of gain provided by the active antenna designs since it is not practical to define a common certain specification for GPS antennas around the world [27]. Also, additive noise from the cascaded front-end components is different for each design which emerges a need of an adjustment for each receiver. Furthermore, it should be noted that although signal power level of global positioning system lies beneath the thermal noise floor, power level of the noise signal is not stable and requires AGC [23]. Third objective is adjusting the gain in the presence of an RF interference. If one examines the spectra of the authentic GPS signals from the air, they will look like noise obeying Gaussian distribution. But when an interference is added to the GPS signals, it becomes a sine wave and the dynamic range of the whole signal becomes enormous so AGC must be included in pragmatic applications [58].

3.3.2 AGC Monitoring for Spoofing and Interference Detection

As it is discussed in Chapter 3.1, absolute power monitoring can detect presence of an attack against global positioning systems. AGCs have power monitoring systems to dynamically adjust the output power of the automatically gain controlled amplifiers. Many GPS receivers employ automatic gain control circuitries to increase dynamic range of their ADCs. Therefore, if it is desired to build a GPS receiver having capability of detecting spoofing signals, absolute power monitoring function can be realized with an AGC circuitry.

It is desirable to implement lower-bit ADCs in a receiver system since they are easy to implement, they have low power consumption and their sizes are smaller. But ADCs having lower number of bits have smaller dynamic ranges. It is crucial to have

smaller size along with low power consumption for mobile systems. Therefore, lower-bit ADCs is favorable to complete the RF receiver chain. To use lower-bit ADCs, AGCs can be employed to increase its dynamic range.

Spoofing and interference detection with gain monitoring of the AGC circuitries have many advantages as discussed in Chapter 2. One of the advantages is that AGC circuitries are readily available in many COTS GNSS receivers due to their advantages discussed above, thus no additional hardware is needed. Combining AGC monitoring with $\mathrm{C/N_o}$ monitoring can provide determining whether the attack is a spoofing or an interference [29].

3.3.2.1 Developing Practical Thresholds for AGC and $\mathrm{C/N_o}$ Monitoring

Threshold for AGC coupled with $\mathrm{C/N_o}$ monitoring can be developed using empirical data as presented in Chapter 2. Apart from determining a threshold with empirical data, according to a technique offered in [30], the determining a threshold may not depend to empirical data.

Empirical data can be examined by using sliding window technique to prevent from false alarms. Moving average technique can reduce false alarms since it collects and takes average of the AGC and $\mathrm{C/N_o}$ values which smoothens the data.

Sliding window for moving average is defined as shown below.

$$\vec{\Delta}\psi_i = \psi_i - \frac{1}{N}\sum_{j=1}^{N}\psi_j \tag{3.15}$$

where $\vec{\Delta}\psi_i$ is the sliding window metric, which are in our case $\vec{\Delta}\mathrm{AGC}$ or $\vec{\Delta}\mathrm{C/N_0}$. ψ_i is the instantaneous reading and $\frac{1}{N}\sum_{j=1}^{N}\psi_j$ is the moving average for the readings. It is important to note that Equation 3.15 of $\vec{\Delta}\mathrm{C/N_0}$ is processed with the strongest

visible satellite. For instance, if there are 13 visible satellites over the horizon, the highest C/N_0 value is taken account, other 12 C/N_0 levels are not processed with the metric. Because C/N_0 values can vary due to changing elevation angles of the satellites relative to receiving antenna which fluctuates the C/N_0 values over a period.

After gathering C/N_0 values of the satellites of clean non-spoofed skyline on a clear day over a time, the highest C/N_0 values of the satellites must be determined. These values create a baseline for C/N_0 readings. Note that each receiver configuration has its own gain and noise figure values, some of them uses active antennas while other does not, therefore each receiver has differences in C/N_0 readings. Since each receiver chain result different C/N_0 values in the same conditions, each receiver must be calibrated before performing spoofing detection tests. This task can be achieved by gathering C/N_0 values of the satellites over a period of clean non-spoofed skyline on a clear day.

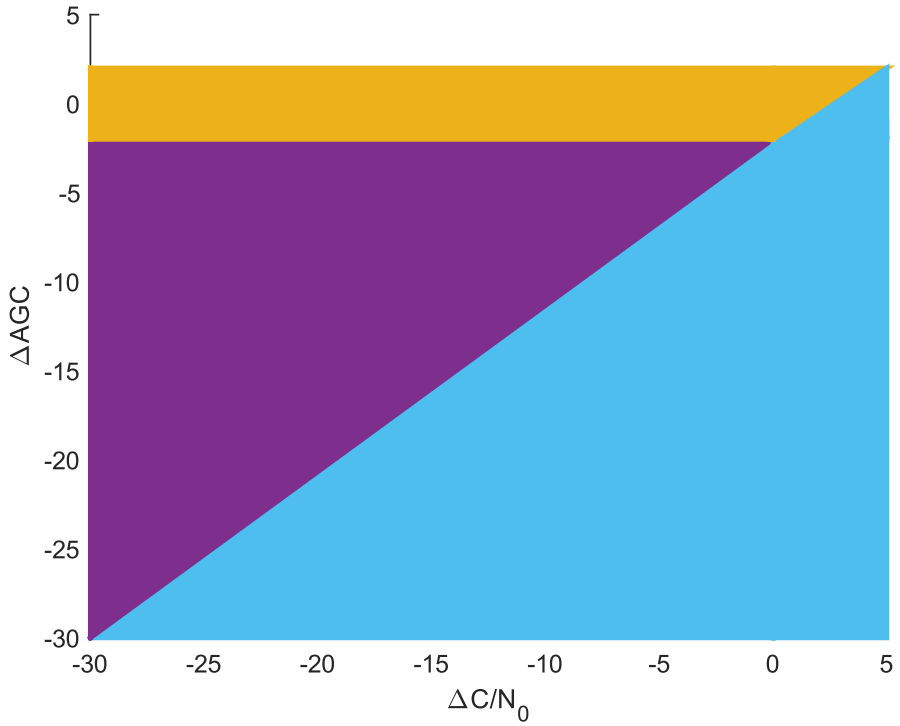

Figure 3.8. Received power monitoring thresholds [30]

In Figure 3.8, there are four main zones representing nominal case and intentional interference cases which are jamming and spoofing interference attacks.

Orange band represents AGC and C/N_0 relation of the authentic GPS signals. In nominal case, C/N_0 of the received signals have a variance explaining the span of the orange band. In nominal case, C/N_0 values that are measured by a certain receiver can change due to weather conditions, age of the satellites on the visible sky, and unintentional interference sources.

Blue zone represents spoofing likely region of the AGC - C/N_0 graph. Spoofing signals having smaller power advantage over authentic signals do not cause a significant drop in AGC values. On the other hand, even spoofing attacks having subtle advantage over authentic signals causing higher C/N_0 levels that eases to detect presence of a spoofing attack. Higher amplitude of spoofing signals causes higher C/N_0 values and higher AGC drop.

Purple zone characterizes cases which jamming attacks are more likely. As amplitude of the jamming signals increases, the more C/N_0 drop and AGC drop occurs.

Furthermore, while higher C/N_0 indicates presence of a spoofing attack, smaller C/N_0 values are not necessarily caused by jamming attacks. Smaller C/N_0 can be an indication for a spoofing attack equipped with noise padding.

As an improvement for power monitoring, if a GPS receiver is wanted to be implemented in a system without using a COTS receiver, practical small size AGC circuitries can be designed by using a variable gain amplifier, a coupler and an RF power detector. This circuitry can be realized at RF section or at IF section the receiver or at the baseband. Lots of GPS receivers use direct conversion receiver topology, therefore radio frequency is directly down converted to baseband frequency. But as it is stated in [4] and [3] receivers may have an IF section which gives a possibility that implementing AGC circuitries at IF section.

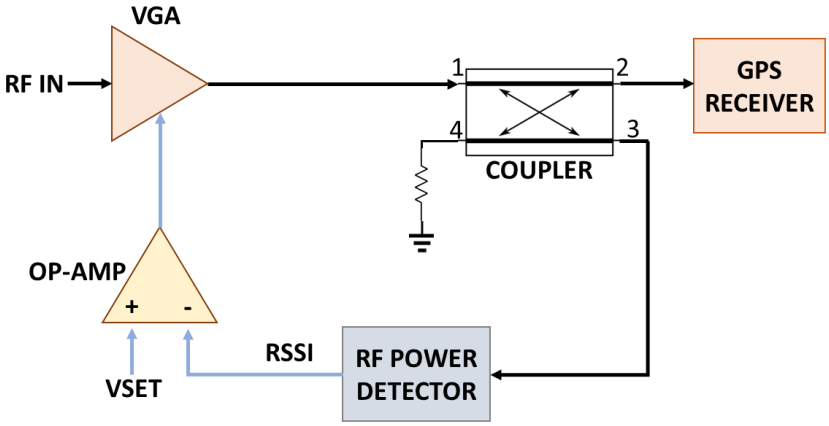

Figure 3.9. Practical AGC Circuitry at RF Domain

As can be seen from Figure 3.9, gain setting of the VGA can be regulated by measuring its output power. If output power of the VGA is higher than its expected value, the gain is reduced, otherwise the gain is increased. There are two major classes of VGAs which are input VGA (IVGA) and output VGA (OVGA) [59]. Both VGA types have fixed-gain stages and variable gain or variable attenuation stages. While in IVGA topology, a variable attenuation stage is followed by a fixed gain stage [60] in a OVGA topology fixed gain stage is followed by a variable gain stage. It is preferable to design AGC systems with IVGAs since low distortion at its output port which is independent from its gain setting. OVGAs are not suitable to be used for AGC applications because their output signal handling capability is low. But note that, IVGAs comprise of attenuators before their gain. If we recall the Friis formula [50], total noise figure of a receiver system is affected most by the beginning of the system. Hence, we can say that noise figure of the IVGA topology is not ideal to design a low noise receiver. Therefore, performance of the receiver would be better in terms of noise figure if AGC amplifiers are not used at the beginning of the receiver chain. It is important to provide adequate gain before these amplifiers to reduce total noise figure of the receiver chain.

3.3.3 Detection for Other GNSS Constellations

Since Galileo, Beidou and IRNSS are all CDMA systems, power monitoring systems introduced above can be applied to Galileo, Beidou and IRNSS satellite systems. This makes power monitoring systems highly adaptable to other constellations and effective solution to determine intentional interference attacks against GNSS.

3.4 Signal Quality Monitoring

Signal quality monitoring techniques have drawn significant interest and have been favored for spoofing detection because of their simplicity and efficacy. SQM metrics are calculated from correlator outputs of the code tracking loops. The main objective of tracking loops is enhancing accuracy of frequency and code phase factors, keeping track and demodulating the navigation data from a specific satellite.

To examine behavior of the correlator outputs under spoofing conditions, initially it is convenient to analyze nominal case of the tracking stage of the receiver. As can be seen from Figure 3.10, incoming GPS signal is demodulated by first mixing with the carrier wave replica and then PRN code replica. It is important that tracking loop must generate exact replicas of both the carrier and the code arising a need for phase locked loops.

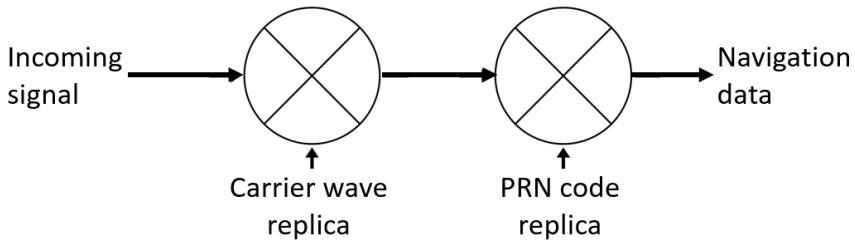

Figure 3.10. Demodulation scheme

At the input of the receiver, L1 C/A signal can be shaped as shown below.

$$s^k(t) = \sqrt{2P_C}C^k(t)D^k(t)\cos(2\pi f_{L1}t) \tag{3.16}$$

where P_C represents received signal power from satellite k, $C^k(t)$ and $D^k(t)$ denotes C/A code sequence and navigation data correspondingly. Also, $\cos(2\pi f_{L1}t)$ is the carrier signal and f_{L1} is the frequency of the carrier signal.

After down conversion and A/D conversion, the signal becomes discrete in time with n in units of $1/f_s$.

$$\mathrm{s}^k(n) = C^k(n)D^k(n)\cos(\omega_{IF}n) \tag{3.17}$$

Recalling the main goal of the tracking loops as obtaining the navigation data, it is obvious that carrier removal must be done. Carrier removal is done by multiplying the incoming signal with its replica as shown in Figure 3.10.

After multiplying the signal with carrier copy, the dot product becomes as shown below.

$$\mathrm{s}^k(n)\cos(\omega_{IF}n) = -\frac{1}{2}C^k(n)D^k(n) - \frac{1}{2}\cos(2\omega_{IF}n)\,C^k(n)D^k(n) \tag{3.18}$$

First term can be obtained by applying low pass filtering operation. Hence, we get,

$$\frac{1}{2}C^k(n)D^k(n)$$

Following stage is removing the code $C^k(n)$ and obtaining navigation data from the signal. In similar manner to carrier removal, this is done by mixing local replica of the code.

If the code replica is duplicate to incoming code, output of the correlation gets the following form where $ND^k(n)$ is the navigation message multiplied by the N number of points in the signal.

$$\sum_{n=0}^{N-1} C^k(n)C^k(n)\,D^k(n) = ND^k(n) \tag{3.19}$$

In the case of a spoofing attack, authentic and spoofing signals will be combined.

$$\begin{aligned} s^k(t) &= \sqrt{2P_C}C^k(t)D^k(t)\cos(2\pi f_{L1}t) \\ &+ \sqrt{2P_{C_{spoof}}}C^k_{spoof}(t)D^k_{spoof}(t)\cos(2\pi f_{L1}t) \end{aligned} \tag{3.20}$$

Receiver will process the combined signal in a same manner that it does in authentic signals. At the end, receiver will obtain following signal.

$$\sum_{n=0}^{N_{auth}} C^k(n)C^k(n)\,D^k(n) + \sum_{n=0}^{N_{spoof}} C^k_{spoof}(n)C^k_{spoof}(n)\,D^k_{spoof}(n) \tag{3.21}$$

After outlining the general tracking algorithm under nominal and spoofing conditions, PLL and DLL architectures can be discussed. But output parameters of DLL architecture will be discussed more comprehensively since the thesis employs output of the DLL correlators for spoofing detection.

As can be seen from the equations shown above, signal transmitted from the satellites is a bi-phase coded signal. The carrier and C/A signals are received and their frequencies change due to Doppler effect caused by the motion of the satellites and the receiver. To successfully track the GPS satellites, both C/A code and carrier signal must be removed. As a result, the receiver requires two phase-locked loop architectures. Aim of the one of the loops is tracking phase of the C/A code and the other one is the carrier. These two loops must be coupled together as shown in Figure 3.11. Also, it can be seen from the figure, code duplication coming from the code

tracking loop is used to clear C/A code at the beginning of the carrier loop and carrier replica coming from carrier loop clears carrier at the beginning of the code loop.

Code loop generates three outputs if it employs three correlators. These are early, prompt and late. These values are generated by using three local replicas having a phase difference of half chip.

Output of the correlators are compared with each other, then output of the prompt correlator is applied to input by multiplied with the input signal at the beginning of the carrier loop. Figure 3.11 shows the procedure described above.

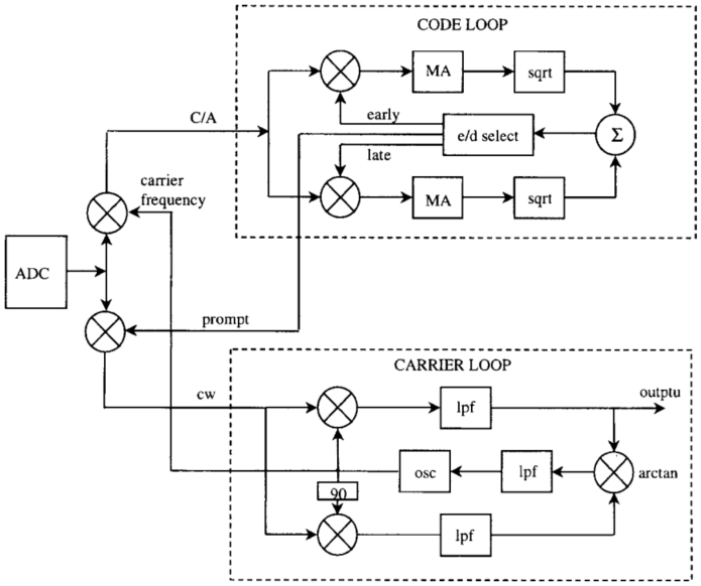

Figure 3.11. Simplified block diagram of DLL and PLL tracking loops [1]

Code phase is being tracked by using correlation property of the codes. After correlation, outputs of the correlators are compared to each other. If amplitude of the late correlator is the highest one, then code phase must be decreased. If prompt replica causes the highest peak, it can be deducted that the phase is properly tracked.

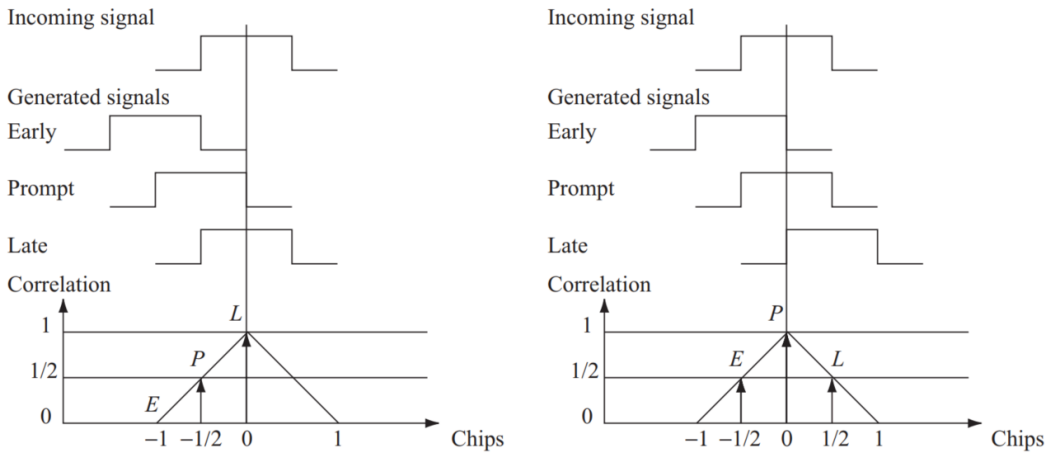

Figure 3.12. Correlation outputs respect to phase of the incoming signal [3]

Ideally, output of the correlation operation is a triangle as can be seen from Figure 3.12. But this only occurs when the bandwidth is not limited. Figure 3.13 shows effect of the limited bandwidth. In practical cases, bandwidth of the receiver is limited causing a round peak in correlation functions. This issue affects spoofing detection algorithms that use the correlation functions. It can be interpreted that, each receiver having different bandwidth values must be evaluated separately when an algorithm regarding to correlation values are employed.

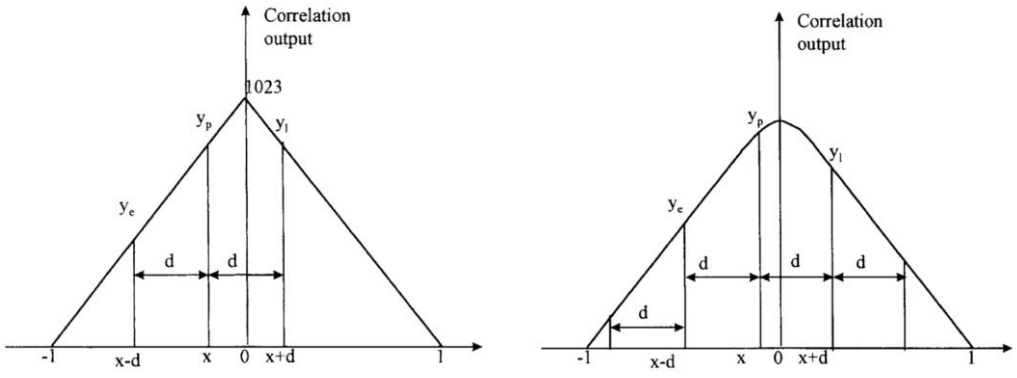

Figure 3.13. Correlation outputs with wide bandwidth and limited bandwidth [1]

DLL with three correlators would not be the ideal design if there is a phase error on the local carrier wave making the signal noisier. Therefore, six correlators are used.

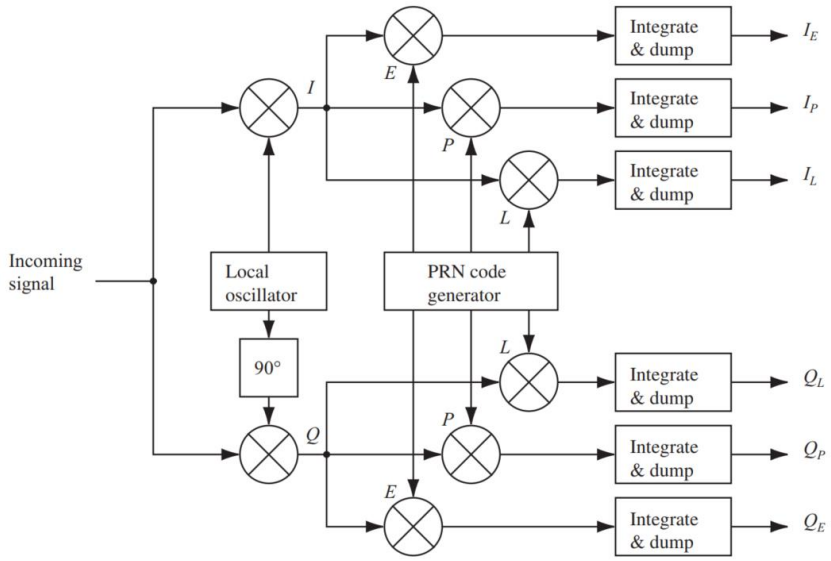

Figure 3.14. Code tracking loop having six correlators [3]

Figure 3.14 depicts total DLL block producing in-phase and quadrature terms. When the local carrier wave is in phase with the input signal, all the energy is deployed in the in-phase arm. In signal quality monitoring methods, these in-phase components of the correlation functions are monitored as can be seen from following section.

3.4.1 Ratio Test Metric

Ratio test metric aims to distinguish the presence of a "deadzone" at the top of correlation function. As it is defined in [34] ratio test metric can be computed as shown below. The metric is easy to utilize thus it is applicable to implement in commercial off-the-shelf receivers.

$$R[k] = \frac{I_E[k] + I_L[k]}{\xi\, I_P[k]} \tag{3.22}$$

where I_E, I_L and I_P are in-phase components of early, late and prompt correlators respectively. Note that assuming to work with a locked PLL, the outputs of $I_E[k]$,

$I_L[k]$ and $I_P[k]$ can be modeled as individually and identically distributed Gaussian process. Independent white noise samples of the received signal produce statistically independent yields and their probability density function is Gaussian. ξ is a constant factor representing the slope of the correlation function. If correlator spacing is equal to the chip duration, ξ becomes equal to 2 [34].

Note that the ratio metric is a ratio between two Gaussian random processes. Hence, the summation is no longer Gaussian which makes $R[k]$ as non-Gaussian metric. But if the noise component of the prompt correlator is negligible, $I_P[k]$ can be treated as a constant value. Since the noise is low, value of the $I_P[k]$ is determined with only received signal power itself. With the hypothesis introduced above, $R[k]$ can be written as shown below.

$$R[k] = \mu[k] + N[k] \tag{3.23}$$

where $\mu[k]$ is the mean value determined by the signal and $N[k]$ is a zero mean independently and identically distributed Gaussian process. Its known variance is σ^2 whose value depends on noise power, shape of the correlation function and the distance between correlators. Approximation in Equation (3.23) is realistic when $\mathrm{C/N_0}$ levels seen by the receiver is high. Especially for the signals having $\mathrm{C/N_0}$ levels higher than $46\ \mathrm{dB/Hz}$ [33].

A Neyman-Pearson detector can be used to determine the decision between two hypotheses. Let the hypothesis H_0 be clean dataset and H_1 spoofing present dataset whose mean values are μ_0 and μ_1 respectively. H_0 is named as null hypothesis and H_1 as alternative hypothesis [61]. Two hypotheses can be formulated as shown below.

$$\mu[k] = \begin{cases} \mu_0 \rightarrow H_0 \\ \mu_1 \rightarrow H_1 \end{cases} \tag{3.24}$$

While μ_0 is constant, μ_1 is determined by the properties of the spoofing signal like ratio and delay between spoofing and authentic signal. Now, a likelihood ratio must be defined to be compared against a threshold which gives the detection of presence of spoofing. Likelihood ratio test can be defined as shown below.

$$LR(R[k]) = \frac{p(R[k]; H_1)}{p(R[k]; H_0)} > \gamma_L \tag{3.25}$$

$p(R[k]; H_1)$ and $p(R[k]; H_0)$ are probability density function of the random variable $M[k]$ and γ is the threshold. Likelihood ratio becomes like shown below if epoch k dependence is omitted. Note that the following equation is valid when $\mu_1 - \mu_0 > 0$.

$$R > \frac{\sigma^2 ln(\gamma_L)}{\mu_1 - \mu_0} + \frac{\mu_1 + \mu_0}{2} = \gamma \tag{3.26}$$

Note that, NP theorem aims the maximum probability of detection for a fixed probability of a false alarm. Threshold value can be obtained directly from the following equation for a given fixed PFA value if M is assumed to be Gaussian, as its requirements discussed above.

$$\gamma > \sqrt{2}\sigma \cdot erfc^{-1}(2P_{FA}) + \mu_0 \tag{3.27}$$

Furthermore, it can be deducted from Equation (3.26), as $\mu_1 - \mu_0$ approaches zero, threshold value diverges to infinity. This means that mean values of the two cases must be distinct. Since μ_1 increases rapidly when there is a spoofing attack in phase with the satellite signal, it is practical to use this metric as a spoofing indicator [33]. Variance of the correlators can be calculated with the equation shown below.

$$\sigma = \frac{N_0}{2T_I} \tag{3.28}$$

where N_0 is the noise density and T_I is the coherent integration time. It is easy to obtain coherent integration time value when software defined GNSS receivers are used. GNSS-SDR [54] is a software defined GNSS receiver allowing to configure specifications of the receiver. Coherent integration time of the receiver can be set by providing a suitable configuration to the receiver. More details about GNSS-SDR will be discussed in Chapter 4.

To evaluate ratio metric under different noise levels, a parameter taking ratio between mean and variance values of the metric can be defined.

$$\tau = \frac{\Delta\mu}{\sigma} \tag{3.29}$$

$\Delta\mu$ represents difference between mean value of the ratio metric under spoofing and nominal conditions and σ is variance of the metric. As noise increases, C/N_0 decreases hence σ decreases. This leads to threshold values of the ratio metric increase. Therefore, detection capability of the metric deteriorates. τ takes high values when the noise is negligible which corresponds to lower thresholds. ROC curves for different noise levels are shown below.

Figure 3.15 below clearly shows that, detection success of the metric is superior on higher C/N_0 levels which corresponds to lower noise levels. This gives the opportunity to discriminate spoofing attacks from variation of the metric due to noise.

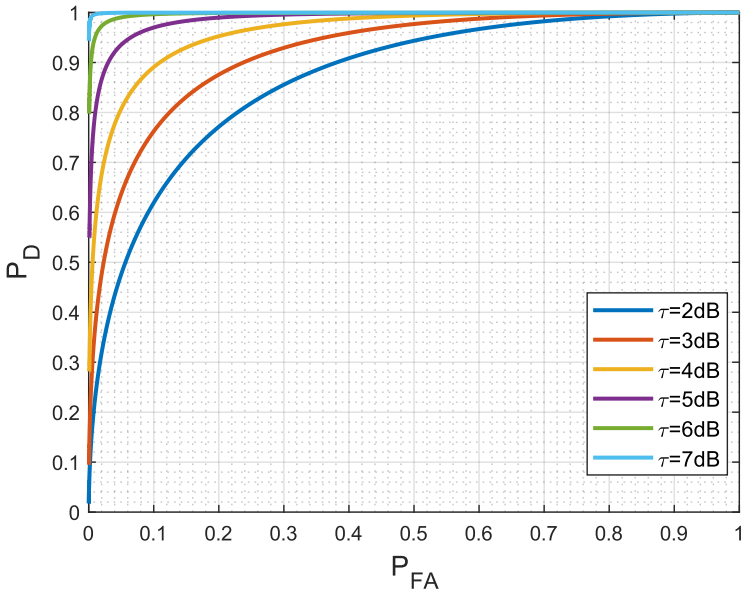

Figure 3.15. ROC curves for ratio metric under different noise levels

Receiver operating characteristic (ROC) curve is a graphic interpretation illustrating the analytical capability of a binary classifier. The curve is built by depicting the probability of detection versus probability of false alarm. Each point on the curve corresponds to a certain value of P_D and P_{FA} for a given threshold.

ROC curve must be above a line whose slope is 45 degrees. This line represents a detector that makes the decision by ignoring the data. The further ROC curve from this line means better detection performance. As can be seen from the Figure 3.16, ratio detector performs better when conditions on the turquoise line is present. Worst detection performance occurs when conditions in blue line occurs which corresponds to higher noise levels.

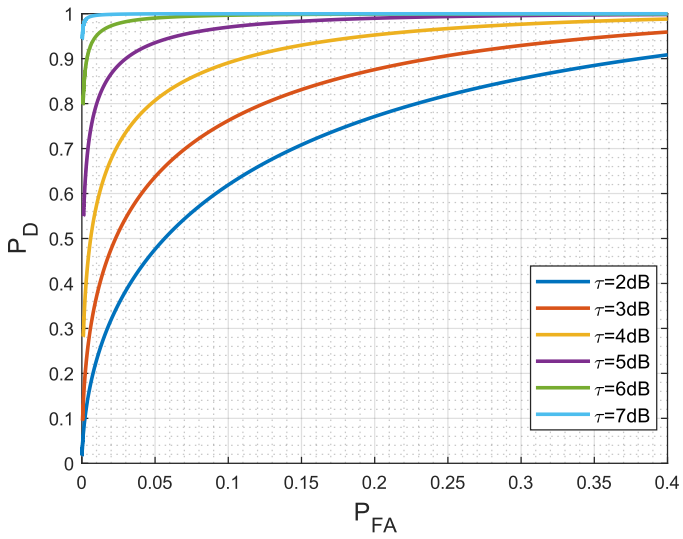

Figure 3.16. Examining ROC curves for smaller PFA values

Figure 3.15 and Figure 3.16 demonstrate that if noise of the ratio metric is small and spoofing attack changes mean values of the metric greater than variation caused by the noise, metric can successfully detect the attacks. Smaller noise enhances the performance.

$R[k]$ is a noisy metric therefore it is practical use sliding window technique for moving average that is introduced in AGC monitoring chapter. Note that both multipath and spoofing phenomenon cause $R[k]$ metric giving a flag. But if sliding

window technique is used for the noisy data, it can help to discriminate between spoofing and the multipath. Since multipath creates peaks at $R[k]$ metric for a shorter duration than peaks created by spoofing [37].

For a successful spoofing detection, first mean and variance values of the clean dataset must be examined. Acquired values are used for threshold calculation for a desired PFA. Then, for a determined window length, spoofing can be detected if there is a cumulative flag above thresholds. This procedure can be applied to other SQM metrics discussed below.

3.4.2 Delta Test Metric

Goal of the delta test metric is detecting asymmetries of the correlation peak. The metric can be calculated as the difference of the linear mixture of multiple correlator values as shown below as it is defined in [62].

$$\Delta[k] = \frac{I_E[k] - I_L[k]}{\xi\ I_P[k]} \tag{3.30}$$

Delta metric is symmetric, therefore under spoofed-free and multipath-free conditions, $\mu_\Delta = 0$ [62]. Furthermore, under clean conditions, nominal variance equals to $(C/N_0\ T_I)^{-1}$.

3.4.3 Early Late Phase Test Metric

This metric computes the phase disparity between the early and late correlators. It is the only metric incorporating the quadrature components. Like the delta ratio, mean value of the early late phase metric is $\mu_{\mathrm{ELP}} = 0$ when there is no spoofing [35].

$$ELP[k] = \tan^{-1}\left(\frac{Q_L[k]}{I_L[k]}\right) - \tan^{-1}\left(\frac{Q_E[k]}{I_E[k]}\right) \tag{3.31}$$

3.4.4 Magnitude Difference Test Metric

The magnitude difference metric as described in [62] is shown below.

$$MD[k] = \frac{|x_E[k]| - |x_L[k]|}{|\,x_P[k]|} \tag{3.32}$$

where $|x_E[k]|$, $|x_L[k]|$ and $|x_P[k]|$ are magnitudes of the correlation functions for early, late and prompt values. This metric also offers symmetry like delta metric meaning that its interference and multipath-free value must equal to 0 giving that $\mu_{\mathrm{MD}} = 0$.

3.4.5 Sliding Window Techniques

Sliding window technique for moving average is previously introduced in $\mathrm{C/N_0}$ monitoring methods. In this chapter, another smoother technique named as sliding window for moving variance is discussed. This metric is computed as shown below.

$$MV[n] = \frac{1}{w}\sum_{i=(n-1)w+1}^{n+w} x(i)^2 - \left(\frac{1}{w}\sum_{i=(n-1)w+1}^{n+w} x(i)\right)^2 \tag{3.33}$$

where $x(i)$ is the value of the existing sample, w is the length of the one sub domain and n is the number of sub domains.

Sliding window for moving variance is computed by taking difference between the mean of the squares of the sub domain and square of the mean over the sub domain [37]. Then the window shifts to next sub domain and makes the same calculations as can be seen from the Figure 3.17.

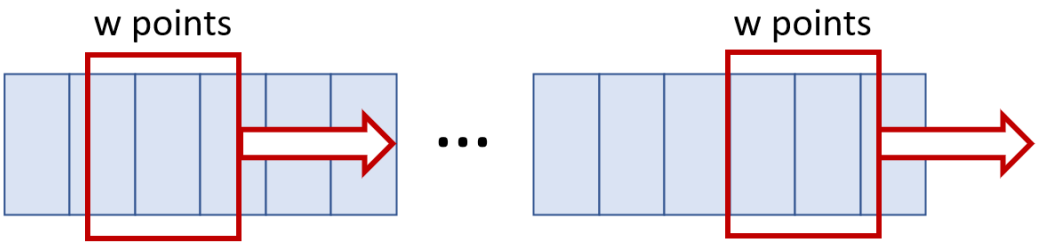

Figure 3.17. Computation of sliding window metric

3.4.6 Determining Thresholds for SQM Metrics

As discussed previously, under the assumption of SQM metrics being a Gaussian distributed variable, PFA can be computed for certain upper and lower thresholds as shown below [37].

$$P_{fa} = \int_{Th_u}^{\infty} f_c(x)dx + \int_{-\infty}^{Th_l} f_c(x)dx = erfc\left(\frac{Th_u - \mu_i}{\sqrt{2\sigma_i^2}}\right) \tag{3.34}$$

$$P_{fa} = erfc\left(\frac{Th_u - \mu_i}{\sqrt{2\sigma_i^2}}\right) = erfc\left(\frac{\mu_i - Th_l}{\sqrt{2\sigma_i^2}}\right) \tag{3.35}$$

where $f_c(x)$ represents the probability density function of the selected SQM metric in the absence of interference sources and $erfc(\cdot)$ is the complementary error function. For a selected PFA, upper and lower thresholds can be obtained by using the expressions shown below.

$$Th_u = \mu_i + \sqrt{2\sigma_i^2}erfc^{-1}(P_{fa}) \tag{3.36}$$

$$Th_l = \mu_i - \sqrt{2\sigma_i^2}erfc^{-1}(P_{fa}) \tag{3.37}$$

σ_i^2 is the nominal variance of the selected SQM metric and can be calculated as shown below [37].

$$\sigma_i^2 = \delta \cdot \sigma_0^2 = \frac{\delta}{2T_{int} \cdot C/N_0} \tag{3.38}$$

δ takes value of 1 when the selected metric is ratio metric, takes value as 2 when the metric is delta metric and 8 for the ELP metric. δ also depends on correlator spacing, the values given above is valid when correlator spacing equals to 0.5chip. T_{int} is the integration time [37]. By using clean datasets, parameters above can be computed to obtain thresholds for each SQM metric.

Threshold of sliding window of moving variance for each PRN can be computed as shown below [37].

$$Th = \mu_i + m_{exp} \cdot \sigma_i \tag{3.39}$$

In Equation (3.39), μ_i is the long period mean value of the moving variance of clean dataset. m_{exp} is the expansion factor related to probability of false alarm. Finally, σ_i is the standard deviation of the moving variance of clean dataset.

Expansion factor values takes certain values for each PFA. By determining the desired PFA, expansion factor can be chosen. Table for each expansion factor respect to PFA values can be seen on [37].

CHAPTER 4

IMPLEMENTATION AND RESULTS

4.1 Generating Spoofing Signals

On chapter 2.1, various spoofing methods are discussed. On this thesis spoofing methods employing GPS signal simulator are implemented. As a GPS signal simulator, an open-source software is used [21]. After creating GPS signals, to convert IQ pairs and generate physical RF signals, software defined radios can be utilized.

GPS-SDR-SIM can produce either static or dynamic scenarios. While in static scenario, RINEX navigation file for GPS ephemerides, latitude, longitude and height information are required, to create dynamic scenario, additional to RINEX navigation file, a user motion file in ECEF format is required. But sampling rate of the user motion data must be 10 Hz. By using those information, GPS-SDR-SIM can generate the simulated pseudo range and Doppler for the GPS satellites in view. Then simulated range data is used to create I/Q samples stored in a binary file that can feed an SDR to be transmitted through.

HackRF requires signed bytes as an input data format, ADALM Pluto demands signed 16-bit interleaved I/Q pairs. Since each SDR has DACs having different properties, binary files must be created accordingly to each SDR.

While HackRF comprises of 8-bit DAC, ADALM Pluto comprises of 12-bit DAC. Since ADC and DAC of the ADALM Pluto has higher number of bits, it has better

dynamic range than HackRF. This property can be useful to increase SFDR by making GPS spoofing signals much higher than unwanted spurious signals.

Table 4.1 Preferred data types for selected SDRs

Name of the SDR	*Sample Stream*	*Number of Bits*
HackRF	$[S_0^I], [S_0^Q], [S_1^I], [S_1^Q], \ldots$	8+8
ADALM-Pluto	$[S_0^I], [S_0^Q], [S_1^I], [S_1^Q], \ldots$	16+16

HackRF is a half-duplex transceiver system comprising of a direct conversion (zero-IF) topology [63]. ADC and DACs of the HackRF can operate up to a sampling frequency of 20 Msps. Since it is a direct conversion transceiver, this corresponds to an RF bandwidth of up to 20 MHz. On the other hand, ADALM Pluto employing AD9363 having one transmit and one receive channel offers a full-duplex transceiver system. Sampling frequency of the ADALM Pluto can be adjusted up to 20Msps which again corresponds to an RF bandwidth of 20 MHz.

As it is discussed on Chapter 1.1.3, reference clock of the systems plays an important role. To keep errors created by the hardware of the system low, a reference clock having low phase noise and high stability must be employed.

ADALM Pluto uses Rakon's 40 MHz RXO3225M low jitter crystal oscillator. Its total frequency stability due to temperature change, initial start-up, supply variation and load variation is ±25 ppm [64]. This is a problematic issue since GPS needs a highly stable reference clock as it is discussed on previous chapters. Furthermore, ADALM Pluto has no capability to be driven from an external clock, therefore it is impractical to be used in GPS applications unless soldering another clock to its board. Conversely, HackRF allows to use external clocks by employing a clock buffer.

Comparison between HackRF and ADALM Pluto shows it would be practical to use HackRF as a GPS simulator since it gives more controllability to its user. Even

though other properties are in favor of ADALM Pluto, HackRF provides enough sampling rate and dynamic range to transmit GPS signals.

Software defined radios use zero-IF topology which creates an issue called as DC spike or LO leakage. This problem originates from imperfectness of the mixer. In the multiplication operation of the baseband signal and LO signal, it is desired to not to observe LO frequency at the output. But generally, this property cannot be satisfied since isolation between the RF port and the LO port is not infinite.

To overcome this problem, certain adjustments can be performed. Baseband gain and IF/baseband amplifier gain of the HackRF can be increased. Baseband gain can be increased by increasing amplitude of the values stored in the I/Q file. IF amplifier gain setting can be increased to improve amplitude of the baseband signals further. Since the LO frequency is not present before mixing operation, high amplification leads to a stronger baseband signal helping to improve difference between amplitude of spurs and RF signal. Figure 4.1 shows output of the SDR with no LO presence.

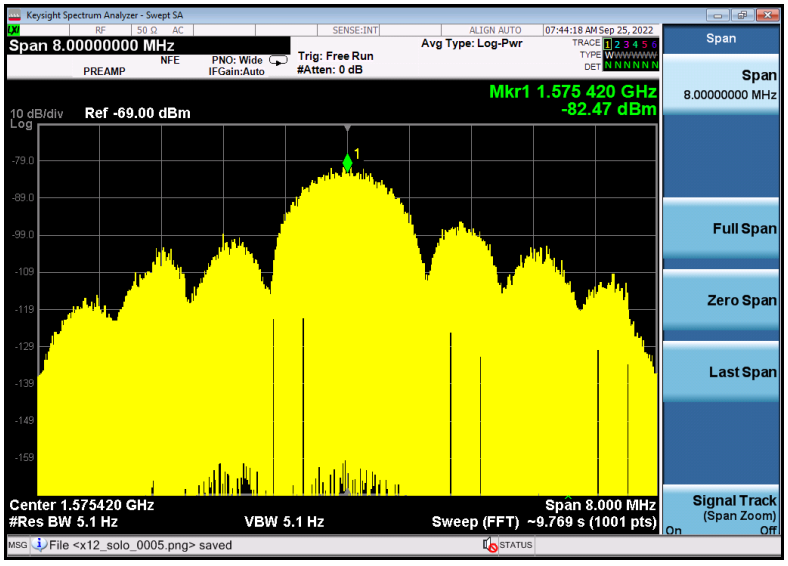

Figure 4.1. Output of the HackRF within 8 MHz bandwidth

Gain of the IF amplifiers can be increased up to 47 dB. In this thesis, rest of the experiments will be conducted by setting gain of the IF amplifiers as 12 dB and I/Q files are configured accordingly to utilize the whole dynamic range of the transmitter

chain of the HackRF. Note that HackRF has an 8-bit DAC, therefore I/Q file provided to DAC has values varying from -256 to 256.

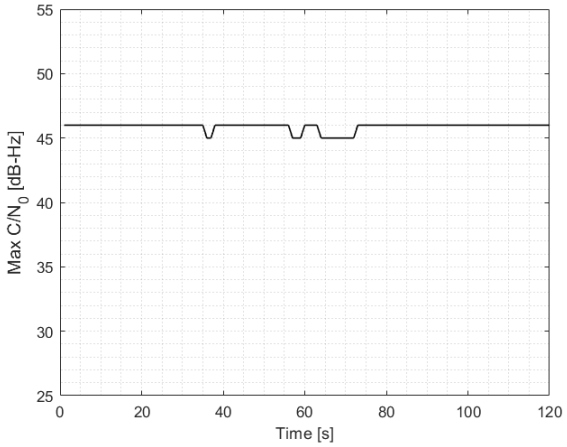

Figure 4.2. Stable C/N_0 values observed by the receiver

For GPS applications, output power of the HackRF must be low even for an overpowered spoofing attack. Therefore, it is crucial to characterize output power of the transceiver correctly to perform successful spoofing attacks having desired power advantage over the authentic GPS signals.

Before building a spoofing test setup and performing spoofing, output power of the HackRF must be characterized. A spectrum analyzer can be employed for precise measurement of the power transmitted by the HackRF.

To be able to measure low signal levels from a spectrum analyzer, settings of the spectrum analyzer must be configured accordingly. Spectrum analyzers contain internal preamplifiers and variable attenuators. Their proper adjustments become crucial for low power applications. The preamplifier of the spectrum analyzer is turned off in its default mode but it can be turned on to be able to decrease noise floor of the amplifier and increase the sensitivity. By turning on the preamplifier, noise floor extension improvement can be up to 12dB [65]. Also, internal attenuation must be adjusted to its lowest level which is 0dB. Furthermore, there is another important property that can decrease noise floor of the spectrum analyzer which is

resolution bandwidth. Resolution bandwidth is defined as 3dB bandwidth of the intermediate frequency filter of the spectrum analyzer. As smaller as it gets, noise floor of the spectrum analyzer falls. Its effect on the noise can be calculated directly by using thermal noise equation.

By taking account concerns mentioned above, settings of the spectrum analyzer are adjusted like shown below in the Table 4.2 for the rest of the thesis.

Table 4.2 Spectrum Analyzer Settings

Parameter	Value
Resolution Bandwidth	1 Hz
Internal Preamplifier	ON
Internal Attenuation	0 dB
Marker Bandwidth	2 MHz

With settings shown in Table 4.2, output of the HackRF is connected to the spectrum analyzer. 2 MHz band power for a single satellite is shown below.

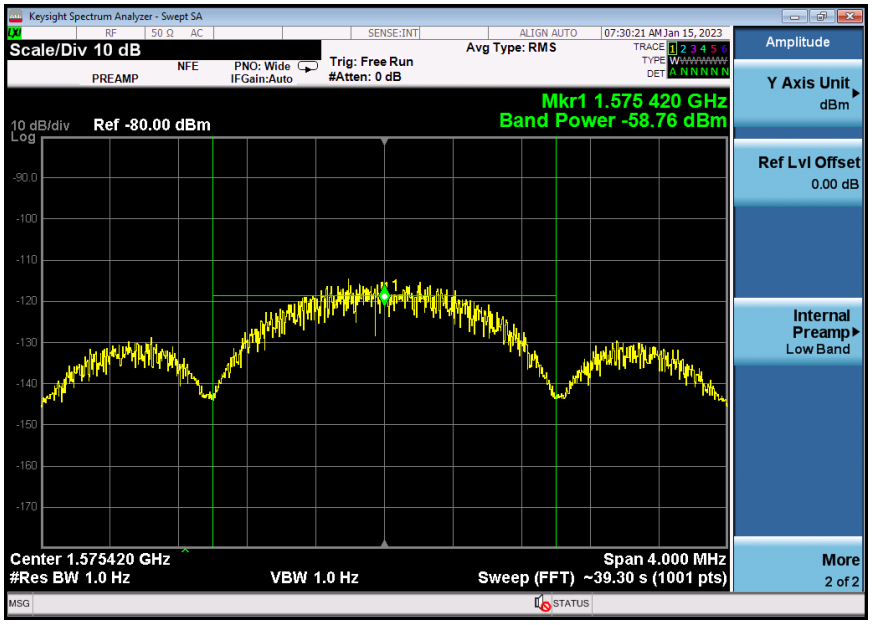

Figure 4.3. Band power in a 2 MHz bandwidth of a single satellite

Figure 4.4 shows output of the SDR while transmitting multiple satellites. If we compare with Figure 4.3, we can see that band power is raised. Since GPS is a CDMA system, every satellite contributes certain amount of power hence this raises the measured band power.

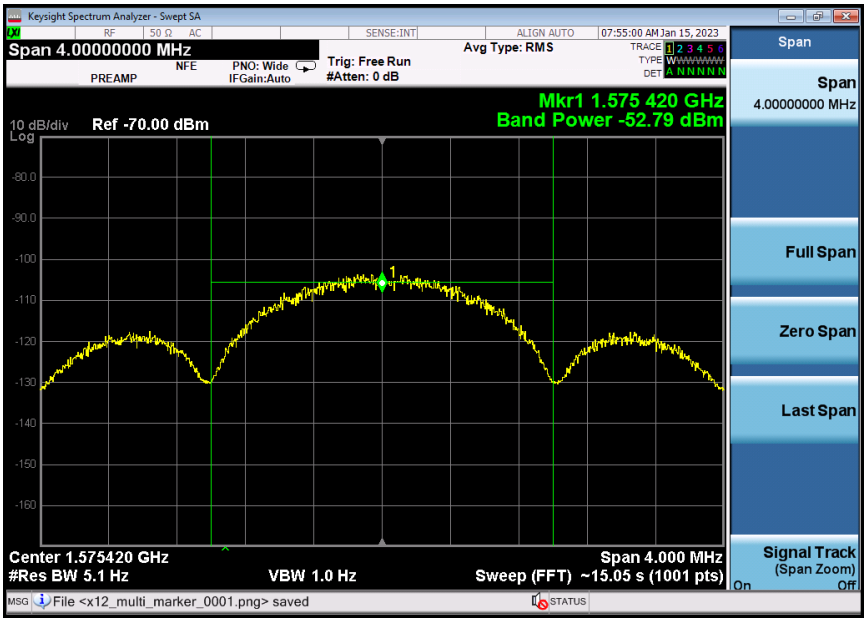

Figure 4.4. Band power in a 2 MHz bandwidth of multiple satellites

4.1.1 Suitable TCXO Selection for GPS Signal Simulator

HackRF requires a 10 MHz CMOS reference clock [63]. As it is mentioned in Chapter 1, errors created by the reference clock can lead Doppler measurement and position solution errors.

GPS receiver may not lock to signals transmitted by the GPS simulators employing the reference clocks having poor stability [66]. Because Doppler frequency search algorithm in the acquisition stage of the receivers have a certain bandwidth and the receiver does not search the frequencies beyond this bandwidth. Reference clocks

placed in transmitter adds additional frequency deviation in GPS signals. Hence, transmitter equipped with clock having poor stability probably will not spoof a receiver.

Furthermore, as it is stated in [67], phase noise of the crystal oscillator can be used by the receiver to discriminate spoofing attacks. If all the issues mentioned above are considered, it is important to choose a low phase noise and highly stable crystal oscillator for successful spoofing attacks.

From Figure 4.5, it can be seen that the TCXO that will be used in the experiments has 1 ppm frequency error and has a low phase noise.

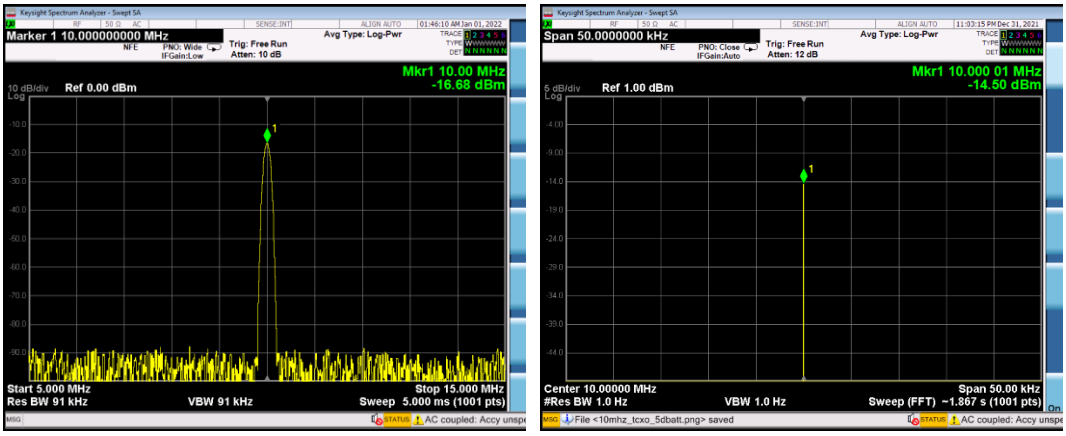

Figure 4.5. 10MHz HCMOS signal in frequency domain

4.2 Hardware Domain Test Setups

As Chapter 2.3 suggests, software domain and hardware domain setups can be utilized. Hardware domain setups for simplistic overpowered attack and overpowered attack with noise padding is examined on both cold-start and tracking modes of the GPS receivers. HackRF SDR, a noise generator, Wilkinson combiners, attenuators, a TCXO, a bias tee, an active antenna and low noise amplifiers are used to implement the scenarios.

4.2.1 Overpowered Attack and Detection with C/N_0 Monitoring

Overpowered attack can be demonstrated by using HackRF. As it is stated previously, TX IF gain and transmitted I/Q data will be same for all experiments. To change the power at the receiver side, attenuators will be employed.

In this chapter, attenuators can be regarded as FSPL between satellites and receivers. Evidently, output power of the HackRF is much lesser than actual output power of the satellites but since output power of the HackRF remains constant for all setups, output power adjustments are realized using the attenuators. Furthermore, LNA placed in front of the receiver can be regarded as an active antenna. This LNA has a gain of 22 dB and noise figure of 1.2 dB. If the LNA and NEO-6M together are considered as a receiver chain, noise figure of the NEO-6M will not contribute more to the chain.

As it is discussed in the Chapter 1, in cold-start mode, a GPS receiver has no prior knowledge regarding to its location, ephemeris and almanac. Furthermore, if the GPS is placed indoor, the receiver has no line of sight with the authentic satellites. To simulate this scenario, a GPS receiver in cold-start mode can be directly connected to the spoofing transmitter chain. Diagram of this scenario is shown in Figure 4.6.

This is one of the hardest scenarios to detect spoofing. Since it does not track the satellites, the receiver cannot perform sliding window technique for C/N_0 values.

Since there is no GPS signal reception, even subtle power levels can overtake GPS receiver. The setup shown in Figure 4.6 can also be useful to observe the behavior of the GPS receiver respect to varying power levels of the received signal.

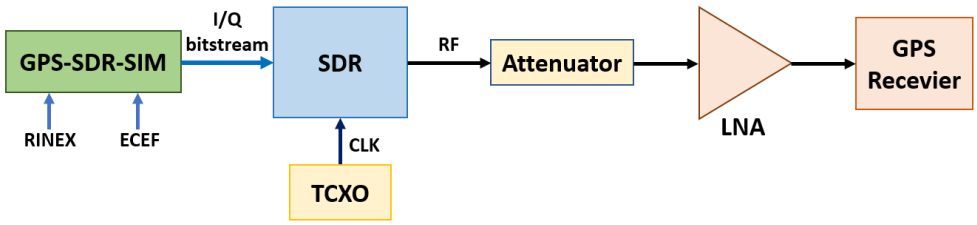

Figure 4.6. Spoofing a GPS receiver in cold-start mode

This setup provides a common understanding about how GPS receiver behaves respect to varying levels of GPS signals. Following results are obtained for varying values of attenuators.

Note that, measured band power for output of the GPS signal simulator configured as to transmit single satellite is -58.7 dBm, as it is mentioned previously. Hence, placing a 50 dB attenuator yields -108.7 dBm band power.

Figure 4.7 shows C/N_0 values respect varying attenuator values. Top-left, Top-right, middle-left, middle-right and bottom depict 85 dB attenuation, 75 dB attenuation, 65 dB attenuation, 60 dB attenuation, 50 dB attenuation respectively. If insertion loss of the 4-meter cable placed after the attenuators, which is 5 dB, is taken account then total attenuation increases by 5 dB.

As can be seen from the figure, as attenuation increases C/N_0 values drop which is an expected result. 85 dB attenuation yields -148.6 dBm band power corresponding to 25.26 dB-Hz. Mean measured value is 27 dB-Hz.

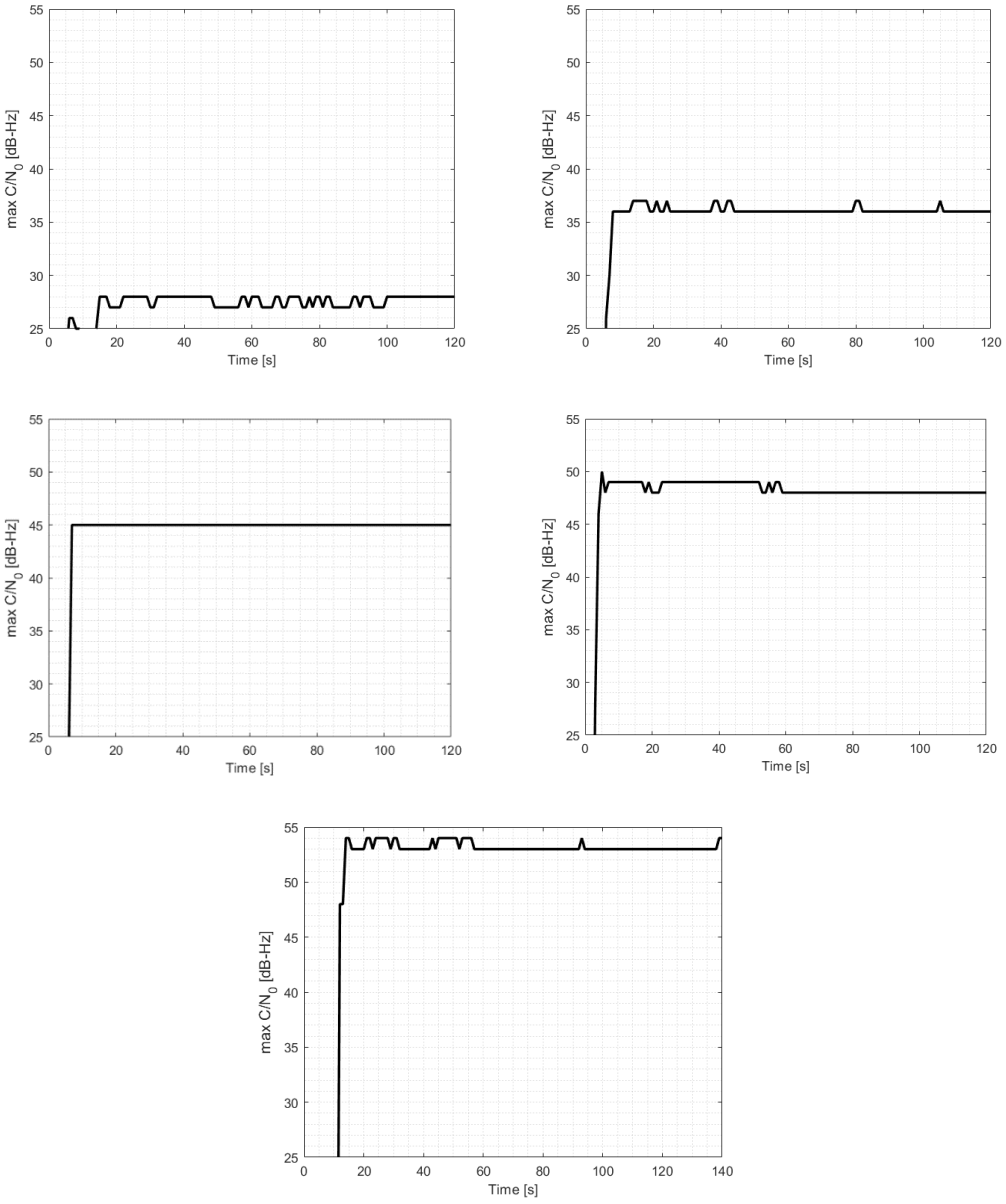

Figure 4.7. Results respect to varying values of attenuators. Top-left 85 dB attenuator, Top-right 75 dB attenuator, Mid-left 65 dB attenuator, Mid-right 60 dB attenuator, Bottom 50 dB attenuator

Setups employing 75 dB attenuator, 65 dB attenuator, 60 dB attenuator yield -138.7 dBm, -128.7 dBm, -123.7 dBm band power corresponding to 35.26 dB-Hz, 45.26 dB-Hz, 51.26 dB-Hz. If the noise figure of the system is considered, they approximately become 35 dB-Hz, 44 dB-Hz, 50 dB-Hz and mean measured values are 36 dB-Hz, 45 dB-Hz, 48 dB-Hz respectively.

AGC values which are measured as 6800 and remain constant during the various signal levels. AGC values closely depend to receiver properties. They will be discussed more in the following chapters.

To demonstrate spoofing attack to a GPS receiver which has already been tracking the satellites, setup shown in Figure 4.8 is utilized. To implement the setup shown in Figure 4.8, an L-band bias-tee and a Wilkinson combiner are designed.

In tracking mode, GPS receiver can employ previous information gathered from the satellites to detect spoofing attacks. Sliding window technique introduced in Chapter 3 can effectively monitor variations in the C/N_0 values.

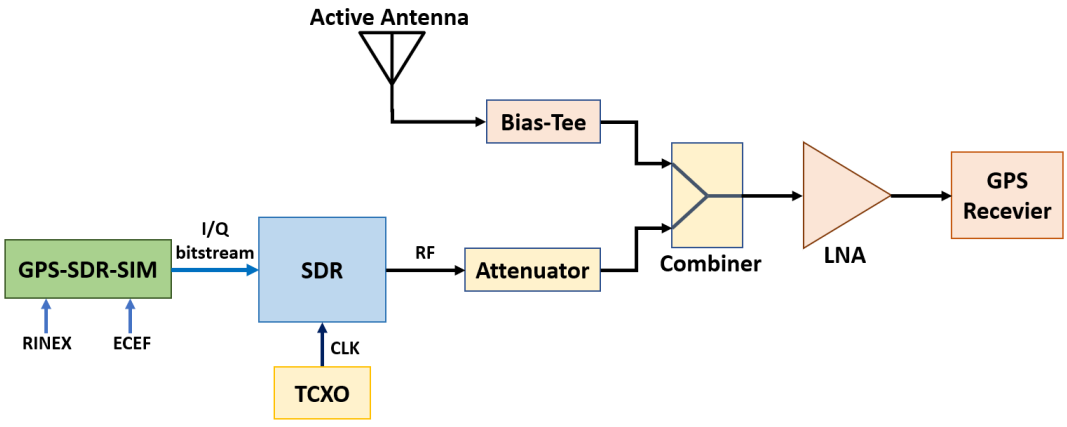

Figure 4.8. Spoofing a GPS receiver in cold-start and tracking mode

To calculate the GPS signal levels introduced to the receiver, chain starting from the antenna must be analyzed. Antenna is an active antenna having 28 dB gain and 1.5 dB noise figure [68]. Also, antenna is comprised of a 5-meter RG174 cable whose insertion loss corresponds to 7.5 dB. With connectors and bias tee that are considered, a total 8 dB loss is introduced before the combiner.

If antenna receives a signal level of -130 dBm, LNA placed inside of the antenna amplifies it by 28 dB, RG174 cable and bias-tee attenuates it by 8 dB, Wilkinson combiner attenuates it by 3 dB. Hence at the input of the LNA, a total -107 dBm band power is achieved.

Since the gain of the amplifier is high enough to compensate these losses, noise figure of the receiver chain does not vary much from 1.5 dB. Losses after the LNA of the active antenna do not make a significant contribution to overall noise figure.

Thermal noise power equals to -110.8 dBm in 2 MHz bandwidth, therefore if the signal band power is -130 dBm C/N_0 equals to 43.8 dB-Hz. C/N_0 is deteriorated by the noise figure of the receiver, which is approximately 1.5 dB, received C/N_0 becomes 42.3 dB-Hz. This is the minimum received C/N_0 for this receiver topology, independent from weather conditions and presence of interference sources.

Figure 4.9 shows C/N_0 values of the setups employing 30 dB and 40 dB attenuators. Note that output power of the HackRF for a single satellite is -58.7 dBm, placing a 30 dB and 40 dB attenuators make signal level at the input of the LNA -88.7 dBm and -98.7 dBm respectively.

Spoofing signals begin to be transmitted around 100th second in setup employing 30 dB attenuator and around 150th second in setup with 40 dB attenuator. In both setups, first C/N_0 values degrade for a short period of time then increase rapidly due to overpowered spoofing signals.

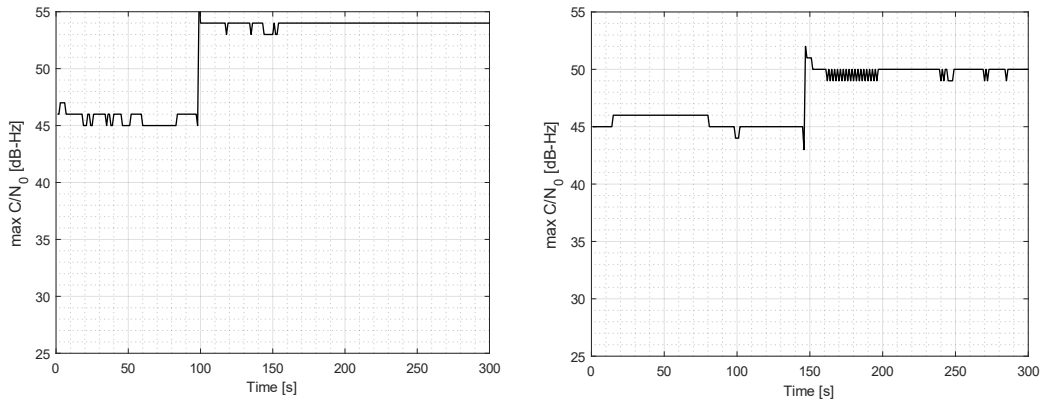

Figure 4.9. C/N_0 values of victim receiver in setup employing 30 dB and 40 dB attenuator

In both setups, mean C/N_0 value of the clean dataset is 45 dB-Hz or 46 dB-Hz indicating that GPS signal power is approximately -103 dBm and -102 dBm at the input port of the LNA. Thus, this gives advantage over the GPS signal power as 15 dB for setup with 30 dB attenuator and 5 dB for setup with 40 dB attenuator.

C/N_0 values and sliding window for 5 seconds of the C/N_0 values of clean dataset can be seen from below.

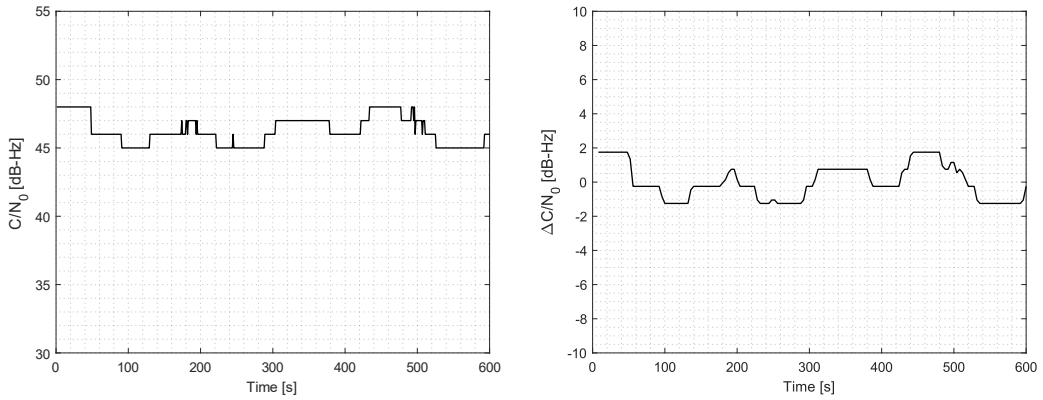

Figure 4.10. Nominal C/N_0 values and sliding window values of the sky in different days

As can be seen from the Figure 4.10 shown above, C/N_0 variation of the nominal dataset is ±2 dB-Hz for that specific location where the experiments are conducted.

Examining Figure 4.10 and Figure 4.11 gives the opportunity to define a threshold for the expected values. Sudden increases in C/N_0 values clearly indicate presence of overpowered spoofing attacks because increase is higher than variation of nominal values of the metrics.

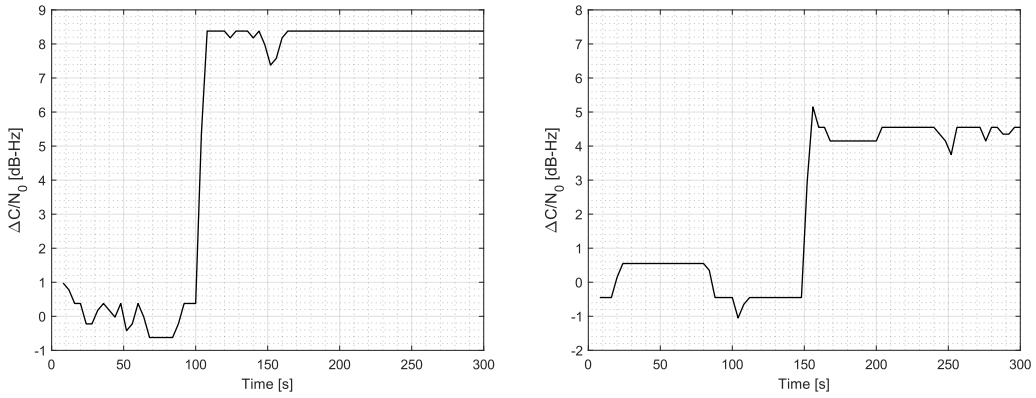

Figure 4.11. Sliding window values of victim receiver in setup employing 30 dB and 40 dB attenuator

4.2.2 Overpowered Attack with Noise Padding and Detection with AGC and C/N_0 Monitoring

As it is discussed on previous chapters, since it is hard to determine the location of victim receiver without additional hardware which complicates the design and increases the cost of spoofer, transmitter circuitry can employ an additional broadband noise source to adjust C/N_0 levels by raising noise level intentionally.

As a noise source, Keysight 346B is used. The instrument utilizes shot noise of the diodes and generates white noise from 10kHz to 18GHz. When supplying a +28V to its BNC input, 5.6kHz oscillator becomes working and its output is rectified as the supply for the constant current source. Then an avalanche diode fed by the previous circuits generates the desired noise at the output of the instrument. Simplified diagram of the noise source is shown in Figure 4.12.

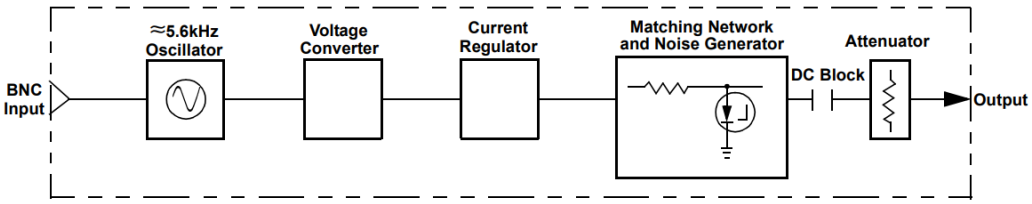

Figure 4.12. Simplified diagram of the noise source [69]

Output power of the noise source must be calibrated to obtain desired noise levels. To measure output power level of the noise generator, firstly noise floor level seen by the spectrum analyzer terminated with a matched load must be measured.

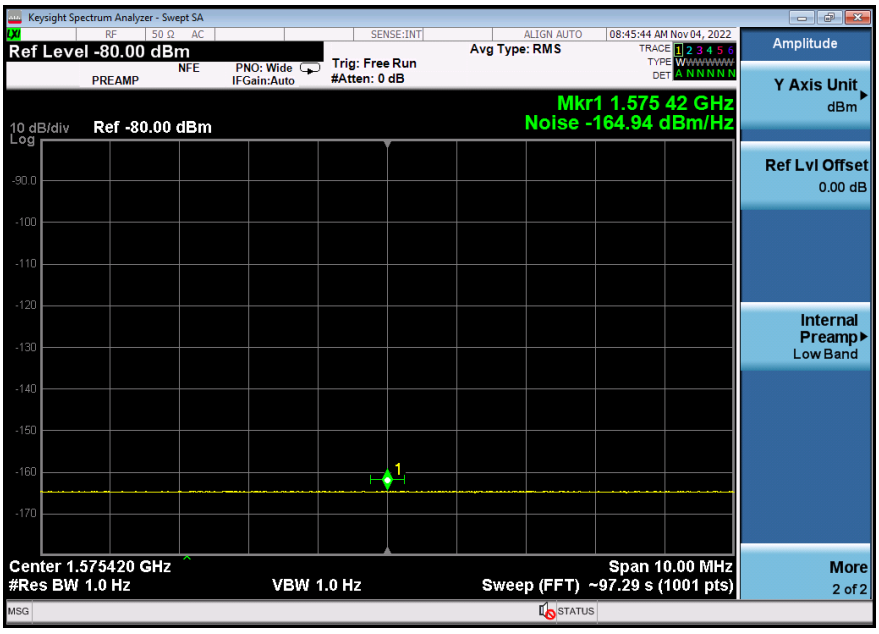

Figure 4.13. Noise floor measured by the spectrum analyzer

Figure 4.13 shows noise floor measured by the spectrum analyzer which is 10 dB higher than the actual noise floor caused by noise figure of the spectrum analyzer. Figure 4.14 shows measured noise power in 2 MHz bandwidth.

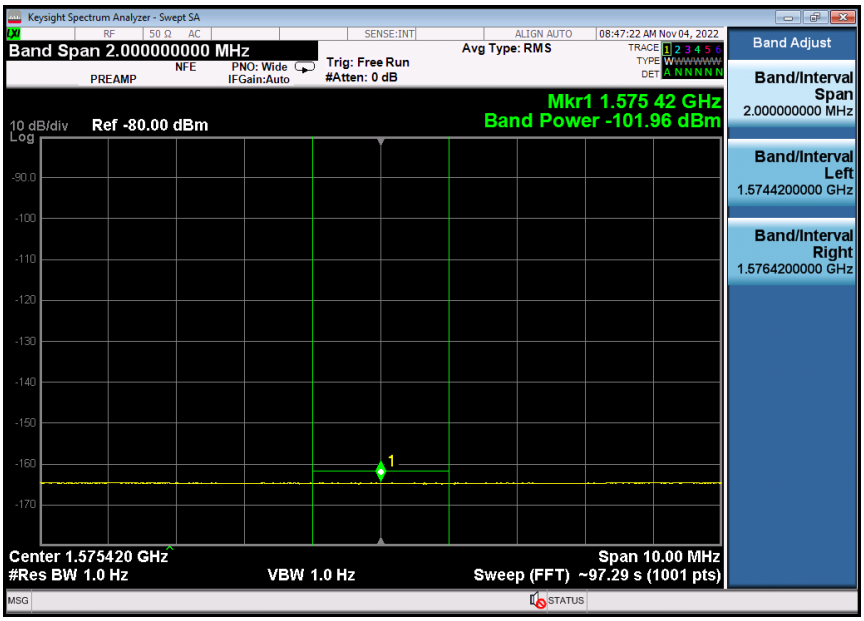

Figure 4.14. Noise floor measured by the spectrum analyzer in a 2 MHz bandwidth

Connecting output of the noise generator to the spectrum analyzer, following screens shown in Figure 4.15 and Figure 4.16 are obtained.

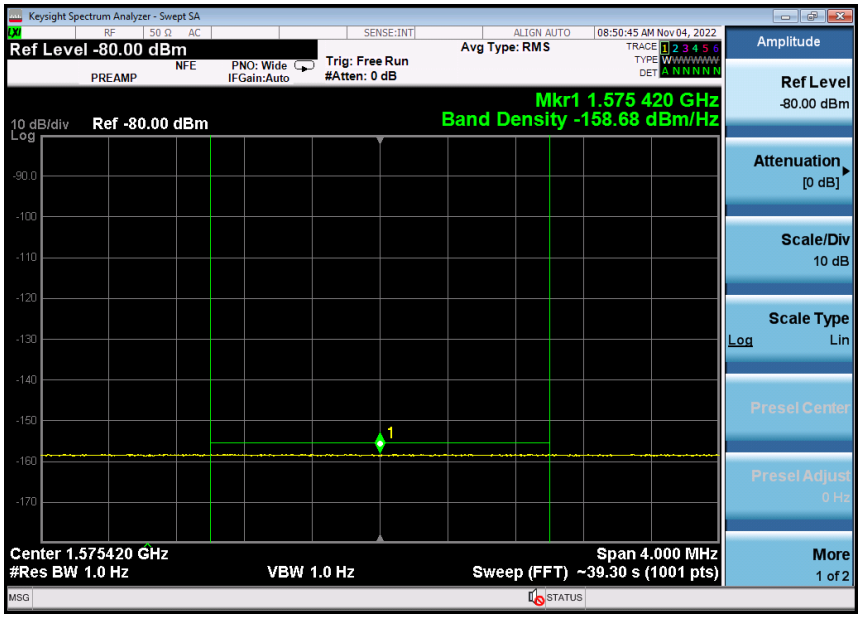

Figure 4.15. Band density of the noise generator in a 2 MHz bandwidth

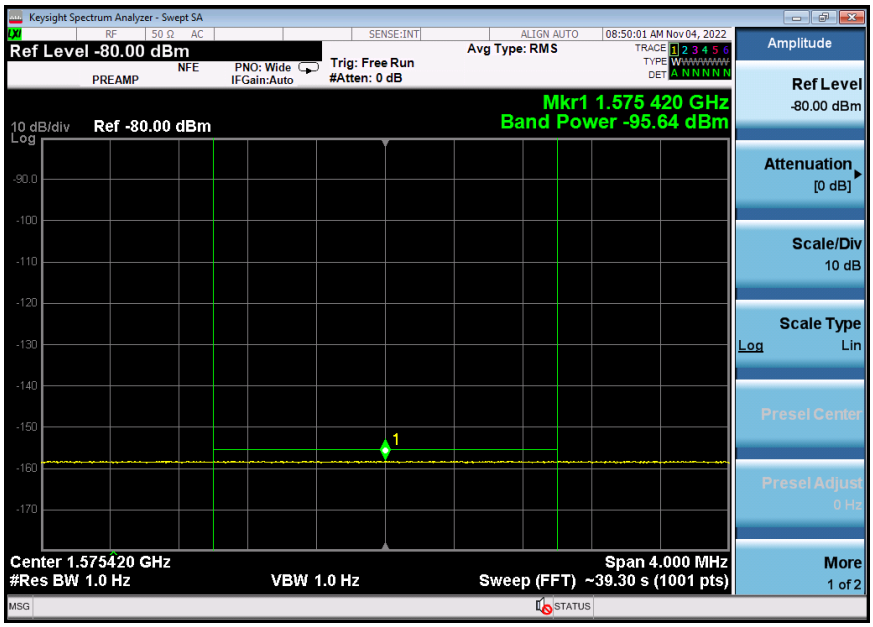

Figure 4.16. Band power of the noise generator in a 2 MHz bandwidth

Figure 4.15 and Figure 4.16 demonstrate that noise generator can raise noise floor level in certain bandwidth. In L1 band, noise floor is raised with a flat frequency response.

While measuring a signal or a noise power close to noise floor level, a certain adjustment must be done as it is shown in Figure 4.17. Therefore, if there is a measurement result whose value is 6dB higher than the noise floor, its real amplitude value can be found by subtracting 1.5dB from its measured value. If the real output power of the noise generator is wanted to be calculated which is measured as -95.64 dBm in 2 MHz bandwidth, the result would be -97.14 dBm.

Low noise amplifiers can be placed after the noise generator to obtain higher output powers. Band power of the noise generator cascaded with 20dB LNA is shown in Figure 4.18 and Figure 4.19. Note that, since measurements shown in Figure 4.18 and Figure 4.19 is 15dB higher than the noise floor, it is not necessary to recalculate their values.

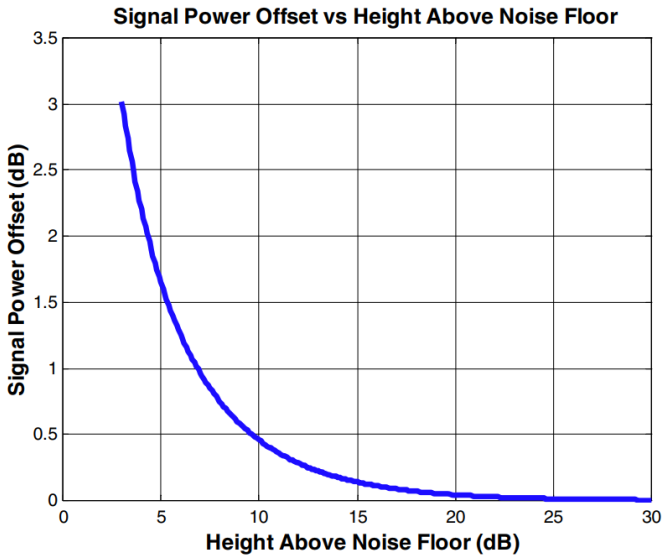

Figure 4.17. Measured signal power offset due to low power level [70]

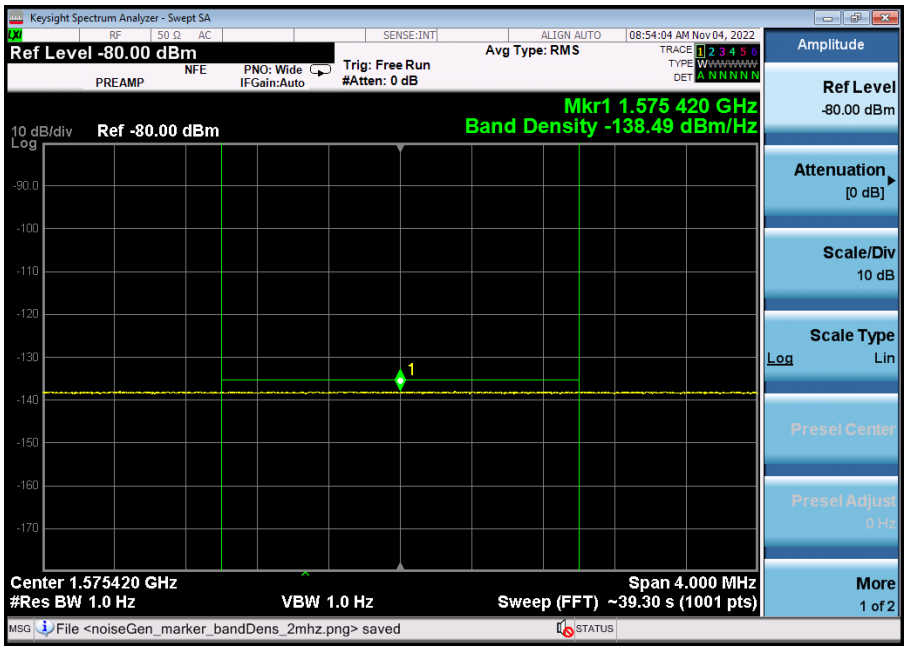

Figure 4.18. Band density in a 2 MHz bandwidth of the noise generator cascaded with an LNA having 20dB gain

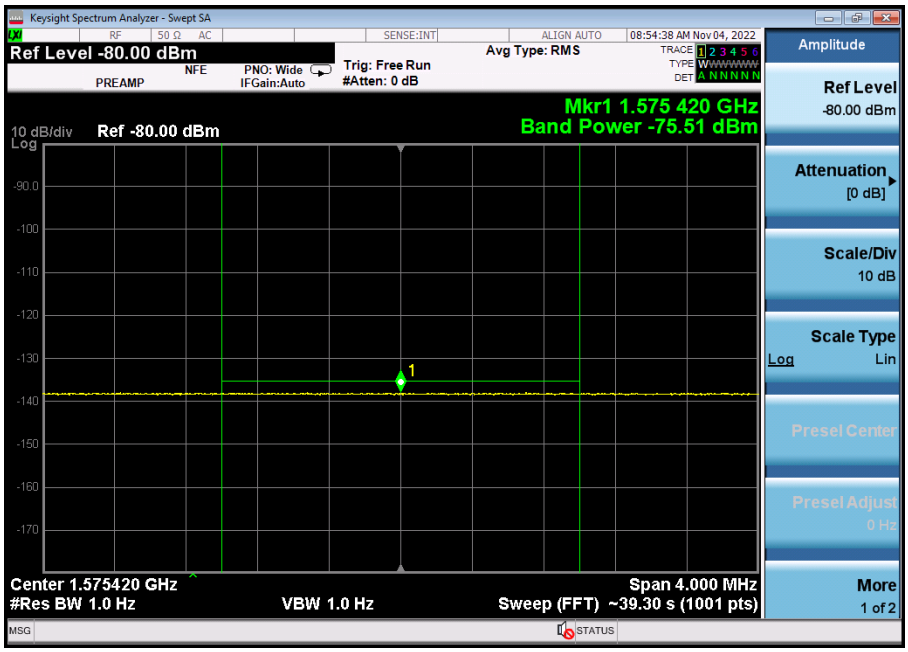

Figure 4.19. Band power in a 2 MHz bandwidth of the noise generator cascaded with an LNA having 20dB gain

Results clearly show that by applying 20 dB gain to output of the noise generator, noise floor level can be raised by 20 dB. So, desired noise floor level can be adjusted by applying suitable gain at the output of the generator. According to noise power levels measured above, desired SNR levels of the GPS signals can be generated if correct GPS signal power levels are summed up with correct noise power levels. SNR level of the GPS signals at the precorrelation stage is around -20 dB as it is discussed on previous chapters. The spoofer can adjust transmitted GPS signal level to obtain desired SNR values. For example, output of the noise generator can be combined with GPS signal level of -117.14 dBm and noise generator cascaded with an LNA can be combined with a GPS signal power of -95.5 dBm.

Spoofing with noise padding setup is implemented as shown in Figure 4.20 and Figure 4.21. Note that gain blocks might have a wideband operating frequency range, therefore an additional filter can be placed in front of the gain blocks since noise source generates a broadband noise which can saturate the amplifiers.

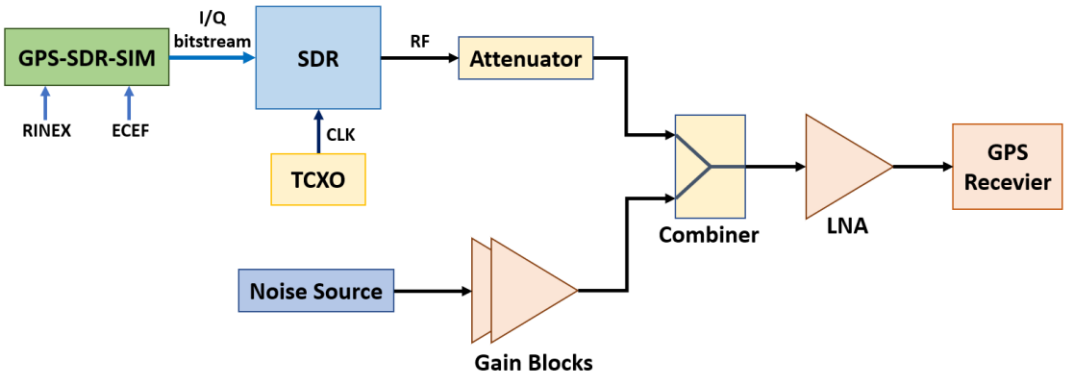

Figure 4.20. Simplified diagram of spoofing a GPS receiver in cold-start mode with noise padding

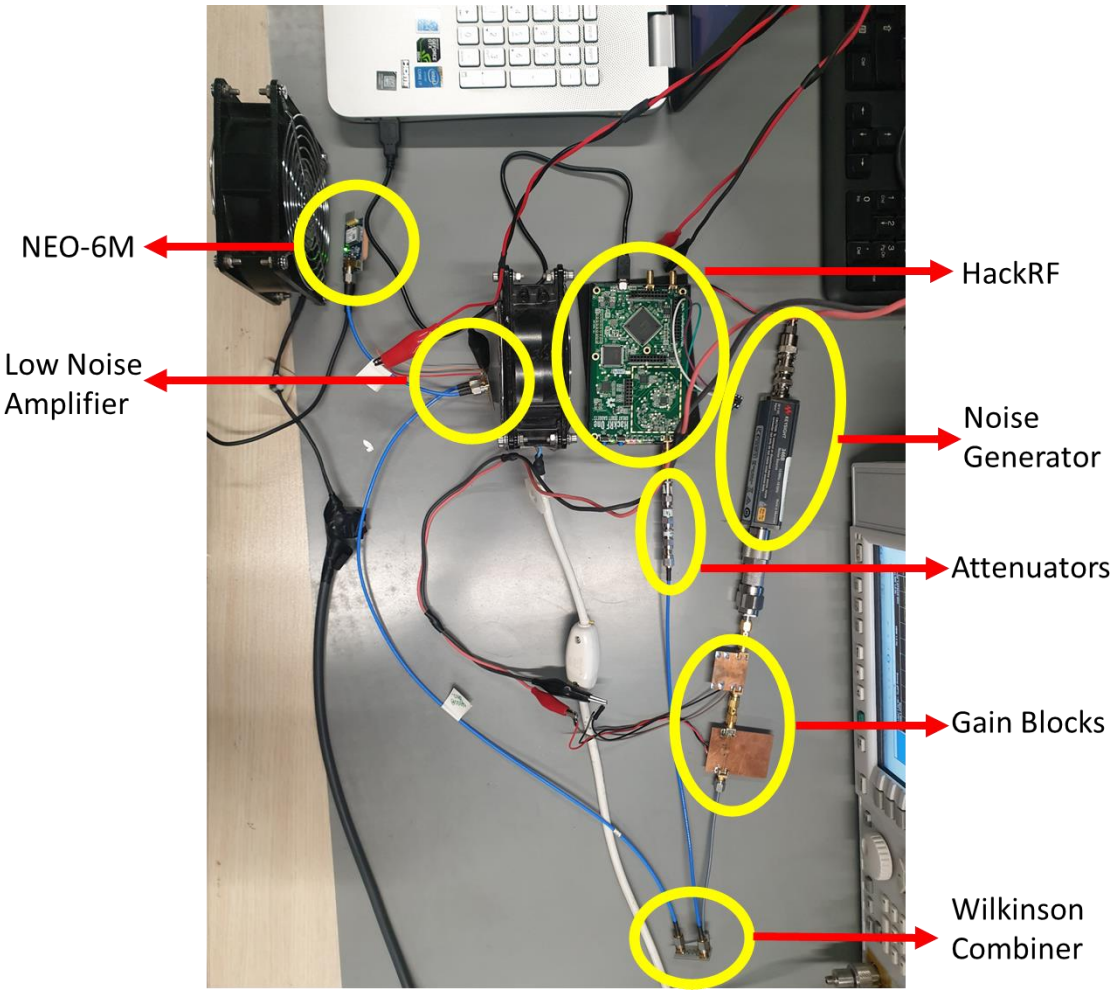

Figure 4.21. Spoofing a GPS receiver in cold-start mode with noise padding

Note that, Figure 4.21 does not represent the final setup for the experiment. Although components that are used for the experiment stay same, distance between the components are increased to avoid unnecessary couplings. Cable after the combiner is a 4-meter cable having insertion loss of 5 dB. Figure above is kept because it shows the test setup clearly.

If gain of the gain blocks is set to 20 dB, noise power in a 2 MHz bandwidth equals to -75.51 dBm as can be seen from Figure 4.19. For -20 dB SNR, corresponding noise power levels related to HackRF band power levels are tabulated below. Attenuation refers to attenuation after HackRF and noise power gain refers to gain setting of the gain blocks after first amplifying stage having 20 dB gain. Furthermore, note that cable losses between SDR - combiner and noise generator - combiner are below than 0.5 dB, therefore cable losses are neglected.

$$-58.7_{dBm} - ATT_{dB} - (NGen)_{dBm} - (Gain\ Block\ gain)_{dB} = -20 \qquad (4.1)$$

$$(NGen)_{dBm} + (Gain\ Block\ gain)_{dB} = -75.5dBm \qquad (4.2)$$

Table 4.3 HackRF Band Power and Related Gain of Noise Generator Circuitry

Attenuation	HackRF Band Power	Noise Power for -20 dB SNR	Required Gain After First GB
0	-58.7 dBm	-38.7 dBm	57
20	-78.7 dBm	-58.7 dBm	17
30	-88.7 dBm	-68.7 dBm	7
40	-98.7 dBm	-78.7 dBm	-3
50	-108.7 dBm	-88.7 dBm	-13

According to power levels shown on the Table 4.3, if a setup realizing 40 dB attenuation after HackRF combined with noise generation circuitry is built, it is

intended to observe SNR levels of -23 dB corresponding to C/N_0 levels of 40 dB-Hz as it is calculated on Chapter 3.

Figure 4.22 from top-left to bottom it shows maximum C/N_0 values collected by the receivers employed by the setups described in

Table 4.4 in order. Attenuation value in the table refers to attenuator values incorporated after HackRF and gain of the gain block means that gain value applied after the noise generator.

Table 4.4 HackRF Band Power and Related Gain of Noise Generator Circuitry

Setup Number	Attenuation	Gain of Gain Block
1	50 dB	20 dB
2	40 dB	20 dB
3	30 dB	20 dB

It is clear that from the results, C/N_0 values linearly change with GPS signal power. Also, it proves that C/N_0 values can be effectively adjusted to a desired level by applying white noise onto created GPS signal.

Figure 4.22 shows C/N_0 values read by the receiver when setup described above is built. It is supposed that variations of the C/N_0 values at the first seconds in Figure 4.22 are caused by initial C/N_0 estimation of the receiver.

After the values are settled into a certain level, small variations within 1 dB are observed. This can be caused by wrong measurement of the receiver or uncertainty created by instantaneous output power of the HackRF and instantaneous gain values of the amplifiers. Also, 1 dB change in C/N_0 values does not necessarily mean 1 dB power change since the NMEA-0183 protocol which is used by the NEO-6M reports satellite C/N_0 levels to the nearest digit [52].

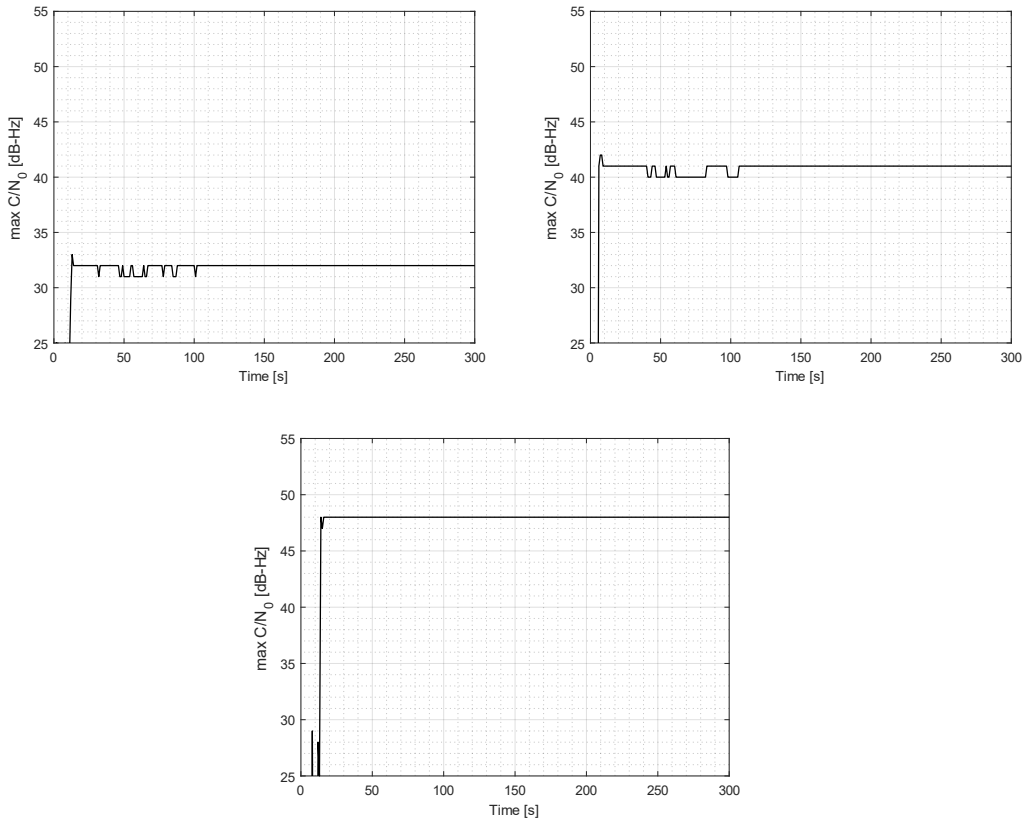

Figure 4.22. Maximum C/N_0 levels of setups with noise padding

If similar calculations that are done on Chapter 3 are repeated for the test setups, expected SNR levels for setup 1, setup 2 and setup 3 can be obtained as -33.25 dB, -23.25 dB and -13.25 dB respectively. These SNR levels correspond to C/N_0 levels of 29.6 dB-Hz, 39.6 dB-Hz and 49.6 dB-Hz, theoretically.

Along with C/N_0, AGC values are useful to monitor noise component at the input of the receiver. When input of the receiver is terminated with 50 Ω load, AGC values are observed as shown below.

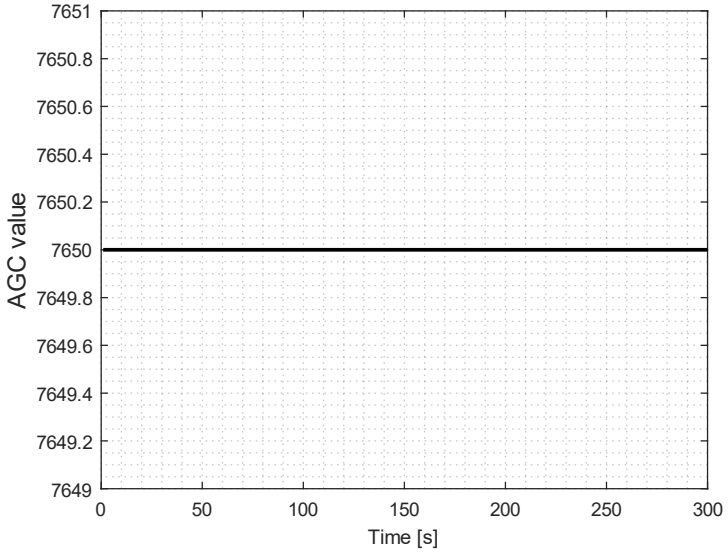

Figure 4.23. AGC values read by GPS receiver for terminated input

AGC values decrease, as can be seen from Figure 4.24, when noise source and SDR begin to transmit and AGC values stay at the same level regardless from the values of attenuators.

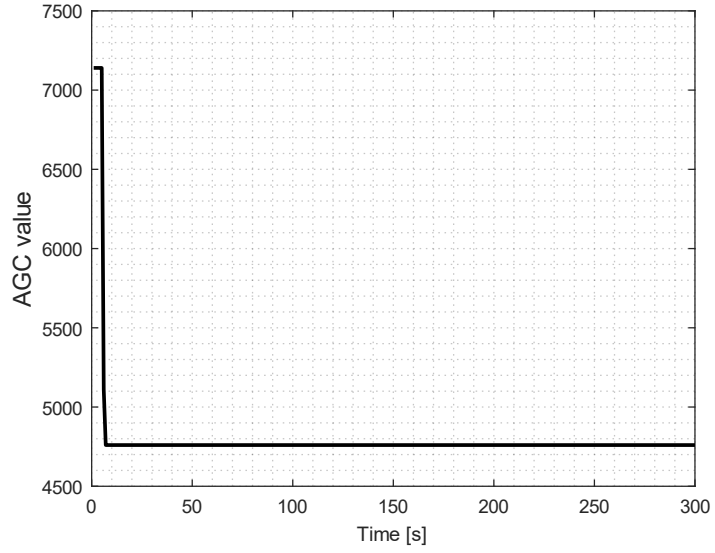

Figure 4.24. AGC values when noise padding circuitry begins to transmit

After implementing test setups for spoofing COTS receiver operating in cold-start mode and having no access to authentic satellites, a more realistic scenario can be implemented by combining output of an active GPS antenna to test setup shown in Figure 4.21. Motivation behind this setup is spoofing a receiver who has already tracking GPS satellites since overpowered spoofing attack with noise padding can be used for spoofing GPS receivers who have been already locked to authentic GPS signals created by authentic GPS satellites.

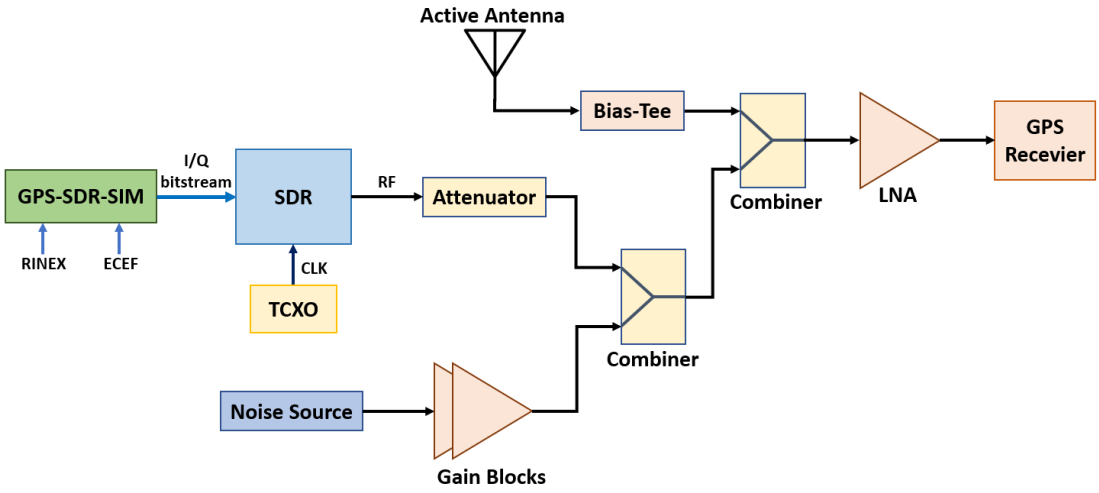

Figure 4.25. Diagram of spoofing a GPS receiver tracking satellites

To implement the setup shown in Figure 4.25, an L-band bias-tee and L-band Wilkinson combiners are designed.

By using the setup shown in Figure 4.25, before transmitting spoofing signals, nominal AGC values of the sky are collected.

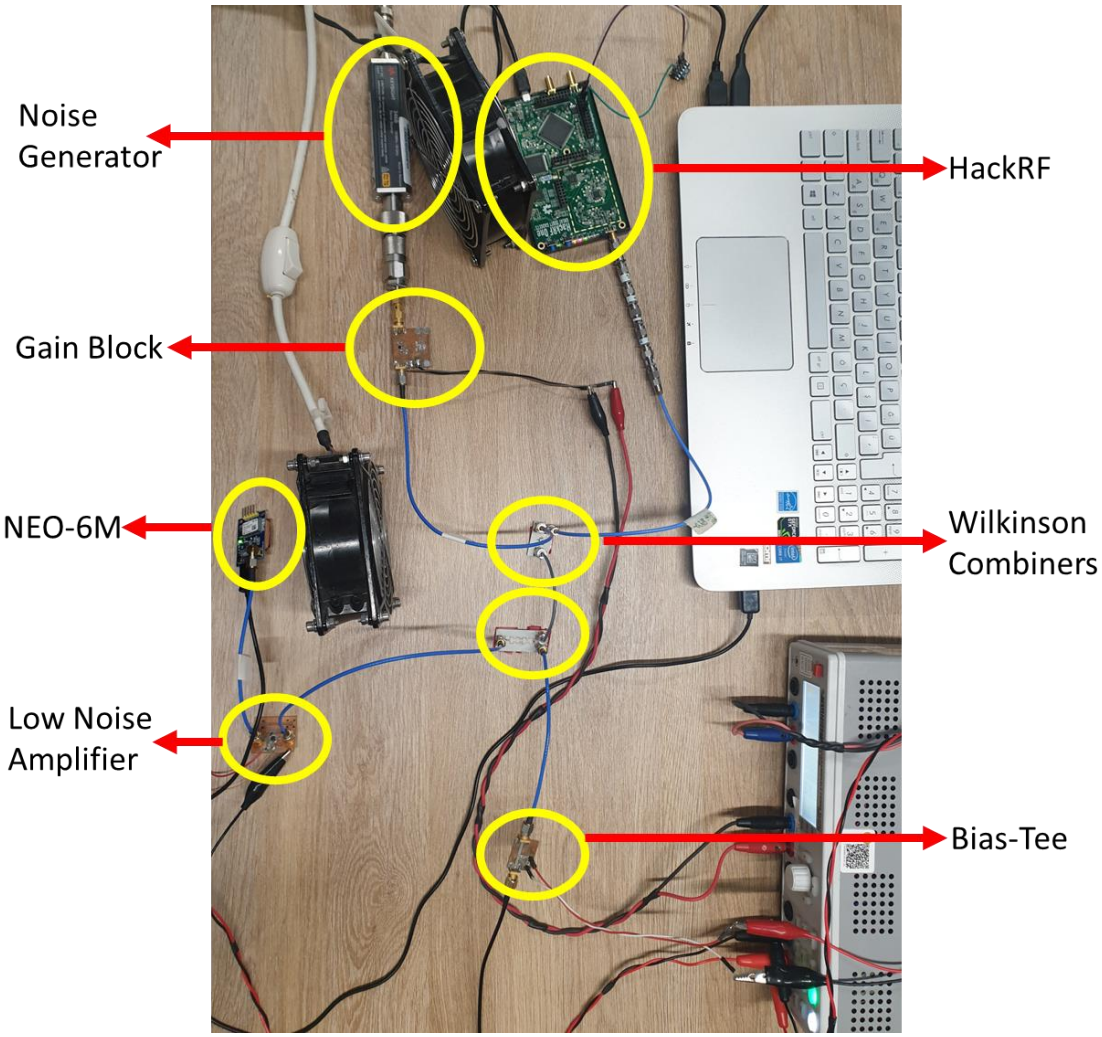

Figure 4.26. Test setup of spoofing a GPS receiver tracking satellites

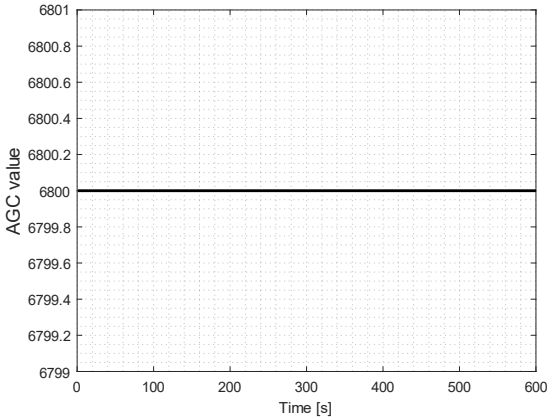

Figure 4.27. Nominal AGC values of the setup

Setup shown in Figure 4.26 is implemented with a 40 dB attenuator. Attack starts around 150th second by turning on noise padding circuitry. C/N_0 values fall sharply when the circuitry is powered on. After several seconds, SDR begins to transmit spoofing signals. Hence, C/N_0 values increase rapidly. Mean value after spoofing attack becomes 41 dB-Hz.

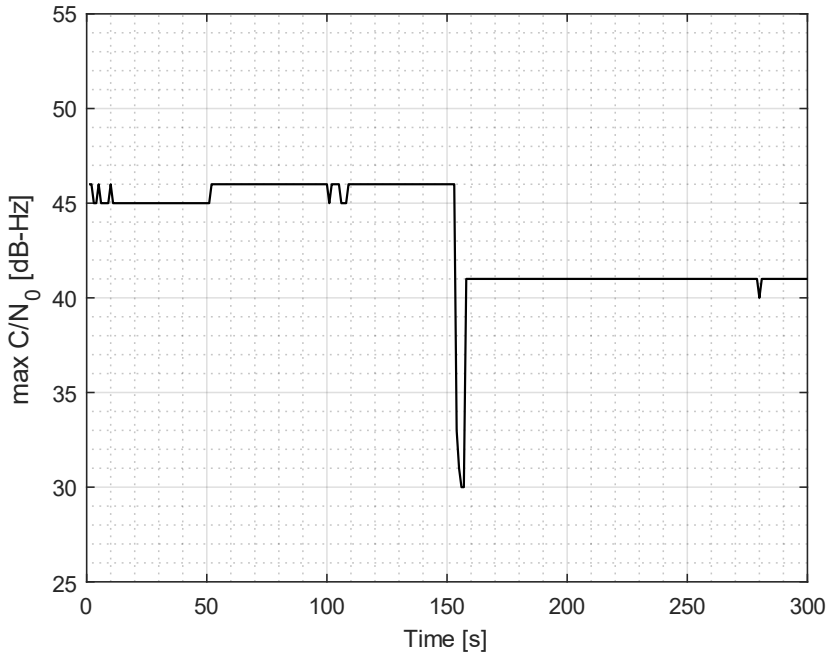

Figure 4.28. Maximum C/N_0 levels of a receiver tracking authentic satellites that is spoofed by noise padding circuitry employing 40 dB attenuator

As can be seen from Figure 4.28, after 7 seconds later from powering on the noise padding circuitry, C/N_0 levels of the receiver are changed to desired levels. Figure below shows moment of time and location spoofing of the receiver. 94 seconds after spoofing affecting C/N_0 levels, time measurement of the receiver is spoofed. Location measurement of the receiver is lost when time of the receiver is spoofed. Then 41 seconds later, location of the receiver is spoofed.

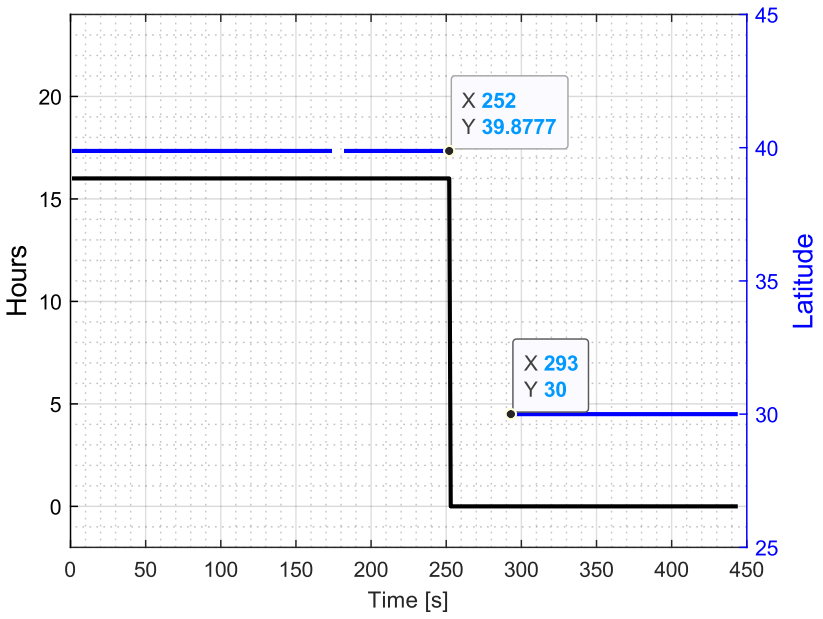

Figure 4.29. Timing of time and location spoofing of the receiver

Behavior of the sliding window values of the spoofing attack is shown below. Unlike the behavior of the spoofing attacks shown in the previous chapters, sliding window values do not increase. They fall sharply then their mean value becomes much lower than mean value of the authentic signals. At first glance, this behavior might give clue about a possible jamming attack since the receiver possesses lower sliding window values respect to nominal values. A 12 dB fall followed by a 6 dB increase looks like an effect of a jammer decreasing its output power. All in all, smaller metric values do not indicate presence of a spoofing. Because spoofing signals need power advantage over authentic signals to overtake the receiver. It would be unlikely to takeover receiver with lower C/N_0 levels.

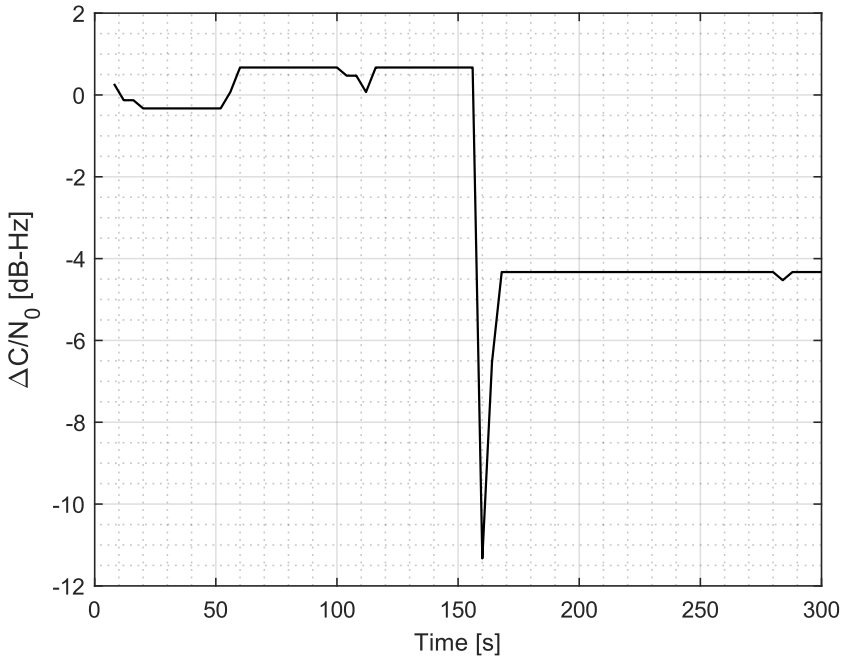

Figure 4.30. Sliding window values of a receiver tracking authentic satellites that is spoofed by noise padding circuitry employing 40 dB attenuator

C/N_0 metric gives information about ratio between the carrier signal and the noise component. Thus, C/N_0 metric and its sliding window value do not provide adequate information to identify this kind of attacks. By the virtue of AGC values monitoring ambient noise power levels, the type of the attack can be identified.

As can be seen from Figure 4.31, AGC values decrease after noise padding circuitry is powered and stay on the same level. As it is discussed previously, if this attack were a jamming attack, received jamming power would have been decreased because of instant increase of the C/N_0 values. But that is not the case, since an increase in AGC values is not observed. Hence, by using information gathered from AGC and C/N_0 metrics together, attacks can be discriminated.

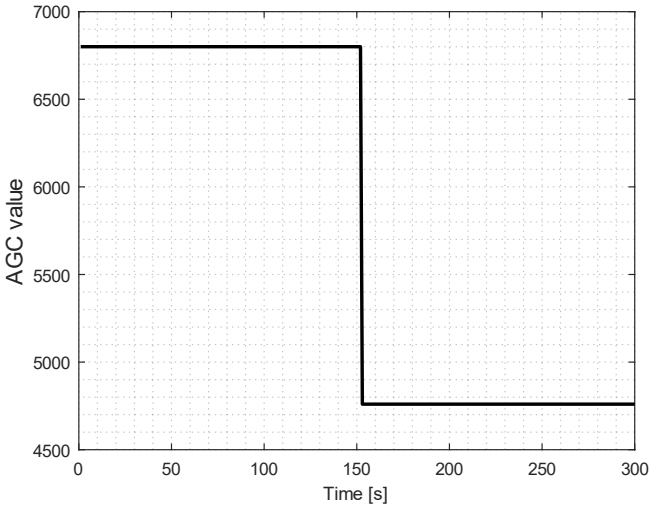

Figure 4.31. AGC values of a receiver tracking authentic satellites that is spoofed by noise padding circuitry employing 40 dB attenuator

Another set of results for successfully executed spoofing attack can be shown below. Only difference between the execution of the experiments is waiting period between start of transmitting of noise padding circuitry and start of transmitting spoofing signals. SDR begins to transmit spoofing signals 10 seconds after noise circuitry is powered on. C/N_0 values and sliding window values are shown below.

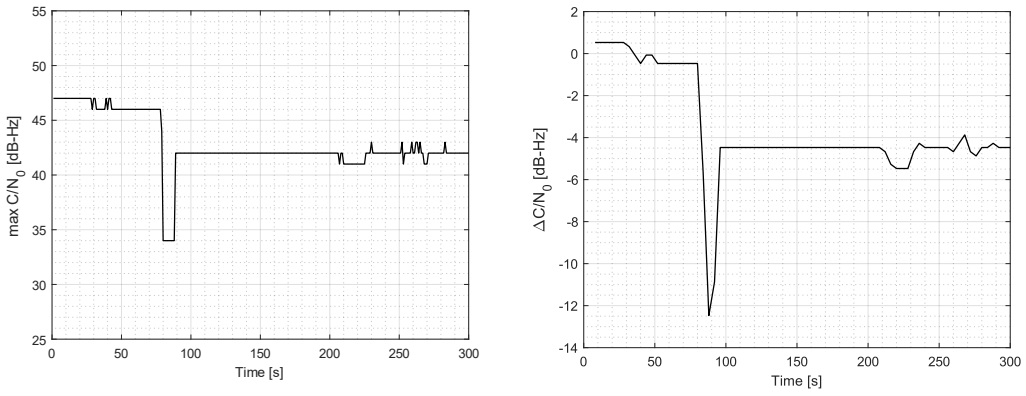

Figure 4.32. Same setup with a waiting period

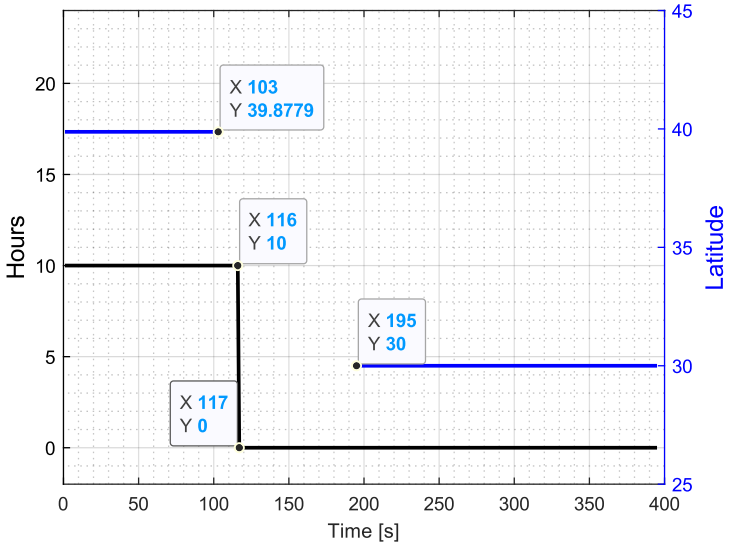

Figure 4.33. Timing of location and time spoofing of the receiver

Both setups demonstrate successful spoofing attacks by deliberately raising the noise floor and transmitting the spoofing signal with adequate level. Spoofing detection with AGC coupled with C/N_0 monitoring successfully detects attacks and discriminates jamming between spoofing.

4.3 Software Domain Test Setups

For software domain test setups, GPS-SDR-SIM [21], GNSS-SDR [54] and TEXBAT files [16] can be employed.

4.3.1 GNSS-SDR Architecture

GNSS-SDR is a software defined receiver providing demodulation and decoding of the navigation data. It can also compute observables and position solutions. Receiver chain of the GNSS-SDR is highly customizable allowing to change the parameters in input filter, sampler, acquisition and tracking blocks. Maximum Doppler frequency value to be searched, Doppler step size, threshold and probability of false alarm of acquisition, PLL bandwidth, DLL bandwidth, spacing between the correlators are just some of the parameters that can be configured by the user. Also, by providing suitable configuration information to the receiver, parameters like satellite IDs can be obtained and Doppler shift, amplitude of correlators, estimated C/N_0 values, code frequency can be calculated.

Furthermore, GNSS-SDR has adapting handling algorithms supporting different sampling frequencies, intermediate frequencies and sample resolutions [43]. This property makes easier to integrate SDRs like USRP, ADALM-Pluto, RTL-SDR and HackRF to the software defined GNSS receiver [71].

4.3.2 Spoofing Detection with SQM in TEXBAT Scenarios

TEXBAT is a battery of recorded spoofing scenarios for evaluating authentication techniques of GPS [16]. Efficacy of proposed authentication method can be evaluated by using implemented testbed scenarios capable of simulating realistic spoofing attacks. Since recording the scenarios and sharing with GPS community around the world, TEXBAT scenarios became a de-facto standard for evaluating

spoofing detection methods. In the paper it is stated that as of September 2014 the list of users includes Stanford University, NovAtel Inc., Texas A&M University, Lockheed Martin and u-blox [72].

Comprising eight different scenarios currently, the TEXBAT scenarios are useful to undertake GPS spoofing scenarios in software domain. The scenarios are created by combining a receiver antenna with a GPS spoofer, hence a total combined signal comprising of authentic and spoofing signals are obtained by the receiver which is National Instruments RF signal capture hardware. TEXBAT scenarios are captured as complex 16-bit samples at a rate of 25 Msps and stored into different datasets [16].

In these scenarios, both dynamic and static are simulated. Furthermore, spoofing types of these scenarios are classified regarding to its frequency lock of spoofing signal to authentic signals and power advantage over authentic signals. Scenarios named as locked implies Doppler frequency of the spoofing signals are locked to authentic signals and named as overpowered means that spoofing signals have a power advantage around 10 dB over the authentic signals. To test signal quality metrics, four scenarios among them are selected.

In this chapter, the datasets are fed into an open-source receiver, GNSS-SDR. The receiver is configured accordingly to be able to monitor the correlator outputs and calculate the SQM metrics with the help of MATLAB software. In this chapter, behavior of the SQM metrics is examined respect to spoofing type and power advantage of spoofing signals over the genuine signals. Since SQM metrics are favored to monitor distortion in correlation function, power-matched attacks which creates the most distortion at the correlation function are examined.

As theoretical background is examined on the Chapter 3, SQM metrics can be calculated from correlator parameters during the tracking stage of the receiver topology. Along with ratio metric and delta metric, sliding window of these metrics are calculated using the correlator parameters. Furthermore, threshold values for each metric are calculated respect to a desired probability of false alarm value.

Table 4.5 Texas Spoofing Battery Scenarios for Testing SQM Metrics

Scenario Designation	Spoofing Type	Power Adv. (dB)	Freq. Lock
Static Match-Power Time Push	Time	1.3	Locked
Static Match-Power Pos. Push	Position	0.4	Locked
Dynamic Match-Power Pos. Push	Position	0.8	Locked

Sampling frequency of the receiver is set to 5 MHz and three correlators are employed. Spacing between the correlators is 0.5 chips. Furthermore, for calculating detection thresholds, expansion factor, m_{exp} is determined as 4 and detection window is 2 seconds unless a different detection window is specified.

Thresholds are calculated for each PRN by using variance and mean values of the clean dataset. Spoofing attacks start at a certain second in the datasets mentioned above. Before beginning of the attacks, receiver recording datasets only collects authentic signals allowing to accumulate correlator values to construct a threshold for nominal values.

Static Match-Power Position Push

In this scenario, the spoofing signals deceiving position information of the receiver have a power advantage of 0.4 dB. Also, its doppler frequency is locked to authentic signals.

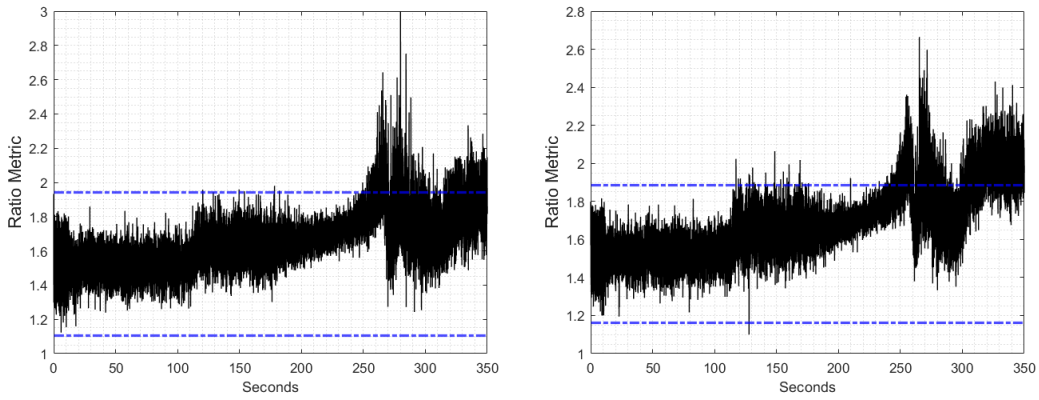

Figure 4.34. Ratio Metric and Thresholds for PRN 3 and PRN 23

As can be seen from Figure 4.34, after initial spoofing signal injection which is around 100th second, values of the ratio metric increases but still manages to not to be detected by the threshold in PRN 3. Injection of the spoofing also increases the variance of the metric. Then around 180th second, power of the spoofing signal is increased which explains lower amplitude variance of the metric. After 200th second, position push starts and amplitude variation of the metric increases drastically.

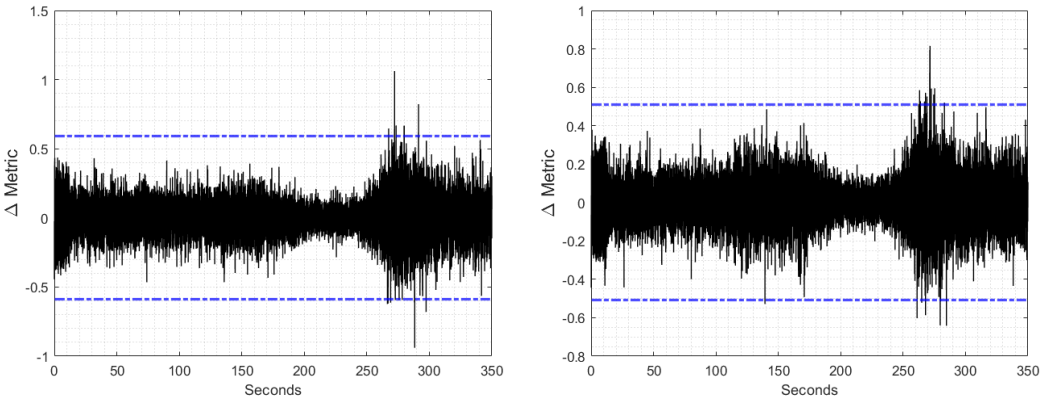

Figure 4.35. Delta Metric and Thresholds for PRN 3 and PRN 23

Similar behavior on delta metrics can be observed, increasing spoofing power leads decreasing variation and position push amplifies the variation due to interaction which causes metric taking values over the detection threshold.

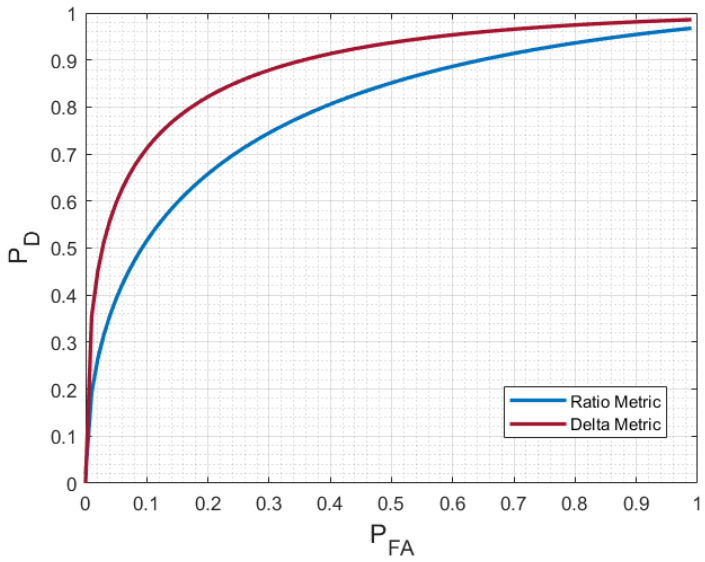

Figure 4.36. ROC curves for static match-power position push scenario

Comparison between the metrics is realized by using ROC curves as can be seen from Figure 4.36. Since ratio metric is more susceptible to noise, performance of the delta metric happens to be better than ratio metric.

Sliding window method introduced in Chapter 3, can be utilized to detect spoofing attacks. Also, thresholds for sliding window are calculated according to equations shown in Chapter 3.

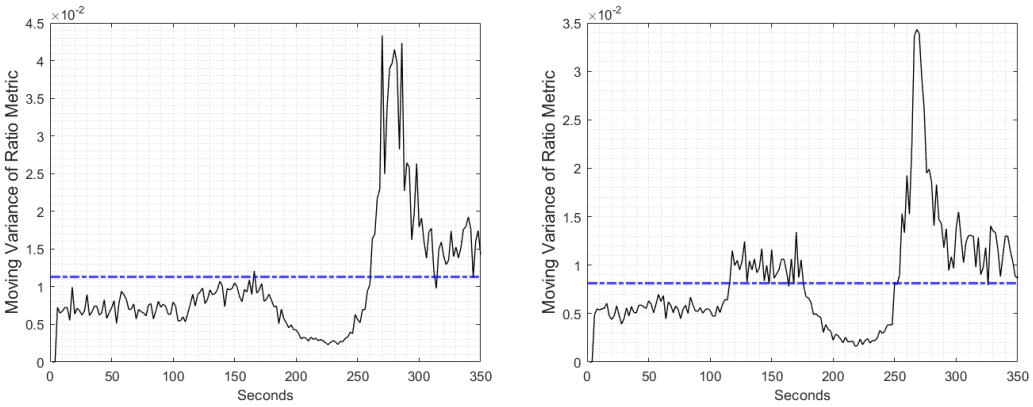

Figure 4.37. Ratio Metric Sliding Window and Thresholds for PRN 3 and PRN 23

As it is stated for behavior of the ratio metrics, increasing amplitude of the spoofing signal triggers detection threshold. If sliding window of PRN 23 is examined, it can be seen that sliding window method makes spoofing amplitude increase around 150th more explicit and it is detected by the threshold.

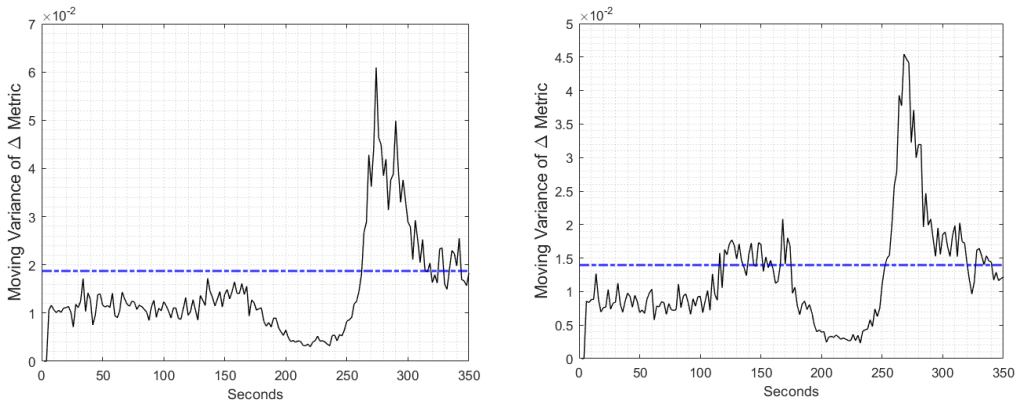

Figure 4.38. Delta Metric Sliding Window and Thresholds for PRN 3 and PRN 23

Static Match-Power Time Push

Second scenario is called as “static matched-power time push”. Intention of the spoofing signals is deceiving time measurement of the receiver with a power advantage of the 1.3dB. Furthermore, in this scenario, Doppler frequency of the spoofing signals which begins to be transmitted from around the 120th second is locked to authentic signals. Like the previous scenario, Doppler frequency of the spoofing signals are locked to authentic signals.

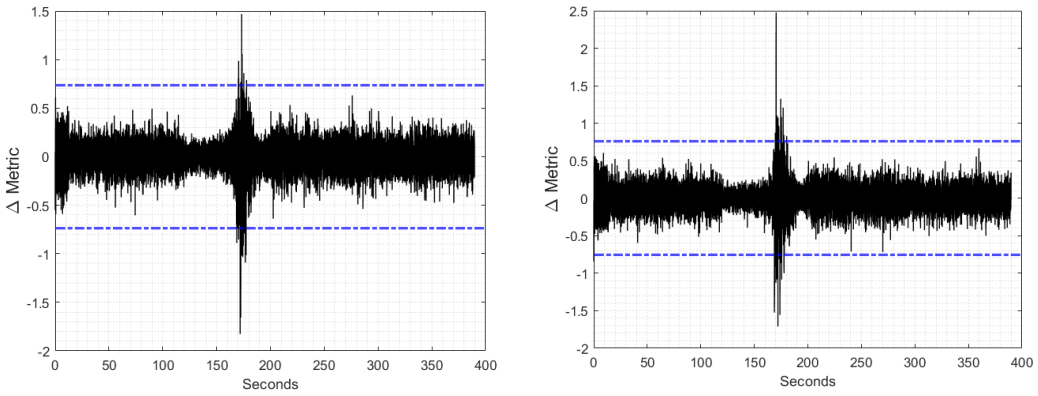

Figure 4.39. Delta Metric and Thresholds for PRN 16 and PRN 19

In Figure 4.39, amplitude variance of the metric decreases around after 100th second when the spoofing signals began to be transmitted. This indicates power advantage of the spoofing signals. After the 150th second, time push starts and interaction between authentic signals and spoofing signals causes sudden changes in delta metric. In Figure 4.40, ratio metric shows a response similar to delta metric against spoofing signals. Enormous variations on the ratio metric continues in longer interval compared to delta metric. Unlike position push, after injection of the spoofing signals, increased variation of the metrics is not observed.

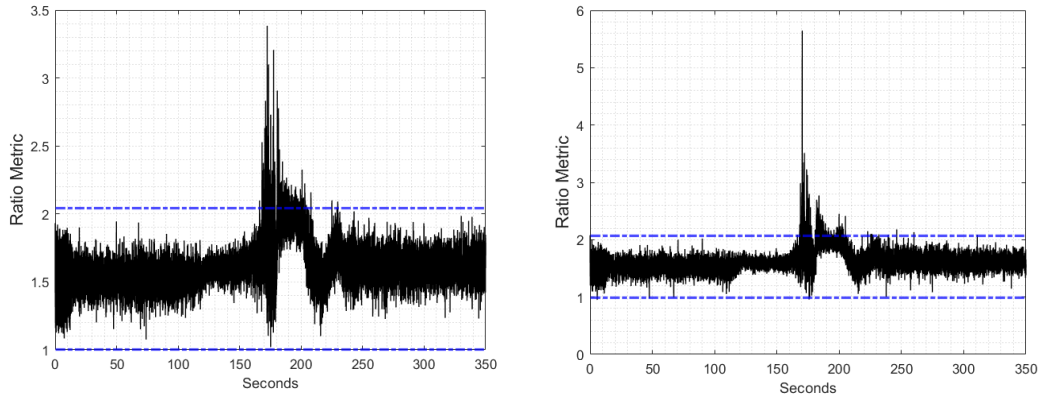

Figure 4.40. Ratio Metric and Thresholds for PRN 16 and PRN 19

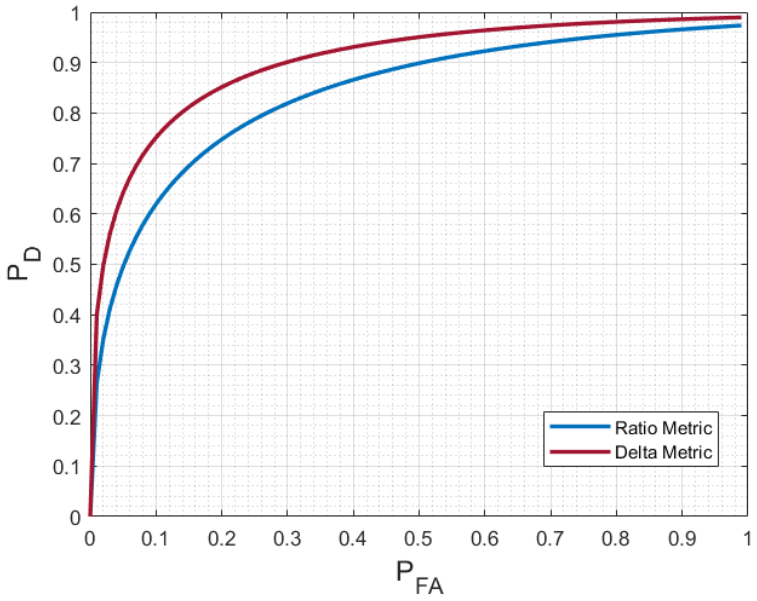

Figure 4.41. ROC curves for static match-power time push

Similar to previous scenario, ROC curves that are depicted on Figure 4.41 shows superior detection success of delta metric over ratio metric. Both metrics demonstrate better performances compared to previous scenario because in this scenario power advantage of the spoofing signals is greater than the previous one. This is an expected result if discussion on Chapter 3 is recalled.

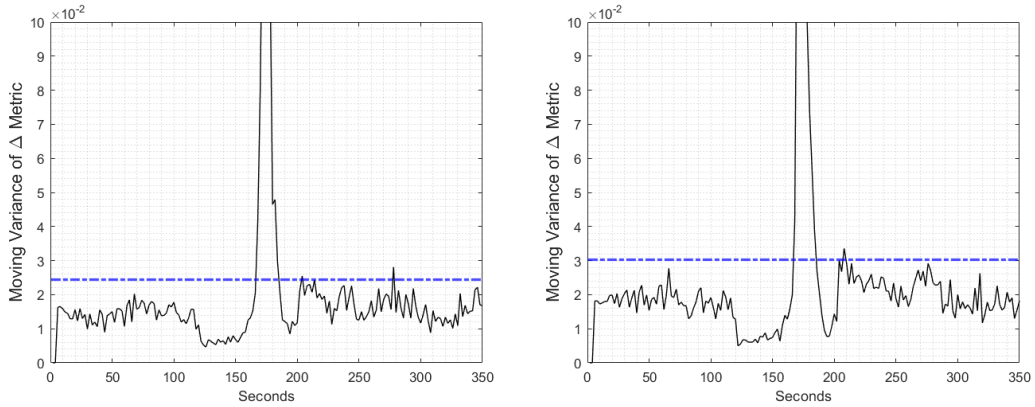

Figure 4.42. Delta Metric Sliding Window and Thresholds for PRN 16 and PRN 19

In Figure 4.42 and Figure 4.43 decrease in the sliding window metrics is observed. After 150th second, sudden change indicates spoofing attack. Behavior of the moving variance metric is similar to previous scenario. Sudden increase is caused by distortion at the correlation function.

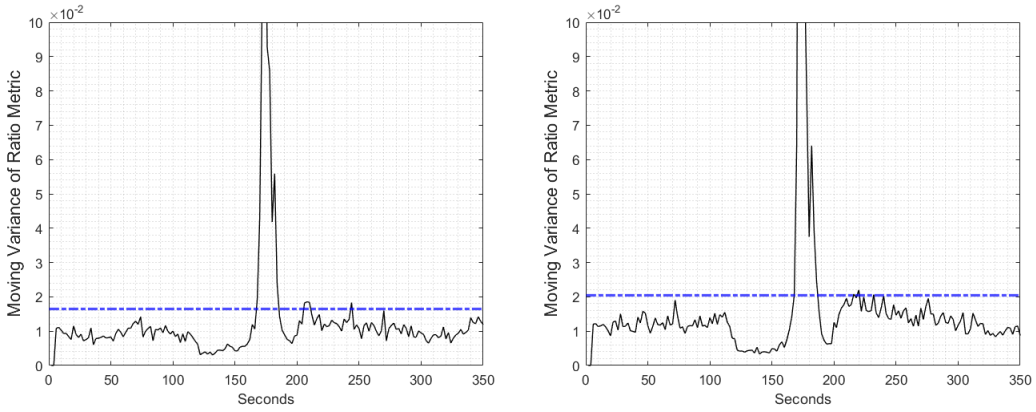

Figure 4.43. Ratio Metric Sliding Window and Thresholds for PRN 16 and PRN 19

Dynamic Match-Power Position Push

Fourth and final scenario is called as “dynamic matched power position push”. Its power advantage is 0.8 dB and Doppler frequency of the spoofing signals are locked to authentic signals. Furthermore, the attack applies a position push.

Frequency locked attack mode in dynamic platforms is not a common attack methodology because of its arduous implementation. To align the spoofing signals to true signals, knowledge for the position of the receiver must be very precise. For example, if an alignment within 1/6 of a carrier cycle is desired to be achieved, the position of the victim receiver antenna must be known within 3 cm radius. Considering the dynamic scenario which the victim receiver has a velocity and a moving direction, it is hard to execute and succeed a frequency locked attack in dynamic applications [73].

Also, as it is stated in [16], dynamic applications create interactions between authentic signals and natural multipath, fading effects. Effects of the multipath are observed on SQM metrics in this scenario.

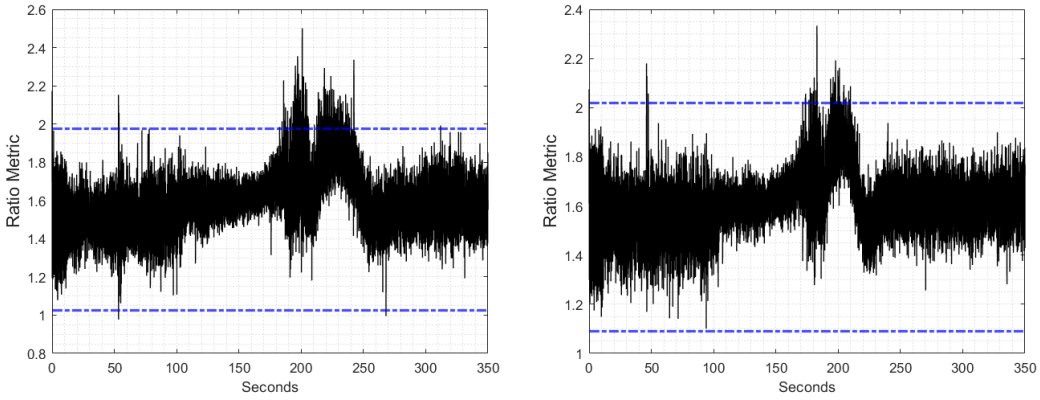

Figure 4.44. Ratio Metric and Thresholds for PRN 18 and PRN 22

As can be seen from Figure 4.44, before the beginning of the spoofing attack, the metric gets higher values than upper threshold. These spurious peaks can indicate an occurrence of a multipath.

If the peaks created by multipath interference and spoofing attack is compared, it can be deducted that peaks created by spoofing have higher width. They span bigger time periods. On contrary, multipath does not create peaks that cover large period in the time axis.

To overcome spurious effects of the multipath, interpretation mentioned above can be used. After calculating values of the ratio metric, a “detection window” can be constructed. Instead raising a flag at every time when the threshold is breached, an algorithm that accumulates metric values in a detection window can be constructed. For example, a detection window covers 500 samples. If only 2 samples are over the threshold values within the window, then spoofing detector does not raise a flag. But if values of the 300 samples reaches above the threshold, then it can be deducted that there is a spoofing attack and spoofing flag can be raised. Obviously, to construct

such an algorithm, a clean dataset must be examined as a calibration phase. Number of samples raising a flag will closely depend to period of the detection window and statistics of the clean dataset.

CHAPTER 5

CONCLUSION

In this thesis work, spoofing generation and detection methods are investigated by employing both hardware and software domain testing setups. Spoofing methods are introduced respect to their sophistication level and detection methods for each of them are tried to be specified.

Thesis introduces theoretical background to successfully generate spoofing attacks and to find their detection methods. Furthermore, an extensive literature review shows currently researched methods for GPS spoofing.

In hardware domain spoofing setups, time and location information of COTS GPS receivers are spoofed using overpowered spoofing attacks with or without noise padding property. Implementation in the thesis proved that simple overpowered attacks are useful against receivers operating in cold-start mode. On the other hand, receivers operating in tracking mode is harder to be spoofed by using this method. The spoofer needs to increase its power level to take advantage over authentic GPS signals but still manage to generate reasonable power levels to avoid detection by C/N_0 monitoring. Simple overpowered spoofing attacks can be detected easily by using C/N_0 monitoring technique since they need power advantage over authentic signals. Furthermore, it is hard to transmit at the correct power levels if instant location of the receiver is not known within an accuracy.

A more sophisticated spoofing method is overpowered spoofing with noise padding. It is shown that by correctly adjusting output power of noise padding circuitry, C/N_0 levels of spoofing signals observed by the receiver can be adjusted to a desired level. This attack can misguide C/N_0 monitoring technique since it can adjust carrier-to-noise ratio to a desired level. The receiver must incorporate an AGC monitoring algorithm to detect the attacks.

In software domain, sophisticated attacks such as frequency-locked, power-matched scenarios are investigated. An open-source test battery and an open-source GNSS receiver are used. GNSS receiver are configured to perform signal quality monitoring algorithms. Correlator values of tracking stages of the GNSS receiver are monitored with various metrics. Furthermore, to smoothen the data outputted by the metrics certain smoother metrics are employed. Thresholds for each metric are computed. In dynamic scenarios SQM metrics raised false spoofing flags due to possible multipath interference. All of the spoofing scenarios and their detection methods are summarized into a table which can be seen below.

Table 5.1 Classification of spoofing types and their detection methods

Spoofing Type	**Anti-Spoofing Type**
Overpowered attack with GPS simulator	C/N_o monitoring
Overpowered attack with GPS simulator equipped with noise padding	C/N_o coupled with AGC monitoring
Matched power attack	Signal Quality Monitoring

Along with achievements mentioned above, future aspects of the field are enormous. Integrating introduced methods to other GNSS systems can be yet alone an important future work. In the thesis, spoofing attacks are detected by using AGC values. Characterizing these values by sweeping spoofing power can improve ability of the receiver of detecting and discriminating the attacks. Furthermore, analytical detection thresholds for AGC values can be derived by the virtue of characterization. Also, behavior of the values can be modeled under different conditions to enhance robustness of the detection method. These enhanced methods can increase further the reliability of the GPS receivers.

REFERENCES

[1] J. B.-Y. Tsui, Fundamentals of Global Positioning System Receivers: A Software Approach, John Wiley & Sons Publication, 2005.

[2] National Research Council, he Global Positioning System for the Geosciences: Summary and Proceedings of a Workshop on Improving the GPS Reference Station Infrastructure for Earth, Oceanic, and Atmospheric Science Applications, Washington, DC: The National Academies Press, 1997.

[3] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder and S. H. Jensen, A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach, Boston: Birkhauser, 2007.

[4] M. S. Braasch and J. V. Dierendonck, "GPS Receiver Architectures and Measurements," in *Proceedings of the IEEE*, Delft, 1999.

[5] E. D. Kaplan and C. J. Hegarty, Understanding GPS Principles and Applications, 2nd ed., Boston, Mass: Artech House, 2006.

[6] E. Rebeyrol, C. Macabiau, L. Ries, J.-L. Issler, M. Bousquet and e. al., "Phase noise in GNSS transmission / reception system," in *ION NTM 2006, National Technical Meeting of The Navigation*, Monterey, 2006.

[7] R. Cerda, Understanding Quartz Crystals and Oscillators, Artech, 2014.

[8] R. B. Pereira, "GNSS Applications," European Space Agency, 2011.

[9] M. Psiaki and T. Humphreys, "Civilian GNSS Spoofing, Detection, and Recovery," *Integrated Satellite Navigation, Sensor Systems, and Civil*

Applications, no. Position, Navigation, and Timing Technologies in the 21st Century, 2021.

[10] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," *International Journal of Navigation and Observation,* 2012.

[11] C. Günther, "A Survey of Spoofing and Counter-Measures," *Journal of the Institute of Navigation,* vol. 61, no. 3, pp. 159-177, 2014.

[12] S. Z. Khan, M. Mohsin and W. Iqbal, "On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions," *PeerJ Computer Science,* no. doi: 10.7717/peerj-cs.507, 6 May 2021.

[13] S. Goff., "Reports of Mass GPS Spoofing Attack in the Black Sea Strenghten Calls for PNT Backup," 24 July 2017. [Online]. Available: https://insidegnss.com/reports-of-mass-gps-spoofing-attack-in-the-black-sea-strengthen-calls-for-pnt-backup/.

[14] D. P. Shepard, J. A. Bhatti and T. E. Humphreys, "Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle," *GPS World,* vol. 23, no. 8, pp. 30-33, 2012.

[15] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation,* Savannah, USA, 2008.

[16] T. Humphreys, J. Bhatti, D. Shepard and K. Wesson, "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*, Nashville, 2012.

[17] J. Bhatti and T. E. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection," *Navigation,* vol. 64, no. 1, pp. 51-66, 2017.

[18] P. Montgomery, T. Humphreys and B. M. Levina, "Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proceedings of the Institute of Navigation International Technical Meeting*, Anaheim, California, 2009.

[19] M. L. Psiaki and T. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE,* vol. 104, 2016.

[20] "GPS, Glonass, Galileo, BeiDou Receiver Testing Using a GNSS Signal Simulator Application Note," Rohde & Schwarz, 2014. [Online]. Available: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_application/application_notes/1gp86/1GP86_2E_GNSS_Receiver_Testing.pdf.

[21] T. Ebinuma, "GPS-SDR-SIM," GitHub, 2015. [Online]. Available: https://github.com/osqzss/gps-sdr-sim.

[22] R. Yang, Z. Song, L. Chen, Y. Gu and X. Xi, "Assisted Cold Start Method for GPS Receiver with Artificial Neural Network-Based Satellite Orbit Prediction," *Measurement Science and Technology,* vol. 32, 2020.

[23] E. McMilin, D. S. D. Loranzo, P. K. Enge and D. M. Akos, "Spoofing Detection and Anti-Jam Mitigation for GPS Antennas". United States of America Patent 10,690,776, 23 June 2020.

[24] J. Chen, S. Zhang, H. Wang and X. Zhang, "Practicing a Record-and-Replay System on USRP," in *Proceedings of the Second Workshop on Software Radio Implementation Forum*, 2013.

[25] C. Cristodaro, L. Ruotsalainen and F. Dovis, "Benefits and Limitations of the Record and Replay Approach for GNSS Receiver Performance Assesment in Harsh Scenarios," *Sensors*, vol. 18, no. 7, 2018.

[26] B. M. Ledvina, W. J. Bencze, B. Galusha and I. Miller, "An in-line anti-spoofing device for legacy civil GPS receivers," in *Proceedings of the Institute of Navigation*, San Diego, California, 2010.

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

[28] E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter and P. Enge, "Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers," in *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, Virginia, 2018.

[29] D. Miralles, A. Bornot, P. Roquette, N. Levigne, D. M. Akos, Y.-H. Chen, S. Lo and T. Walter, "An Assessment of GPS Spoofing Detection Via Radio Power and Signal Quality Monitoring for Aviation Safety Operations," *IEEE Intelligent Transportation System Magazine,* vol. 12, no. 3, 2020.

[30] S. Lo, F. Rothmaier, D. Miralles, D. Akos and T. Walter, "Developing a Practical GNSS Spoofing Detection Thresholds for Receiver Power Monitoring," in *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation*, St. Louis, 2021.

[31] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan and G. Lachapelle, "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array," in *ION GNSS12 Conference*, Nashville, 2012.

[32] A. Konovaltsev, S. Caizzone, M. Cuntz and M. Meurer, "Autonomous Spoofing Detection and Mitigation with a Miniaturized Adaptive Antenna Array," in *Proceedings of the 27th International Technical Meeting of the ION Satellite Division*, Tampa, 2014.

[33] E. Garbin Manfredini, "Signal processing techniques for GNSS anti-spoofing algorithms. PhD thesis," Politecnico di Torino, Torino, 2017.

[34] J. Huang, L. L. Presti, B. Motella and M. Pini, "GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky," *ICT Express*, vol. 2, no. 1, pp. 37-40, 2016.

[35] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao and W. Feng, "GNSS Spoofing Detection by Means of Signal Quality Monitoring (SQM) Metric Combinations," *IEEE Access*, vol. 6, pp. 66428-66441, 2018.

[36] C. Sun, J. W. Cheong, A. Dempster, L. Demicheli, E. Cetin and H. Zhao, "Performance assessment of multi-metric joint detection technique for anti-spoofing," in *International Global Navigation Satellite Systems Association IGNSS Conference*, Australia, 2018.

[37] L. Li, C. Sun, H. Zhao, H. Sun and W. Feng, "GNSS Spoofing Detection Using Moving Variance of Signal Quality Monitoring Metrics and Signal Power," in *International Conference on Communications and Networking*, Beijing, 2020.

[38] M. Irsigler and G. W. Hein, "Development of a Real-Time Multipath Monitor Based on Multi-Correlator Observations," in *Proceedings of the*

18th International Technical Meeting of the Satellite Division of The Institute of Navigation, Long Beach, 2005.

[39] J. A. Bhatti, T. E. Humphreys and B. M. Ledvina, "Development and Demonstration of a TDOA-Based GNSS Interference Signal Localization System," in *2012 IEEE/ION PLANS Conference*, Myrtle Beach, 2012.

[40] P. Swaszek, S. Pratz, B. Arocho, K. Seals and R. Hartnett, "GNSS Spoof Detection Using GNSS Spoof Detection Using," in *ION GNSS+*, Tampa, 2014.

[41] C. Tanil, S. Khanafseh, M. Joerger and B. Pervan, "An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position," *IEEE Trans. on Aerospace and Electronic Systems,* vol. 54, no. 1, p. 131–143, February 2018.

[42] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan and e. al., "GPS Spoofing Detection using RAIM with INS Coupling," in *IEEE/ION PLANS Meeting*, 2014.

[43] J. Arribas Lazaro, "GNSS Array-based Acquisition: Theory and Implementation," in *Centre Tecnologic de Telecomunicacions de Catalunya*, Barcelona, 2012.

[44] Electronic Communications Committee, "ECA TABLE IN THE FREQUENCY RANGE 8.3 kHz to 3000 GHz," [Online]. Available: https://www.grss-ieee.org/wp-content/uploads/2014/07/ECA_European_Table_of_Frequency_Allocations_May_2014.pdf. [Accessed May 2014].

[45] B. Razavi, RF Microelectronics, 2nd ed., New Jersey, New York: Prentince Hall, 2012.

[46] M. Lichtman, "PySDR: A Guide to SDR and DSP using Python," 2022. [Online]. Available: https://pysdr.org.

[47] C. Calvo, "Obscurities & Applications of RF Power Detectors," 2007. [Online]. Available: https://www.ieee.li/pdf/viewgraphs/rf_power_detectors.pdf.

[48] J. Lange, "Interdigitated Strip-Line Quadrature Hybrid," in *G-MTT International Microwave Symposium*, 1969.

[49] Ş. Uysal and H. Aghvami, "Synthesis, design, and construction of ultra-wide-band nonuniform quadrature directional couplers in inhomogeneous media," *IEEE Transactions on Microwave Theory and Techniques,* vol. 37, no. 6, 1989.

[50] D. M. Pozar, Microwave Engineering, 4th ed., New York: Wiley, 1998.

[51] H. Friis, "Noise Figures of Radio Receivers," *Proceedings of the IRE,* vol. 32, no. 7, 1944.

[52] U-BLOX, "U-BLOX NEO-6M GPS Receiver Datasheet," U-BLOX, 2011. [Online]. Available: https://www.u-blox.com/en/product/neo-6-series.

[53] U-BLOX, "ZED-F9P GPS Receiver Datasheet," U-BLOX, 2022. [Online]. Available: https://www.u-blox.com/en/product/zed-f9p-module.

[54] C. Fernandez and J. Arribas, "GNSS-SDR," 2011. [Online]. Available: https://github.com/gnss-sdr/gnss-sdr.

[55] P. Enge, D. Akos, J. Do, J. B. Simoneau, L. W. Pearson, V. Seetharam and A. J. Oria, "Measurements of Man-Made Spectrum Noise Floor," NASA Technical Reports Server, Washington DC, 2004.

[56] J. P. A. Perez and S. C. P. B. C. Lopez, Automatic Gain Control: Techniques and Architectures for RF Receivers, London: Springer, 2011.

[57] B. Parkinson and J. Spilker, Global Positioning System: Theory and Applications, New York: American Institute of Aeronautics, 1996.

[58] Z. Zhou and Y. C. Wei, "The Influence of Automatic Gain Control on Narrowband Frequency Domain GPS Anti-Jamming Receiver," in *International Conference on Communication Technology*, Tianjin, 2021.

[59] D. Whitlow, "Design and Operation of Automatic Gain Control Loops for Receivers in Modern Communications Systems," *Microwave Journal,* 1 May 2003.

[60] Analog Devices, "ADA4961," Analog Devices, 2021. [Online]. Available: https://www.analog.com/en/products/ada4961.html. [Accessed 2021].

[61] S. Kay, Fundamentals of Statistical Signal Processing, Volume II: Detection Theory, Prentice Hall, 1998.

[62] K. D. Wesson, D. P. Shepard, J. A. Bhatti and T. E. Humphreys, "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," in *ION GNSS Conference*, Portland, Oregon, 2011.

[63] M. Ossmann, "Hardware Components of HackRF," 28, 01 2021. [Online]. Available: https://hackrf.readthedocs.io/en/latest/hardware_components.html?highlight=dac#hardware-components.

[64] Analog Devices, "ADALM-PLUTO Hardware," 12 May 2021. [Online]. Available: https://wiki.analog.com/university/tools/pluto/hacking/hardware.

[65] Keysight Technologies, "Keysight Signal Analyzer Specifications Guide," [Online]. Available: https://www.keysight.com/zz/en/assets/9018-

72001/technical-specifications/N9030A-PXA-Signal-Analyzer-Specifications-Guide.pdf. [Accessed October 2021].

[66] A. Broumandan, R. Siddakatte and G. Lachapelle, "An Approach to Detect GNSS Spoofing," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 8, pp. 64-75, 2017.

[67] W. Wang, I. A. Sanchez, G. Caparra, A. McKeown, T. Whitworth and E. S. Lohan, "A Survey of Spoofer Detection Techniques via Radio Frequency Fingerprinting with Focus on the GNSS Pre-Correlation Sampled Data," *Sensors*, vol. 21, no. 9, 2021.

[68] Chang Hong Information Co. Ltd., "Datasheet of GPS Active 28dB Antenna RG174," [Online]. Available: https://www.digikey.com/en/products/detail/adafruit-industries-llc/960/5353630.

[69] Keysight, "Noise Source Operating and Service Manual," 26 June 2018. [Online]. Available: https://www.keysight.com/zz/en/support/346B/noise-source-10-mhz-18-ghz-nominal-enr-15-db.html.

[70] Broadcom Corporation and Cisco Systems Inc., "Digital Transmission: Carrier-to-Noise Ratio, Signalto-Noise Ratio, and Modulation Error Ratio," January 2012. [Online]. Available: https://web.archive.org/web/20160304080134/http://www.broadcom.com/collateral/wp/CMTS-WP101-R.pdf.

[71] C. Fernandez and J. Arribas, "GNSS-SDR: Configurations," 2022. [Online]. Available: https://gnss-sdr.org/conf/.

[72] T. Humphreys, "TEXBAT Datasets 7 and 8," [Online]. Available: https://rnl-data.ae.utexas.edu/datastore/texbat/texbat_ds7_and_ds8.pdf. [Accessed 2016 March 16].

[73] T. E. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073-1090, 2013.