DESIGN AND IMPLEMENTATION OF L1 C/A GPS TRANSMITTER FOR SPOOFING APPLICATIONS

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

BY

YUNUS EMRE TUNÇYÜREK

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

DECEMBER 2022

Approval of the thesis:

DESIGN AND IMPLEMENTATION OF L1 C/A GPS TRANSMITTER FOR SPOOFING APPLICATIONS

submitted by **YUNUS EMRE TUNÇYÜREK** in partial fulfilment of the requirements for the degree of **Master of Science** in **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 Electronic Engineering**

Prof. Dr. Şimşek Demir
Supervisor, **Electrical and Electronic Engineering, METU**

Examining Committee Members:

Prof. Dr. Gönül Turhan Sayan
Electrical and Electronic Eng, METU

Prof. Dr. Şimşek Demir
Electrical and Electronic Eng, METU

Prof. Dr. Temel Engin Tuncer
Electrical and Electronic Eng, METU

Prof. Dr. Gülbin Dural
Electrical and Electronic Eng, METU

Prof. Dr. Asım Egemen Yılmaz
Electrical and Electronic Eng, Ankara University

Date: 01.12.2022

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 : Yunus Emre Tunçyürek

Signature :

ABSTRACT

DESIGN AND IMPLEMENTATION OF L1 C/A GPS TRANSMITTER FOR SPOOFING APPLICATIONS

Tunçyürek, Yunus Emre
Master of Science, Electrical and Electronic Engineering
Supervisor: Prof. Dr. Şimşek Demir

December 2022, 83 pages

GPS is one of the main positioning services used in both military and civilian applications. It is possible to design a custom GPS Transmitter by using the SDR platform and periodically published Orbital Parameters. The realization of such a system brings spoofing threats for GPS Receivers. In this thesis, the baseband GPS signals are created by considering the pseudoranges and Doppler Frequencies for the specific user position with respect to the satellite positions whose orbital parameters are open to access. In addition, created baseband signals are translated to the RF stage through SDR, and the impact of the system on commercial GPS receivers are analyzed for the different kind of scenarios involving static and moving users in different directions. Finally, the hardware's default TCXO-based clock is replaced with that of OCXO-based to examine its influence on the GPS performance. The performance of the suggested system is measured with the U-Blox and Mobile Phone's GPS receivers. Also, the system is tested with receivers having access to the real GPS signals to explore the spoofing capability.

Keywords: GPS Transmitter, SDR, Spoofing, Doppler, L1 C/A

ÖZ

YANILTMA UYGULAMALARI İÇİN L1 C/A GPS ALICI TASARIMI VE GERÇEKLEMESİ

Tunçyürek, Yunus Emre
Yüksek Lisans, Elektrik ve Elektronik Mühendisliği
Tez Yöneticisi: Prof. Dr. Şimşek Demir

Aralık 2022, 83 sayfa

GPS askeri ve sivil uygulamalarda kullanılan konumlandırma servislerinden birisidir. Gelişen SDR teknolojisi ve periyodik olarak yayınlanan Yörünge Parametreleri sayesinde özel bir GPS Verici tasarlamak mümkündür. Bu durum GPS alıcılar için aldatılma tehtidi oluşturur. Bu tezde yörünge parametreleri erişime açık olan uydu konumlarına göre belirli kullanıcı konumu için görünür mesafeler ve Doppler Frekansları dikkate alınarak temel bant GPS sinyalleri oluşturulmuştur. Buna ek olarak, oluşturulan temel bant sinyalleri SDR aracılığıyla RF katmanına taşınmış ve sistemin ticari bir GPS Alıcısı üzerindeki etkisi, static ve arklı yönlerde hareket eden kullanıcıları içeren farklı senaryolar için analiz edilmiştir. Son olarak, donanımın varsayılan TCXO tabanlı saati, GPS performansı üzerindeki etkisini incelemek için OCXO tabanlı saatle değiştirilir. Önerilen sistemin performansı U-Blox ve Cep Telefonu GPS Alıcıları ile ölçülmektedir. Ayrıca sistem yanıltma becerisini keşfetmek için gerçek GPS sinyallerine erişimi olan alıcılarla test edilir.

Anahtar Kelimeler: GPS Verici,SDR, Şaşırtma, Alıcı, L1 C/A

To my parents

ACKNOWLEDGMENTS

I would like to express my deepest appreciation to my supervisor Prof. Dr. Şimşek Demir for his guidance, advice, criticism, encouragements, and insight throughout the research.

I would like to thank Berat Yüksel, Muhammed Tonga and Abdulkerim Çekinmez for their valuable support.

I special thank Batuhan Başar for his help me solder oscillator evaluation board.

I would like to give special thanks to my wife, Didem, for her endless support and love.

I want to thank my family as a whole for their continued support and care.

This work is partially funded by Scientific and Technological Research Council of Turkey under grant number TUBİTAK 2210-A

TABLE OF CONTENTS

CHAPTERS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

ABBREVIATIONS

SDR: Software Defined Radio

TOW: Truncated Time of Week

GPST: GPS Time

UTC: Coordinated Universal Time

TTFF: Time to First Fix

MPS: Meter per Second

SV: Satellite Vehicle

MSL: Mean Sea Level

DOP: Dilution of Precision

LNAV: Legacy Navigation Data

CNAV: Civil Navigation Data

C/N: Carrier-to-Noise Ratio

SPS: Standard Positioning Service

PPS: Precise Positioning Service

PRN: Pseudorandom Noise

PVT: Position, Velocity and Time

A/D: Analog to Digital

LLA: Latitude, Longitude, Altitude

CHAPTER 1

INTRODUCTION

GPS is a widely used positioning service that was developed in USA in the late of ‘70s. It provides different positioning services to users, depending on Navigation Data Types, Encryption methods, and Carrier Frequencies. One of the most widely used GPS services is the L1 band C/A code phase positioning service, whose navigation data is unencrypted. In this system, unencrypted navigation data are modulated with proper ranging codes that identify corresponding satellites. Since navigation data is unencrypted and satellite-specific ranging codes are available, it is possible to realize these operations by employing Software Defined Radio (SDR).

Using a SDR system, this GPS service can be counterfeited by creating hypothetical satellite transmissions which can spoof the GPS receiver to lock onto the intended position, time, and velocity (PVT). An ongoing modernization process aims to prevent GPS vulnerability to attempted spoofing signals. Nevertheless, replacing it with a modernized one may take a long because L1 C/A GPS services are still widely used in many applications. A spoofer can pose a significant threat against numerous applications such as surveying, navigation, military, and electrical transmission (e.g.) because many depend heavily on the synchronized and accurate timing system as well as positioning services that are provided by GPS systems [1]. In addition, GPS is the primary source of PVT information for the areas where it is not possible to connect to modern network systems such as Ethernet, GSM, and Wi-Fi. Therefore, a potential spoofing attack against a GPS System may halt operations in those areas.

The crucial position of incorporated GPS systems in various types of applications increases the significance of the necessary research related to the detection and prevention of spoofing of GPS services. The fundamental step of research efforts starts with implementing a well-designed GPS Transmitter system that can adequately imitate satellites.

In this thesis, it is aimed to create a GPS Transmitter System and evaluate its performance on a commercial GPS Receiver under different movement scenarios. To achieve this, navigation data corresponding to a specific date and SVs are accessed through the NASA CDDIS website. Then, the data are encoded via MATLAB's toolbox. The toolbox is utilized to create SV-specific ranging codes. These ranging codes modulate the navigation data by considering the code phases and Doppler Frequencies retrieved from the pseudoranges values, which are also computed via the MATLAB toolbox. Those static signals are realized in the Adalm-Pluto SDR [2] and applied to the commercial GPS receiver. Then, the performance of the suggested transmitter is evaluated by considering the real GPS expectations and receiver-satellite geometry. Also, the receiver moving in different directions with different velocities are implemented to evaluate performance in different aspects. Then, the clock of the SDR is replaced by a superior one to assess the effects of the clock accuracy on the GPS performance. Finally, the proposed system is evaluated as a spoofer by applying the signals to the receiver with an antenna. This design may give the opportunity to create a test bench for the Satellite Navigation System. The system is adaptable to a wide range of satellite-based positioning services as long as the orbital and clock parameters are available. Hence, it is possible to evaluate the navigation performance of the hypothetical satellites as if they are moving in the sky.

1.1 History

In the twentieth century, Cold War competition between the USA and USSR triggered the emergence of the GPS and GLONASS systems. Aerospace Corporation in the USA started a study on satellite-based navigation programs in 1963, while USRR initiated a similar program in 1960. USA and USRR launched their first navigation satellites in 1967, Timation and Kosmos-192, respectively. The USA started to develop the NAVSTAR GPS program in 1973, launching the first NAVSTAR Satellite thereafter. GLONASS program's first satellite was launched in 1982, and five years later International geodetic community began to use GLONASS [3].

In the beginning of 1990s, the USA declared GPS would be available to the international community in the form of Standard Positioning Services (SPS). Hence, it created millions of businesses with tremendous revenue. However, the GLONASS system failed to create such an impact, although it was also freely accessible to the international community. GLONASS was restored, and it will probably succeed in commercial applications soon [3].

Today, several navigation services other than GPS and GLONASS are in use. These are Galileo systems under development by European Union, BeiDou system being created by the People's Republic of Chine, Quasi-Zenith Satellite System (QZSS) being developed by the Japanese, and Indian Regional Navigation Satellite Systems (NAVIC) being designed by Indian Government. QZSS and NAVIC provide only regional positioning services and BeiDou systems are under development to expand its services into global [4].

1.2 GNSS Systems

The most notable and widespread GNSS systems are GPS, GLONASS, and Galileo. These GNSS systems generally consist of three components: the user segments, the space segments, and the control segments. User segments refer to the receiver side in which users' position, time, and velocities are computed and provided. The space segments correspond to the satellites. Finally, the control segments manage the operation of the system [5]. These components are depicted in Figure 1.1.

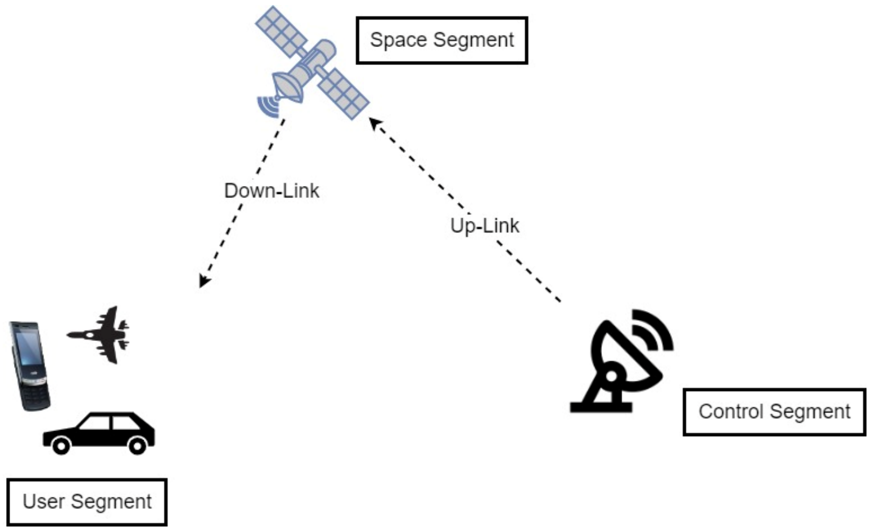


Figure 1.1: GNSS Segments

1.2.1 GPS

Thirty-one operational satellites constitute the GPS Space Segment. These are located in six different orbital planes. The Control Segment maintains the following tasks:

- Uploading the commands and navigation data to satellites
- Checking the health, positions, and velocities of orbital satellites
- Monitoring the GPS performance

The GPS offers two primary services for users: Standard Positioning Service (SPS) and Precise Positioning Service (PPS). The SPS is a standard accuracy positioning service available to all GPS users. SPS accuracy is controlled by the "Selectivity Available" policy, which aims to degrade the service's accuracy if necessary intentionally. The PPS is a more accurate service offered only to the only authorized users [6]. GPS Signals utilize three different carrier frequencies called L1(1575.42MHz), L2(1227.6MHz), and L5(1176.45MHz). Also, two principal ranging codes are involved in GPS systems: Coarse/Acquisition (C/A) and

Precision Code (P(Y)). C/A codes are modulated into the L1 carrier. P(Y) codes are modulated into both L1 and L2 carriers. Also, C/A codes are utilized as civil ranging codes, and P(Y) codes are encrypted to prevent the access of unauthorized users to services. Hence, SPS service use C/A codes while PPS users can use either P(Y) codes or both P(Y) and C/A codes.

1.2.2 Galileo

Galileo offers four different services to users: Open Service (OS), a freely available mass-market product providing simple positioning and timing. The Second service is an encrypted, highly accurate, and guaranteed service called Commercial Services (CS) or Galileo High Accuracy Service (HAS). The third of them is Public Regulated Service (PRS), allocated for only government-authorized users with encrypted data. That service is also access-controlled and more robust. Finally, The Search and Rescue Service (SAR) is designed to provide support for search and rescue activities. Its working principle is to collect signals from emergency beacons and forward those emergency signals to national rescue centers.

1.2.3 GLONASS

GLONASS provides military service as well as civilian service. Its Space Segment consists of 24 operational satellites which move along three different orbital planes. Satellites are equally distributed along these planes, 8 per single plane [7]. Its control segments are used to track the satellites for the detection of orbit and clock, send the navigation message to space segments, and synchronize the time of satellites. Although the GLONASS frequency plan is mainly based on two different carrier frequencies called G1(1602MHz)-G2(1246MHz), another carrier frequency denoted by G3(1204.74MHz) is stated in different publications. GLONASS navigation signals utilize two main codes: S-Code with standard accuracy and P-code with high accuracy signals. The S-Code is only modulated on the G1 band, while P-Code is modulated on both G1 and G2. Unlike GPS, GLONASS uses Frequency-Division Multiple Access (FDMA) [8].Thanks to FDMA, Satellites are differentiated with respect to their frequencies. FDMA method increases the resistance of the GLONASS signals against interference by offering frequency diversity. However, the receivers processing FDMA signals are required to have higher bandwidth than the original signal bandwidth [7].

1.3 Vulnerability of GPS System

GPS services are crucial for many applications such as navigation, infrastructure, surveying, etc. Due to weak power level at the receiver side, satellite signals are vulnerable to corruption by intentional interferences such as spoofing and jamming. Therefore, this weakness of the GPS system draws the attention of all segments [1].

1.3.1 Jamming

Jamming signals within the appropriate band and power level overpower actual GPS signals at the receiver side and degrade the performance or cause the receiver to lose track. GPS signals arriving at the receiver have a feeble level, even lower than thermal noise. Handling such a weak signal requires a large front-end gain. Jamming interference with sufficient power can make the gain stages go into saturation. Suppose the saturated front-end stage spoils the receiver signals. In this case, the tracking and acquisition stages cannot operate properly, no matter what algorithm is implemented in the digital part [9]. Fortunately, the AGC stage automatically control the receiver gain to maintain the constant RMS power at input of A/D stages. That gain value can also serve as indicator of the jamming interference level [1].

To evaluate jamming signals’ effect on the A/D section, one should consider two types of A/D conversions: pre-correlation A/D and post-correlation A/D. Spreading process is performed prior to A/D conversion in the post-correlation A/D. Post-correlation A/D takes advantage of this process against jamming interference since the interference signal spreads over the chipping code bandwidth. On the other hand, jamming signals directly come to the A/D stage for the pre-correlation A/D. Hence, the spread process does not propose any resistance to jamming interference for this type of A/D [10]. The impact of the spreading process on the jamming interference for the post-correlation A/D is formulated in Equation 1.1, where J^2 is jamming power and P_r is the received signal power.

$$(\frac{J}{S}) = \frac{J^2}{P_r} \tag{1.1}$$

Here $(\frac{J}{S})$ corresponds to the ratio of the jamming power to the signal power at the receiver input. After the spreading process, the ratio turns into the form seen in Equation 1.2, where $R_b$and R_c are data modulation bandwidth and chipping rate, respectively.

$$(\frac{J}{S}) = \frac{J2R_b}{P_r R_c} \tag{1.2}$$

For the GPS L1 C/A, R_b and R_c are 50Hz and 1.023MHz. Hence, the spreading process in the post-correlation A/D suppress the jamming effect in proportion to process gain. Note that if the jamming signals are perfectly aligned with GPS PRN codes, their effect doesn't degrade with the spreading process.

1.3.2 Spoofing

GPS spoofing is deceiving the receiver by applying a counterfeit GPS signal. In that way, the receiver locks onto these fake signals and calculates the incorrect position, time, and velocity solutions. Especially the civilian GPS is more vulnerable to spoofing since the content of these signals is not authentic. On the other hand, the military GPS content is restricted to only authorized users and is vulnerable to only meaconing-type attacks, as mentioned below.

The main spoofing types are categorized below:

- Simplistic Attack

The main components of this attack are the GPS simulator and a suitable Radio Front-End. The simulator generates fake GPS signals by inserting the Doppler frequencies and code phases concerning the specific user position, time, and velocity. The spoofing signals hardly synchronize with the actual GPS Signals; therefore, it is easily detected. [1]. One of the difficulties for the spoofer is to make the receiver lose the lock of actual signals. It is overcome by applying the jamming signals before the spoofing signals [11].

- Intermediate Attack

For this type of attack, the spoofer consists of the GPS receiver as well as the transmitter. The spoofer system utilizes knowledge of its own position and target position to align the phase of the counterfeit signals with the real signal. Then, correlation peaks of actual GPS signals and fake signals match. The power level of fake signals is gradually increased to avoid being detected. Finally, the receiver locks onto the counterfeit signals. Such a synchronized spoofing signal is hard to be detected by the receiver. The common countermeasure for this type of attack is to distinguish the signals by the angle of arrival. However, this countermeasure can be overcome by using multiple receiver-transmitter spoofers. In that, the spoofer can also mimic the direction of arrival [11].

- Meaconing attack

The previous spoofers regenerate the ranging codes and data bits. A meaconing attack depends on collecting the broadcasting satellite’s signals without any digital signal process. Spoofer broadcasts the collected signals by introducing sufficient gain to overwhelm the real signal power at the receiver side and proper delay. Also, data content and spreading codes are not required to be known for this type of spoofer. Therefore, it can deceive not only the civilian GPS but also the military GPS [12]

1.4 Outline of the Thesis

In Chapter 1, namely Introduction, widely used GNSS services are introduced. It is emphasized that the competition between the GLONASS and GPS. Also, the historical development of GNSS services is mentioned. The vulnerabilities of the GPS system are proposed by highlighting jamming and spoofing threats. Also, the main motivations behind the thesis are described.

In Chapter 2, the literature review on the GPS transmitter concepts are presented. The Chapter 2 covers the brief architecture of the GPS system. Navigation Data are briefly mentioned, and signal structure of the GPS are described in the chapter. Also, the necessary concepts for the GPS positioning system are examined

Chapter 3 describes the positioning concept by providing the fundamental processes, steps, and equations. Also, the crucial parameters for the GPS performance evaluation are derived and discussed in this chapter.

In Chapter 4, the hardware implementation of the transmitter and the generation of the satellite signals are explained in detail. Then, the proposed system's capability for implementing the different user scenarios: stationary and dynamic users moving vertically and horizontally are observed through the commercial GPS receiver. Also, the impact of the transmitter's clock on the GPS performance is investigated by changing the default clock of SDR. The proposed system is also tested on the mobile phone to reveal the GPS performance's dependence on the receiver type. Finally, the hypothetical signals are applied to the receiver with a GPS antenna to observe the proposed system's spoofing ability.

In Chapter 5, the main achievements of the suggested system are briefly described. Also, the conclusions of this research and future works are presented in this chapter.

CHAPTER 2

GPS ARCHITECTURE

GPS positioning operation is performed based on the ranging code and navigation data emitted from the SVs. Hence, understanding the component of the GPS architecture is mandatory for the successful implementation of the GPS transmitter. This chapter reviews the GPS signals structures, modulation techniques, and navigation data. Also, the reference frames utilized in the GPS positioning process are briefly described. Note that the chapter emphasizes SPS services components; C/A code and LNAV. Furthermore, Doppler Effects, and Clock Accuracy concepts are discussed in the context of GPS systems.

2.1 Literature Survey

The primary step of a GPS Spoofing System is to design a GPS Transmitter; therefore, in the literature, GPS Transmitter Design is mainly explored in the context of GPS Spoofing research.

In [13], the author proposes a GPS simulator that creates GPS transmitter signals with respect to given user positions and processes the created signal via GPS Receiver Model. The Entire model is realized in a MATLAB-based Software environment. It is obtained that Noise Power is inversely proportional to position error between the estimated and observed user positions. It points out that Doppler Frequency has a slight impact on this kind of error, as well as clock accuracy.

In [1], the authors investigate that tendency of GPS receivers to lock onto artificial GPS signals. They also examine which hardware platforms are appropriate for creating realistic GPS transmission in terms of frequency, bandwidth, and output power. They mention that spoofing systems using multiple transmitters can be much harder to prevent if properly designed. Researchers also provide a comprehensive list of successful GPS Spoofing attacks in the real world.

In [14], authors utilize the open-source GPS-SDR-SIM software to perform successful GPS Spoofing via Pluto -SDR. They also briefly investigate the impact of clock accuracy on receiver performance parameters, notably received Doppler Frequency. TCXO and OCXO, with different ppm values, are compared in terms of frequency variance. Also, the proposed system is tested against commercial GPS Receivers located in different platforms such as U-Blox, a car GPS, and a mobile Phone’s GPS. They also emphasize that inconsistent power levels and Doppler values may cause a failed spoofing attempt. They demonstrate that these failures can be prevented by re-adjusting the power level and replacing the clock with accurate ones.

In [15], the authors also used GPS-SDR-SIM software to accomplish GPS Spoofing System. The proposed GPS system’s effects on moving and stationary targets are investigated. Moreover, they also examine the impact of spoofing signals on a stationary drone which is supposed to keep in a fixed position through position control algorithms employed. In that way, the drone’s motion gives insight to the spoofing performance. In an identical manner to [15], moving and stationary receivers are exposed to GPS Spoofing Signals in [16]. It is realized that Measured Doppler Frequency is consistent with the predicted Frequency. Also, they list the required periods to lock onto Spoofing Signal for different receiver states.

In his paper [11], Humphreys investigated the spoofing prevention capability of receivers and suggested different spoofing attacks. It is stated that GPS Receiver may flag up as an indicator of the Spoofing Signal. One way to circumvent such a preventive measure is jamming the GPS receiver prior to the Spoofing attempt. In the paper, they model a Spoofer Channel and demonstrate how to combine multiple channels to create a single output signal.

2.2 Reference System

2.2.1 Time Reference

GNSS system works based on the measurement of travel time between the receiver and satellites; thereby, an accurate time system is crucial in GNSS Systems. Several time systems currently in use are listed in Table 2.1 [5]. In the context of this thesis, UTC and GPS reference times are highlighted in the following part.

Table 2.1: Different Time Systems

Periodic Process	*Time*
Earth's Rotation	Universal Times(UT0,UT1,UT2) Greenwich Sidereal Time
Earth Revolution	Terrestical Dynamic Time (TDT) Barycentric Dynamic Time(TDB)
Atomic Oscillator	International Atomic Time(TAI) Coordinated Universal Time (UTC) GNSS Reference Time

As seen in Table 2.1, UTC is atomic time derived from 250 caesium clocks and hydrogen masers worldwide. A set of algorithms maintains these clocks to ensure a uniform time origin. In addition to this, that requires leap seconds adjustment so as to keep being synchronized with earth rotation. [4], [5]. On the other hand, the GNSS Reference time scale used in GNSS Systems is a continuous time scale, and different GNSS systems may use different time systems. (e.g., GPS System Time for GPS, Galileo System Time for Galileo). GPS time is referenced to a set of atomic clocks located at the GPS Master Segments and onboard Satellites. It is also referenced to UTC; therefore, it starts at midnight between 5-6 January 1980, which is also starting time of UTC. However, GPS time cannot synchronize with Earth's rotation because the solar day slows by about 1 sec per year. It is handled by UTC, which is periodically adjusted, although it runs at the same speed as GPST. Because of leap seconds inserted into UTC, UTC Time are behind the GPS time by 18s in 2022. The difference between UTC and GPS Time scales, namely leap seconds, is involved in GPS Navigation Data [17]. Nonetheless, conversion from UTC to GPS time may not be a requirement because most modern navigation equipment relies on GPS Time as a time base instead of UTC[18].

GPS Time information is contained in the HOW word of each subframe of Navigation Data in the form of week number and elapsed time of second within the week. Receivers somehow combine these data to derive corresponding GPS Time information, as explained in section 3.2.

2.2.2 Coordinate Reference Frame

An accurate and well-defined coordinate system is essential for catching on to the working principle of the GNSS systems, especially the GPS. In this section, these systems are briefly mentioned. Satellite positions described by the Keplerian orbital Element need to be converted to ECEF, mainly used to compute the position of the receiver or ground object. Since the “xy” plane of ECEF coordinates systems overlaps with Earth’s equatorial plane, it is convenient to utilize ECEF coordinates for the transformation of geodetic coordinates, latitude, longitude, and altitude.

Understanding height measurement on the earth’s surface is necessary for evaluating the GPS outputs. The altitude with respect to the Mean Sea Level corresponds to the Geoid Reference. On the other hand, ellipsoid height, referenced to the ellipsoid, can be defined as a sum of MSL altitude and geoid height relative to the ellipsoid [19]. In this thesis, all the altitude values are given in terms of ellipsoid height to prevent confusion. Further explanation is beyond the scope of this thesis.

2.3 GPS Signal Structure

GPS signals are broadcasted from the satellites and consist of three main components: Ranging Code, Navigation Data, RF Carrier. Generally, the GPS Signals for the L1 and L2 carriers can be modeled as given in Equation 2.1, where the C and P(Y) are C/A and P ranging codes, D, k, and P is navigation data, satellite number, and signal power, respectively.

$$\begin{aligned} x_{L1}^{k}(t) &= \sqrt{2P_{L1}^{k}}\, C^{k}(t)D^{k}(t)\cos\big(2\pi f_{L1}t + \phi(t)\big) \\ &+ \sqrt{2P_{L1}^{k}}\, P(Y)(t)D^{k}(t)\sin\big(2\pi f_{L1}t + \phi(t)\big) \rightarrow L1\ Signal \\ x_{L2}^{k}(t) &= \sqrt{2P_{L2}^{k}}\, P(Y)(t)D^{k}(t)\cos\big(2\pi f_{L2}t + \phi(t)\big) \rightarrow L2\ Signal \end{aligned} \tag{2.1}$$

As equation states, C/A codes are only modulated on L1 carrier while P codes are modulated on both L1 and L2 carrier. Moreover, C/A codes are provided for the SPS user. On the other hand, P codes is assigned for the only PPS users. Doppler effect is included in $\phi\ (t)$ term. Generation of these GPS signals is illustrated in Figure 2.1.

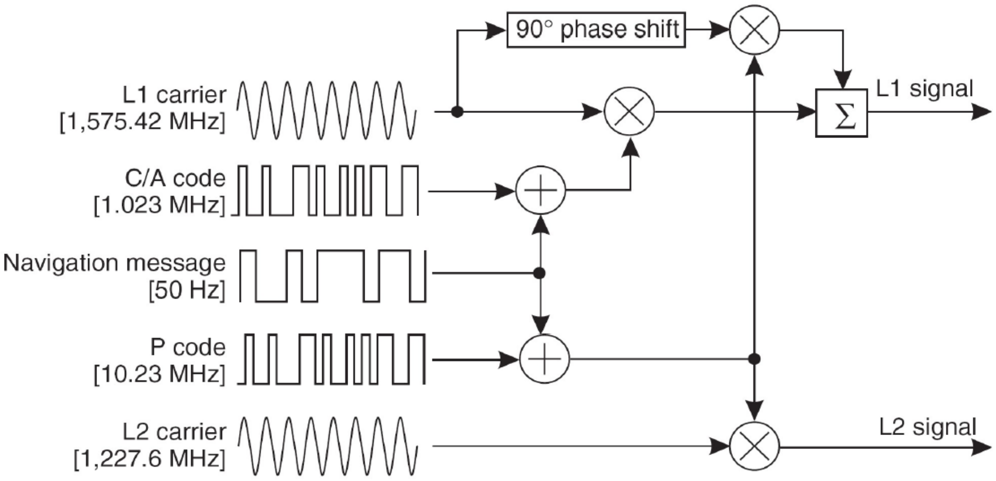


Figure 2.1: Generation of GPS Signals. Adapted from [20]

The power, modulation, and frequency characteristics of these signals are covered in next chapters.

2.3.1 Modulation Properties

GPS systems use Binary Phase Shift Keying (BPSK) and Direct Sequence Spread Spectrum (DSSS). In these methods, the signal channel bandwidth is extended by spreading the signal with Pseudo-Random Noise (PRN) and this spreading process is nothing but the multiplication of the baseband data with the PRN signal. This spread signal is despread in the receiver side to get the baseband signal. Each pulse in the PRN sequence is called the chip, and the rate of that is called the chip rate. In the GPS, BPSK-modulated Navigation Data is spread by C/A codes, a family of PRN Codes. The chip rate of the C/A code is 1023 chip/ms higher than the navigation data bit rate, 50Hz. Because the C/A code is 1ms, one data bit consists of 20 C/A codes. In Figure 2.2, BPSK DSSS modulated GPS Signal is illustrated.

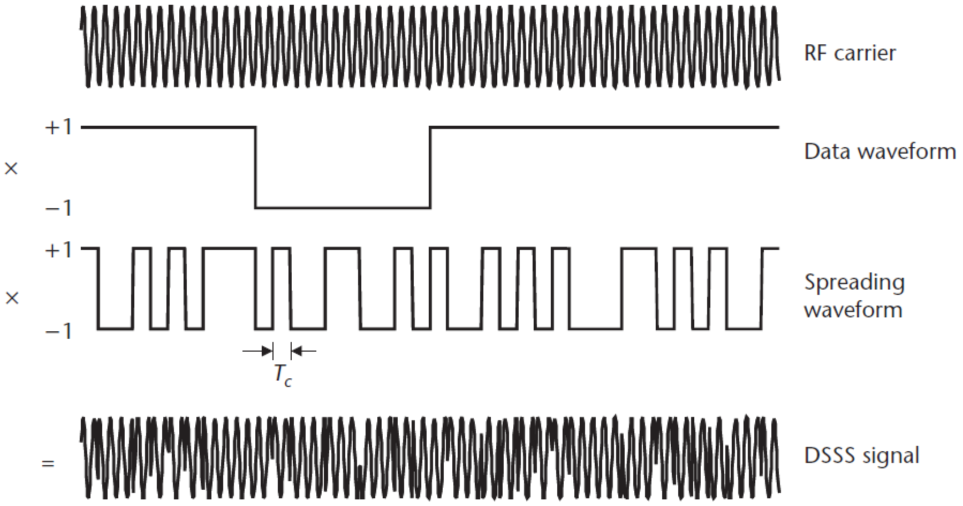


Figure 2.2: BPSK DSSS Modulated GPS L1 C/A signal. Adapted from [9]

C/A codes possess high autocorrelation and low cross-correlation properties. Thanks to these properties, satellites carrying their unique PRN codes are differentiated from each other on the receiver side. This digital communication method is known as Code Division Multiple Access (CDMA), in which different transmitter can simultaneously broadcast their message over the common frequency band [21]. Another convenience of employing CDMA is that multiple users, namely satellites, can transmit their message with specific PRN code, and the number of users is augmentable to a certain limit.

2.3.2 Power and SNR Level

GPS signals propagate around 20000 km, and such a distance causes dramatic Free Space Loss, as provided in Equation 2.2, where R is distance, $f_{L1\,C/A}$ is 1575.42MHz and c is speed of light. Therefore, the received signal strength is supposed to be quite low such that the minimum power level for the L1 C/A GPS systems is around -130 dBm, even beyond the noise floor of the GPS C/A receiver, as provided in Equation 2.3, where -174dBm/Hz is thermal power noise density and 2.046MHz is typical spread code bandwidth for C/A GPS Receiver. Fortunately, DSSS modulation is appropriate for the detecting of the signal with such a low power. The despreading process corresponding to a multiplication of incoming signal with synchronized PRN code submits a substantial gain to received signal power spectral density. This gain is called processing gain and is equal to the ratio of chip rate to bit rate. That gain is calculated for the GPS C/A signals as provided in Equation 2.4.

$$FSL = 20\log_{10}(\frac{f_{L1\ C/A}\ 4\pi R}{c}) \cong\ 183dB \tag{2.2}$$

.

$$Noise\ Floor = -174\frac{dBm}{Hz} +\ \ 10\log 2.046MHz = -111\ dBm \tag{2.3}$$

.

$$43dB = \left(\frac{T_b}{T_c}\right)_{dB} \tag{2.4}$$

T_c is period of the chip and T_b is period of data bit. These are 20ms and 977ns respectively. After the despreading process, received signal power increases approximately to -97dBm, which is above the thermal noise floor, $-111dBm$, as stated in Equation 2.5.

$$-130dbB_{recei.power} + 43dB_{process\ gain} = 97dBm >\ -111dBm_{Noise\ Power} \tag{2.5}$$

On the other hand, if the unwanted signals, such as another satellite signal or interference, are multiplied with a local replica of the PRN code, the output signal extends over a wider bandwidth. The output power Spectrum of despreding process is depicted in Figure 2.3, where the W1 corresponds to spreading signal, and “Signal 1” and “Signal 2” are wanted and unwanted ones, respectively [22]. Hence, the DSSS method reduces the vulnerability of the GPS receiver to interferences [23].

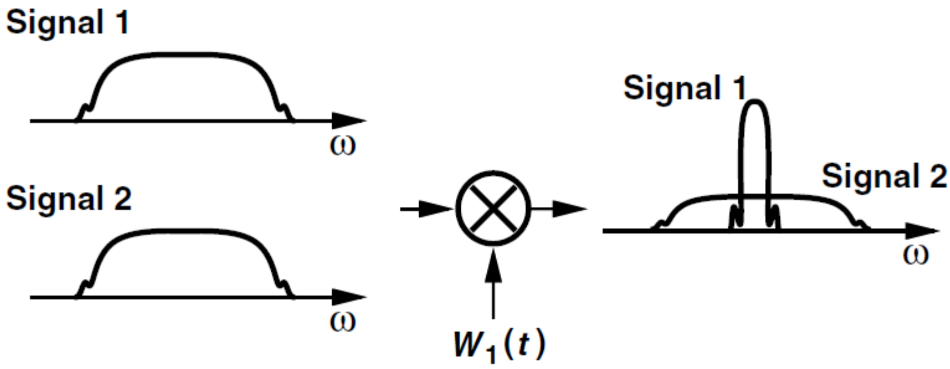


Figure 2.3: Despreading with Intended and Unintended Signals. Adapted from [22]

2.3.3 Doppler Effect and Clock Accuracy

From the point of GPS receiver, GPS transmitters, namely satellites, are moving. Sometimes both the receiver and transmitter may be moving. This relative motion creates Doppler effects on the GPS signals. For the satellites moving with velocity component v_d towards the users, leads to Doppler Frequency shift as stated in Equation 2.6, where f_c is L1 carrier Frequency 1575.42MHz and c is speed of light.

$$f_d = \frac{f_c v_d}{c} \rightarrow Doppler\ Frequency\ Shift \tag{2.6}$$

The illustration of creation of Doppler frequency in GPS system is shown in Figure 2.4

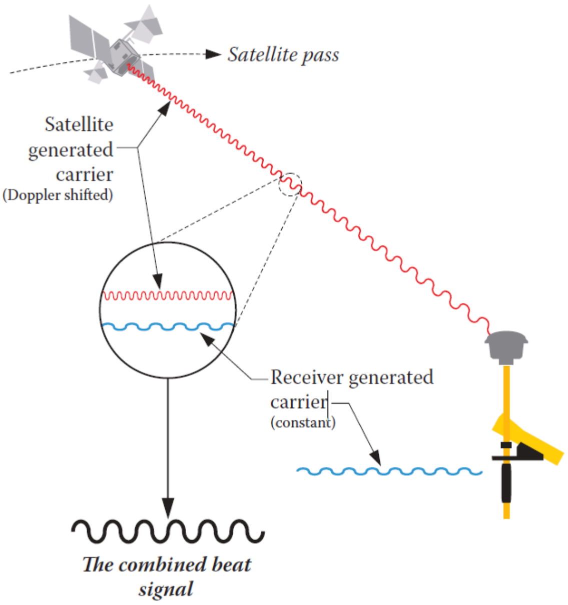

Satellite pass
Satellite generated carrier (Doppler shifted)
Receiver generated carrier (constant)
The combined beat signal

Figure 2.4: Doppler Effects on GPS System. Adapted from [24]

The satellite's velocity component towards the users strictly depends on the satellite constellation and the user's position. Therefore, different Doppler Frequencies are observed for the different satellites and user positions. The maximum Doppler Frequency shift for the stationary receiver is around ±5kHz. However, Doppler Frequency may extend these values for the moving receiver. Furthermore, Doppler Frequency can arise from the transmitter and receiver oscillator instability as well as the motion of Tx and Rx. The satellites contain the atomic clock, which is highly stable to provide accurate timing information. On the other hand, receiver side lacks highly stable clocks due to their high cost [16]. A typical GPS transmitter has a clock with a few parts per billion (ppb) at most. The clock is one of the most crucial parts of the GPS system since the time information is managed by the signal generated by the clocks. Any drift or instability may cause a tragic mistake in positioning accuracy.

2.4 GPS Navigation Data

In this section, LNAV navigation data broadcasted on the L1 band are examined. The navigation data bit rate is only 50 Hz. It corresponds to a 20ms duration for each bit. A single word consists of the 30 bits, corresponding to 600ms. Ten words create a subframe with a 6sec duration. Five subframe constitutes 1 page (frame). The whole GPS LNAV Data consists of 25 pages with a 12.5 min duration. Table 2.2 shows navigation data structures and corresponding durations [25].

Table 2.2: GPS Navigation Data Sub-Sections

Structure	Number of Bits	Time Duration
1 bit	1	20ms
1 word	30	600ms
1 subframe	300	6000ms
1 frame(page)	1500	30000ms
1superframe	37500	750000ms

2.4.1 TLM and HOW

Each subframe in the navigation data sequence starts with TLM and HOW words. Both are created by satellites. TLM is transmitted prior to HOW word. These bits are necessary for GPS positioning since they provide the receiver with synchronization and time information. Each TLM word begins with an 8-bits preamble and ends with a 6-bits parity. The rest are assigned as TLM messages, reserved bits, and integrity status flag. TLM word contains the information for the PPS users. HOW word contains 17MSB of truncated version of TOW counts, flag bits, and subframe ID. It ends with 8-bits parity [25].

All GPS operations are performed based on GPS time referenced to UTC. Z-count is a fundamental GPS Time unit consisting of 29-bit, the 10 MSBs of it assigned to the week number, and 19 LSBs corresponding to the time of the week (TOW). As mentioned before, the truncated version of TOW, 17MSBs, is located in the HOW word of each subframe, and the first subframe includes 10-LSB of Z-count. The Unit of TOW count is 1.5 sec, and its range is between 0 and 403.199. The largest unit, 403.199, is equal to the seconds of the one week, 604.800. Also, the unit of TOW in the HOW word is 6sec since the truncated version of the TOW is 17-bits and converting 19 bits to the truncated 17 bits version requires multiplication with 4 (1.5 sec x 4=6). It is crucial that the zero-state of the truncated TOW represents the start of the next subframe, so it takes “1” instead of “0” for the end/start of the week. Figure 2.5 shows the relationship between Z-Count and truncated TOW.

On the other hand, 10 MSB of the Z-count accounts for the week number starting from the midnight of the 5th of January 1980/morning of the 6th of January 1980. After 1023, it starts over; therefore, the former 1024 weeks must be considered for the transforming current week into the Z-count’s week.

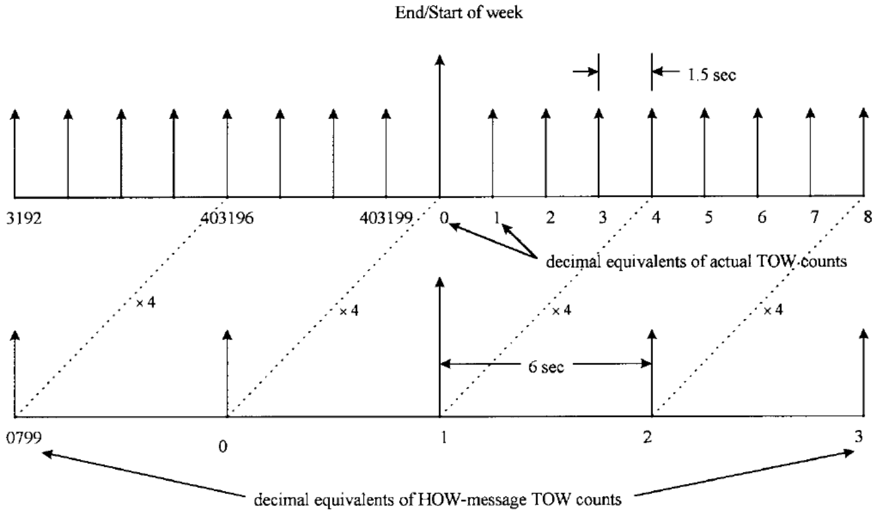

End/Start of week
1.5 sec
3192
403196
403199
0
1
2
3
4
5
6
7
8
decimal equivalents of actual TOW counts
× 4
× 4
× 4
× 4
6 sec
0799
0
1
2
3
decimal equivalents of HOW-message TOW counts

Figure 2.5: Z-Count and Truncated TOW in HOW Word. Adapted from [18]

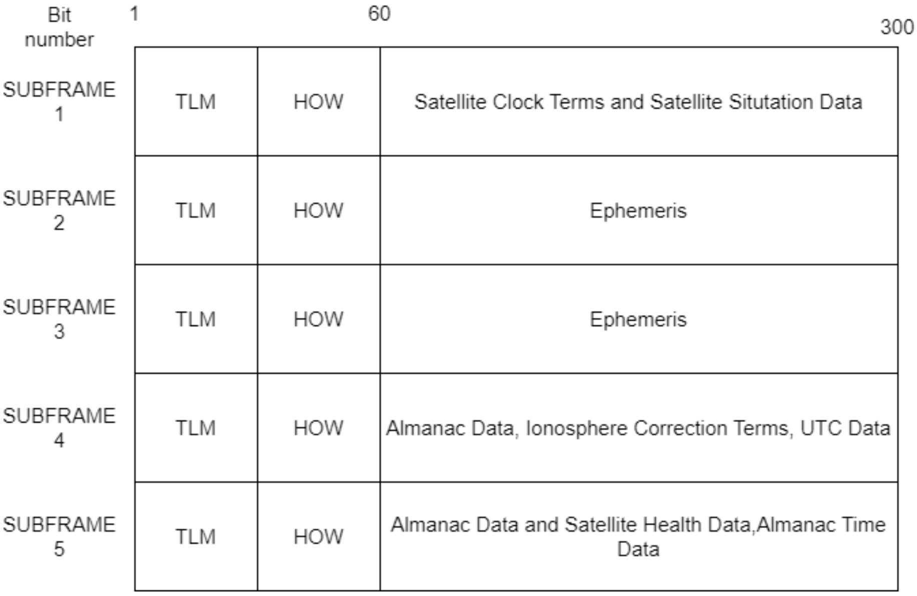
2.4.2 Subframe’s Data

One page of navigation data is comprised of 5 subframes. Each of the subframes contains different information. Subframe 1 includes the satellite clock correction terms, GPS week number, and reference clock time information. Also, the differential group delay and the issue of the date clock are contained on Subframe 1. Table 2.3 shows some of the Subframe 1 data. Ephemeris parameters of the satellites are contained in Subframes 2 and 3. This information is estimated from the least square fit of the propagated ephemeris of the Satellites [26]. In section 3.2, it is examined how to use these parameters in the positioning algorithm.

Table 2.3: Data on the Subframe 1

Symbol	Definitions
t_{oc}	Clock Data Reference
a_{f0}	Satellite Clock Offset
a_{f1}	Satellite Clock Drift
a_{f2}	Satellite Clock Drift Rate
T_{gd}	Group Delay Term
IODC	Issue of Date Clock

Subframes 4 and 5 basically consist of the almanac data, ionosphere correction terms, and UTC conversion parameters. Hence, the data of these subframes are not mandatory for the computation of the position [18]. The overall structure of navigation data allocation in subframes is depicted in Figure 2.6.



SUBFRAME 1	TLM	HOW	Satellite Clock Terms and Satellite Situtation Data
SUBFRAME 2	TLM	HOW	Ephemeris
SUBFRAME 3	TLM	HOW	Ephemeris
SUBFRAME 4	TLM	HOW	Almanac Data, Ionosphere Correction Terms, UTC Data
SUBFRAME 5	TLM	HOW	Almanac Data and Satellite Health Data,Almanac Time Data

Figure 2.6: Overall Structure of Five Subframes

The ephemeris data are accessible through the NASA “Crustal Dynamics Data Information System” (CDDIS) [27] and published as a “Receiver Independent Exchange Format” (RINEX) file. These files are generated by processing the broadcast ephemeris data transmitted by the GPS Ground Control Stations. RINEX file content is provided in the [28] and necessary to understand for retrieving broadcast data.

CHAPTER 3

GPS POSITIONING

The GPS system involves multiple satellites to find the receiver's position located at x_u, y_u, z_u . Once the receiver receives signals from the minimum four different satellites, it can compute its own 3D position. Note that the system with four unknowns requires four different equations to be solved; the 3D positioning problem is interpreted as a system with four unknowns by considering the clock offset error to be an unknown. The principle of positioning is visualized in Figure 3.1. In this part, only the code-phase positioning is covered although carrier-phase measurement can be used for the GPS Positioning. The present chapter deals with the positioning procedure in three subsections: Pseudorange computations, Satellite Positioning, and User positioning. Also, quality parameters relevant to the positioning output are briefly explained in this part.

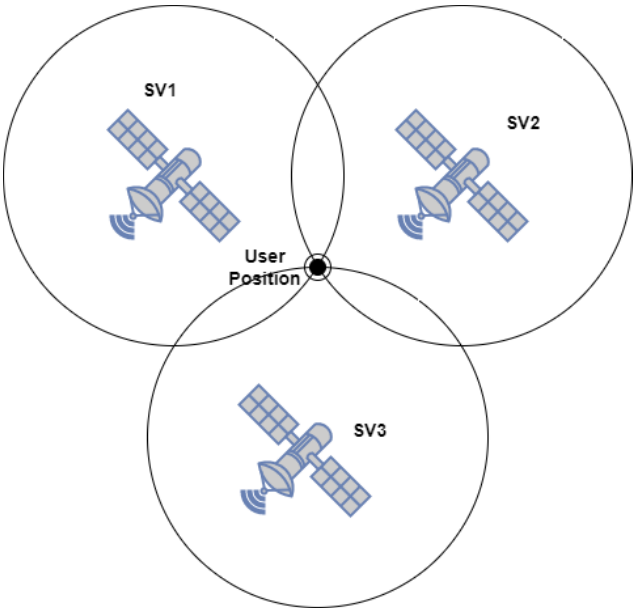


Figure 3.1: Satellite-Based Positioning Model

3.1 Pseudorange Computations

Pseudorange is the apparent distance from the satellite to the receiver. It is computed from the travel time of the signals from the satellite to the receiver by considering the speed of the GPS signal in the sky. Those GPS signals are made up of ranging codes, specifically C/A codes. The receiver also creates a replica of C/A codes locally to be correlated with incoming code (C/A). The replica is gradually shifted in time until the maximum correlation value is obtained to compute the time of travel. Pseudoranges are derived from the multiplication of the time and speed of light in the sky. Pseudorange values do not fit the exact geometric distance between satellite and receiver because satellite and receiver clock errors, ionosphere, and troposphere errors (e.g.) are not involved in these estimations [5], [18]. Figure 3.2 depicts the locally generated replica and incoming satellite signals at the maximum correlation point.

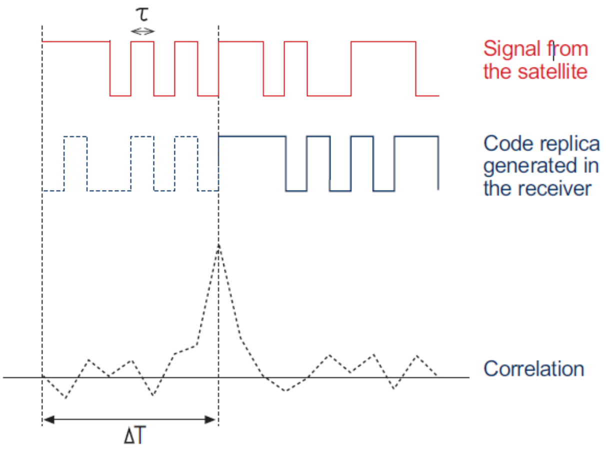

τ
Signal from the satellite
Code replica generated in the receiver
Correlation
ΔT

Figure 3.2:Measurement of Travel Time with Ranging Code Replica. Adapted from [5]

Pseudoranges computed from the correlation of the ranging code can be expressed in Equation 3.1. As the equation implies, Transmission and reception time which are represented by T_1 and T_2, respectively, are being measured in reference to different time scales, satellite time scale and receiver time scale, respectively.

$$R = c\big(t_{rec}(T_2) - t^{sat}(T_1)\big) \tag{3.1}$$

Pseudorange equation can be written in the form of Equation 3.2 by considering the non-synchronized clocks in receiver and transmitter, signal propagation-related error terms such as ionosphere and troposphere errors, and relativistic effect.

$$R = \rho + c(\delta t_{rec} - \delta t^{sat}) + TR_r + \epsilon_R + I_r + T_{gd} \tag{3.2}$$

The terms in Equation 3.2 can be defined as follows:

- ρ : shows geometric distance between the satellite and the receiver.
- δt_{rec} is receiver clock offset.
- δt^{sat} is satellite clock offset and it can be obtained by using decoded navigation data.
- TR_r tropospheric delay
- T_{gd} accounted for the effect of satellite group delay
- I_r ionosphere delay which can be solved from a model by using coefficient from broadcast empheresis.
- ϵ_R shows receiver noise error
- R represents the Pseudorange

Receiver Clock Errors cannot be avoided, although most of the other error terms can be modeled and corrected. Then, it is assigned as a unknown term in the position equation. By the way, there are a few additional parameters that might be included in this formula, such as instrumental delay, multipath effect etc.; nevertheless, they are ignored for simplicity in this thesis.

Satellite clock offset δt^{sat} can be separated into two terms as in Equation 3.3:

$$\delta t^{sat} = \delta T_r + \delta T_{sat} \tag{3.3}$$

The term δT_{sat} are corrected by the information inserted in the navigation data as stated in Equation 3.4:

$$\delta T_{sat} = a_{f0} + a_{f1}(\mathrm{t} - \mathrm{t_{0e}}) \quad + a_{f2}(\mathrm{t} - \mathrm{t_{0e}})^2 \tag{3.4}$$

a_{f0}, a_{f1}, a_{f2} are clock offset, clock drift and clock drift rate respectively, as listed in Table 2.3. Also, these terms are provided in the navigation message corresponding to given epoch time $\mathrm{t_{0e}}$.

Relativistic correction term δT_r are attributed to orbital eccentricity and given in seconds as follows in Equation 3.5 [4]:

$$\delta T_r = F e_s \sqrt{a} \sin E_k \tag{3.5}$$

F is a constant,$-4.442807633\, x\, 10^{10}\, \frac{sec}{\sqrt{meter}}$ derived from earth universal gravitational parameter and the speed of light and e_s , a are ephemeris parameters as listed in Table 3.2. Also, E term is computed iteratively as stated in Equation 3.10.

T_{gd} is group delay term and obtained from the subframe 1 data provided in Table 2.3.

I_r, ionosphere error term arises from the dispersive characteristic of the ionosphere. More clearly, GPS signals propagate with the frequency-dependent speed in the ionosphere, which exhibits different characteristics in a daily cycle. Therefore, the ionosphere error term depends on the time of day. That kind of error leads to a delay in the ranging code and stream data. Also, ionosphere error is usually higher at low elevation angles, so it can be diminished by avoiding using satellites below a certain elevation mask [4]. Dual frequency receivers (L1/L2) with two carriers can compensate for most of the ionosphere effect thanks to the dispersive nature of the ionosphere layer. On the other hand, only the L1 frequency receiver can correct more than 50 percent of ionosphere-related errors [3] by utilizing the ionospheric data inserted on page 18 and subframe 4 of the navigation message.

Unlike the ionosphere, the troposphere layer is a non-dispersive medium up to 30GHz. Its effect is associated with its refractive behavior, which is identical to the delay in the arrival of GPS Signals. Also, the observed impact of the Troposphere depends on satellite constellation. Tropospheric delay is more significant for the user at lower altitudes [24]. In Table 3.1, impact of different error terms on the Pseudorange are listed [5].

Table 3.1: Error terms' Impacts on Pseudorange

Type of Measurement Content	Value
Geometric Range	20000km
Relativistic Clock Correction	<13m
Ionospheric Delay	2-30m
Tropospheric Delay	2-30m
Receiver Clock offset	<300km
Satellite clock offset	Up to hundreds of km

3.2 Calculation of Satellite Positions

Obtaining satellite position are mandatory to compute user position. Time of transmission (TOT) should be computed for the satellite position calculation as the measurement are based on signal reception time. Also, both of user and satellite positions should be measured in the same reference system. ECEF frame is appropriate for the computation of user position on the earth and used as a reference frame for the satellite and user position [4], [18].

The time of transmission (TOT) can be directly computed from the receiving time and Pseudoranges. As a result, the corresponding TOT with referenced to Satellite clock is given by Equation 3.6.

$$t^{sat}(TOT) = t_{recevier}(receiving\ time) - Rc \qquad (3.6)$$

Nevertheless, both of times measurement above lacks the clock corrections. By inserting these terms into Equation 3.6, TOT measurement is given by Equation 3.7:

$$t^{sat}(TOT) - \delta t^{sat} = t_{rec}(receiving\ time) - \delta t_{rec} - Rc \qquad (3.7)$$

Note that TOT can be computed with another method which doesn't require any Pseudorange measurement. The approach of this algorithm is that to obtain transit time by iteration assuming that initial receiver position is known [5].

Once transmission time is computed, satellite positions can be calculated. However, the TOT values should account for the cross over between end and beginning of the week.

TOT can be obtained from TOW (Time of Week) as pointed out in section 2.4.1. Cross-Over adjustment for the end/beginning of the week is made on TOT as stated in Equation 3.8

$$\begin{gathered} t_k = t - t_{oe} > 302400 \quad then\ t_k = t_k - 604800 \\ t_k = t - t_{oe} < -302400 \quad then\ t_k = t_k + 604800 \end{gathered} \qquad (3.8)$$

where t_{oe} corresponds to epoch time encoded in the navigation data, 302400 is half time of week in seconds, t is corrected GPST.

In Table 3.2, Broadcast ephemeris parameters required for the satellite position computation are listed. They remain valid for 2 hours typically and it should be avoided to use them after certain time since the extrapolation error grows exponentially after the validity duration [5].

Table 3.2: Broadcast Ephemeris Data for the satellite position calculations

Parameter	Definition
t_{oe}	Ephemeris reference epoch in seconds of week
$\sqrt{a}$	Square root of semi-major axis
e	Eccentricity
M_0	Mean Anomaly at reference epoch
ω	Argument of Perigee
i_0	Inclination at reference epoch
Ω_0	Longitude of ascending node at the beginning of the week
δn	Mean Motion Difference
$\dot{i}$	Rate of inclination angle
$\dot{\Omega}$	Rate of node's right ascension
c_{uc}, c_{us}	Latitude Argument correction
c_{rc}, c_{rs}	Orbital Radius correction
c_{ic}, c_{is}	Inclination correction

Later on, the correction of time and satellite positions are computed by the following Equations 3.9-3.16 sequentially as stated in the [5]:

- Compute mean anomaly for t_k:

$$M_k = M_o + \left(\frac{\sqrt{\mu}}{\sqrt{a^3}} + \delta n \right) t_k \qquad (3.9)$$

- Find eccentric anomaly E_k from the eccentricity and Mean Anomaly. Note that the problem is solved iteratively due to non-linearity:

$$E_k = M_o + e \sin E_k \qquad (3.10)$$

- Compute true anomaly v_k with eccentricity anomaly and eccentricity:

$$v_k = \arctan\left(\frac{\sqrt{1 - e^2} \sin E_k}{\cos E_k - e}\right) \qquad (3.11)$$

- Compute argument of latitude u_k by true anomaly v_k, argument of perigee ω , and correction terms c_{uc}, c_{us} :

$$u_k = \omega + v_k + c_{uc}\ \cos 2(\omega + v_k) + c_{us} \sin 2(\omega + v_k) \tag{3.12}$$

- Compute radial distance r_k by taking c_{rc} , c_{rs}.terms into account:

$$r_k = a(1 - e \cos E_k)\ + c_{rc}\ \cos 2(\omega + v_k) + c_{rs} \sin 2(\omega + v_k) \tag{3.13}$$

- Compute inclination angle i_k of the orbital plane from the inclination $i_0$at the epoch time t_{oe} and correction terms c_{ic} and c_{is} :

$$i_k = i_0\ + \dot{i}\ t_k\ +\ c_{ic} \cos 2(\omega + v_k) + c_{is} \sin 2(\omega + v_k) \tag{3.14}$$

- Compute the longitude of ascending node λ_k .Right ascendation Ω_0 at the beginning of the week is used in this calculation. Therefore, time correction term t_k is included in this equation to correct change in longitude of the ascending node from reference epoch time t_{oe} :

$$\lambda_k = \Omega_0\ + (\dot{\Omega} - \omega_E)\, t_k - \omega_E\, t_{oe} \tag{3.15}$$

All of computed parameters are in the orbital frame. Transformation from the orbital frame to ECEF frame is made by the following formula provided in Equation 3.16:

$$\begin{bmatrix} x_k \\ y_k \\ z_k \end{bmatrix} = \begin{bmatrix} \mathrm{r_k} \cos(\omega + v_k) \cos \lambda_k - \mathrm{r_k} \sin(\omega + v_k)\ \sin \lambda_k \sin i_k \\ \mathrm{r_k} \sin(\omega + v_k) \cos \lambda_k + \mathrm{r_k} \sin(\omega + v_k)\ \cos \lambda_k \cos i_k \\ \mathrm{r_k} \sin(\omega + v_k)\ \sin i_k \end{bmatrix} \tag{3.16}$$

3.3 Calculation of User Positions

Basic positioning equations are depicted in Equation 3.17 bearing in mind that the receiver clock error terms are assign as unknown required to be solved.

$$\rho_i = \sqrt{(x_i - x)^{2} + (y_i - y)^{2} + (z_i - z)^{2}} + \delta t_{rec} \qquad (3.17)$$

where $i = 1,2,3..n$ are satellite numbers and $x, y, z, \delta t_{rec}$ are unknowns which are user coordinates and receiver clock offset.

The system above constitutes a non-linear problem which is required to be linearized. The linearization starts by assuming the initial position of receiver as the x_0, y_0, z_0 which is often chosen as (0,0,0)[17]. Equation 3.17 can be extended for the multiple satellites as provided in Equation 3.18.

$$\begin{aligned}
\rho_1 &= \sqrt{(x_1 - x)^{2} + (y_1 - y)^{2} + (z_1 - z)^{2}} + c\,\delta t_{rec} \\
\rho_2 &= \sqrt{(x_2 - x)^{2} + (y_2 - y)^{2} + (z_2 - z)^{2}} + c\,\delta t_{rec} \\
\rho_3 &= \sqrt{(x_3 - x)^{2} + (y_3 - y)^{2} + (z_3 - z)^{2}} + c\,\delta t_{rec} \\
&\;\;\ldots.. \\
\rho_n &= \sqrt{(x_n - x)^{2} + (y_n - y)^{2} + (z_n - z)^{2}} + c\,\delta t_{rec}
\end{aligned} \qquad (3.18)$$

For the approximate solution around (x_0, y_0, z_0) , suggested non-linear system can be linearized as in Equation 3.19 based on Taylor Expansion, where $dx = x - x_0$ $dy = y - y_0$ $dz = z - z_0$.

$$\rho_i - \rho_{i0} = \frac{x_0 - x_i}{\rho_{i0}}\,dx + \frac{y_0 - y_i}{\rho_{i0}}\,dy + \frac{z_0 - z_i}{\rho_{i0}}\,dz + c\delta t_{rec} \qquad (3.19)$$

It can be converted into to matrix form for the multiple satellites, as shown in Equation 3.20.

$$\begin{bmatrix} \rho_1 - \rho_{10} \\ \cdots \\ \cdots \\ \rho_n - \rho_{n0} \end{bmatrix} = \begin{bmatrix} \frac{x_0 - x_1}{p_{01}} & \frac{y_0 - y_1}{p_{01}} & \frac{z_0 - z_1}{p_{01}} & 1 \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ \frac{x_0 - x_n}{p_{0n}} & \frac{y_0 - y_n}{p_{0n}} & \frac{z_0 - z_n}{p_{0n}} & 1 \end{bmatrix} \begin{bmatrix} dx \\ dy \\ dz \\ c\,\delta t_{rec} \end{bmatrix} \qquad (3.20)$$

Once number of satellites is higher than numbers of unknown, system become overdetermined system which can be solved with Least Square Method. Solving the matrix equation results in position estimations of receiver as stated in Equation 3.21.

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} + \begin{bmatrix} dx \\ dy \\ dz \end{bmatrix} \tag{3.21}$$

Equation 3.21 are solved iteratively to obtain new estimation of receiver position until error terms between two consecutive solution is below determined threshold level. Convergence of iterative solution is necessary for GPS receiver to give fixed receiver position. Typically, a few cycles of iteration are sufficient to converge even if initial assumption of position starts from (0,0,0) [7]. The visualization of this iterative solution is depicted in Figure 3.3.

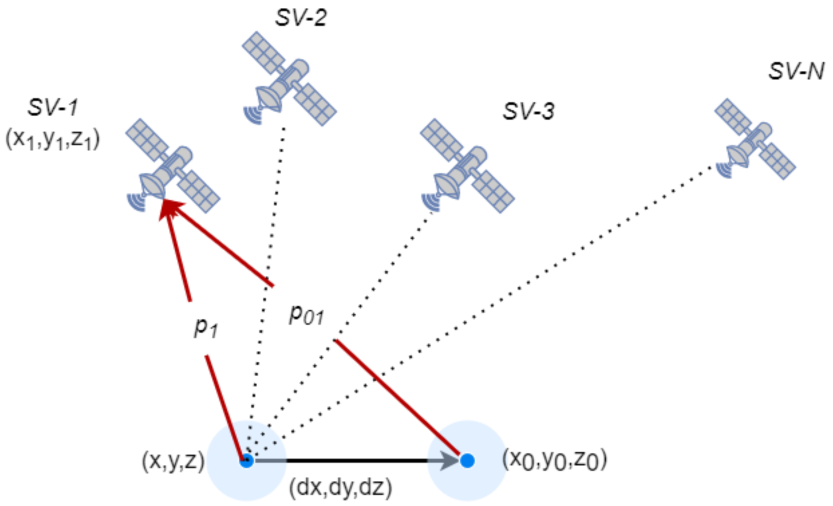


Figure 3.3: GPS Positioning Illustration

The final linear model for the known Satellite positions and initial position estimation can be written explicitly as stated in Equation 3.22.

$$\delta p = p_1 - p_{01} = Gx + \epsilon \tag{3.22}$$

δp accounts for residual between the measured and targeted Pseudorange. G defines "geometry matrix" showing Receiver-Satellite Geometry. x is unknown deviation vector defined as differences between approximated and targeted user positions as well as receiver clock deviation. ϵ defines any unmodeled error terms as well as measurement error [5], [29].

3.4 DOP and Accuracy Estimations

The residual term δp are recalculated for each iteration of computation for the user position. δp is computed by concerning the final position and measured Pseudoranges. This measurement is usually used as an indicator of quality of new position estimate [30].

Another quality indicator is computed from covariance Matrix which is defined in Equation 3.23.

$$A = (G^T G)^{-1} = \begin{bmatrix} q_{xx} & q_{xy} & q_{xz} & q_{xt} \\ q_{xy} & q_{yy} & q_{yz} & q_{yt} \\ q_{xz} & q_{yz} & q_{zz} & q_{zt} \\ q_{xt} & q_{yt} & q_{zt} & q_{tt} \end{bmatrix} \tag{3.23}$$

where G is geometry matrix as provided as stated in 3.22. As Geometry matrix is only dependent upon Satellite constellation for the specific Receiver position, the provided quality indicator is only linked to receiver-Satellite positions. The A matrix leads to computation of Dilution of Precision (DOP) values as a quality indicator. Generally, overall measurement errors are modelled by combining Dilution of Precision and uncertainty of the measurement as stated in Equation 3.24.

$$\sigma = \sigma_0 \mathrm{DOP} \tag{3.24}$$

where σ accounts for uncertainty in position, and σ_0 is uncertainty in the measurement, namely the standard deviation of the Pseudorange measurement error and called user equivalent range error (UERE).

Different DOP factors are used to evaluate the ambiguity in GPS positions since GPS Position is computed from three-dimensional solution [24]. These factors are investigated as follows:

- PDOP: Position Dilution of Precision

$$PDOP = \sqrt{q_{xx}^2 + q_{yy}^2 + q_{zz}^2}$$

- HDOP: Horizontal Dilution of Precision

$$HDOP = \sqrt{q_{ee}^2 + q_{nn}^2}$$

- VDOP: Vertical Dilution of Precision

$$VDOP = \sqrt{q_{uu}^2}$$

- TDOP: Time Dilution of Precision

$$TDOP = \sqrt{q_{tt}^2}$$

- GDOP: Geometric Dilution of Position

$$GDOP = \sqrt{q_{xx}^2 + q_{yy}^2 + q_{zz}^2 + q_{tt}^2}$$

q_{uu}, q_{ee}, q_{nn} terms correspond to "A" matrix's elements in East, North, Up coordinate system [5]. DOP measurements constitutes a relation between the precision in measurement (σ_0 or UERE) and positioning (σ). For example, 6m measurement error with the 5 PDOP corresponds to 30m accuracy. DOP with smallest value shows the optimum satellite configuration for specific user position. Then, it is favourable to minimize DOP values by choosing proper satellites Also, while number of satellites used in navigation problem increasing, DOP values usually reduce, thereby, smaller position error. On the other hand, Satellites embracing the higher volume in the sky leads to good DOPs [24]. Other indicators for the accuracy estimation are defined as below.

- 2D RMS error ≅ HDOP σ_0
- 3D RMS error = 2.2 (2D RMS error)

CHAPTER 4

EXPERIMENTAL DESIGN AND RESULTS

This chapter discusses GPS Transmitter Model Implementation and Experimental Results in detail. Firstly, the generation of Ephemeris data and C/A Code are examined. Secondly, the calculations of Pseudoranges and Doppler Rates for the specific position are described. Thirdly, overall implementation of these, Pseudoranges, Doppler Frequencies, Ephemeris Data, and C/A codes are provided. Also, the implementation of the GPS Transmitter on Adalm-Pluto Software Defined Radio (SDR) is explained by providing the transmitter's Front-End structure. A series of tests are conducted to investigate the performance of the suggested GPS System via U-Blox GPS Receiver. It is investigated the capability of the suggested system for the different types of hypothetical users. Finally, the spoofing ability of the proposed transmitter is examined, so the GPS Antennas for L1 band are connected to U-Blox receiver and the transmitting SDR. Then, the response of the receiver is observed.

4.1 Generation of Ephemeris Data and Ranging Code

In order to generate ephemeris data and Gold Code, MATLAB "HelperGPSNAVDataEncode" and "HelperGPSCACode" functions included in Satellite Communication Toolbox are utilized. "HelperGPSNAVDataEncode" function can generate LNAV (Legacy Navigation Data) and CNAV (Civil Navigation Data). "HelperGPSCACode" are used to generate ranging codes: C/A, P(Y) ,and L2 CM-/L2 CL-Code or a combination[31] L1 C/A Code GPS systems comprise LNAV data modulated with C/A ranging codes. Therefore, only C/A code and LNAV data creation are covered in this part. LNAV data which consists of 37500 bits are encoded by considering the GPS standard which is explained in [25]. Subframe 4 and Subframe 5, in which almanac data, Ionosphere correction terms are located, are intentionally assigned as logic one because these are not mandatory for successful GPS L1 C/A implementation. Only the TLM and HOW words of these subframes are encoded in the proposed GPS System. Figure 4.1 shows created navigation data stream and highlighted subframe 4&5 bits. Subframe 1, 2,3 data are obtained by reading RINEX navigation files that describe satellite orbital parameters. One of the concerns is that time of epoch (TOE) values in navigation data imported from the RINEX file should be compatible with used TOW values.

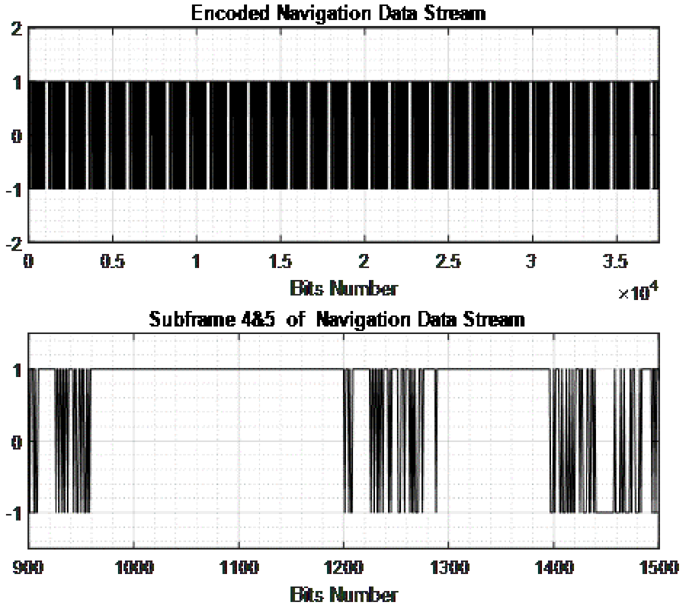


Figure 4.1: Navigation Data Bits

C/A streaming codes are generated with “HelperGPSCACode” function for each of the allocated satellites. These codes have 1023 sample length with 1ms duration. As stated in section 2.3.1, C/A codes possess high autocorrelation and low cross-correlations properties. These properties of generated C/A Codes of SV1 and SV2 are exhibited in Figure 4.2a, 4.2b, respectively. The generated Navigation Data is spread with these high-rate C/A codes for each satellite.

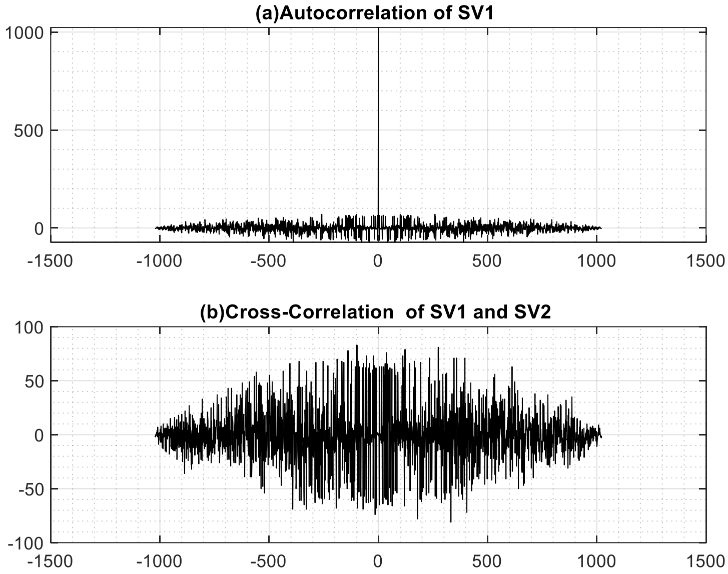


Figure 4.2: Autocorrelation (a) and Cross-Correlations (b) of C/A Codes

4.2 Calculation of Pseudorange and Doppler Rate

Pseudorange calculation is necessary for solving a set of equations to determine user location [32]. It is computed by considering the time of transmission from the satellite to the user and the time of arrival at the receiver [33]. Moving satellites leads to alternating pseudoranges; hence, Doppler shifts on carrier frequency and C/A codes. Because The Doppler Frequency shift imposed on C/A codes is quite small, it is not incorporated in the suggested design. Nevertheless, this type of Doppler Shift can create slight misalignment between received and locally generated C/A codes [18]. To calculate pseudoranges between the satellites and users, one needs to know the satellite and users' position for the given time.

“gnssconstelliation” function released in MATLAB Satellite Toolbox is used to compute satellite positions in the proposed GPS design.

The computed ranges cannot be utilized directly because the receiver will correct them as if they include error terms, as described in section 3.1. However, these computed ranges correspond to the geometric ranges between the satellites and the receiver. Then, these ranges are converted into pseudoranges by applying the correction terms inversely. Note that there is no need to take Ionospheric correction into consideration since atmospheric effects do not corrupt pseudoranges during the experiments. Moreover, a few correction terms, such as relativistic effect, and troposphere error, are not implemented in the design for simplicity. Initially, distances are found for the calculated satellite positions and given user position, hence travel time. Then, the satellite positions are extrapolated backward to the transmission time with the help of satellite velocities. After that, the correction terms including the satellite clock correction terms are applied to these ranges, and raw pseudoranges are obtained. Corrected and raw pseudoranges for the parameters tabulated in Table 4.1 are demonstrated in Figure 4.3.

Table 4.1: Specifications for the GPS Scenario

	Value
User Position(LLA)	[39.890630°, 32.781826°, 120m]
TOW	590400
Used SV’s	SV4, 6, 7, 9, 30
Duration	180sec

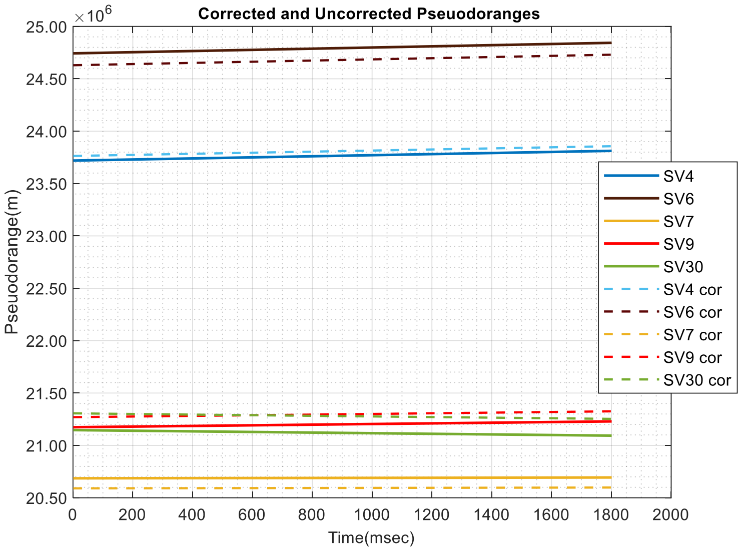


Figure 4.3: Corrected and Uncorrected Pseudoranges for Specs. in Table 4.1

Pseudoranges are estimated at the time by considering leap seconds arising from a disparity between UTC and GPS Time, as discussed in section 2.2.1. The time when pseudorange is calculated corresponds to the time of transmission of next subframe[33]; thereby, the corresponding code phase must be applied starting from the next subframe after 6s. Navigation Data should also be applied in the same manner.

Doppler Frequency shift can be calculated from the rate of change in pseudoranges as stated in Equations 4.1-4.3. The minus sign corresponds to satellite approaching the users, while plus sign does satellites receding from users[34]. In section 4.3, the realization of negative Doppler Frequency in suggested GPS system is explained in detail.

$$\delta T = t_{i+1} - t_i \rightarrow Time\ Increment\ for\ Pseudorange\ Measurement \qquad (4.1)$$

$$\frac{\rho_{i+1} - \rho_i}{\delta T} = v_D \rightarrow Velocity\ Towards\ the\ User\ Position \qquad (4.2)$$

$$f_{Doppler} = \frac{v_D f_c}{c} \rightarrow Doppler\ Frequency\ on\ Carrier\ Frequency \qquad (4.3)$$

δT defines sampling time for the computation of satellite position. It also accounts for the sampling time for pseudoranges and Doppler Frequency computations. This sampling time is called the update period in the rest of the thesis.

4.3 Hardware Implementation

Hardware implementation is necessary for the suggested GPS system to be evaluated in an experimental environment. Therefore, Adalm-Pluto SDR platform is used to implement the system since it is a cost-effective experimentation platform that provides users with a wide range of learning resources. Moreover, Pluto SDR’s hardware specifications[2] are sufficient for successful GPS signal transmission, which are mentioned in section 2.3. The device specifications for the Transmitter side are listed below;

- 300-3800MHz RF Coverage with 2.4Hz Step Size
- 200-20.000 Hz Adjustable Channel Bandwidth
- 65.1 -61.440 kSps Sampling Rate with 5Hz Step Size
- 12-bit DACs
- 25 ppm Frequency Accuracy

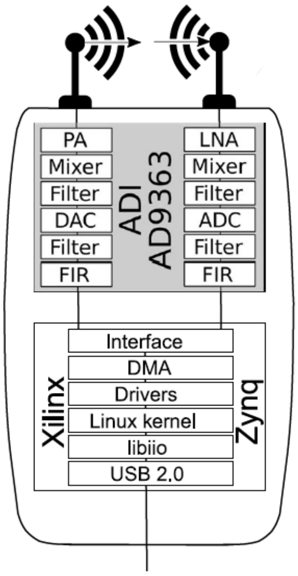


Figure 4.4: Block Diagram of Adalm-Pluto. Adapted from [2]

Like all the modern SDR system, the Pluto SDR Transmit chain possess the components, which converts I&Q samples into analog baseband form and then translate this form into the RF domain. Pluto SDR comprises of two primary parts: Analog-RF component and Communications Mechanism, as illustrated in Figure 4.4. It makes sense to mention Analog RF part of SDR in this thesis. That part utilizes a direct-conversion transmitter whose schematic is shown in Figure 4.5 [22], which directly translates baseband signal, as stated in Equation 4.4, into the RF spectrum by skipping IF stage in the manner of quadrature up-converter [22]. It is worth taking deep dive into the Quadrature Up-Conversion to clarify translation of IQ signals into baseband analog form. This type of upconverter not only translates baseband signals into the RF form but also suppresses the unwanted sidebands. Likewise, the unwanted side of up-converted Doppler Frequency can be rejected by this type of up-conversion.

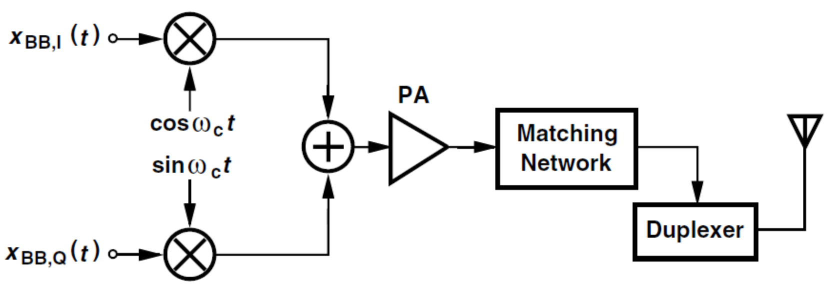


Figure 4.5: Direct Conversion Transmitter Model. Adapted from [22]

$$X_{BB,Q}(t) = A(t)\cos(\omega_{bb}t)$$

$$X_{BB,I}(t) = A(t)\sin(\omega_{bb}t) \qquad (4.4)$$

Upconverting these baseband signals into the RF stage can be stated as in Equations 4.5-4.6:

$$x(t) = \sin(\omega_c t)X_{BB,Q}(t) + X_{BB,I}(t)\cos(\omega_c t) \rightarrow Output\ Signal \qquad (4.5)$$

$$x(t) = A(t)\cos\big((\omega_{bb} + \omega_c)t\big) \rightarrow One\ SidedTranslated\ RF\ \ Signal \qquad (4.6)$$

Inserting $\omega_{doppler}$ and ω_{L1} into ω_{bb} and ω_c terms in Equation 4.6 , output signal will become Doppler Shifted version of GPS L1 frequency as proposed in Equation 4.7, where ω_{L1} is 2π1575.42MHz and $\omega_{Doppler}$ is corresponding Doppler Shift.

$$x(t) = A(t)\cos\left(\left(\omega_{L1} + \omega_{Doppler}\right)t\right) \qquad (4.7)$$

This type of up-conversion gives opportunity for the realization of negative Doppler Frequency on hardware platform. If the phase of I&Q components in Equation 4.5 are shifted by 90-degree, output signal will be as follows in Equation 4.8;

$$x(t) = A(t)\cos\left((\omega_c - \omega_{bb})t\right) \qquad (4.8)$$

Inserting $\omega_{doppler}$ and ω_{L1} into ω_{bb} and ω_c terms in Equation 4.8, negative Doppler Shift are realized , as stated in Equation 4.9.

$$x(t) = A(t)\cos\Big(\big(\omega_{L1} - \omega_{Doppler}\big)t\Big)$$

The output of SDR is the sum of all allocated satellite signals. Even if the output power of SDR is kept constant, the C/N ratio tends to reduce when the number of allocated satellites increases

4.4 Evaluation of Results through U-Blox GPS Receiver Module

Here it is explored the response of the GPS receiver to the proposed GPS transmitter. The aim is to check whether the suggested GPS transmitter is feasible to make the GPS receiver lock onto the estimated user position under several circumstances. U-Blox GNSS Receiver Platform is utilized as GPS Receiver. Because of that, it can provide users with comprehensive message sets such as NMEA, RXM, UBX [35]. Related evaluation software, U-Center, is a free and powerful evaluation and visualization tool [36]. In Figure 4.6, a block diagram of the test setup is shown.

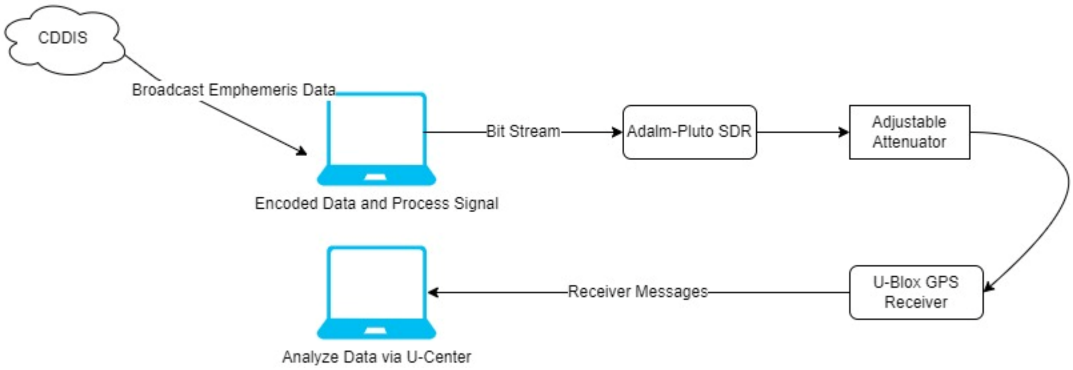


Figure 4.6: Block Diagram of Test Setup

The measurement setup is exhibited in Figure 4.7. An adjustable attenuator and DC block are inserted between the SDR and U-Blox receiver to prevent any DC leakage and to keep output power in the specific scale.

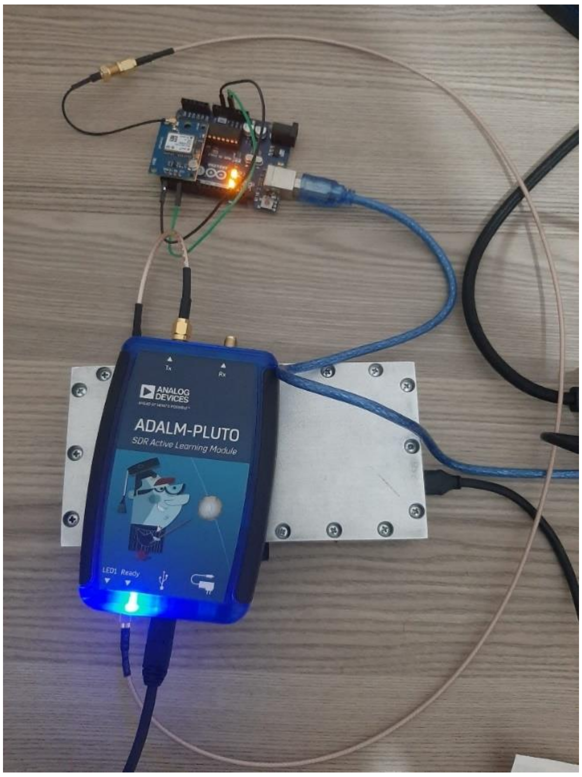
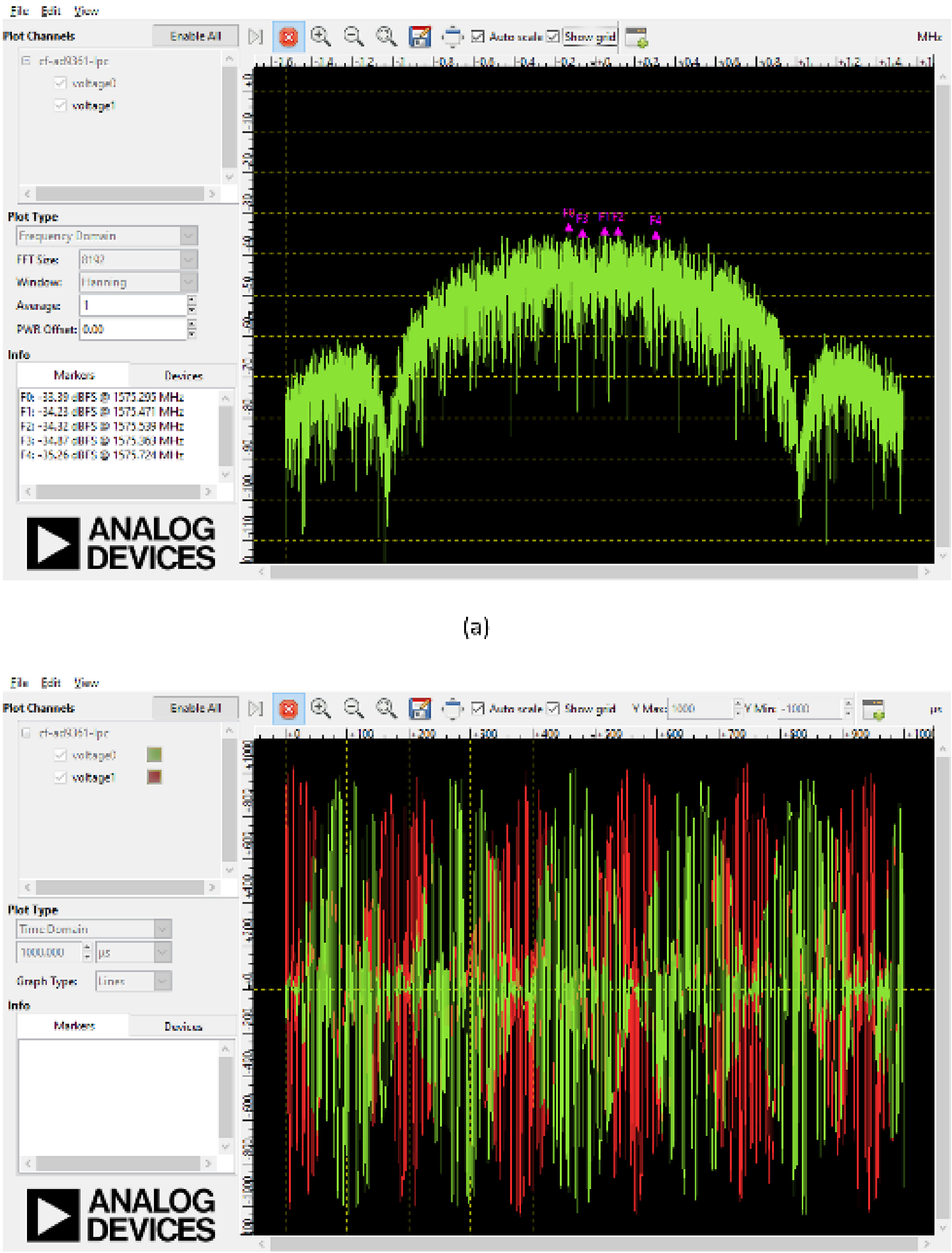


Figure 4.7: Measurement Setup

SDR Output Spectrum is visually checked prior to the overall GPS test to ensure that output frequency is consistent with the GPS L1 band. Figures 4.8 a and b illustrate a single satellite signal's output spectrum and waveform. As shown in Figure 4.8, the output envelope corresponds to the data stream modulated with Doppler Frequency, and the output spectrum is restricted in [-1.023MHz,1.023 MHz] as expected.



Plot Type: Frequency Domain
FFT Size: 8192
Window: Hanning
Average: 1
PWR Offset: 0.00

Info — Markers

F0: -33.39 dBFS @ 1575.295 MHz
F1: -34.23 dBFS @ 1575.471 MHz
F2: -34.32 dBFS @ 1575.539 MHz
F3: -34.87 dBFS @ 1575.360 MHz
F4: -35.26 dBFS @ 1575.724 MHz

(a)

Plot Type: Time Domain
1000.000 μs
Graph Type: Lines

(b)

Figure 4.8: Output Spectrum (a) and Time Domain (b) Waveform for A Single Satellite System.

4.4.1 U-Blox GNSS Receiver

GPS Output messages are accessed through U-Center GNSS Receiver Module; therefore, it is beneficial to understand the working principle of those receivers by examining the messages and flag descriptions in U-Center. Here, flag and message types are described as follows.

- Position Fix Type: It can be 2D,3D or No Fix value
- Position within Limits (FixOK): Position and velocity valid and within DOP and ACC Masks.
- Residual: Pseudo range residuals in centimetres.
- Qi: Signal Quality Indicator.
    - 0: This channel is idle
    - 1: Channel is searching
    - 2: Signal acquired
    - 3: Signal detected but unusable
    - 4: Code Lock on Signal
    - 5, 6, 7: Code and Carrier locked

Unless the output parameters are within a range defined in Table 4.2, the “Position Fix Limits” flag is not up even if Fix Position (3D or 2D) is observed. In other words, A fix status is only valid if it passes the navigation output filters. During all the trials, the output limits of U-Blox are adjusted, as tabulated in Table 4.2.

Table 4.2: Navigation Output Filters

	Value
PDOP Mask	25
TDOP Mask	25
HDOP Mask	25
PACC Mask(m)	100
Min. Elevation Mask(degree)	5

4.4.2 Static User Position

First, to examine the functionality of the GPS Transmitter, GPS signals are created for stationary user position and applied to the U-Blox GPS receiver. As mentioned in section 4.2, Satellite Positions are updated at a specific rate, and Pseudorange and Doppler Frequencies change depending upon these updates. Table 4.3 illustrates input parameters for the stationary position. The targeted user position is around Middle East Technical University Electrical-Electronic Engineering Building, as seen in Figure 4.9. The scenario is generated by using the ephemeris data taken from the [37].

Table 4.3: Scenario Specifications

	Value
Targeted Position(LLA)	[39.890630, 32.781826, 120]
Transmitter Device	Adalm-Pluto SDR with default clock
TOW	590400
# of Used SV’s	5(SV4,SV6,SV7,SV9,SV30)
Output Power(dBm)	-105dBm
Sampling Time (MSps)	3.069
Tx Channel Bandwidth(MHz)	5
Update Period	100ms
Receiver Device	U-Blox NEO-6M
Duration	180sec

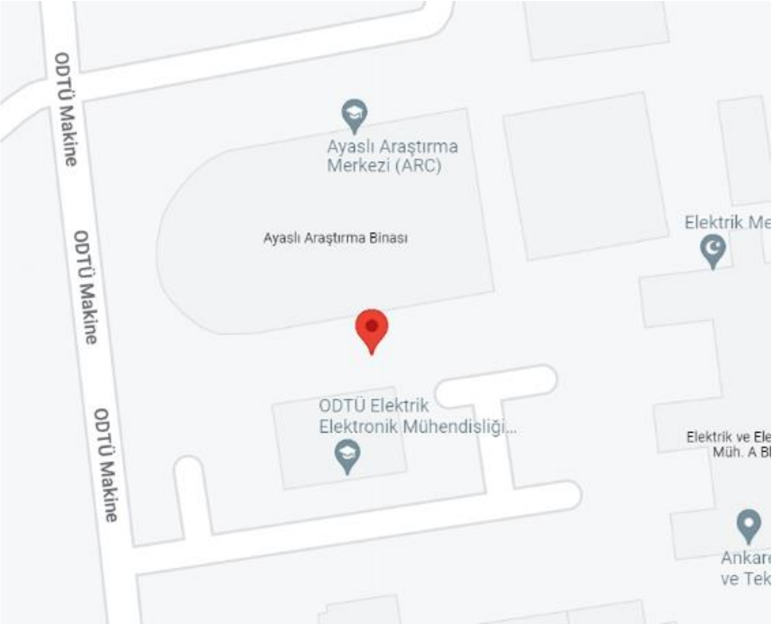

ODTÜ Makine
ODTÜ Makine
ODTÜ Makine
Ayaslı Araştırma Merkezi (ARC)
Ayaslı Araştırma Binası
Elektrik Me
ODTÜ Elektrik Elektronik Mühendisliği...
Elektrik ve Ele Müh. A Bl
Ankar ve Tek

Figure 4.9: The Target User Position

Output variables relevant to evaluate the GPS performance are accessed through the U-Blox Receiver, as listed below. The estimated Doppler Frequency is compared to the measured one to briefly evaluate the transmitter's hardware performance. Also, PDOP output is checked by considering the satellite constellation and the user position.

- Doppler Frequency
- TTFF(Time to First Fix)
- User Positions
- Accuracy and PDOP value

A certain amount of frequency shifts occurs between the measured and calculated Doppler values, as shown in Figure 4.10. It is attributed to the clock accuracy of Adalm-Pluto since clocks in real satellites exhibit a few ppb accuracies at most while the default clock of Adalm-Pluto works within ±25 ppm accuracy. The deductions coincide with the ones made in [14], [16]. As opposed to the real satellite system, the common transmitter emits all the allocated channels.

Therefore, the frequency shift and fluctuations shown in Figure 4.10 are nearly identical for all the satellites. Note that the TTFF value is assigned as the initial time for the time-domain plots.

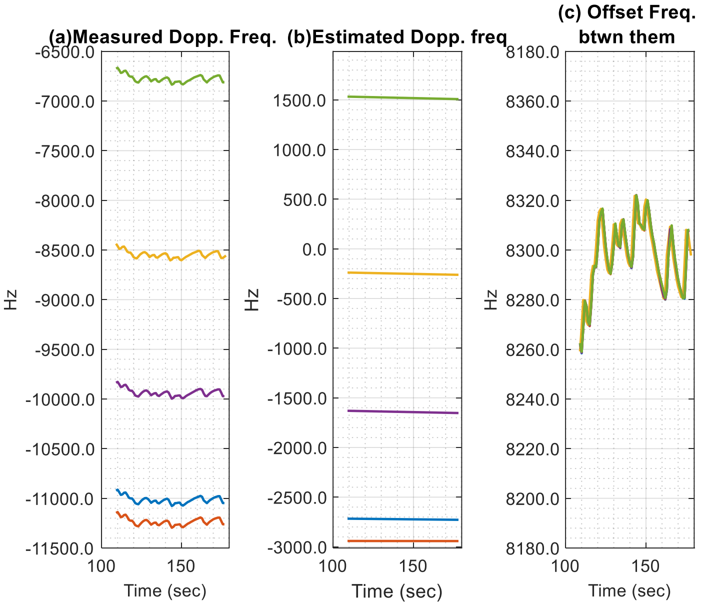


Figure 4.10: Comparison of Measured and Estimated Doppler Frequency for the Satellites

The resulting User Position depicted in Figure 4.11 is nearly same with targeted user position. The measured and the estimated Latitude and Longitude values are visualized in Figure 4.12. There is a slight deviation between them. Although these visualized measurements give an insight about performance of GPS, it is better to measure it through 3D Accuracy and PDOP. PDOP and 3D accuracy values are measured as around 10.2 and 32m respectively.

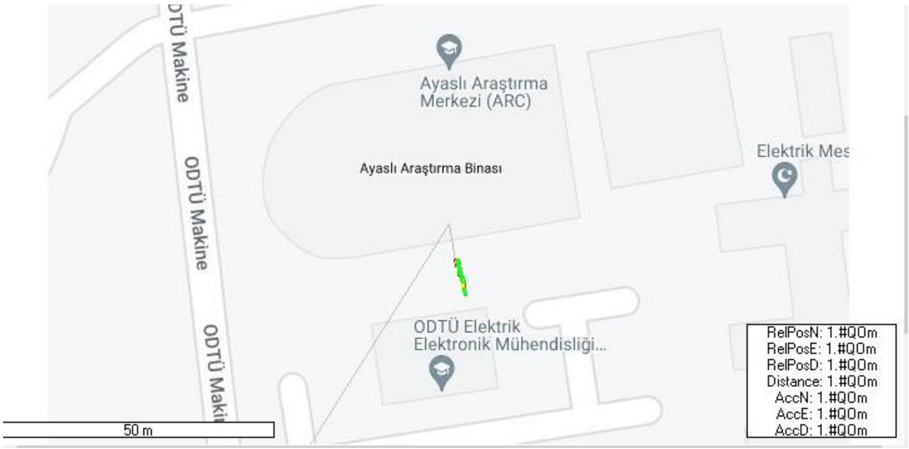


Figure 4.11: Measured User Position

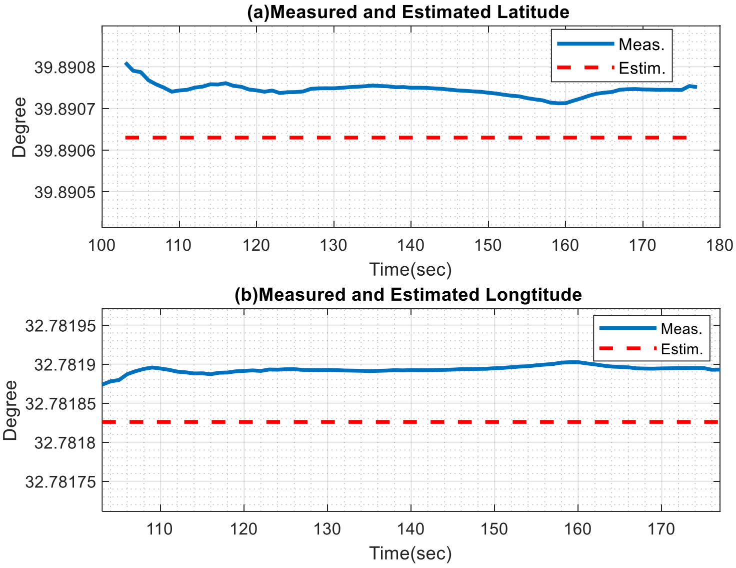
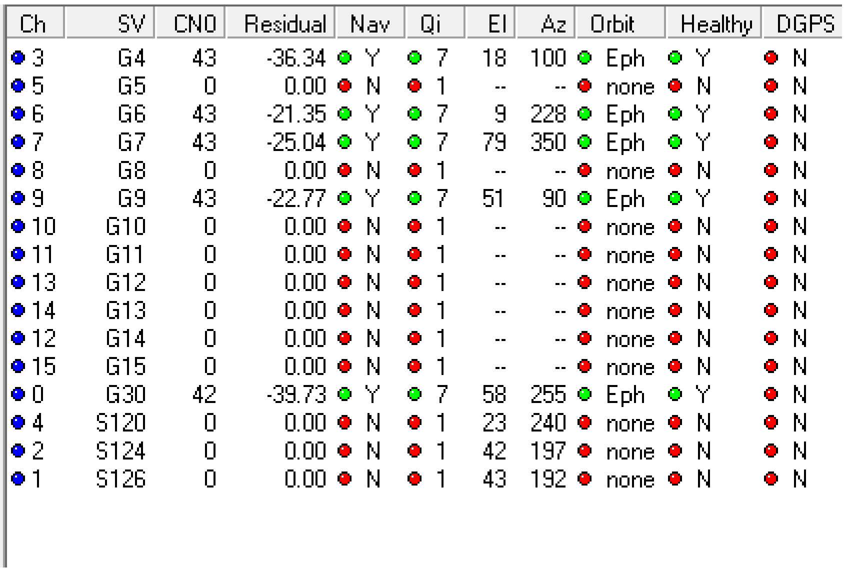


Figure 4.12: Comparison of Measured and Estimated Geodetic Coordinates (Latitude, Longitude) of User Position

The discrepancy between the estimated and measured position may results from many factors. As mentioned before, relativistic effects and Doppler Shifts on the C/A codes are not implemented in the suggested GPS system. Both may lead to deviation in the Pseudorange estimation. This deviation brings in the error in the position computed by the receiver [38].

Following U- Center screenshot indicates the receiver output responses to proposed scenario. As depicted in Figure 4.13, satellites with 3,4,7,9, and 30 PRN acquire the “Carrier&Code Phase Locked” status and navigation solution utilizes ephemeris of them.



Ch	SV	CNO	Residual	Nav	Qi	El	Az	Orbit	Healthy	DGPS
● 3	G4	43	-36.34	● Y	● 7	18	100	● Eph	● Y	● N
● 5	G5	0	0.00	● N	● 1	--	--	● none	● N	● N
● 6	G6	43	-21.35	● Y	● 7	9	228	● Eph	● Y	● N
● 7	G7	43	-25.04	● Y	● 7	79	350	● Eph	● Y	● N
● 8	G8	0	0.00	● N	● 1	--	--	● none	● N	● N
● 9	G9	43	-22.77	● Y	● 7	51	90	● Eph	● Y	● N
● 10	G10	0	0.00	● N	● 1	--	--	● none	● N	● N
● 11	G11	0	0.00	● N	● 1	--	--	● none	● N	● N
● 13	G12	0	0.00	● N	● 1	--	--	● none	● N	● N
● 14	G13	0	0.00	● N	● 1	--	--	● none	● N	● N
● 12	G14	0	0.00	● N	● 1	--	--	● none	● N	● N
● 15	G15	0	0.00	● N	● 1	--	--	● none	● N	● N
● 0	G30	42	-39.73	● Y	● 7	58	255	● Eph	● Y	● N
● 4	S120	0	0.00	● N	● 1	23	240	● none	● N	● N
● 2	S124	0	0.00	● N	● 1	42	197	● none	● N	● N
● 1	S126	0	0.00	● N	● 1	43	192	● none	● N	● N

Figure 4.13: U-Center Status Screenshot for the Proposed Scenario

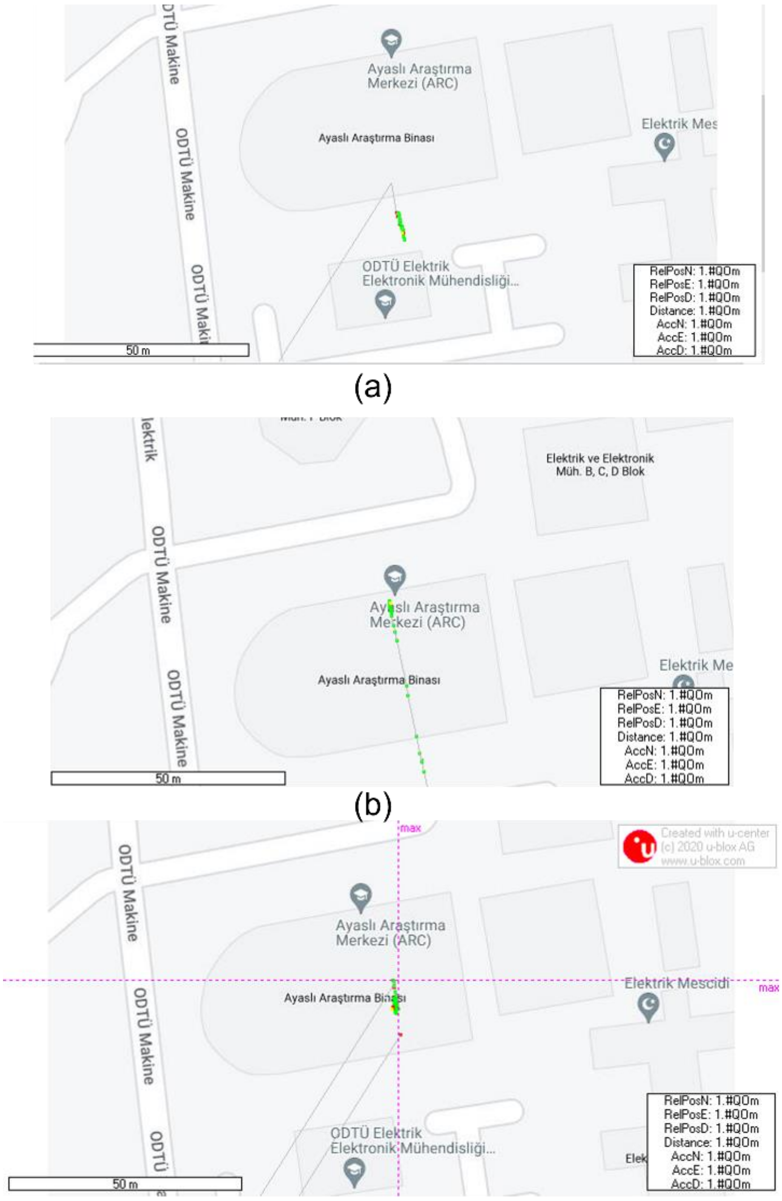
The impact on the GPS performance is examined after changing update periods to 10ms, 50ms, 100ms, 250ms, and 500ms, respectively. In all trials, the scenario duration is limited to 180s, and all other specifications in Table 4.3 remain the same. Measured PDOPs and Accuracy values versus update periods are provided in Table 4.4. These output values are computed after multiple measurements to ensure accuracy and reliability.

Table 4.4: Output Performance Values of Suggested System for 180 Seconds Transmission

Update Period	10ms	50ms	100ms	250ms	500ms
3D Accuracy(m)	37	42	39	94	138
PDOP	10.2	10.1	10.2	20.2	30.2
TTFF (sec)	107	109	108	174	-

Provided PDOP value are measured at the 180^{nd} seconds of scenario and nearly equal to estimated PDOP value ,10.132. Because DOP values depend on only the satellite constellation and receiver position, they can be calculated without requiring any receiver.

For 10ms, 50ms, 100ms trials, the observed performance parameters are similar. The measured user positions for those trials are also very close to each other as visualized in Figure 4 14 (a) (b) (c).



(a)

(b)

(c)

Figure 4.14: Measured User Positions for 10ms (a),50ms (b),100ms (c) Update Periods

The performance degradation is observed for a 250ms update period. Accuracy and PDOP values, 94m and 20.2, barely meet requirements of “Position within Limits (FixOK) ” flag defined in section 4.4.1. The measured user position for the 250ms case shown in Figure 4.15 are far away from target user position shown in Figure 4.9. Also, the “Fixed Position within the Limits” occasionally loss at the receiver during the scenario.

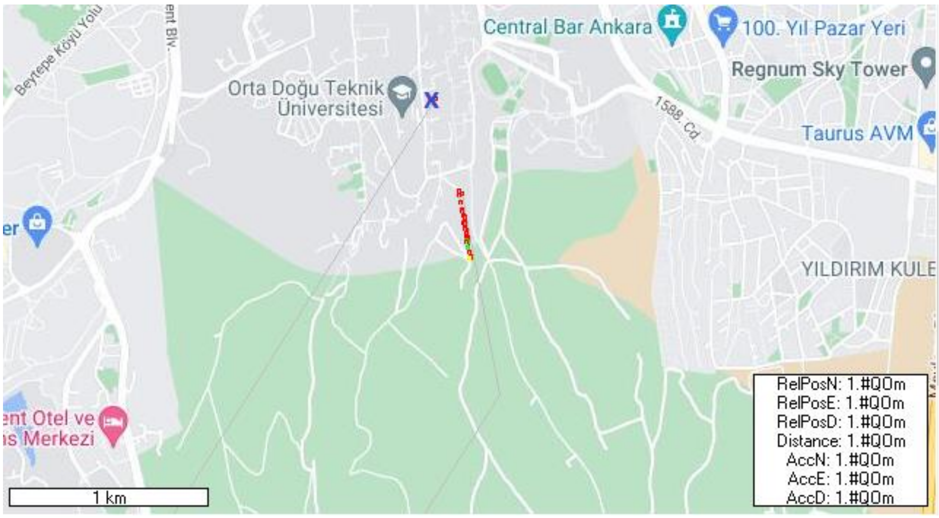


Figure 4.15: Measured User Position for 250ms Update Period (Blue Mark shows target Position, Red and Green marks show measured “Not Fixed” and “Fixed Positions respectively)

Although “Position Fix” status is obtained for the trial with a 500ms update period, the “Position-Fix in Limit” flag isn’t up throughout the experiment duration since both DOP and Accuracy values exceed the output navigation limits provided in Table 4.1. Furthermore, the measured user position for the 500ms is far from the target user positions, as depicted in Figure 4.16. As compared to the target user position in Figure 4.9, the resulting position is randomly spread around a few km away from the target user position. Note that red marks represent positions that are out of Fix Limits.

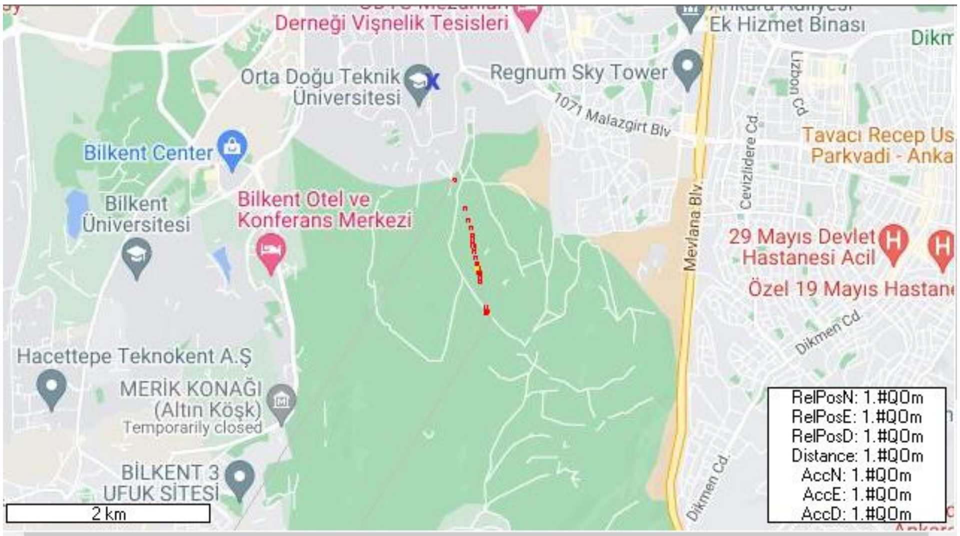


Figure 4.16: Measured User Position for 500ms Update Period (Blue Mark shows Estimated Position, Red Points show measured ones)

As a results, higher update period beyond some value leads to higher positioning error and lower positioning accuracy.

4.4.3 Dynamic User Position

In addition to a scenario with the static user, moving users are realized in the suggested GPS system since the requirements for moving receivers' detection are also met by the proposed GPS Transmitter. Indeed, a moving receiver may lead to the Pseudoranges variation depending on its movement as well as the satellites' movements. Those variations bring in Doppler Frequency shifts depending on the direction of motion and distribution of the satellites throughout the sky. The hypothetical users who move vertically and horizontally are modeled to measure GPS performance for the different movement models.

4.4.3.1 Vertical Movement

The vertical motion is realized by increasing the user altitude during the last 70 seconds of the scenario duration because position fixing occurs around 110 sec. Velocities are incremented for successive trials until the GPS Receiver cannot turn into “Fix Status” mode. The measured velocities and altitudes are compared to the actual velocities and altitudes values. Also, U-Blox is being operated in “Portable Mode,” which allows detecting receivers with higher speeds and altitudes than the default “Stationary Mode”. Table 4.5 shows corresponding upper limits of the the U-Blox, as provided in [35].

Table 4.5: Dynamic Platform Mode

Mode	Max Altitude(m)	Max.Velocity(m/s)	Max.Position Deviation	Acceleration
Portable	12000	310	Medium	Low
Stationary	9000	10	Low	**

As seen in Figure 4.17, the measured and estimated velocities nearly match. However, convergence to correct velocities takes some time, around 100-150ms. There is a slight offset in the range of 90m at most between measured and estimated altitude values. The movement with more than 55.56 m/s speed cannot be fixed by the GPS receiver, even though the velocity requirements in Table 4 are not violated. Even if the code and carrier lock status of satellites are achieved for such a movement, PVT estimation cannot be carried out correctly by the receiver algorithm.

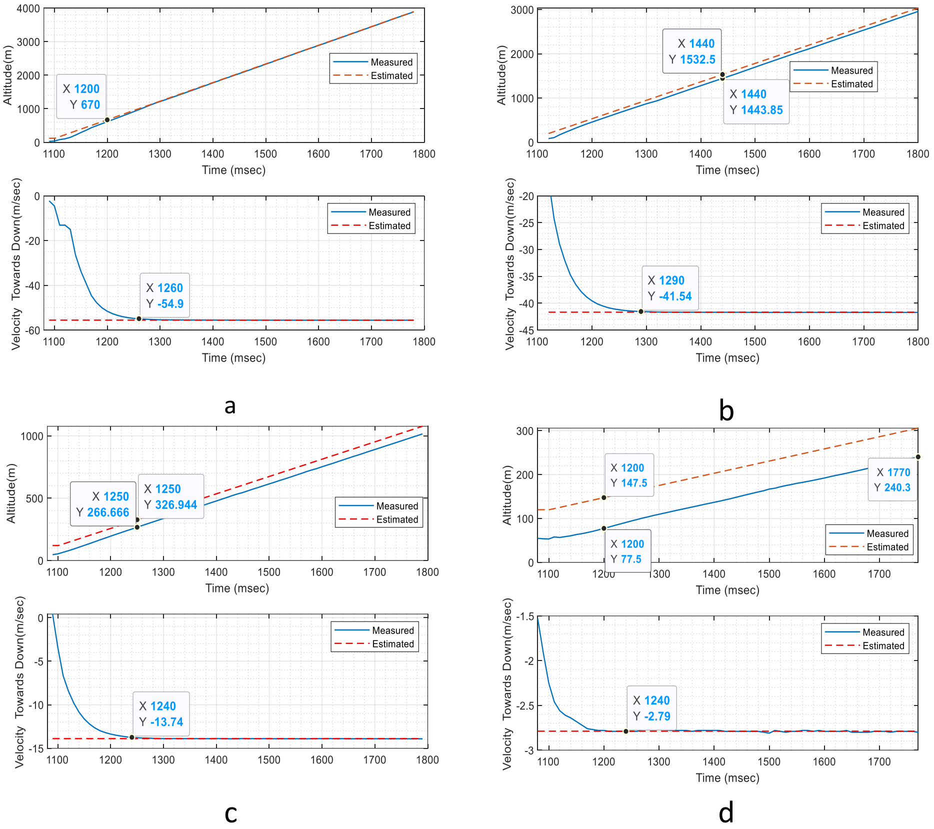


Figure 4.17: Measured and Estimated Altitudes and Velocities for Trials with 55.56 m/s (a), 41.67m/s (b), 13.89 m/s (c), 2.78 m/s (d) speeds towards the sky

4.4.3.2 Horizontal Movement

In this part, the hypothetical users are moved along the earth’s surface in a constant direction, as demonstrated in Figure 4.18. Velocities are incremented by reducing overall motion time while the scenario’s start/end points and total durations are kept constant. In that way, the direction of motion is preserved for all trials. In Table 4.6, the corresponding times and velocities are listed.

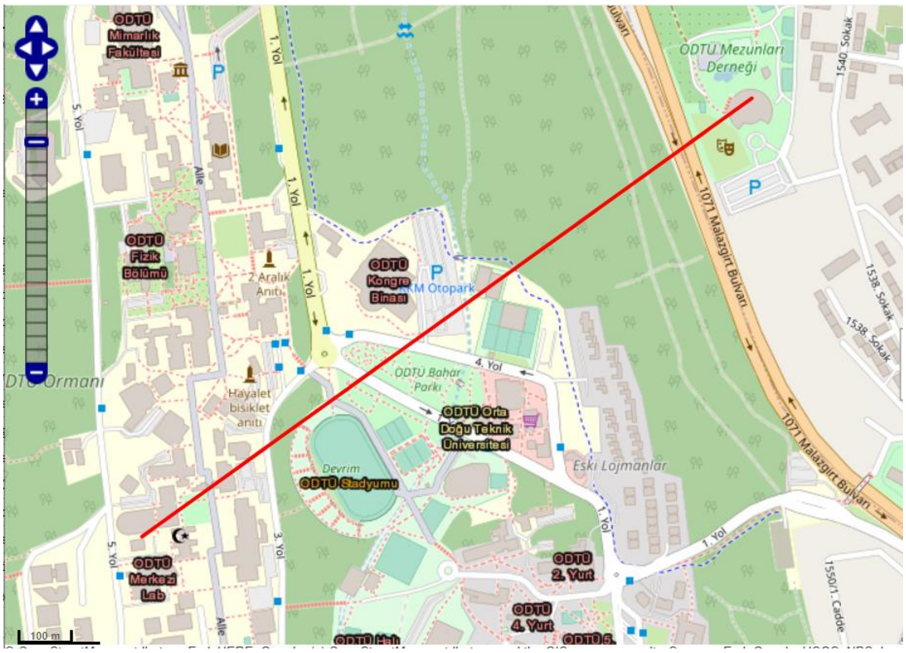


Figure 4.18: Visualization of the User Movement

Table 4.6: Horizontal Movement Specifications

Movement Duration(sec)	Initial Time(sec)	Absolute Velocity Vector(m/sec)	Total Duration(sec)
70	110	19.5	180
30	150	45.7	180
20	160	68.5	180
18	162	76.1	180
15	165	91.4	180
10	170	137.5	180

Measured Routes and target routes for the different velocities are visualized in Figure 4.19. For velocities greater than 68.5 m/s, the measured position drifts apart from the target route during the initial acceleration. It implies that this level of acceleration cannot be tracked correctly in GPS Receiver. Also, the receiver cannot trace the velocities beyond the 137.5 m/s and fails to retain the fix status. As a result, the velocity change rate influences GPS performance negatively [39]. On the other hand, the overall constant position shift in measured routes can't be associated with values of the velocities smaller than 91.4 m/s because no evident correlation can be concluded from the results. Although it is not possible to obtain the estimated linearization point of non-linear ranging equations performed by U-Blox, it is assumed that the initial estimation of linearization points can cause this kind of overall offset in the position solution.

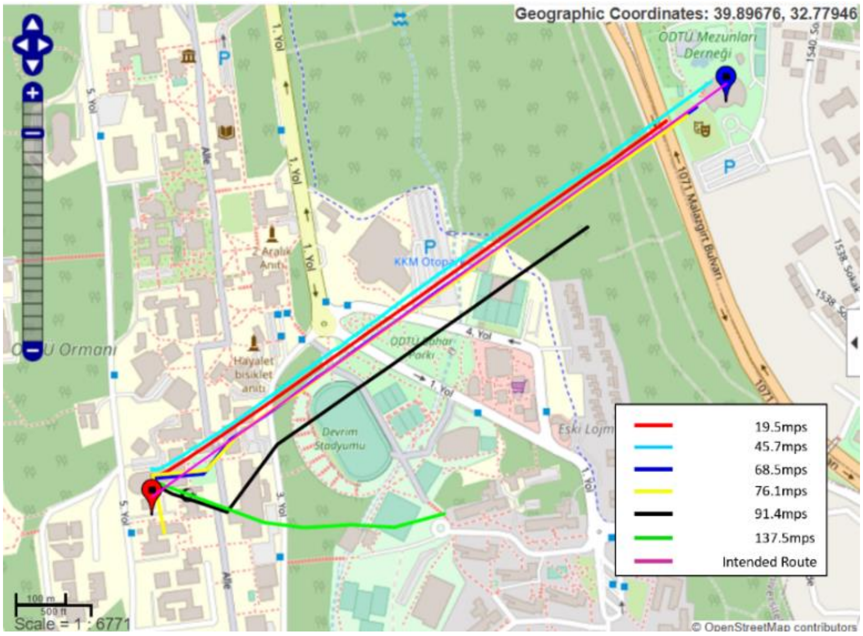


Figure 4.19: Measured and Estimated Routes for Different Velocities

In Figure 4.20, Measured and actual velocities are shown. From Figure 4.20 and 4.17, it can be concluded that the accuracy of measured velocities for case of vertical movement is better than the case of horizontal movement. In horizontal movement, there has been a more significant offset between the actual and measured velocities. It can be attributed that the accuracy of velocities measurement strictly depends on the direction of movements. Also, the performance of the GPS receiver depends on both satellites' constellation and movement direction.

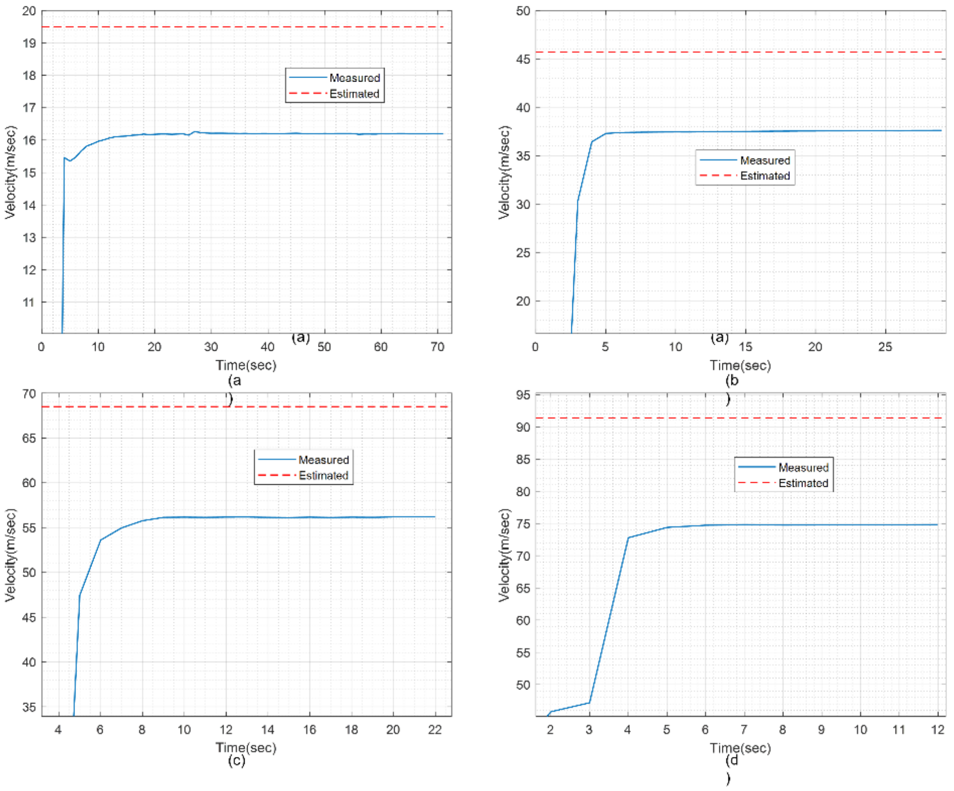


Figure 4.20: Actual and Measured Speed for the Vertical Movements

4.4.4 Impact of Clock Parameters on GPS Results

The default reference clock of Pluto exhibits $\pm 25ppm$ frequency accuracy. As stated previously, the frequency accuracy of that clock cannot keep up with the real GPS signal source having much more accurate atomic clocks with a few ppb frequency accuracies at most [14]. Oven Type Crystal Oscillator (OCXO) with $\pm 20ppb$ accuracy is connected to SDR as an external clock reference for suppressing this drastic difference. The impact of this replacement is evaluated in terms of the Doppler Frequency and position accuracy. All measurements in this part are carried out, one after another, so that ambient temperature is kept constant as much as possible because the ambient temperature substantially influences crystal oscillators' performance. In Figure 4.21, SDR hardware with an external clock is depicted. That configuration is named “Case 1”, and the default configuration is named “Case 2” for simplicity.

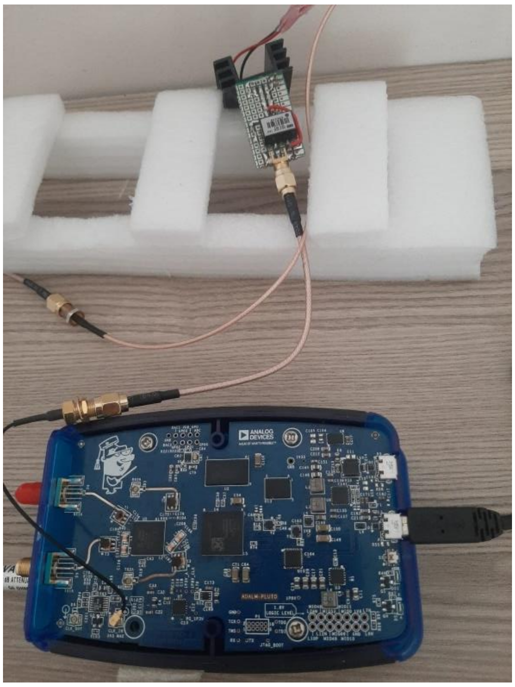


Figure 4.21: Hardware of External Clock Connected Pluto SDR

The estimated Doppler Frequencies are compared with the measured Doppler Frequencies for Case 1 and Case 2. As mentioned in section 4.4.2, It is possible to access Doppler Frequency measurement through the U-Blox. The previous scenario, based on Table 4.3, is reperformed for Case 1 and 2 separately. The estimated and measured Doppler Frequencies for those cases are illustrated in Figure 4.22 and 4.23.

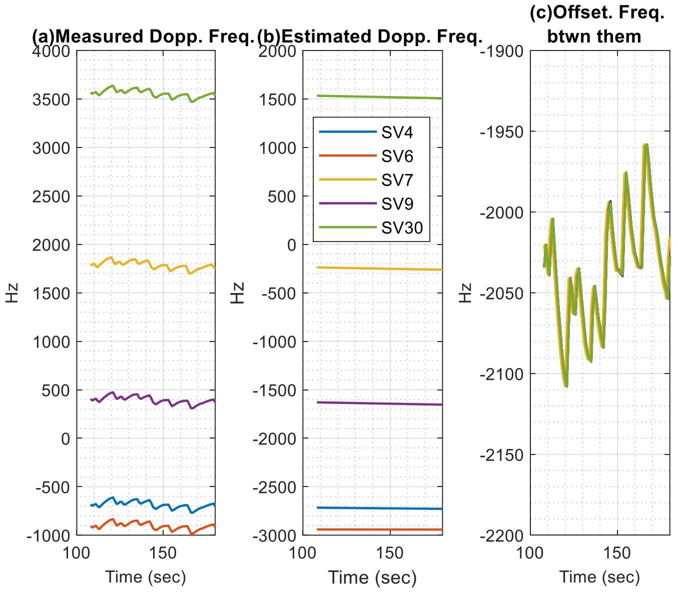


Figure 4.22: Doppler Frequencies for the Case 1 (a) Measured (b) Estimated (c) Difference of them.

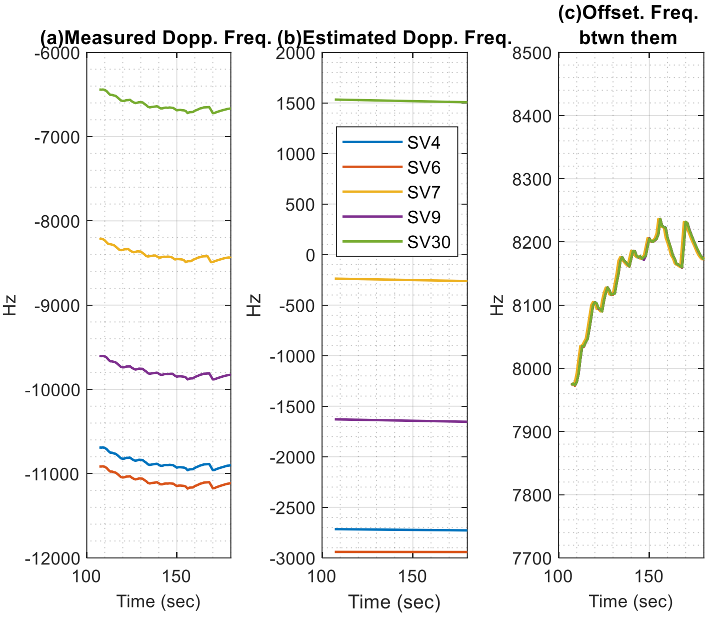


Figure 4.23: Doppler Frequencies for the Case 2 (a) Measured (b) Estimated (c) Difference of them.

For Case 2, the frequency offset from the estimated ones is nearly 8kHz.It is consistent with the previously measured frequency shifts provided in section 4.4.1. The offset reduces to around 2kHz for Case 1. Still, the measured frequency doesn't match the estimated ones. The movement is not the only reason behind the Doppler Frequency Shifts. Receiver and Transmitter Clock drifts have a considerable effect on the Frequency Shift. Also, the soldering of OCXO crystal and supply noise may corrupt the clock accuracy. Such an improvement in the measured Doppler Frequency is also compatible with the results stated in [14].

Regarding position accuracy, OCXO fed configuration gives better position accuracy. 3D accuracy versus time graphs for the two cases are illustrated in Figure 4.24. The results indicate importance of transmitter clock accuracy. Transmitter clock drifts reduce positioning accuracy since they lead to deviation from the GPS time [38].

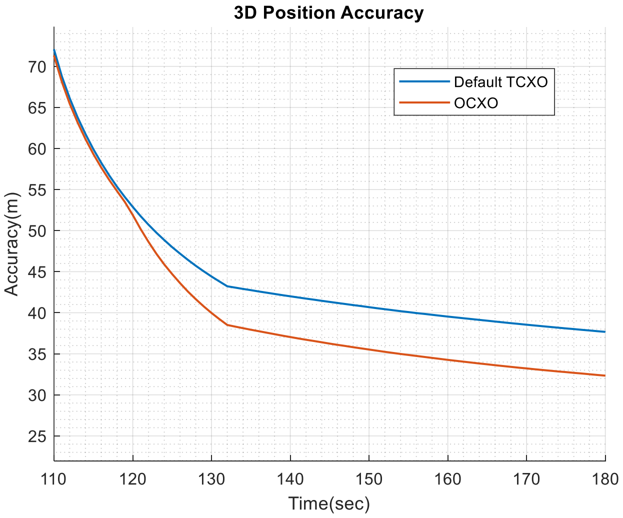
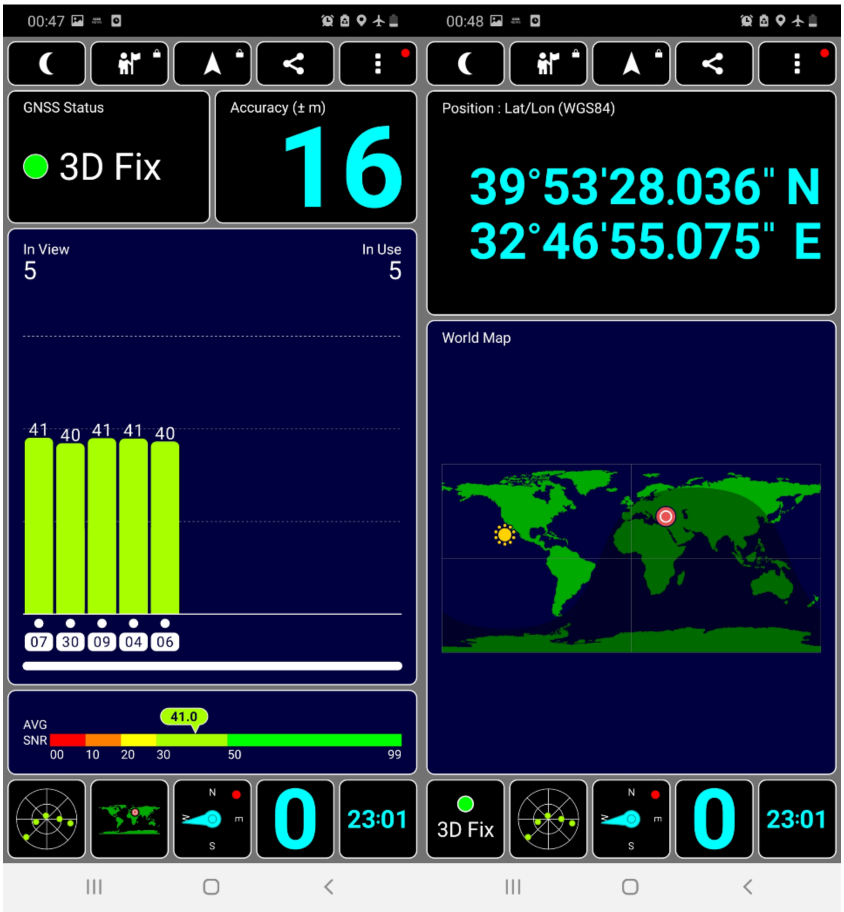


Figure 4.24: 3D Position Accuracies for the TCXO and OCXO Connected Receivers

The suggested transmitter system (Case 2) is also tested on the mobile phone. The airplane mode is enabled to guarantee that positioning services provided by GSM, WiFi, e.g., are not active. The fixed position is observed for Case 1. On the other hand, even the transmitting satellites cannot be detected in Case 2. Figure 4.25 illustrates the mobile phone’s GPS outputs.



00:47

GNSS Status
3D Fix

Accuracy (± m)
16

In View
5

In Use
5

00:48

Position : Lat/Lon (WGS84)
39°53'28.036" N
32°46'55.075" E

World Map

AVG
SNR
41.0

0
23:01

3D Fix
0
23:01

Figure 4.25: Mobile Phone Demonstration

Latitude and longitude values in Figure 4.25 are provided in terms of degrees, minus, and seconds. After converting them into decimal form, (Lat. 39.89111112, Lon. 32.78196528), it is observed that measured and estimated values are nearly same. Also, the time information in Figure 4.24 is in the UTC+3 scale.

The mobile phone’s GPS receiver calculates the position with 16m accuracy, better than ~32m provided by the U-Blox. The receiver hardware, especially the clock, is a key component for GPS accuracy. The receiver with a better clock provides a more accurate position [40].

4.5 Spoofing Implementation

In this section, the GPS L1 antenna is connected to GPS U-Blox receiver, and spoofing GPS signals are broadcasted from the OCXO-connected SDR with the GPS L1 antenna as illustrated in Figure 4.26. Then, the receiver's response to the spoofing signals is examined while the receiver has access to authentic satellite signals. Firstly, the receiver which already has a solution based on authentic SVs is exposed to the spoofing signals. Secondly, these spoofing signals are broadcasted just after the cold start of the receiver. These are named Scenario 1 and Scenario 2, respectively. The experiment is conducted in Istanbul, while the target position is in Ankara. Also, the satellites used in the experiment differ from the previous ones. Table 4.7 shows the parameters used in the experiment. Note that visible satellites can change with time and the antenna's position. Also, the real TOW value corresponds to the initial time of the experiment and increments by time.

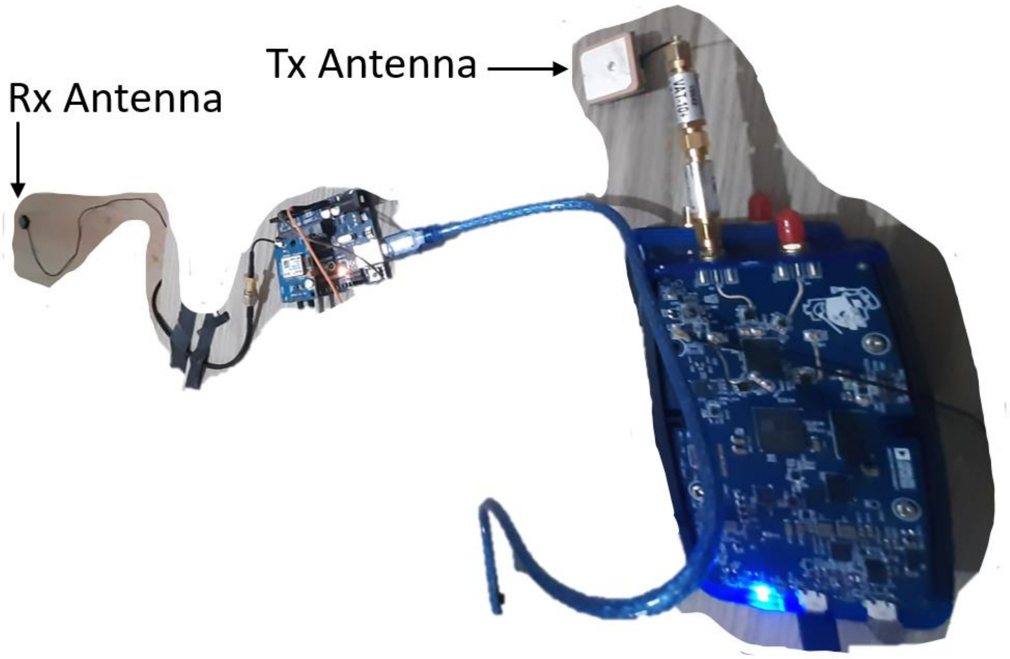


Figure 4.26: Spoofing Setup with Antennas

Table 4.7: Parameters for the Spoofing Experiment

Type	Spoofing	Authentic
SVs	SV5, 6, 11, 18, 25, 31	SV18, 23, 10, 16, 26
TOW start	151200	~166400
Duration(sec)	180(last 40 sec. dynamic)	--
Position (Lat,Lon)	[39.890630, 32.781826]	[40.9324, 29.15166]

- Scenario 1: Receiver which has a solution

For this scenario, receiver cannot use the spoofing signals for the navigation solution even though it tracks these signals. Also, observable data such as pseudoranges, doppler frequencies, and carrier phases are not computed for the spoofing signals.

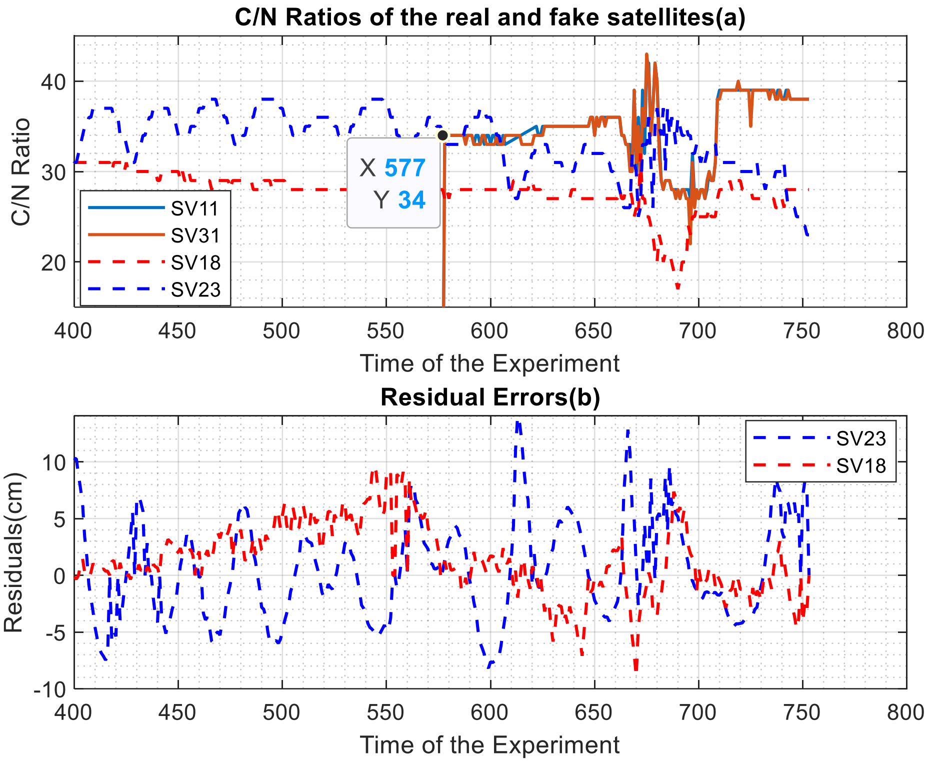


Figure 4.27: C/N Ratios (a) and Residuals (b) of the Real and Counterfeit SVs

Figure 4.27 depicts the C/N ratios and residual errors for the authentic satellites (SV18,23) and counterfeit satellites (SV18, SV31, SV11). Note that SV18 is common to both. As the figure implies, the C/N ratio of SV18 is different from those of other counterfeit SVs since the receiver tracks authentic SV18. Meanwhile, the transmission of the spoofing signals does not influence the residual errors of authentic satellites, including the common SV18. Figure 28 illustrates the measured positions for this scenario.

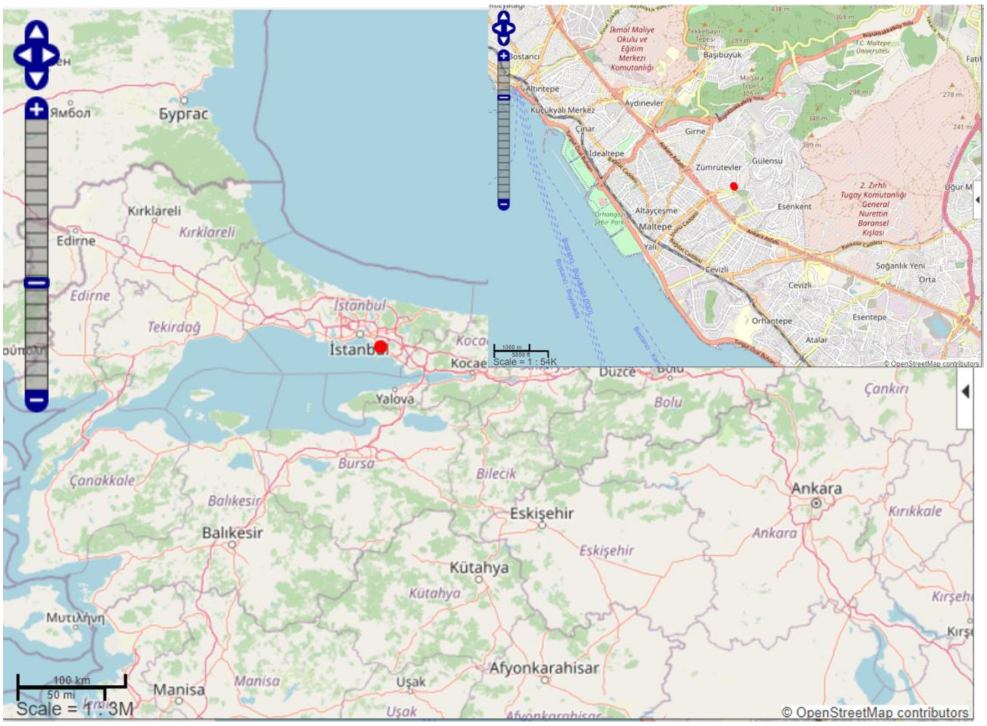
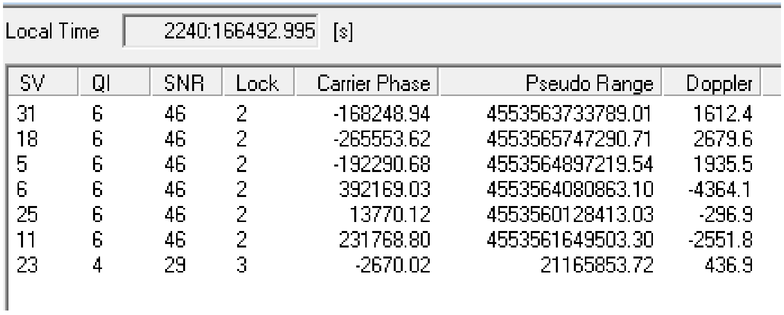


Figure 4.28: Measured Position for the Scenario 1

- Scenario 2: Receiver just after cold start

In this scenario, two different situations are observed. Firstly, if the receiver locks into real signals prior to spoofing signals, it doesn’t compute ephemeris parameters of the spoofing signals even if it tracks these signals. GPS time and week information is referenced to authentic satellites no matter whether the receiver goes into the lock status. In Figure 4.29, the range measurements for the counterfeit satellites and authentic satellite (SV23) are depicted. As illustrated in Figure 4.29, the receiver cannot correctly compute the pseudoranges of the counterfeit satellites as long as any authentic satellite's information is already solved. Also, obtained TOW value corresponds to the actual time of the experiment.

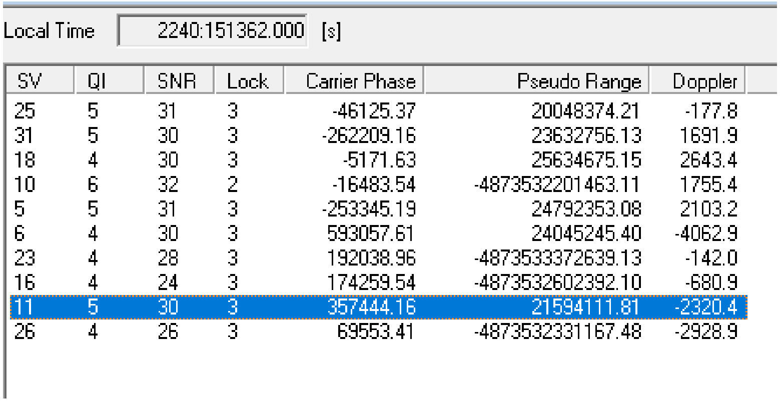


Local Time 2240:166492.995 [s]

SV	QI	SNR	Lock	Carrier Phase	Pseudo Range	Doppler
31	6	46	2	-168248.94	4553563733789.01	1612.4
18	6	46	2	-265553.62	4553565747290.71	2679.6
5	6	46	2	-192290.68	4553564897219.54	1935.5
6	6	46	2	392169.03	4553564080863.10	-4364.1
25	6	46	2	13770.12	4553560128413.03	-296.9
11	6	46	2	231768.80	4553561649503.30	-2551.8
23	4	29	3	-2670.02	21165853.72	436.9

Figure 4.29: Observable Outputs of Receiver Connected to Authentic Signals

On the other hand, if the spoofing signals are decoded prior to the authentic signals, the receiver obtains solutions based on the spoofing signals. The receiver's antenna is moved away from the window to make the receiver first lock into the spoofing signals. Figure 4.30 shows measured observables of the receiver which locks into the spoofing signals. As seen in Figure 4.29, the receiver does not correctly calculate the range of the authentic signals (SV10, SV23, SV16, SV26), which are not used in the navigation solution. However, after the end of the scenario, the receiver can track the authentic signals and provide the solution even if cold start mode is not enabled.



Local Time 2240:151362.000 [s]

SV	QI	SNR	Lock	Carrier Phase	Pseudo Range	Doppler
25	5	31	3	-46125.37	20048374.21	-177.8
31	5	30	3	-262209.16	23632756.13	1691.9
18	4	30	3	-5171.63	25634675.15	2643.4
10	6	32	2	-16483.54	-4873532201463.11	1755.4
5	5	31	3	-253345.19	24792353.08	2103.2
6	4	30	3	593057.61	24045245.40	-4062.9
23	4	28	3	192038.96	-4873533372639.13	-142.0
16	4	24	3	174259.54	-4873532602392.10	-680.9
11	5	30	3	357444.16	21594111.81	-2320.4
26	4	26	3	69553.41	-4873532331167.48	-2928.9

Figure 4.30: Observable Outputs of Receiver Connected to Spoofing Signals

Figure 4.31 shows the measured position for the spoofing signals. The scenario represents the receiver which is stationary until the last 40 seconds of the duration. Then, the receiver starts to move in the direction same as the one in section 4.4.3 with 45.7 m/s.

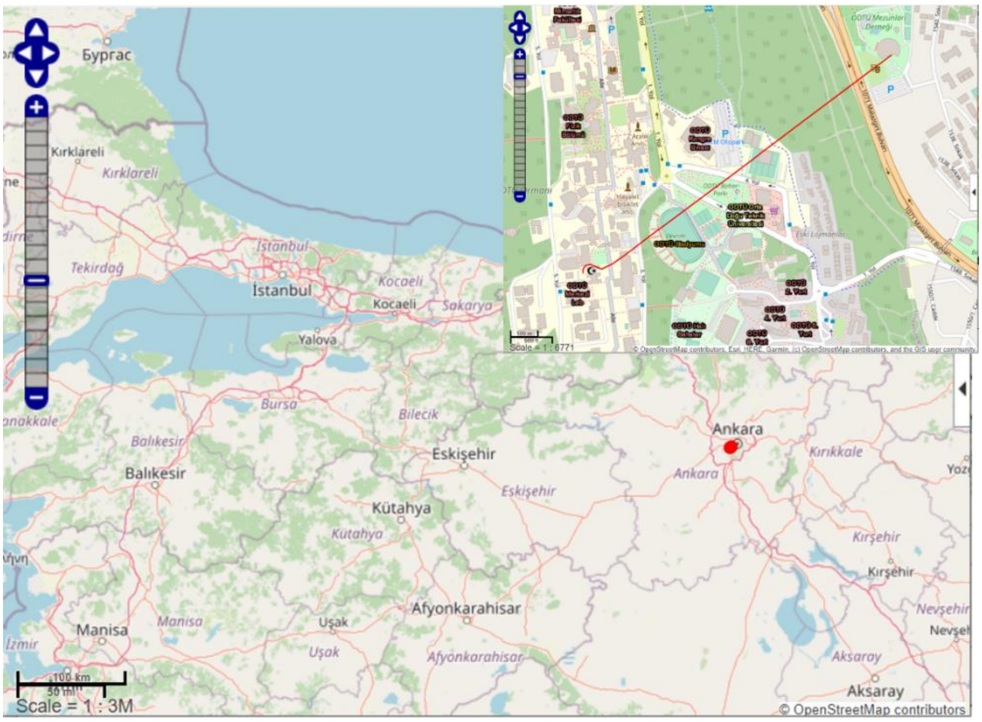


Figure 4.31: Measured Position for the Spoofing Signals

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

The importance of GNSS services dramatically continues to increase since their invention. GNSS becomes an essential part of technology in many fields, ranging from agriculture to the military. By the improvements in technology, the design of a low-cost hypothetical civilian GPS transmitter is now readily available. Such a transmitter accounts for the main step of GPS spoofers, which pose a great threat against positioning services. Also, the realization of the system can create a test bench platform for the SVs on board. Indeed, estimation of the positioning service performance requires not only the receiver but also the SV parts.

The main purpose of this thesis is an implementation of a GPS transmitter using SDR and make the receiver obtain position, velocity, and time solutions. Thereby, civilian GPS signals are generated by combining periodically published Navigation Data, proper ranging code, and calculated observable parameters such as Pseudoranges and Doppler Shifts. Navigation data for the civilian GPS is open to access, and an algorithm for the generation of ranging codes is available. MATLAB software platform provides a sort of toolbox for the computation of the observable parameters for the determined SVs-user group. Adalm-Pluto SDR fulfills the requirement of the GPS transmitter and converts the digitized GPS signals into the analog domain. Finally, the realized signals are injected into the commercial receiver by the cable. In this work, it is verified that the suggested GPS transmitter is capable of modeling a hypothetical stationary and dynamic user moving vertically or horizontally and making the receiver acquire the lock status. During all experiments, the transmitting signals are applied to GPS Receiver in cold start mode in which the receiver has no remembered information. The resulting positions are slightly shifted from the estimated ones, especially in the vertical direction. The deviation, in the range of 8kHz, between the estimated and measured Doppler Frequencies is observed. To reduce the deviation, an OCXO-based clock is connected to SDR as a reference, and a static scenario is performed on the same GPS receiver. As a result, Doppler deviation reduces to ~2kHz. Moreover, the measured velocity deviates from the estimated ones in the moving user scenario. The error term in the velocities is higher for the scenario with the horizontally moving receiver as compared to the vertically moving receiver. It is also observed that the moving user model cannot be handled by the receiver if its velocity is greater than a certain limit. Beyond the limit, the receiver loses track of the signals. However, this velocity limit is less than the receiver's limit and depends on the direction of the motion. Also, it is investigated that the update period of basic observables, Pseudoranges, and Doppler frequencies influences the performance of the GPS. Beyond a 250ms update period, the receiver gets into difficulty providing the position within limits. For the 500ms, the receiver is unable to generate valid position solution. The inconsistencies can be attributed to the fact that real GPS Satellites have higher quality transmitter components than Pluto SDR does; for example, real GPS transmitters utilize atomic clocks while Pluto SDR lacks such a clock. Also, the real satellites' movements lead to continuous change in the code phases and Doppler Frequencies. However, the proposed design should process those terms discretely. That can be another reason behind the discrepancies. Finally, ignoring the clock correction terms and Doppler Shifts on the ranging code may lead to the deviation in the observables, mainly Pseudoranges. It can bring in such discrepancies. It is not easy to perfectly mimic the GPS transmitter signals. Furthermore, measured positioning accuracy cannot be directly compared with real GPS expectations because it depends on the many parameters, receiver type, number of satellites etc. The generated signals are also applied to the mobile phone via OCXO-connected SDR and create 16m positioning accuracy which is higher than that of the scenario which involves the OCXO-connected SDR as a transmitter and U-Blox as a receiver, around 32m. It demonstrates importance of the receiver type to positioning accuracy. On the other hand, the predicted PDOP value,10.132, is consistent with measured one, ~10.2 ,and it is only related to SVs constellations relatives to receiver. The created signals are also broadcasted from SDR with a GPS L1 antenna, and the U-Blox receiver's responses to these spoofing signals are analyzed when the GPS L1 antenna is connected to the receiver. It is observed that the suggested transmitter is not feasible to make the receiver, which already has a valid solution or the navigation information such as time and ephemeris data, lock into the spoofing signals. On the other hand, spoofing signals control over the receiver if the receiver decodes spoofing signals first. It shows the importance of the time required for decoding the navigation data. Therefore, receivers not acquiring the authentic signals sufficiently are easily spoofed. Also, the proposed spoofing system is capable of the deceive receiver into dynamic and stationary PVT solutions.

5.2 Future Work

In future work, a higher sampling rate can be used to increase the robustness of the system. Also, ignored terms such as code phase Doppler Frequency and relativistic effect can be incorporated into the system. The system can be evolved into test-bench platform for the satellite positioning systems. In addition, the number of used SVs can be increased, and different constellations can be chosen to evaluate the positioning quality. On the other hand, during the experiments, it was realized that GPS receivers produce consistent observables independent of the position locked status. It may lead to the emergence of GPS-based indoor positioning services. In this kind of positioning services, the receivers can be used to compute user position in a particular area if the customized hypothetical GPS transmitters are located in specific positions within that area. Finally, the suggested system can be evolved into a spoofer system which allows misleading GPS receivers to compute false position, time, and velocity solutions.

REFERENCES

[1] N. Aerospace Centre, “NLR-Netherlands Aerospace Centre CUSTOMER: Agentschap Telecom GNSS spoofing Revised Edition,” 2019. [Online]. Available: www.nlr.nl

[2] A. M. Wyglinski, R. Getz, T. Collins, and D. Pu, *Software-defined radio for engineers*. Artech House, 2018.

[3] I. G. Petrovski, *GPS, GLONASS, galileo, and beidou for mobile devices*, vol. 9781107035843. 2012. doi: 10.4324/9781139565455.

[4] M. S. Grewal, L. R. Weill, and A. P. Andrews, *Global positioning systems, inertial navigation, and Integration,* Second Edition. 2007.

[5] Jaume. Sanz Subirana, J. Miguel. Juan Zornoza, and Manuel. Hernández-Pajares, *Fundamentals and algorithms. Vol. 1*. ESA Communications, 2013.

[6] U. S. C. Guard, “Navstar GPS user equipment introduction (public release version),” *Papers Published in Journal of Navigation*, vol. 1, pp. 5–6, 1996.

[7] J. W. Betz, *Engineering satellite-based navigation and timing: global navigation satellite systems, signals, and receivers*. John Wiley & Sons, 2015.

[8] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle, “GNSS - Global Navigation Satellite Systems,” 2007.

[9] E. D. Kaplan and C. Hegarty, *Understanding GPS/GNSS: Principles and applications*. Artech house, 2017.

[10] M. Wildemeersch and J. Fortuny-Guasch, “Radio frequency interference impact assessment on global navigation satellite

systems," *EC Joint Research Centre, Security Tech. Assessment Unit, Tech. Rep*, pp. 50–51, 2010.

[11] 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 (ION GNSS 2008)*, 2008, pp. 2314–2325.

[12] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[13] T. Ahmet and E. Süzer, "GPS Verici ve Alıcısı Sinyal Simülasyonu," Yüksek Lisans, Eskişehir, 2017.

[14] G. Goavec-Merou, J. M. Friedt, and F. Meyer, "Gps spoofing using software defined radio," *l'OSU THETA Franche-Comté-Bourgogne*, pp. 4–9, 2019.

[15] J. Cao, "Practical gps spoofing attacks on consumer drones," Ph.D dissertation, University of Hawai'i at Manoa, 2020.

[16] M. I. Ahmad, "A Low Cost Mass-Market Deployable Security Approach Against GPS Spoofing Attacks," Ph.D dissertation, Clemson University, 2018.

[17] A. El-Rabbany, *Introduction to GPS: The Global Positioning System*. Boston,MA: Artech House , 2002.

[18] J. Bao and Y. Tsui, *Fundamentals of global positioning system receivers : a software approach*. John Wiley & Sons, Inc., 2000.

[19] X. Li and H. J. Götze, "Ellipsoid, geoid, gravity, geodesy, and geophysics," *GEOPHYSICS*, vol. 66, no. 6, pp. 1660–1667, 2001, doi: 10.1190/1.1487109.

[20] A. Küpper, *Location-based services: fundamentals and operation*. John Wiley & Sons, 2005.

[21] J. G. Proakis and M. Salehi, *Fundamentals of communication systems*. Pearson Education India, 2007.

[22] B. Razavi, *RF microelectronics*, vol. 2. Prentice hall New York, 2012.

[23] K. Zhang, “Investigating GPS Vulnerabilty.” pp. 24–27, 2013.

[24] J. van Sickle, *GPS for Land Surveyors*, vol. 4. CRC press, 2008.

[25] A. Flores, “NAVSTAR GPS Space Segment/Navigation User Segment Interfaces.” US Air Force, 2020.

[26] A. Leick, L. Rapoport, and D. Tatarnikov, *GPS satellite surveying*. John Wiley & Sons, 2015.

[27] C. E. Noll, “The crustal dynamics data information system: A resource to support scientific analysis using space geodesy,” *Advances in Space Research*, vol. 45, no. 12, pp. 1421–1440, Jun. 2010, doi: 10.1016/j.asr.2010.01.018.

[28] I. Romero, “The Receiver Independent Exchange Format Version 3.05.” 2020.

[29] R. Langley, “Dilution of Precision,” *GPS World*, pp. 52–59, 1999.

[30] H. S. Cobb, “GPS pseudolites: Theory, design, and applications.,” Ph.D dissertation, 1997.

[31] The MathWorks Inc. (2021), “Satellite Communications Toolbox User’s Guide R2022a.” 2021. [Online]. Available: www.mathworks.com

[32] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, “On the requirements for successful GPS spoofing attacks,” in

Proceedings of the 18th ACM conference on Computer and communications security, 2011, pp. 75–86.

[33] Jeffery. Cooper, *Introduction to partial differential equations with MATLAB*. Birkhäuser, 1998.

[34] David. M. Pozar, *Microwave Engineering*, Fourth Edition. S.l.: JOHN WILEY & SONS, 2012.

[35] “u-blox 6 Receiver Description Including Protocol Specification,” 2013. [Online]. Available: www.u-blox.com

[36] N. text of specified style in document, “u-center GNSS evaluation software for Windows User Guide,” 1998. [Online]. Available: http://www.u-blox.com

[37] International GNSS Service (IGS). (1992). Daily 30-Second GPS broadcast ephemeris data NASA Crustal Dynamics Data Information System. Accessed July 25, 2022 Subset obtained :time period: 2022-07-09. https://doi.org/10.5067/GNSS/GNSS_DAILY_N_00

[38] D. Sathyamoorthy, S. Shafii, Z. F. M. Amin, A. Jusoh, and S. Z. Ali, “Evaluating the effect of Global Positioning System (GPS) satellite clock error via GPS simulation,” in *IOP Conference Series: Earth and Environmental Science*, Jul. 2016, vol. 37, no. 1, p. 012013. doi: 10.1088/1755-1315/37/1/012013.

[39] M. C. Varley, I. H. Fairweather, and R. J. Aughey, “Validity and reliability of GPS for measuring instantaneous velocity during acceleration, deceleration, and constant motion,” *J Sports Sci*, vol. 30, no. 2, pp. 121–127, 2012, doi: 10.1080/02640414.2011.627941.

[40] T. K. Yeh, C. Hwang, G. Xu, C. S. Wang, and C. C. Lee, “Determination of global positioning system (GPS) receiver clock

errors: Impact on positioning accuracy," *Meas Sci Technol*, vol. 20, no. 7, p. 075105, 2009, doi: 10.1088/0957-0233/20/7/075105.