A Software Defined GPS Signal Simulator Design

Zhenhe Pan

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Computer Engineering

Yaling Yang, Chair
Patrick R. Schaumont
Chao Wang

February 18, 2014
Blacksburg, Virginia

Keywords: GPS simulator, software defined, GPS interference, spoofing

A Software Defined GPS Signal Simulator Design

Zhenhe Pan

(ABSTRACT)

The Global Positioning System (GPS) signal simulator plays a critical role in developing and testing GPS receivers. Unfortunately, very few commercial GPS signal simulators are user-friendly for security researchers because they fail to generate abnormal GPS signals, which are fundamentally important.

In this thesis, we develop a cost efficient software defined GPS signal simulator. To reduce the design complexity, we make some reasonable assumptions about the GPS system. This simulator is able to generate clean GPS signals, as well as polluted GPS signals by jamming, multi-path, and spoofing interferences. In addition to simulating GPS signals for a single stand alone antenna, our simulator is also able to simulate GPS signals for multiple antennas, simultaneously. These features of the simulator will immensely help the security researchers in the GPS community.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In this chapter, we first discuss our research motivations and objectives, and then give a basic overview about the Global Positioning System (GPS) signals. This lays the foundations which are necessary for understanding simulator design and other related concepts, explained in later chapters. Lastly, we list several seminal works in the past two decades of GPS related research.

1.1 Motivation

1.1.1 The vulnerability of GPS signal

GPS is playing a fundamental role in nearly every aspect of our daily life, because it provides both accurate location (within meter level) and timing information (less than 100 ns) to anyone, anywhere without any charge. While the future of GPS looks promising, it suffers from several alarming security-related issues. These security issues with respect to GPS signals are mainly rooted in two aspects:

1. Low signal power
   GPS signals travel long distances (about 20200 km) before they reach the earth's surface, and the signal power captured by the conventional antenna is only about -160 dBW, which is usually 10∼30 dB below the thermal noise in a GPS receiver.

2. Open signal structure
   The GPS signal structures are completely open to the users, and are well addressed in GPS's interface control documents (ICD) by the U.S. government [1]. This transparency in signal structure pushes the boundaries of GPS research and applications; but on the other hand is open to malicious attacks to generate fake GPS signals that falsify the identity of target GPS users.

1.1.2 The importance of GPS signal simulator

In spite of the crucial role GPS plays in our everyday life it remains very vulnerable to malicious attacks. In light of these dangers, a lot of work is being done in developing anti-interference techniques both in academia and industry. GPS signal simulator plays a fundamental role during the receiver's design and testing process, because it provides a superior alternative for testing compared to live GPS signals in real-world scenarios.

Unlike real-world scenarios, testing with simulators provides full control of the simulated satellite signals and its environmental conditions. With a GPS simulator, users can easily generate and run as many different scenarios as required, with complete control over test conditions. In many cases, these test conditions are very difficult to recreate in real world conditions. Suppose we want to test the dynamic performance of some GPS receivers which are installed in high speed aircrafts. It won't be cost-effective if the only way we can carry out the experiment is by using a real aircraft. Instead, we can get the same test conditions for the GPS signals by using a simulator with aircraft motion parameters.

1.1.3 Current GPS signal simulator status

There are plenty of commercial GPS signal simulators in the market, which expedite the development of modern GPS receivers. However, most of the current commercial GPS signal simulators suffer from the following critical problems.

1. Not cost efficient
   The simulator designers pay a lot of attention to modeling the extremely complicated GPS signal error sources, leading to very rigid simulator designs. A user who wants to work on more general test conditions like "acquiring and tracking GPS signals" with intentional or unintentional interferences, have a difficult task ahead, especially for those who focus on the security-related issues in GPS receivers. Simulating extremely complex error sources requires powerful computational resources, therefore it is not cost-effective. At the end of 2013, the cost to carry out such simulations was tens of thousands of U.S. dollars.

2. Not security oriented
   Most of the current GPS signal simulators provide very little flexibility for the researchers to generate abnormal GPS signals, such as jamming, multi-path, and spoofing interference signals. However, these typical polluted GPS signals are actually of critical value for GPS-security researchers. This is especially true considering that it is relatively easy to capture clean GPS signals, while it remains quite difficult to capture the polluted GPS signals from our real world conditions.

1.2 Research objectives

As we mentioned in the last section, most of current GPS signal simulators are costly, and not quite user-friendly in case of GPS-related security research. In this thesis we address this problem: we have designed a cost efficient and security oriented GPS signal simulator. Our research objectives are summarized as follows:

1. This simulator is able to generate GPS signals for the standard stand alone antenna, since it is the most common testing scenario in GPS applications.
2. Additionally, it can simulate GPS signals for multiple antennas as well, considering the antenna array's capability in detecting and mitigating some stubborn interferences in GPS receivers.
3. The simulator should be security focused, which means that it is able to generate not only clean GPS signals but also polluted GPS signals by different interference sources, such as jamming, multi-path, and spoofing. Also, these interferences should be easily controlled by the end-users.

1.3 Backgrounds

1.3.1 GPS signals

Table 1.1: Two kinds of GPS services

L_1 Band	P(Y)	CA
L_2 Band	P(Y)	CA

GPS is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth's surface; where there is an unobstructed line of sight of four or more GPS satellites. GPS consists of three major segments: space segment, control segment, and a user segment .

As shown in Table 1.1, GPS provides two kinds of service in two different frequency bands simultaneously: the standard positioning service (SPS) and the precision positioning service (PPS). The main difference in these two services is that the GPS satellite transmits two different ranging codes: the Coarse/Acquisition (CA) code, which is freely available to the public, and the restricted Precision $P(Y)$ code, usually reserved for military applications. In this thesis, we will only focus on the CA code in the L_1 frequency band. If there is no special specification, the GPS signals always mean the CA signal in the L_1 frequency band.

GPS is a typical code division multiple access (CDMA) system, which means all the GPS satellites share the same frequency while each satellite has a unique pseudocode.

Figure 1.1 is the simplified GPS signal generation process. For satellite i, its transmitting signal can be expressed as:

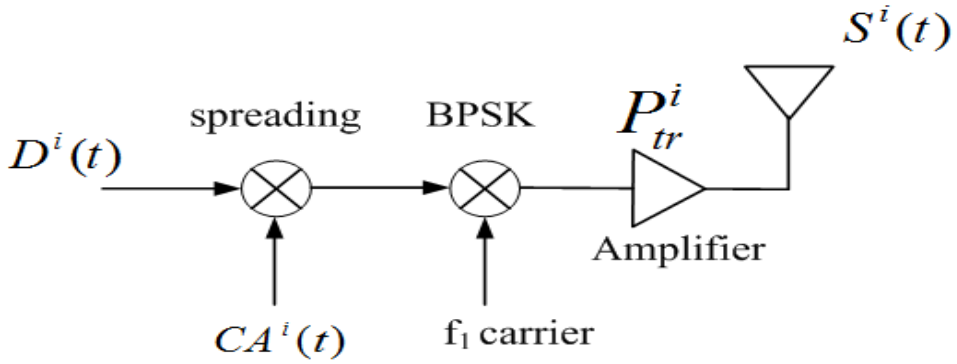

Figure 1.1: Simplified GPS signal generator

$$s^{(i)}(t) = \sqrt{2P_{tr}} * CA^{(i)}(t) * D^{(i)}(t) * cos(2\pi f_1 t + \theta_0^{(i)}) \tag{1.1}$$

- θ the initial phase of the carrier.
- f_1 carrier frequency, which is 1575.42 MHz.
- P_{tr} GPS satellite's transmission power, which is about 20 W. When the GPS signal reaches the Earth, its power is about -160 dBW if there is no blocking objects.
- $CA(t)$ The CA code is also called pseudo-random noise (PRN), whose chip rate is 1.023 MHz, and its period is 1 ms which means that it has 1023 chips during one period, and one chip time duration is 977.5 ns. Each satellite has a unique CA code, and we can name a satellite according to its transmission CA code number [2]. For example when we say satellite $sat(i)$, it denotes the satellite that is using $CA(i)$ as it ranging pseudo-code. The CA code is required to have very good auto-correlation and cross-correlation properties because it is used to differentiate the GPS satellites.
- $D(t)$ The navigation message is 50-bit per second stream, which is comprised of the satellite Ephemeris data, TOW, GPS clock errors, etc. The navigation message is the core of the GPS system, which is used to determine the GPS signal's transmission time and GPS satellite location at that transmission time. The details of $D(t)$ is well explained in [2].

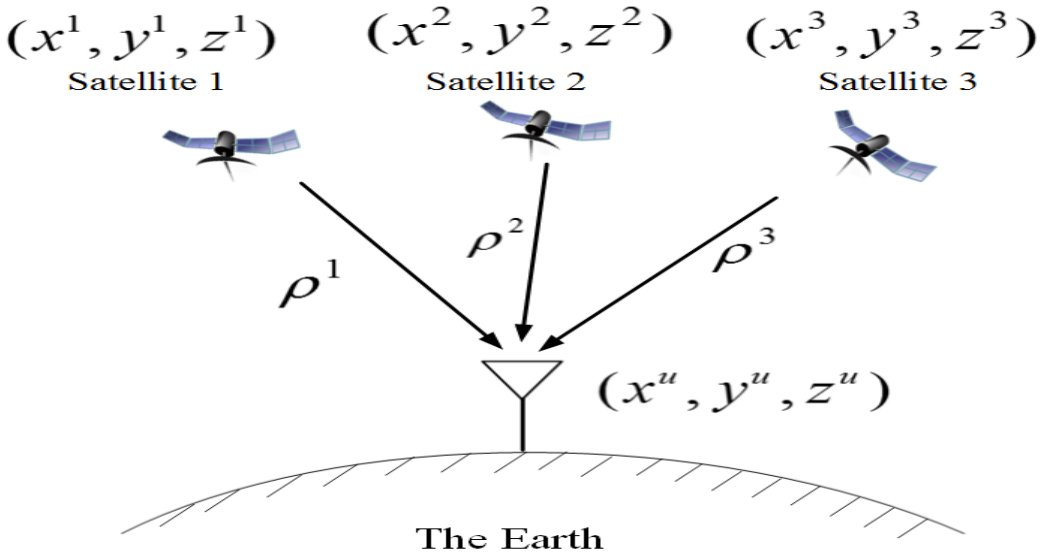

Figure 1.2: Triangle geometry location principle

1.3.2 GPS receiver

Principle The GPS's positioning principle is shown in Figure 1.2. Suppose we are given three satellites' locations $P^{sat_i} = (x^i, y^i, z^i)$, and their distances to the GPS receiver ρ^i, where $i = 1, 2, 3$. Usually the GPS receiver does not have a perfect clock, and its clock must have some bias error compared to GPS time system. Therefore, a fourth satellite is required to compute the user's location as well as the local clock error by solving the following equations [3].

$$\sqrt{(x^1 - x^u)^2 + (y^1 - y^u)^2 + (z^1 - z^u)^2} = \rho^1 + c * t_{err} \tag{1.2}$$
$$\sqrt{(x^2 - x^u)^2 + (y^2 - y^u)^2 + (z^2 - z^u)^2} = \rho^2 + c * t_{err} \tag{1.3}$$
$$\sqrt{(x^3 - x^u)^2 + (y^3 - y^u)^2 + (z^3 - z^u)^2} = \rho^3 + c * t_{err} \tag{1.4}$$
$$\sqrt{(x^4 - x^u)^2 + (y^4 - y^u)^2 + (z^4 - z^u)^2} = \rho^4 + c * t_{err} \tag{1.5}$$

, where c is the speed of light, and t_{err} is the local clock error.

As we can see from the above equations, to solve the receiver position, we first need to know the satellites' locations (x^i, y^i, z^i), and their distances to the receiver ρ^i. Suppose the GPS receiver can successfully decode the GPS signal navigation bits, and then knows about each acquired GPS satellite's orbital parameters. According to Kepler's theorems [4], the receiver can compute the GPS satellite locations (x^i, y^i, z^i) and its distances to the receiver ρ^i at the transmission time t_{tr}. Therefore, the most fundamental thing in GPS receiver is to measure the GPS signal's transmission time, t_{tr} as accurately as possible. GPS receiver relies on the navigation message and phase lock loop (PLL) to get the transmission time.

1.4 Related work

1. Industry
   GPS signal simulator research is advancing at a rapid rate due to the wide deployment of the GPS receivers and the great improvements in the semiconductor performance. There are many excellent, mature commercial GPS simulators manufacturers, such as Spirent, LabSat, NI, etc. Unfortunately, very few technical details are made available to other researchers due to the proprietary designs.

2. Academia
   In the academic research on GPS, we list some major traceable research papers undertaken. Saburo Ifune filed a patent on the GPS signal simulator (publication number: US5093800 A)[5]. This patent presented details about how to simulate GPS RF signal from a hardware approach, and the complex orbit parameters are actually pre-installed in memory instead of generating in real time.

   The authors of [6, 7], designed a software-based intermediate frequency (IF) GPS signal simulator for the L1 CA code. The authors assumed that the GPS signals are always clean, and did not consider the GPS interference signals.

   Byun et al. [8] did a comprehensive work about how to model the multi-path interference of GPS signals. The authors in [9] proposed a low-cost GPS signal simulation approach using the Universal Software Radio Peripheral (USRP) and the Matlab GPS toolbox.

1.5 Organization of the thesis

The results of the thesis are organized as follows:

1. In chapter 1, we discuss our research motivation and objectives. We also briefly present some basic foundations and background about GPS related concepts, which are necessary for understanding aspects of GPS simulator design and the challenges discussed in this thesis.

2. In chapter 2, we describe in detail how to generate the standard stand alone GPS signals. To reduce the simulator design complexity, we make some reasonable assumptions about the GPS system. An experimental result is presented in the last part of this chapter.

3. In chapter 3, we focus on how to generate the polluted GPS signals by some typical interferences, such as jamming, multi-path and spoofing. We also present several experimental results about these polluted GPS signals.

4. In chapter 4, we discuss how to generate GPS signals for multiple GPS antennas. We also provide an example of using a smart GPS antenna to detect and mitigate the wide-band intentional interference.

5. In Chapter 5, we draw conclusions from this work on a security oriented GPS signal simulator, and further discuss our future research directions.

Chapter 2

GPS signal simulation for stand alone antenna

In this chapter, we first discuss the main sources of measurement error in the GPS receiver. The most challenging components of a GPS receiver originate from the signal acquisition and tracking processes, and very few security researchers are interested with the error sources of a GPS System, such as satellite orbital parameters, and satellite clock shifts. To reduce the simulator design complexity, we make some reasonable assumptions about the GPS system. After that, we provide a detailed design of a GPS signal simulator for a stand alone GPS antenna. At the end of this chapter, testing results are presented showing the correct functioning of the simulator and how its accuracy compares against real GPS signals.

2.1 GPS Errors

In GPS systems, the measurement errors can be roughly classified into the following three categories [4] as shown in Figure 2.1.

1. Satellite errors
   The satellites errors are mainly made up of satellite clock errors and satellite ephemeris errors. These errors are mainly because the ground monitor segment cannot describe the satellite orbit and clock accurately. It is also very hard for the GPS receiver to mitigate these errors since they originate from GPS satellites. In addition, considering they are usually much smaller compared with other errors, the satellite errors have less research value in the GPS receiver community.

2. Communication channel errors
   GPS satellites need to transmit signals over a long distance to reach the receiver antenna. During this communication channel, there are multiple random errors, mainly

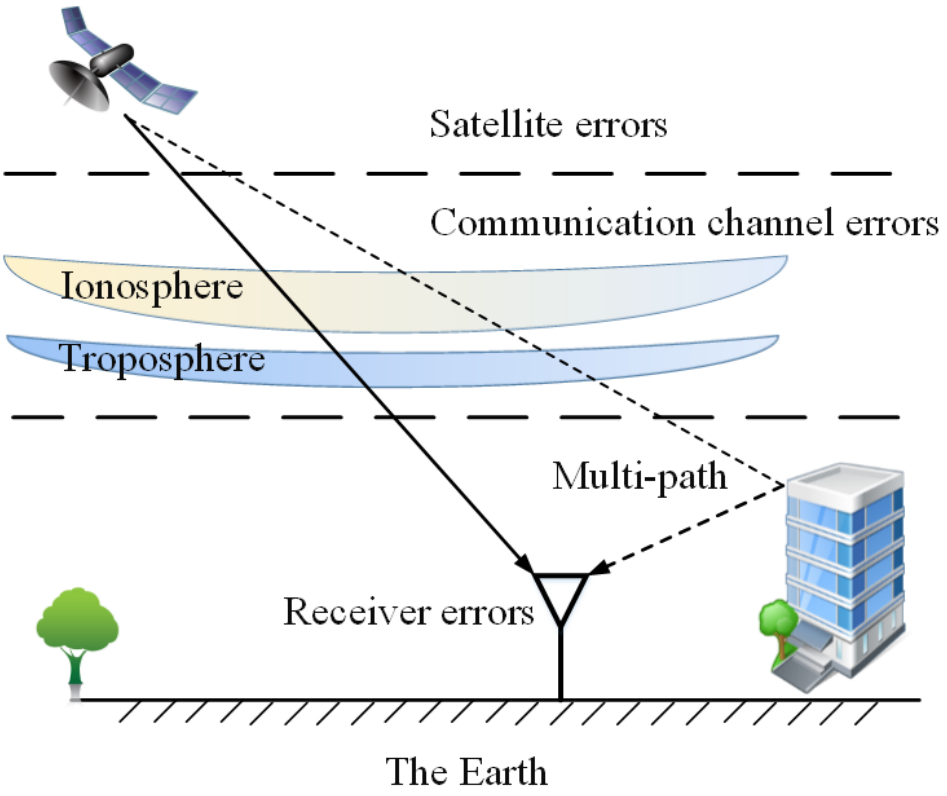

Figure 2.1: Three GPS error sources

due to interference. Some typical interferences are jamming, multi-path, spoofing, etc. Most of the intentional or unintentional interferences actually originate from communication channel errors.

3. Receiver errors
   GPS receivers also introduce some measurement errors, such as thermal noise, local clock errors, computational errors, etc. Since this thesis only focuses on the design of a GPS signal simulator, which is totally independent of receiver errors, such errors are ignored in this thesis.

2.2 Assumptions about GPS

One of the main difficulties of designing a GPS signal simulator is to generate the complex satellite errors in the navigation messages, such as satellite orbital parameters and clock shifts. The irregularity of the GPS satellite's motion and clock shift, makes it a non-trivial task to generate the navigation messages. In addition, the Earth's irregular rotation and shape also aggravates this process.

As we discuss in section 2.1, from the technical perspective, satellite errors have a minor role in GPS receivers, and very few researchers are interested in these errors. Instead, the most valuable research direction in GPS receiver is about the signal acquisition and tracking process, where interference affects the GPS accuracy. As for different navigation messages, GPS receivers simply decode and interpret them differently. Hence, to reduce the simulator complexity while not impairing its applications, we make the assumptions in section 2.2.1 and re-define the navigation messages to design our GPS signal simulator.

Obviously, GPS receivers also need to undergo some modifications because of the changes in the navigation messages. These modifications are quite small but they are worthwhile, considering the greatly reduced design complexity of the simulator.

2.2.1 Assumptions

In this thesis, we make three basic assumptions about a GPS system as follows:

1. GPS Constellation

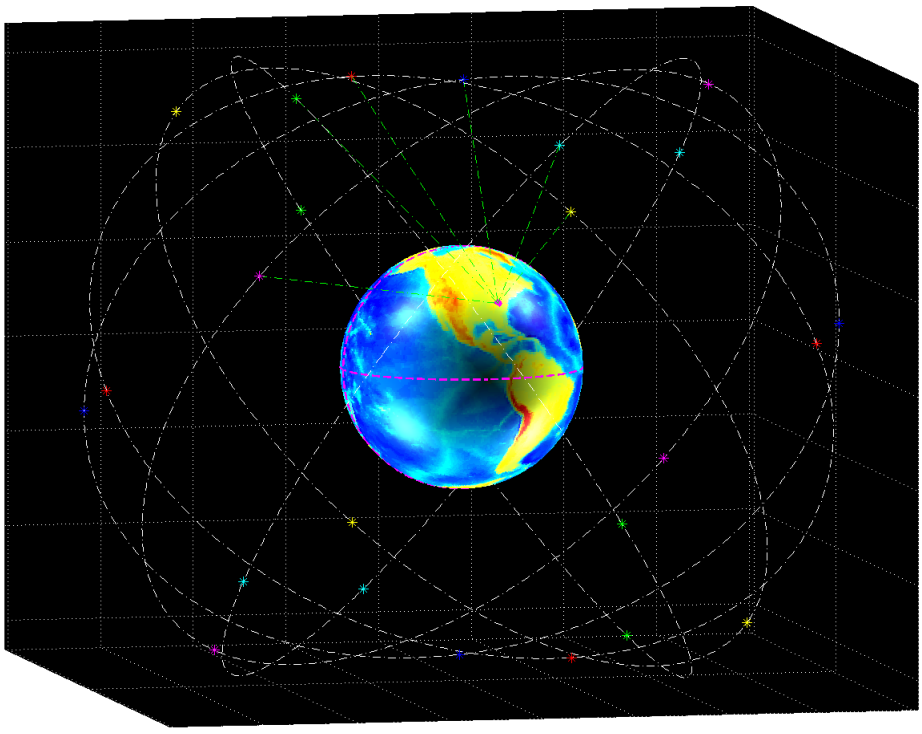

Figure 2.2: Simulated GPS Constellation

There are 30 GPS satellites laying in six perfect circular orbital planes. Each orbital plane has five satellites which are evenly spaced (72^o) with respect to each other. The

six orbital planes have an 55^o inclination (tilt relative to Earth's equator) and are separated by a right ascension of 60^o with the ascending node (angle along the equator from a reference point to the orbits intersection). For each satellite, the orbital radius is some constant value between 26000∼27000 km, and the orbital period is 11 hours 58 minutes. The simulated GPS satellite constellation is shown in figure 2.2.

As we mentioned in subsection 1.3.1, we can name each satellite according to its PRN number, for instance satellite $sat(8)$ means this satellite is using $CA(8)$ as its ranging code. After introducing the concept of orbital plane, we can also name each satellite as $sat(i, j)$, where the satellite under consideration lies in orbital plane i, and is the jth satellite in this plane. Fox example, we can also name $sat(8)$ as $sat(1, 2)$ since it is the third satellite in plane 1. In the following parts of the thesis, we will be using both these naming methodologies alternatively as required.

2. The Earth
   Unlike the real Earth, we assume that the Earth is a perfect sphere with a radius of 6400 km. In addition, we also assume the rotation period is 23 hours 56 minutes and it never changes. In this thesis, whenever we speak of the Earth without any specifications, it refers to this idealized Earth and the not the real Earth.

3. Coordinate system

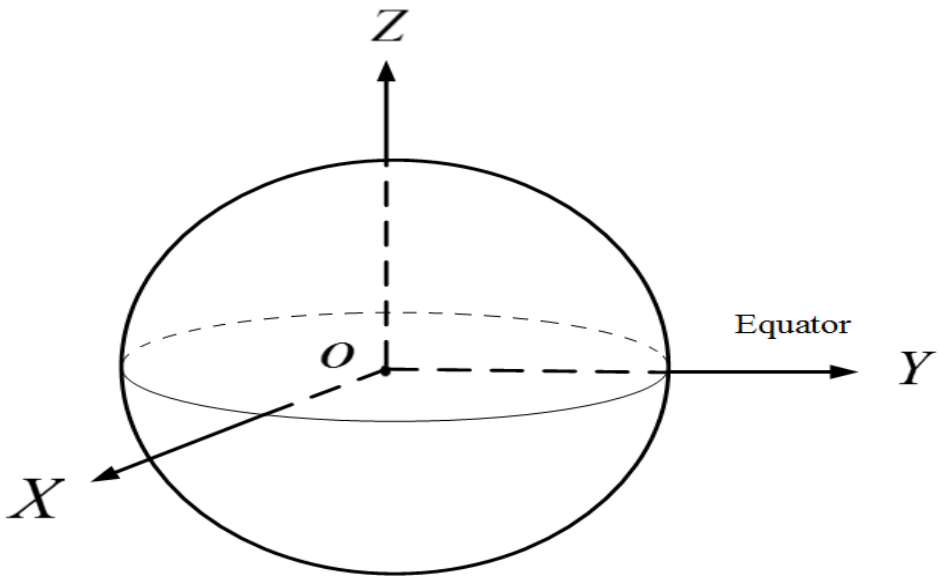

Figure 2.3: The Earth Coordinate System

As shown in Figure 2.3, we use the Earth Coordinate System as our coordinate system because it's relatively easier to describe the GPS satellite and receiver positions with respect to this coordinate system. The Earth's center is used as the origin point of the

coordinate system, the rotation axis is used as the OZ axis, and the equator plane lies in the XOY plane as shown in Figure 2.3.

2.2.2 Re-definition of navigation messages

Because of the assumptions made above about the GPS system, we re-define the navigation messages in our simulator as follows:

1. block 1

   The data in block 1 of the real GPS navigation messages is mainly used to describe the satellite health status, as well as the satellite clock errors. We re-define the data in block 1 as follows.

   - URA(user ranging accuracy)
     In real GPS systems, the URA generated by the ground monitor system, is used to indicate the accuracy of the GPS positioning. Since this word is not very critical in the GPS receiver from a technical perspective, we re-define the URA word as a meaningless field in our simulation system.
   - Health status
     In our simulation system, we simply re-define all the satellites as always healthy because the word, health status, is not critically important from a technical perspective.
   - Satellite clock errors
     In real GPS signals, satellite clock errors are described by three parameters: a_{f0}, a_{f1} and a_{f2}. Usually these GPS clock errors are less than 3 m, and is not the main source of error in the GPS system. For simplicity, we fix a_{f0} as some random number, and set a_{f1} and a_{f2} as zeros. Therefore, the satellite clock error δt^s is equal to a_{f0}.
   - Other fields
     In our simulation system, we assume that the user does not care about other errors such as the ionosphere delay, and therefore re-define all other words in block 1 as meaningless fields.

2. block 2

   The data in block 2 in the real GPS navigation message is used to describe the satellite orbital parameters such as the 16 orbital parameters. Since in our simulator, the GPS constellation is assumed to be a perfect circle, and the satellite moves with a fixed angular velocity, we only need the following two fields in block 2. However, we need to interpret them according to the GPS constellation assumptions.

- t_{oe}
  t_{oe} means the reference time when using the 16 orbital parameters to compute satellite position in the real navigation messages. But in our simulation system, t_{oe} means the starting time of the simulation system. When it is written as zero, it means the simulator's reference starting time is 00:00:00 AM, Jan 6, 1980.
- $\sqrt{a_s}$
  In our simulation system, we re-define $\sqrt{a_s}$ as the orbital radius, which is a constant value between 26000∼27000 km and never changes.
- other fields
  We re-define all the other fields in block 2 as unused fields, and fill them with meaningless random bits.

3. block 3
   Since the data in block 3 is mainly used to describe the information about all satellites' Almanac, GPS time system and UTC (Coordinated Universal Time) system, etc., which are not required for the GPS receiver's instant positioning, we re-define the data in block 3 as meaningless fields, and fill them with random bits.

2.2.3 Modifications in GPS receiver

Due to the assumptions we make about GPS satellites and the re-definitions of navigation messages, some modifications are required in the GPS receiver. Actually, the method of calculating the signal transmission time is the same as with the real GPS receiver. When using our GPS signal simulator, the GPS receiver should use the following procedure to compute satellite location at any specific transmission time.

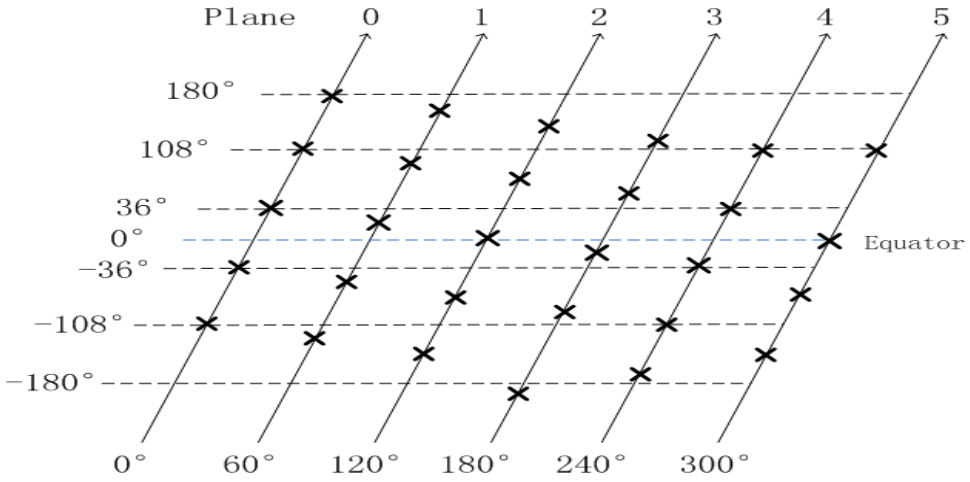

Figure 2.4: GPS satellite initial space phase

As shown in Figure 2.4, for the orbital plane i, we assume the first satellite's initial space phase to be:

$$\Psi_0^i = \frac{12}{180} * \pi = \frac{\pi}{15} i \tag{2.1}$$

where $0 \leq i \leq 5$.

Thus, for any satellite $sat(i,j), 0 \leq j \leq 4$, its initial phase can be expressed as:

$$\Psi_0^{i,j} = \Psi_0^i + 72 * j * \frac{\pi}{180} = \frac{\pi}{15} i + \frac{2\pi}{5} j \tag{2.2}$$

According to the GPS constellation assumptions in section 2.2.1, the rotational angular velocity of a GPS satellite can be expressed as:

$$\Omega_{sat} = \frac{2\pi}{T_{sat}} \tag{2.3}$$

where T_{sat} is the satellite rotation period, which is 11 hours and 58 minutes.

Therefore, for satellite $sat(i,j)$, at time t, its orbital space phase can expressed as:

$$\Psi^{i,j}(t) = \Psi_0^{i,j} + \Omega_{sat} * (t - T_{start}) \tag{2.4}$$

where $\Psi_0^{i,j}$ is the initial orbital phase at starting time given by equation 2.2. In our simulator system, we set T_{start} as 00:00:00 AM, Jan 6, 1980.

In order to compute the satellite location at time t, we suppose there is a virtual satellite which lies in orbital plane 0, and this virtual satellite has the same orbital phase with satellite $sat(i,j)$.

As shown in Figure 2.5, the location of this virtual satellite could be expressed as:

$$P_v^{0,j}(x;t) = R_{orb} * cos(\Psi^{i,j}(t)) \tag{2.5}$$

$$P_v^{0,j}(y;t) = R_{orb} * sin(\Psi^{i,j}(t)) * cos(\alpha) \tag{2.6}$$

$$P_v^{0,j}(z;t) = R_{orb} * sin(\Psi^{i,j}(t)) * sin(\alpha) \tag{2.7}$$

where R_{orb} is the GPS satellite's orbital radius, which is some constant value between $26000 \sim 27000$ km. α is the angular inclination with the Earth's equatorial plane, which is 55^o.

As we discussed in section 2.2.1, the six orbital planes are separated by 60^o right ascension of the ascending node, we can get the satellite $sat(i,j)$'s location by rotating this virtual satellite in orbital plane 0 with an angular rotation of $\beta = \frac{\pi}{3} * i$, with the rotational center as z axis.

Thus, the location of satellite $sat(i,j)$ can be computed as:

$$P_{sat}^{i,j}(x;t) = P_v^{0,j}(x;t) * cos(\beta) - P_v^{0,j}(y;t) * sin(\beta) \tag{2.8}$$

$$P_{sat}^{i,j}(y;t) = P_v^{0,j}(x;t) * sin(\beta) + P_v^{0,j}(y;t) * cos(\beta) \tag{2.9}$$

$$P_{sat}^{i,j}(z;t) = P_v^{0,j}(z;t) \tag{2.10}$$

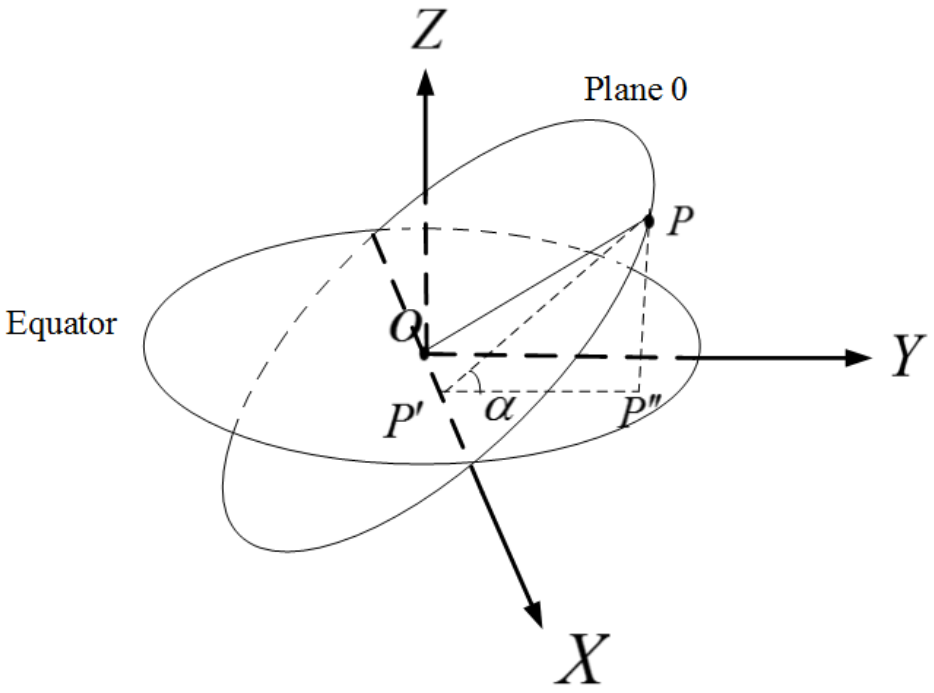

Figure 2.5: GPS satellite position in orbital plane 0.

Hence, at transmission time t, we can compute any satellite's location according to the equations above.

2.3 Signal simulation

2.3.1 Satellite signal

As we mentioned in section 1.3.1, for each satellite i, its transmission signal can be expressed as:

$$s^i(t) = \sqrt{2P_{tr}} * CA^i(t) * D^i(t) * cos(2\pi f_1 t + \theta_0^i) \tag{2.11}$$

Suppose the satellite clock error is a constant value δt^s, then the satellite's transmission signal can be fixed as:

$$s^i(t) = \sqrt{2P_{tr}} * CA^i(t + \delta t^s) * D^i(t + \delta t^s) * cos(2\pi f_1 (t + \delta t^s) + \theta_0^i) \tag{2.12}$$

Suppose the satellite signal takes time $\tau_{prop}(t)$ to travel from the GPS satellite to the receiver antenna, and the power loss is $\alpha(t)$ as shown in Figure 2.6, then the received GPS signal

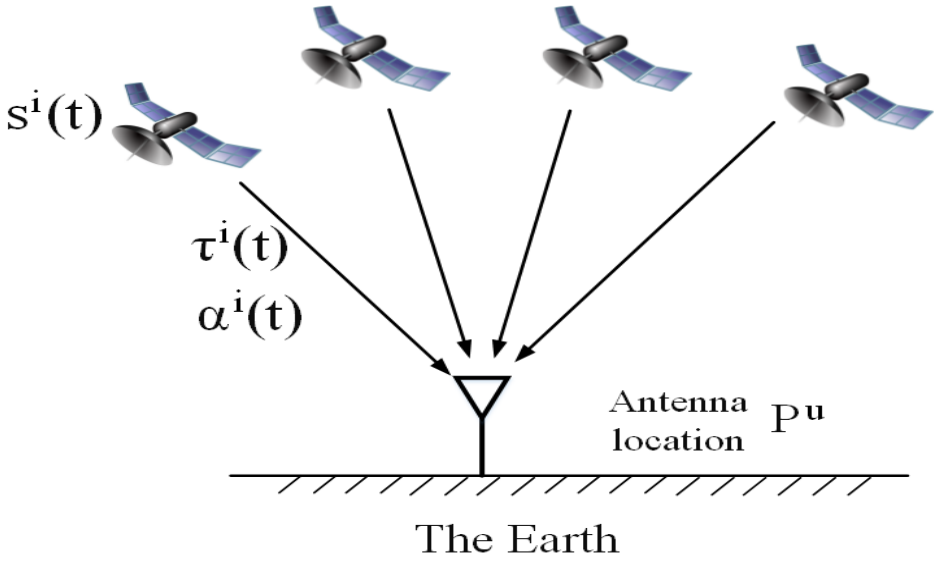

Figure 2.6: GPS signal propagation

from satellite i can be expressed as:

$$s^i_{rec}(t) = \alpha^i(t) * s^i(t - \tau^i_{prop}(t)) \tag{2.13}$$

For the stand alone antenna model, the simulator function can be summarized as: given simulation time t, and the antenna location P^u, the simulator produces the received signal $s_{rec}(t; P^u)$, which can be written as:

$$s_{rec}(t; P^u) = \sum_i \alpha^i(t) * s^i(t - \tau^i_{prop}(t)) + n(t) \tag{2.14}$$

where i means all the GPS satellites visible to the receiver at time t, and $n(t)$ is thermal noise with a spectrum density of -174dBm/Hz.

2.3.2 Propagation time $\tau_{prop}(t)$

As we mentioned in chapter 1, the most important thing in GPS receivers is how to calculate the signal transmission time. While in the GPS simulator system, the most important thing is to estimate the propagation time $\tau_{prop}(t)$ from the GPS satellite to the GPS receiver antenna.

$\tau_{prop}(t)$ is composed of four parts, and can be expressed as:

$$\tau_{prop}(t) = R(t) + I(t) + T(t) + U(t) \tag{2.15}$$

- $R(t)$ is the distance delay

- $I(t)$ is the ionosphere delay
- $T(t)$ is troposphere delay
- $U(t)$ is some unknown delay

We will firstly discuss$I(t), T(t)$ and $U(t)$ in this sub-section, and will discuss $R(t)$ in detail in next sub-section.

1. Ionospheric delay
   The ionosphere is the zone of the terrestrial atmosphere that begins about 60 km above the surface of the Earth and extends itself up to 2000 km. Since security researchers do not care too much about the effects of $I(t)$ in GPS receivers, we simply assume $I(t)$ to be some normal random noise with a mean of 10 m and variance of 3 m in our simulator system.

2. Tropospheric Delay
   Troposphere is the atmospheric layer that extends from the Earth's surface to an altitude of about 60 km. Security researchers do not care too much about the effects of $T(t)$, thus we simply generate $T(t)$ as some normal random noise with a mean of 2 m and variance of 1 m in our simulator system.

3. Unknown delay
   Like the tropospheric Delay, we simply assume that the unknown delay $U(t)$ is a Gaussian random variable with a mean value of 3 m and variance of 1 m in our GPS simulator.

   We also assume that the changing rates of $I(t), T(t)$ and $U(t)$ are all 1 Hz, which means the value of $I(t), T(t)$ and $U(t)$ is updated once per second.

2.3.3 Distance delay $R(t)$

The assumptions we make about the GPS system greatly simplify the computation of $R(t)$ as shown in this part. Distance delay $R(t)$ depends on the receiver location and satellite position. In the following parts of this thesis, we use $L()$ to mean the position of GPS receiver by its longitude, latitude, and height.

1. Receiver location
   Suppose that the receiver's initial location is $P_0^u = L(lat_0, lon_0, hgt_0)$, its location in the Earth's Coordinate System can also be expressed as:

$$P^u(x;t) = (R_{Earth} + hgt_0)cos(lat)cos(lon) \tag{2.16}$$
$$P^u(y;t) = (R_{Earth} + hgt_0)cos(lat)sin(lon) \tag{2.17}$$
$$P^u(z;t) = (R_{Earth} + hgt_0)sin(lat) \tag{2.18}$$

Suppose the GPS receiver moves with two motion parameters $[\overrightarrow{v^u} : \overrightarrow{g^u}]$, where $\overrightarrow{v^u} = [v^u(x), v^u(y), v^u(z)]$ is the initial speed, and $\overrightarrow{g^u} = [g^u(x), g^u(y), g^u(z)]$ is the accelerate rate.

Then the GPS receiver user position should be fixed as:

$$P^u(x;t) = P_0^u(x;t) + v^u(x) * t + 0.5 * g^u(x) * t^2 \tag{2.19}$$
$$P^u(y;t) = P_0^u(y;t) + v^u(y) * t + 0.5 * g^u(y) * t^2 \tag{2.20}$$
$$P^u(z;t) = P_0^u(z;t) + v^u(z) * t + 0.5 * g^u(z) * t^2 \tag{2.21}$$

From the above equations, we can see that adding the motion parameters $[\overrightarrow{v^u} : \overrightarrow{g^u}]$ does not increase the computational complexity of the receiver location. In later part of this thesis, when we use the initial position P_0^u, it also contains the receiver motion parameters $[\overrightarrow{v^u} : \overrightarrow{g^u}]$. And the default $[\overrightarrow{v^u} : \overrightarrow{g^u}]$ is $[\overrightarrow{0} : \overrightarrow{0}]$, which means the receiver antenna is motionless.

2. Visible satellites

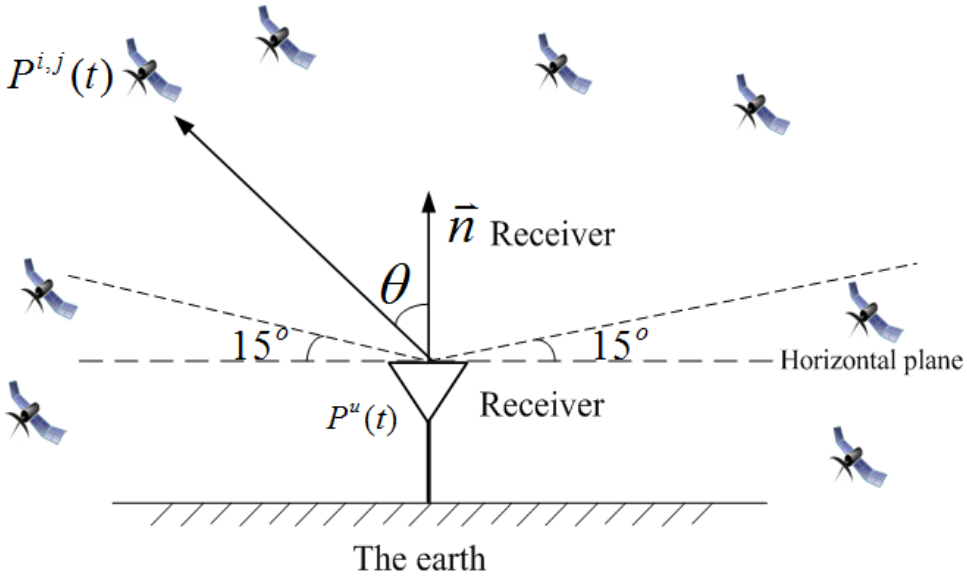

Figure 2.7: Geometry relationship between receiver user and visible satellites

According to our discussion in section 2.2.3, at any given time t, we can compute each satellite $sat(i,j)$'s location $P_{sat}^{i,j}(t)$. At the receiver location $P^u(t)$, we can think the antenna's normal vector as:

$$\overrightarrow{n(t)} = (P^u(x;t), P^u(y;t), P^u(z;t)) \tag{2.22}$$

As we can see from Figure 2.7, for any satellite $sat(i,j)$, only when the angular θ between the vector antenna plane $\overrightarrow{n(t)}$ and $\overrightarrow{P^u(t)P_{sat}^{i,j}(t)}$ is acute, the satellite is visible to the GPS receiver.

However, in the real world, when θ is quite close to $\frac{\pi}{2}$, the satellite signal is prone to suffer severe multi-path interference, high ionosphere and troposphere delay. Therefore, in our simulator system, if θ is greater than 75^o, we can consider the satellite as not visible to the GPS receiver antenna.

Therefore, for each visible satellite $sat(i,j)$, we can get the following equation:

$$cos(\theta) = \frac{\overrightarrow{P^u(t)P^{i,j}_{sat}(t)} \cdot \overrightarrow{P^u(t)}}{\left\|\overrightarrow{P^u(t)P^{i,j}_{sat}(t)}\right\| \cdot \left\|\overrightarrow{P^u(t)}\right\|} \geq cos(75^o) \tag{2.23}$$

As shown in Figure 2.7, satellites $sat(1)$, $sat(2)$, $sat(3)$ and $sat(4)$ are satellites visible to the receiver antenna, while satellites $sat(5)$ and $sat(6)$ are not visible to the receiver even they are above the horizontal plane.

3. Distance delay equation
When the GPS signal reaches the receiver antenna at time t, it actually leaves the

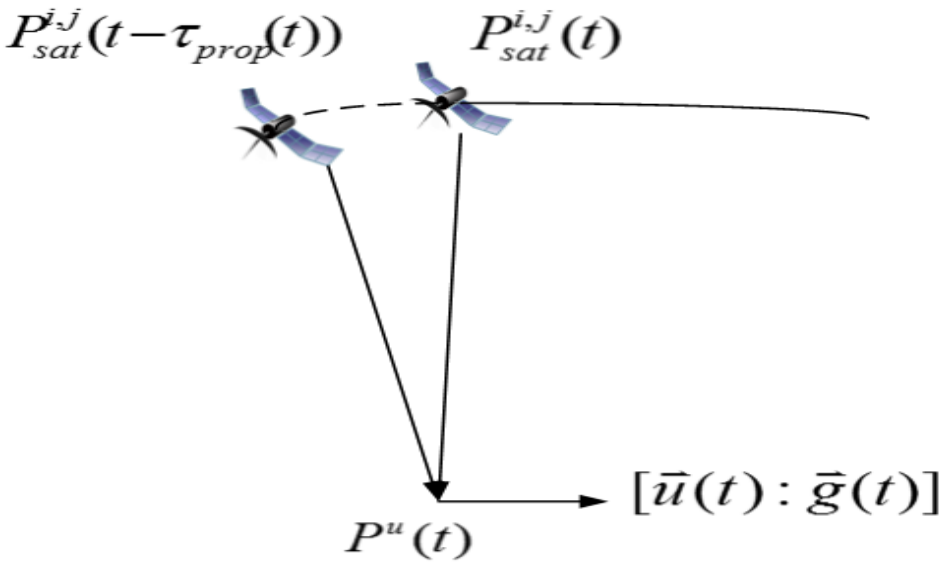

Figure 2.8: GPS signal propagation time.

GPS satellite at time $t' = t - \tau_{prop}(t)$.

According to equations 2.8 - 2.10, we can compute any satellite $sat(i,j)$'s location $P^{i,j}_{sat}(t')$ at time t'. Thus, we can get the following equation:

$$\left\|P^{i,j}_{sat}(t') - P^u(x;t)\right\| = c * R(t) \tag{2.24}$$

Since $\tau_{prop}(t)$ is a pretty small variable (usually about $78ms$), according to Taylor's theorem, we get:

$$P^{i,j}_{sat}(t - \tau_{prop}(t)) = P^{i,j}_{sat}(t) - \frac{\partial P^{i,j}_{sat}(t)}{\partial t} * \tau_{prop}(t) \tag{2.25}$$

we can rewrite the equation 2.24 as:

$$\left\| P_{sat}^{i,j}(t) - \frac{\partial P_{sat}^{i,j}(t)}{\partial t} * \tau_{prop} - P^u(t) \right\| = c * R(t) \tag{2.26}$$

Using the equation 2.15, the above equation can be changed as:

$$\left\| P^{i,j}(t) - P^u(x;t) - \frac{\partial P^{i,j}(t)}{\partial t} * (R(t) + I(t) + T(t) + U(t)) \right\| = c * R(t) \tag{2.27}$$

Since $I(t)$,$T(t)$ and $U(t)$ are already known as discussed in section 2.3.2, by solving equation 2.27, we can compute the distance delay $R(t)$, and then compute the propagation time $\tau_{prop}(t)$ according to equation 2.15.

2.3.4 Power loss l

When GPS signal propagates from the satellite to the receiver antenna, it suffers the following attenuations:

1. Free space loss
   In our simulation system, we use the following model to compute the free space loss as:
   $$l_{space} = (\frac{4\pi d}{\lambda})^2 \tag{2.28}$$
   λ is the wavelength of the GPS signal, which is about 19 cm.
   d is the real propagation distance from the satellite to the receiver antenna, and can be computed as:
   $$d = c * R(t) \tag{2.29}$$
2. Atmosphere loss
   In order to reduce the design complexity, in our simulation system, we consider the atmosphere loss, l_{atm} to be some constant value, which presides in the range 1∼3 dB. Once the value of l_{atm} is chosen, it does not change during the simulation process.
3. Receiver antenna gain
   In our simulation system, the receiver antenna gain, denoted as g^{ant}, is defined by the GPS simulator user. Usually, we set it to be some constant value, which lies in 10∼30 dB. Like l_{atm}, once g_{ant} is defined, it does not change during the whole simulation process.

Thus, when given the above parameters, we can compute the power loss l in equation 2.13 as:

$$l = g_{ant} * l_{atm} * l_{space} \tag{2.30}$$

2.3.5 Simulation algorithm

The input setting configurations to generate the simulated GPS signal for the stand alone GPS antenna are listed as follows:

- initial position P_0^u
- antenna gain g_{ant}
- simulation start time t_{start} and end time t_{end}

After that, the simulation process can be divided as follows:

1. GPS satellite initialization
   For each satellite $sat(i)$, the simulator sets the following satellite parameters:
   - transmission power P_{tr}
   - orbital radius R_{sat}
   - satellite clock error δt^s
   - carrier initial phase θ_0

   These parameters remain unchanged during the whole simulation process. Once these parameters are defined, the navigation messages $D(t)$ are also determined. After that, each satellite signal $s^i(t)$ is determined as:

$$s^i(t) = \sqrt{2P_{tr}} * CA^i(t + \delta t^s) * D^i(t + \delta t^s) * cos(2\pi f_1(t + \delta t^s) + \theta_0^i) \tag{2.31}$$

2. Visible satellite computation
   Since we can compute GPS satellite position and receiver antenna position at any time t, we can find all the satellites visible at that time t according to equation 2.23. Since the visible satellites are changing, we update the set of visible satellites every second.

3. Propagation time $\tau_{prop}(t)$ computation
   For each visible satellite $sat(i)$, we first randomly set $I(t), T(t), U(t)$ according to their properties in section 2.3.2. We also update these delays once per second. After that, we compute the distance delay $R(t)$ according to equation 2.27, and then compute $\tau_{prop}(t)$ according to equation 2.15.

4. Received signal computation
   Once we know the distance delay $R(t)$, we can compute the power loss according to equation 2.30. After that, we can compute the received GPS signal by the antenna as:

$$s_{rec}(t; P_0^u) = \sum_i l^i(t) * s^i(t - \tau_{prop}^i(t)) + n(t) \tag{2.32}$$

The GPS signal simulator algorithm for a stand alone antenna is describe in algorithm 4. The default time step t_{step} is 10 ns, which means the simulated GPS data rate is 100 MHz.

Algorithm 1 stand alone GPS signal simulator

Require: GPS receiver initial position P_0^u
GPS antenna gain g_{ant}
simulation starting time t_{start}
simulation ending time t_{end}
Ensure: $s_{rec}(t; P_0^u)$
initialize each GPS satellite
initialize GPS receiver
compute all the visible satellites to the GPS receiver per second
set $t = t_{start}$ and time step t_{step}
while $t \leq t_{end}$ **do**
for all visible satellite $sv(i)$ **do**
compute the propagation time $\tau^i_{prop}(t)$
compute the received signal $s^i_{rec}(t)$ from satellite $sat(i)$ according to equation 2.13
end for
$t = t + t_{step}$
compute the background noise $n(t)$
compute the received signal $s_{rec}(t; P_0^u)$ by the GPS receiver antenna at location P_0^u.
end while

2.4 Experimental testing

1. Testing model
   We first use the simulator we designed to generate GPS signals after specifying some setting parameters. After that we input these simulated GPS signal into a GPS receiver to verify if the navigation results are consistent with the simulator setting parameters.

   We use the SoftGNSS v3.0 [10] designed by Darius Plausinaitis and Dennis M. Akos as our GPS receiver to verify the simulated GPS signals. Since we re-define the navigation messages in our simulator system, we need to make some modifications as discussed in section 2.4 for the satellite location computing process in the SoftGNSS receiver. Because the SoftGNSS receiver is designed to process the IF signals, thus we also need to convert the simulated signals' carrier frequency from 1575.42 MHz to 8.912 MHz.

2. Simulator settings
   The input settings of the simulator are shown below:

   - $P_0^u = L(37.230^o, -80.414^o, 640)$ in Blacksburg, VA.

- g_{ant} = 20 dB.
- t_{start} is 10:00:00 AM, Jan 20, 2014.
- t_{end} is 10:02:00 AM, Jan 20, 2014, which means the simulation period is 120 seconds.

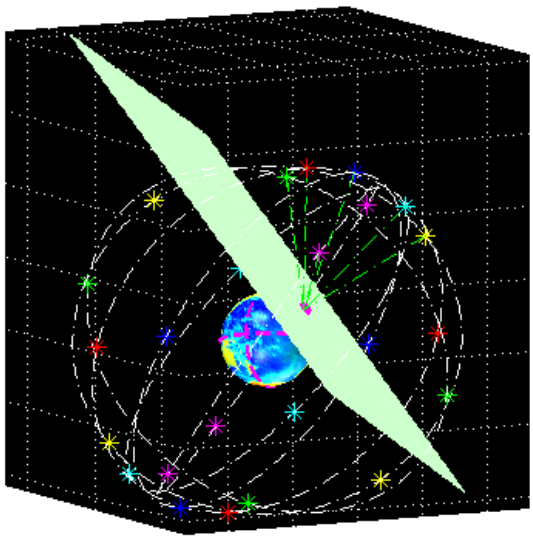

Figure 2.9: Visible satellites in Blacksburg at 10:00:00 AM, Jan 20, 2014

3. Testing results
   Figure 2.9 shows the visible satellites during the simulation period, and Figure 2.10 shows the satellites acquired by the testing receiver when using the simulated GPS signal. As a matter of fact, the these visible satellites are exactly same with acquired satellites by SoftGNSS receiver.

   Figure 2.11 shows the positional accuracy by the SoftGNSS receiver. The computed location is around the initial position P_0^u that we set, and the average location error is about 9.7 ms, which means that when a GPS receiver uses our simulated GPS signals for a stand alone antenna, it can achieve a similar positioning accuracy with the real GPS signals.

2.5 Summary

In this chapter, we design a GPS signal simulator, which can generate GPS signals for the stand alone antenna. To reduce the design complexity, we make some reasonable assumptions

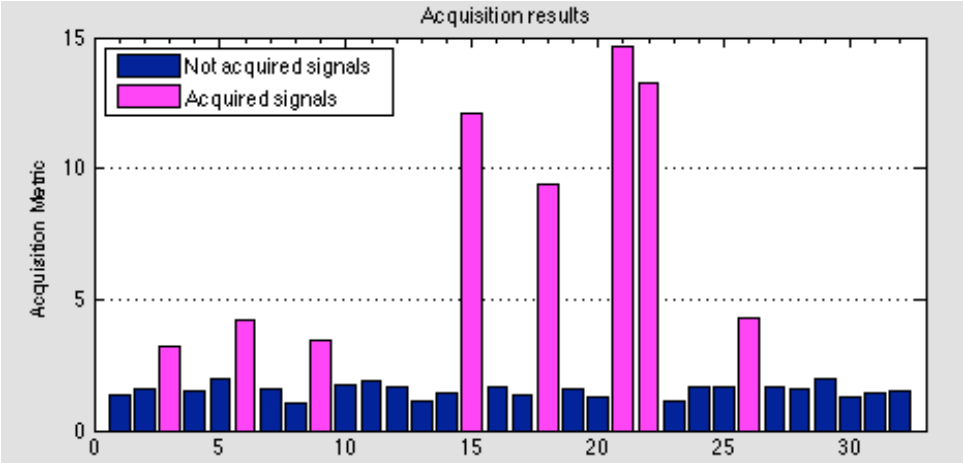

Figure 2.10: The satellites acquired by the testing receiver.

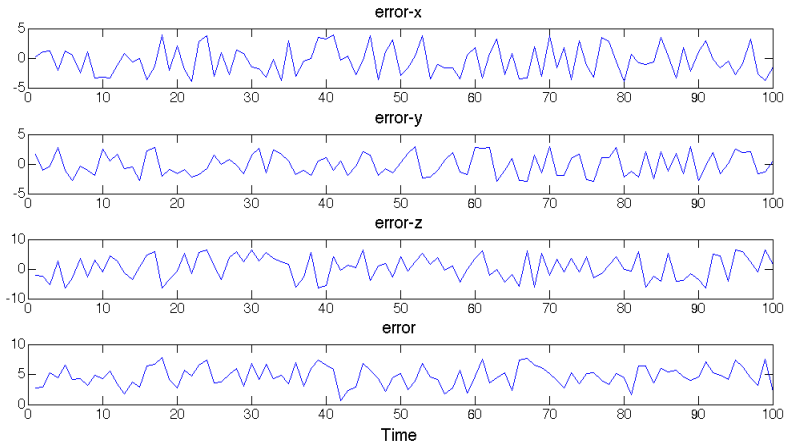

Figure 2.11: The positioning accuracy using the simulated GPS data.

about the GPS system. Since most of the challenging issues with a GPS receiver are related to signal acquisition and tracking processes instead of the navigation bit decoding, these assumptions would not impair the GPS simulator's applications. The user of the simulator only needs to specify some configurational parameters, such as the antenna location and gain, simulation starting time and simulation period. In the last part of this chapter, an example is presented showing how the simulator works correctly for stand alone GPS antenna.

Chapter 3

Interference signal simulation

Generation of GPS signals for stand alone antenna is usually not enough in many cases. This is especially true for those who are focusing on the security issues in GPS receivers. In this chapter, we discuss how to simulate the polluted GPS signals by some interferences such as jamming, multi-path, and spoofing. These interferences are critical to the security researchers in GPS receiver community.

3.1 Interference introduction

GPS signal is generally vulnerable, and can be easily interfered because of its lower transmission power and public signal structure [11]. On one hand, usually when the GPS signal arrives at the antenna, its power is about $10 \sim 30$ dB below the thermal noise in the receiver. On the other hand, GPS signal structure is totally open, and can be utilized by malicious attackers to generate fake GPS signals to falsify some target GPS receiver users.

In this thesis, we divide the GPS interference signals into the following three classes according to its signal structure similarity with the real GPS signals.

1. Jamming
   Jamming is a type of interference signal whose signal structure can be argued to be totally different than the real GPS data structure, and it affects the target GPS receiver by virtue of its relatively stronger signal power with respect to the real GPS signal.

2. Multi-path
   Multi-path interference is a very commonplace phenomenon affecting GPS receivers, especially in some city canyons [8]. Multi-path interference signal has the same signal structure with the real GPS signals, but it is usually considered to be unintentional interference because the reflection object's position is randomly distributed around the

target GPS receiver.

3. Spoofing interference
   Spoofing interference has very similar signal structure [12, 13, 14]. Usually, the Spoofing interference is generated by malicious attackers who intent to falsify some target GPS receivers. In some cases, the Spoofing interference might be real GPS signal, which is collected at a different location. Spoofing interference is considered to be the most difficult and serious interference in GPS receivers.

3.2 Jamming

3.2.1 Jamming model

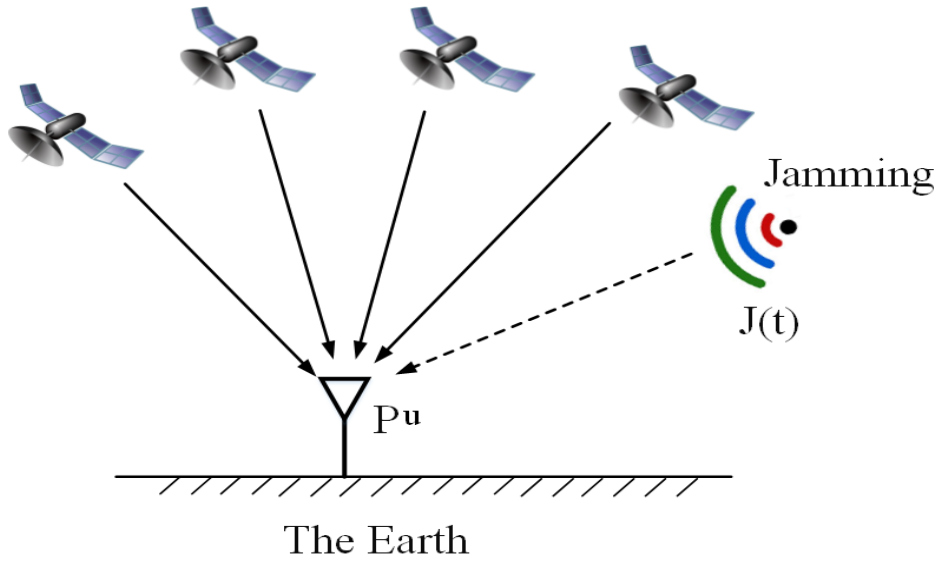

Figure 3.1: Jamming interference model

Figure 3.1 shows a typical jamming interference model. A jamming source is transmitting some interference signal, $J(t)$ to the target GPS receiver at a close location. Usually, this jamming signal has a much stronger power than the real GPS signals received by the target GPS receiver. The jamming signal might be intentional or unintentional interference.

3.2.2 Jamming simulation

The important parameters about the jamming interference model are shown below.

1. BW_{jam}: jamming signal bandwidth.
2. A_{jam}: jamming signal amplitude.
3. f_{jam}: jamming signal frequency.
4. P_{jam}: jamming transmitter position.

Suppose the initial phase is ϕ_{jam}, we can construct the transmission jamming signal with BPSK modulation as:

$$J(t) = A_{jam} * RandChip_{jam} * cos(2\pi f_{jam} t + \phi_{jam}) \tag{3.1}$$

where $RandChip_{jam}$ is a random variable with [-1,1] uniform distribution, and $RandChip_{jam}$ chip rate is $\frac{BW_{jam}}{2}$. These two features can guarantee the jamming signal bandwidth is BW_{jam}

Suppose the jamming signal transmitter location is P^{jam}, then we can compute the free space power loss α_{jam} according to equation 2.28.

Suppose the time delay from P^{jam} to P^u is Δt^{jam}. Thus, the jamming interference received by the target receiver, $s_{jam}(t)$ can be expressed as:

$$s_{jam}(t) = \alpha_{jam} * J(t - \Delta t^{jam}) \tag{3.2}$$

$$\Delta t^{jam} = \frac{d}{c} \tag{3.3}$$

where d is the distance between the jamming signal transmitter location P^{jam} and the target GPS receiver location P^u.

The signal received by the target GPS antenna, $s^{tar}(t)$ has two parts. One is the clean GPS signal received at position P^u, which can be represented by $s_{rec}(t; P^u)$ according to the discussion in chapter 2. The other one is the jamming signal, $s_{jam}(t)$ as shown in the above two equations.

Thus, all the signals received by the target receiver $s^{tar}(t)$ can expressed as:

$$s^{tar}(t) = s_{rec}(t; P^u) + s_{jam}(t) \tag{3.4}$$

3.2.3 Experimental results

1. Continuous wave jamming

Jamming configurations The Continuous wave (CW) jamming setting parameters are summarized as following:

- target GPS receiver antenna location $P^u = (L37.230^o, -80.414^o, 640)$, which is in Blacksburg, VA.
- jamming transmitter location, $P_{jam} = (L37.230^o, -80.414^o, 1640)$, which is exactly 1 km above the target receiver antenna location P^u.
- jamming power is 15 W.
- jamming bandwidth is 0 MHz because the jamming signal is a single frequency signal.

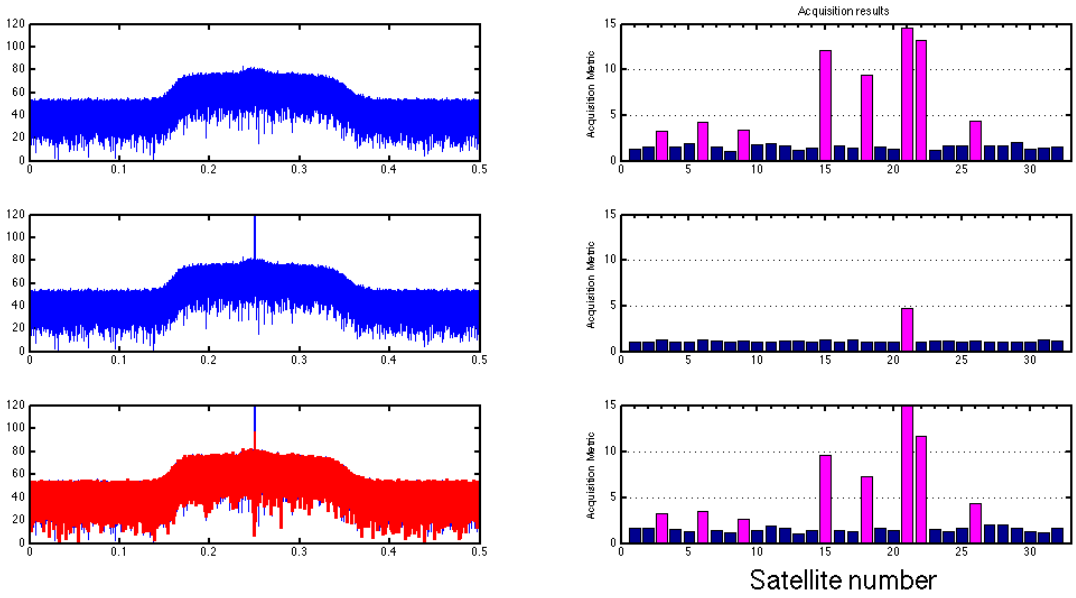

Figure 3.2: CW jamming interference testing results

Testing results Figure 3.2 shows the testing results of the simulated GPS signals with CW jamming interferences. The left side of figure 3.2 shows the simulated GPS signal in the frequency domain, and the right side of figure 3.2 shows the acquired satellites by the testing software defined GPS receiver softGNSS.

- The upper part in figure 3.2 shows when there is no jamming interference, the target GPS receiver is able to acquire 8 GPS satellites.
- The middle part in figure 3.2 shows when the jamming transmitter is switched on, the simulated GPS signals contain a strong CW jamming interference, which is about 30 dB above the average GPS signal power. This strong interference

severely affects the target GPS receiver's acquisition results. As a result, only one GPS satellite signal can be captured successfully, which is shown in the middle right of figure 3.2.

- To further verify if the CW jamming signal is generated correctly, we design a stop-band filter to filter out the jamming interference. The bottom left in figure 3.2 shows the strong CW interference is attenuated severely when using the stop band filter. After this anti-interference filter, we can see that the softGNSS receiver can re-capture the other seven satellites, which are buried in the strong CW jamming signal.

2. Wide band jamming

Jamming configurations The wide band jamming setting parameters are shown below. Actually, the wide band jamming parameters are almost the same with the CW jamming parameters except that the wide band jamming transmission power is 5 W, and the wide band jamming bandwidth is about 3.8 MHz.

- target GPS receiver antenna location $P^u = (L37.230^o, -80.414^o, 640)$ in Blacksburg, VA.
- jamming transmitter location, $P_{jam} = (L37.230^o, -80.414^o, 1640)$, which is exactly 1 km above the target receiver antenna location P^u.
- jamming power is 6 W.
- jamming bandwidth is 3.8 MHz.

Testing results The testing results are shown in Figure 3.3.

- When there is no jamming interference, the testing receiver softGNSS acquires 8 GPS satellites using the simulated GPS signals.
- When the wide band jamming transmitter is switched on, the testing receiver softGNSS can acquire 2 GPS satellites, which are not enough for navigation computations.
- Since this wide band jamming interference is distributed fully over the GPS legitimate frequency band, it is extremely hard to design a frequency filter to mitigate the wide band effects on the real GPS signals. In chapter 4, we will present an example using the smart antenna to mitigate the wide band interference.

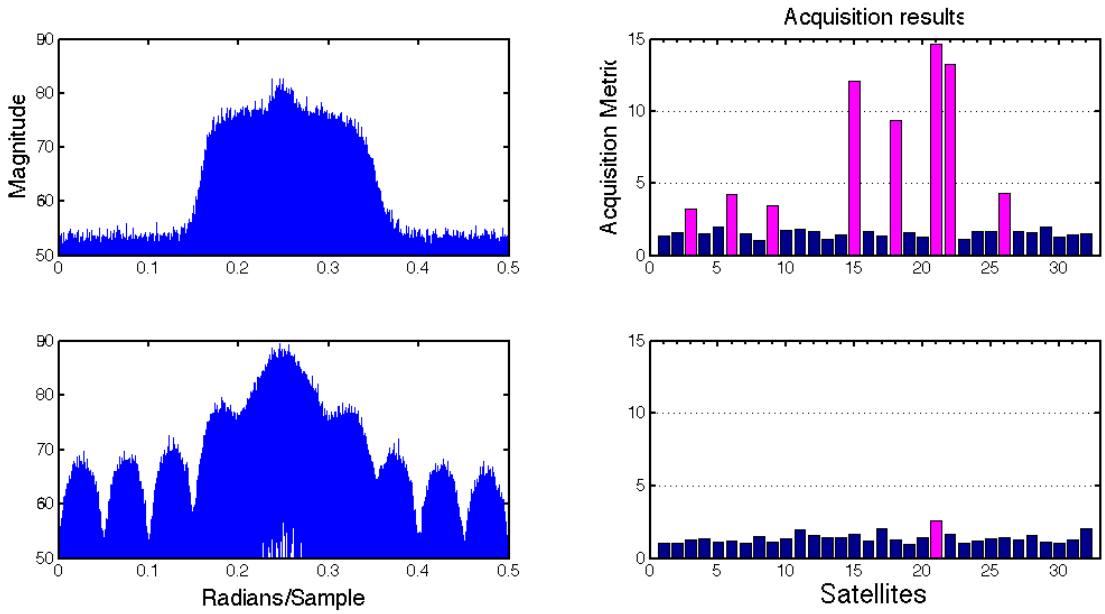

Figure 3.3: Wide band jamming interference testing results

3.3 Multi-path

3.3.1 Multi-path model

GPS multi-path effects occur when reflected satellite signals (from some reflection obejcts around the target GPS antenna) combine with the direct satellite signal. These delayed reflection GPS signals affect the measurements accuracy of GPS receivers. Multi-path interference is usually considered to be a main measurement error source in many GPS receivers. A variety of techniques, such as narrow correlator spacing, have been developed to detect and to mitigate multi-path interference [15].

Figure 3.4 shows a simplified GPS multi-path interference generation model. The target GPS antenna receives not only the direct GPS signals from the GPS satellites, but also the reflected GPS signals by some reflection objects.

3.3.2 Multi-path simulation

The major parameters in the multi-path model are shown below:

1. Reflection location P_{mp}
   Since short delay multi-path interference is mostly seen in the real world, we only

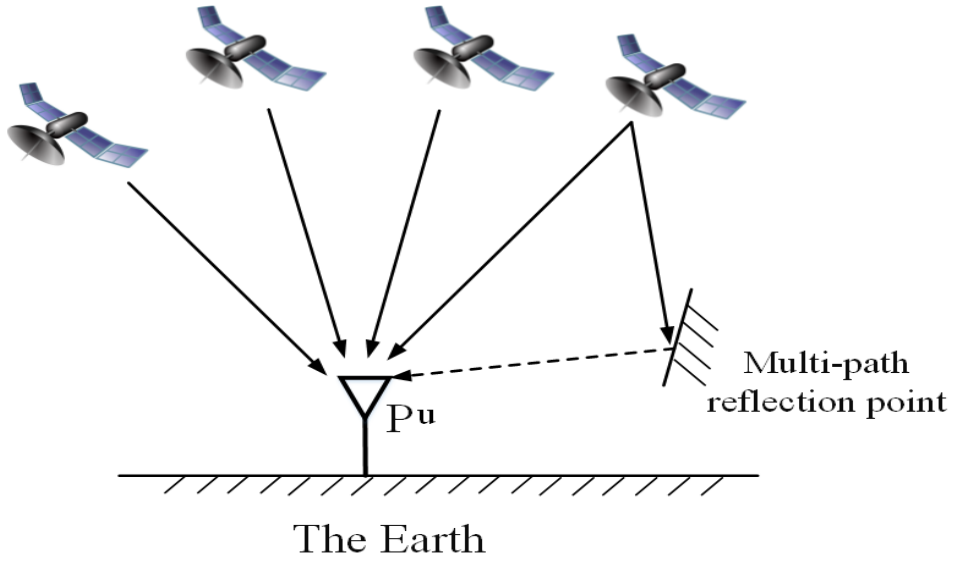

Figure 3.4: Simplified multi-path model

consider that P_{mp} is less than 10 km away from the target GPS receiver antenna position P^u in this thesis.

2. Reflection coefficient Γ
   For simplicity, we assume all the visible satellites have the same reflection coefficient.

As shown in Figure 3.4, in addition to the direct GPS satellite signal, the target GPS receiver also receives another delayed GPS signal, which is reflected by the object at location P_{mp}. We can consider the reflection object as some virtual receiver and transmitter. The reflection object first receives the clean GPS signal at the location P^u, which can be expressed as $s_{rec}(t; P^u)$. Then, the reflection object transmits this received signal $s_{rec}(t; P^u)$ to the target GPS receiver using the reflection coefficient as its transmitter antenna gain. The time delay between the receiving and transmission process is zero.

Suppose the distance between the target receiver and the reflection object is d, so the time delay from the reflection object to the target receiver is $\Delta t = \frac{d}{c}$.

Thus, the received signal by the target receiver can be expressed as:

$$s^{tar}(t; P^u) = s_{rec}(t; P^u) + l_{space} * \Gamma * s_{rec}(t - \Delta t; P_{mp}) \tag{3.5}$$

where l_{space} is the free spatial loss from P_{mp} to P^u and Γ is the reflection coefficient. $s_{rec}(t; P^u)$ is the direct signal from the GPS satellites received by the GPS antenna at location P^u, and $s_{rec}(t; P_{mp})$ is the direct signals received at the multi-path point P_{mp}.

The multi-path signal generation process is almost the same with the clean signal simulation except there are some reflected signals. If the simulator users do not define the reflection

coefficient, then simulator will default the reflection coefficient to be zero, which means there are not multi-path interferences.

3.3.3 Experimental results

1. Simulator settings

   - antenna location $P^u = L(37.230^o, -80.414^o, 640)$
   - multi-path location $P_{mp} = L(37.230^o, -80.415^o, 650)$
   - $\Gamma = 0.8$

   All the other simulator settings are the same with the experiments of chapter 2, such as antenna gain and simulation time.

2. Testing results
   As shown in Figure 3.5, when the multi-path interference is switched on, the softGNSS receiver can still acquire the same GPS satellites but suffers some power loss. This is reasonable considering the existence of the reflected GPS signals, which might be out of phase with the direct GPS signals. We also find that the extra navigation error by the multi-path interference varies from tens of meters to hundreds of meters. As shown in Figure 3.6, the navigation error is about 230 m, which is much larger than the navigation error when using the clean GPS signals.

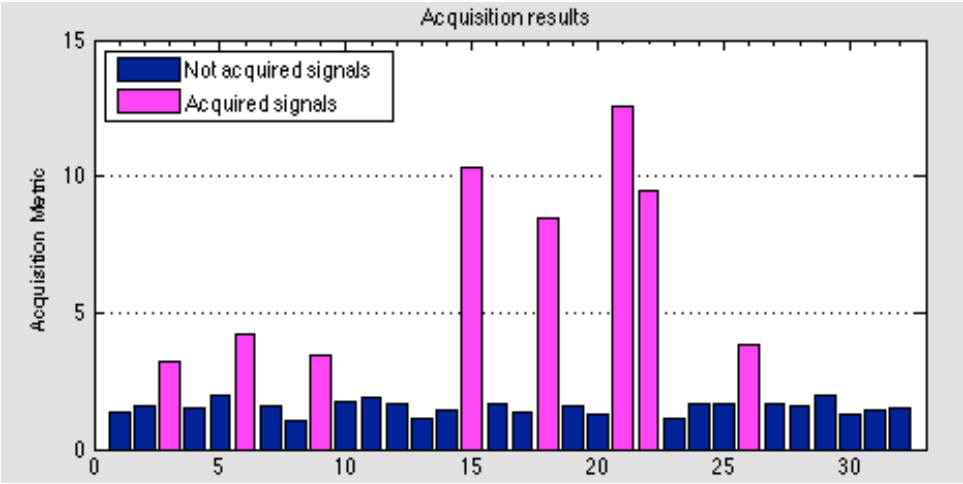

Figure 3.5: Acquired satellites with multi-path

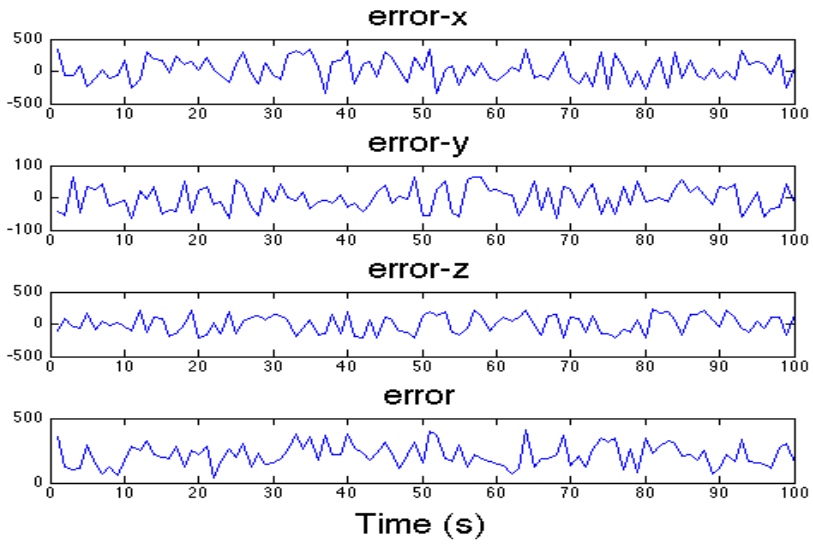

Figure 3.6: Navigation errors with multi-path interference

3.4 Spoofing

3.4.1 Spoofing model

Spoofing is a deliberate interference, which is used for bamboozling GPS receivers into generating some specified fake location. The spoofing attack is potentially causing more serious menace than jamming since the target GPS receiver can hardly detect its existence. Recently the implementation of sophisticated spoofers has become more feasible and less costly due to rapid advances in software-defined radio (SDR) technology.

The spoofing process can be generalized as the scenario shown in Figure 3.7. The spoofer first receives the real GPS signals in some location P_{sp}, and then transmits this received signal at some other location P_{bro}. Usually, the spoofer may introduce some time delay before it broadcasts the received real GPS signal to the target GPS receiver. In addition, the spoofer might also amplify the received signal before it transmits it to the target GPS receiver user.

3.4.2 Spoofing simulation

The important parameters in the spoofing signal simulation are listed as following:

- target GPS location P^u
- spoofer receiver location P_{fake}

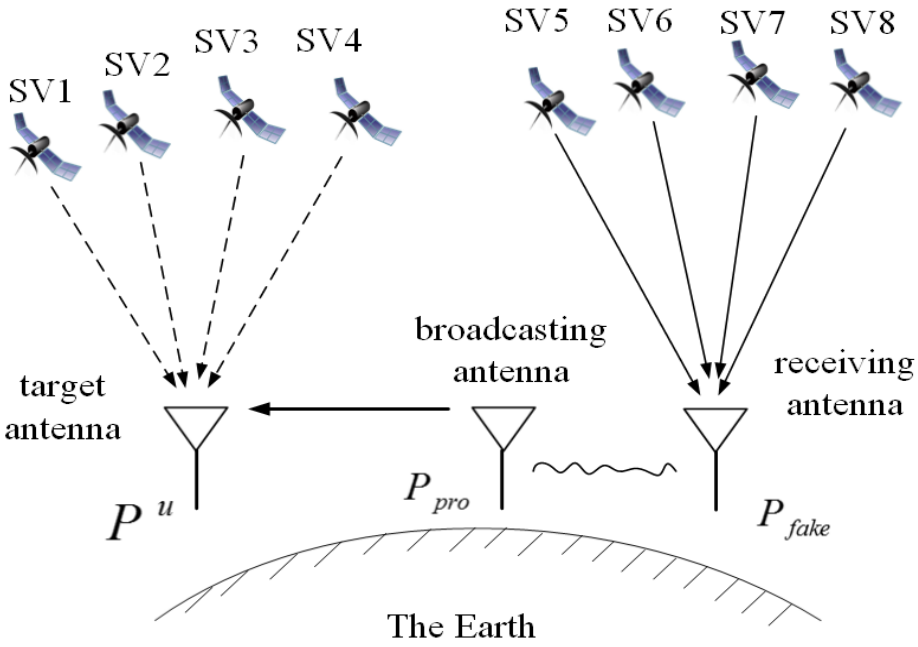

Figure 3.7: Spoofing model

- spoofer transmitter location P_{bro}
- spoofer transmitter gain $gain_{sp}$
- time delay between spoofer transmitter and spoofer receiver ΔT

At location P_{fake}, the received real GPS signals can be expresses as $s_{rec}(t; P_{fake})$.

Thus, at the spoofer transmitter location P_{bro}, the transmitting signal can be expressed as:

$$s_{bro}(t) = gain_{sp} * s_{rec}(t - \Delta T; P_{fake}) \tag{3.6}$$

When the transmission signal arrives at the target GPS receiver, the spoofing interference signal can be written as:

$$J(t) = \alpha_{sp} * s_{bro}(t - \delta t) \tag{3.7}$$

Where δt is the time delay from P_{bro} to P_u, and α_{sp} is the free space power loss from P^{bro} to P^u.

Thus, the received signals by the target GPS receiver can be written as:

$$s^{tar}(t) = J(t) + s_{rec}(t; P^u) \tag{3.8}$$

Where $s_{rec}(t; P^u)$ stands for the real GPS signal received by the target GPS receiver at location P^u.

3.4.3 Experimental results

1. Simulator settings

   - target antenna location $P^u = L(37.230^o, -80.414^o, 640)$
   - spoofer receiver location $P_{fake} = L(37.271^o, -79.941^o, 304)$
   - spoofer transmitter location $P_{bro} = L(37.130^o, -80.409^o, 640)$
   - spoofer transmitter antenna gain $gain_{sp} = 30$ dB
   - time delay $\Delta T = 1$ hour

2. Testing results

   - As shown in Figure 3.8, when the spoofing interference is turned off, the acquisition results of the testing softGNSS receiver are almost the same with the clean GPS signals.
   - As shown in Figure 3.9, when the spoofing interference is switched on, the testing softGNSS receiver acquires 6 GPS satellites. While these satellites are totally different with the satellites in Figure 3.8, and these satellites are actually the visible satellites at location P_{fake} one hour ago.
   - The target GPS receiver has been falsified to acquire the spoofing GPS signals, which are actually collected at location P_{fake}, and the navigation results is pointing around P_{fake} instead of its own location P^u. As we can see from Figure 3.10, the target GPS receiver suffers a bigger measure error (around 25 m) using the P_{fake} as the reference location.

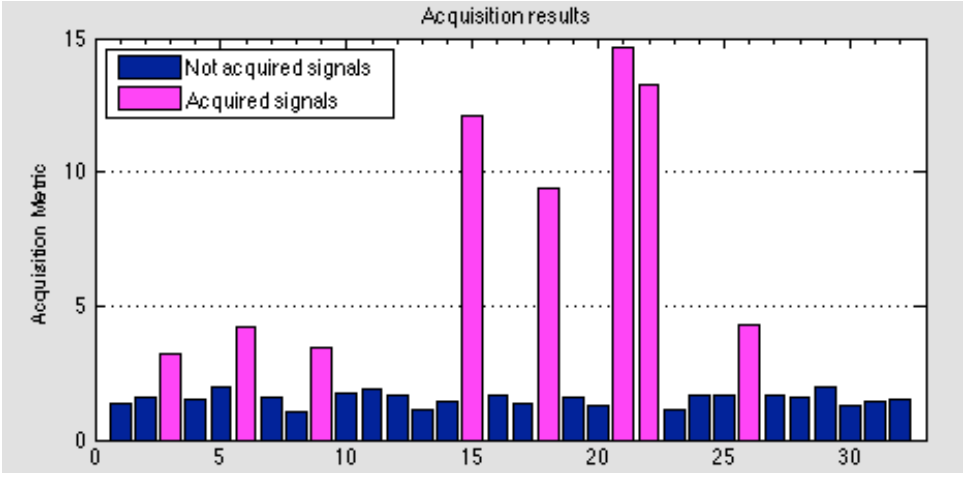

Figure 3.8: Acquisition results without spoofing interference

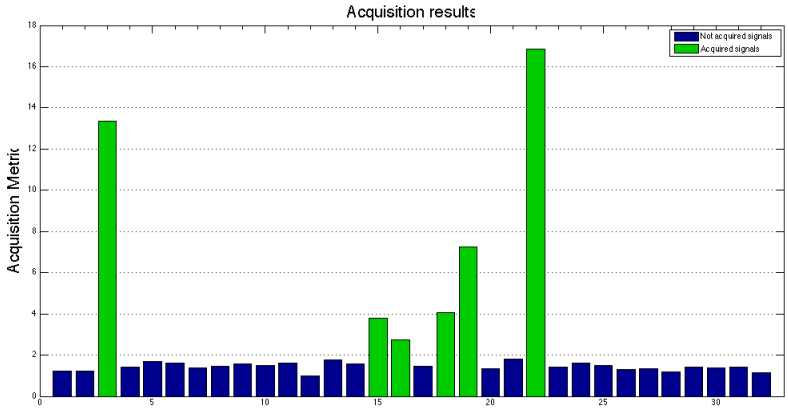

Figure 3.9: Acquisition results with spoofing interference

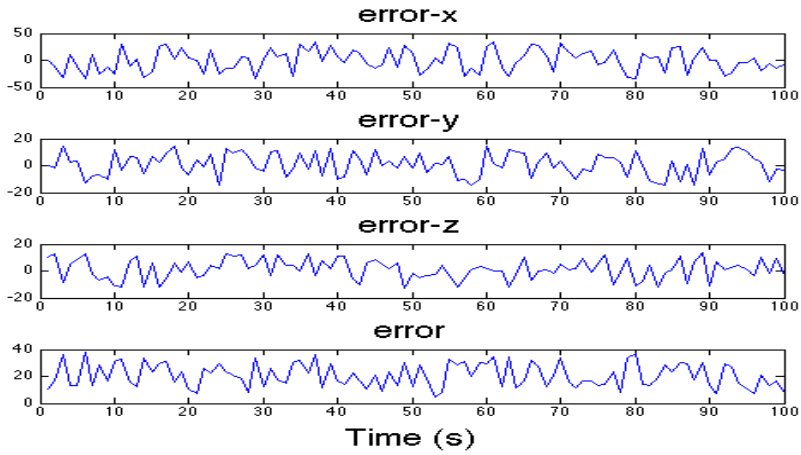

Figure 3.10: Navigation errors (around P_{fake}) with spoofing interference

3.5 Summary

In this chapter, we discuss in detail how the GPS simulator generates some typical interference signals, such as jamming, multi-path, and spoofing, which can be potentially useful in analyzing security issues in GPS receivers. We also show examples to demonstrate that this simulator can generate these polluted GPS signals successfully.

Chapter 4

GPS signal simulation for multiple antennas

In this chapter, we discuss how to simulate both clean and polluted GPS signals for multiple antennas simultaneously. We show these simulator functionalities using a planar smart antenna as an example.

4.1 GPS signal simulation for smart antenna

Using multiple antenna is a very useful anti-interference approach in the GPS receiver community [16]. Figure 4.1 shows a typical smart antenna, which is comprised of nine antenna units for anti-interferences in GPS receivers. These nine antenna units are evenly separated with a distance of half wavelength. Suppose we set up the coordination system using the antenna array plane as the XOY plane, and set the position of antenna $ant(0,0)$ as the original place. For the convenience to explain in the following part, we will call this coordinate system as the planar coordinate system because the antenna array lies in the XOY plane. Since all these antenna units are evenly separated with distance of $\frac{\lambda}{2}$, hence for each antenna $ant(i,j)$, its position in the planar coordinate system is

$$Q^{ant(i,j)} = (\frac{i\lambda}{2}, \frac{j\lambda}{2}, 0) \tag{4.1}$$

where $0 \leq i, j \leq 2$, and λ is the wavelength of the GPS signals.

As we discussed in chapter 2, in our GPS simulator system, we actually use the Earth Coordinate System, which is centered at the idealized Earth center.

In this Earth Coordinate System, the position of antenna $ant(0,0)$ is

$$P^{ant(0,0)} = L(lat_0, lon_0, hgt_0) = (x_0, y_0, z_0)$$

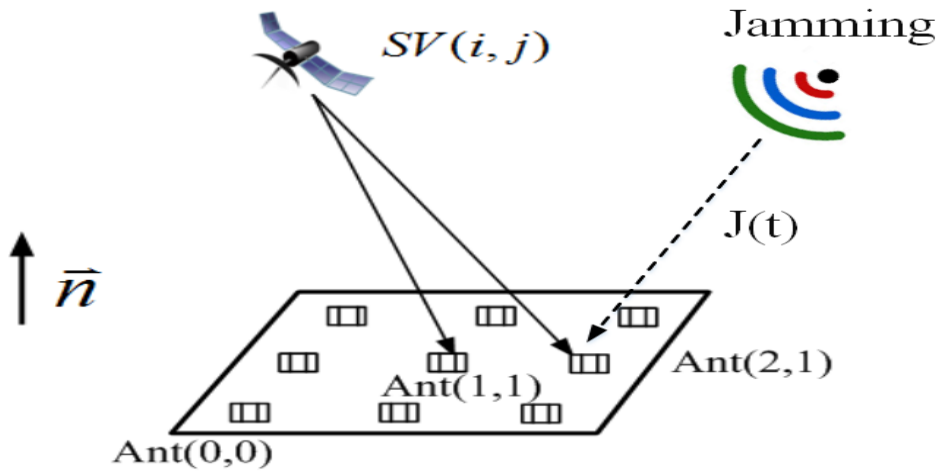

Figure 4.1: Nine units smart antenna

where

$$x_0 = (R_{earth} + hgt_0)cos(lat_0)cos(lon_0) \tag{4.2}$$
$$y_0 = (R_{earth} + hgt_0)cos(lat_0)sin(lon_0) \tag{4.3}$$
$$z_0 = (R_{earth} + hgt_0)sin(lat_0) \tag{4.4}$$

For simplicity, we can assume the normal vector of the antenna plane is $\overrightarrow{n} = (x_0, y_0, z_0)$. Hence, the pending question remains how can we find the positions of all the antenna units in the Earth Coordinate System given each antenna's position in the planar coordinate system?

The Earth Coordinate System can be generated from the planar coordinate system through some linear transformations. For any point A of position $Q(x, y, z)$ in the planar coordinate system, we suppose its position in the Earth Coordinate System is $P(x''', y''', z''')$. We can get the (x''', y''', z''') through the following transforms:

1. Step 1
   Rotate along OX axis with a rotation angle of lat_0, thus
$$x' = x \tag{4.5}$$
$$y' = y * cos(lat_0) - z * sin(lat_0) \tag{4.6}$$
$$z' = y * sin(lat_0) + z * cos(lat_0) \tag{4.7}$$
2. Step 2
   Rotate along OZ axis with a rotation angle of lon_0, thus
$$x'' = x' * cos(lon_0) - y' * sin(lon_0) \tag{4.8}$$
$$y'' = x' * sin(lon_0) + y' * cos(lon_0) \tag{4.9}$$
$$z'' = z' \tag{4.10}$$

3. Step 3
   Shift the original point to (x_0, y_0, z_0), thus,

$$x''' = x'' + x_0 \tag{4.11}$$
$$y''' = y'' + y_0 \tag{4.12}$$
$$z''' = z'' + z_0 \tag{4.13}$$

To summarize, we can get the following transformational relationship between the planar coordinate system and the Earth Coordinate System.

$$\begin{pmatrix} x''' \\ y''' \\ z''' \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & cos(lat_0) & -sin(lat_0) \\ 0 & sin(lat_0) & cos(lat_0) \end{pmatrix} \begin{pmatrix} cos(lon_0) & -sin(lon_0) & 0 \\ sin(lon_0) & cos(lon_0) & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \tag{4.14}$$

As we discussed in chapter 2, once each antenna unit's location $P^{ant(i,j)}$ in the Earth Coordinate System is given, the simulator can generate the simulated GPS signal, $s_{rec}(t; P^{ant(i,j)})$ for that antenna unit. We can think each antenna unit in the smart antenna as an independent stand alone antenna.

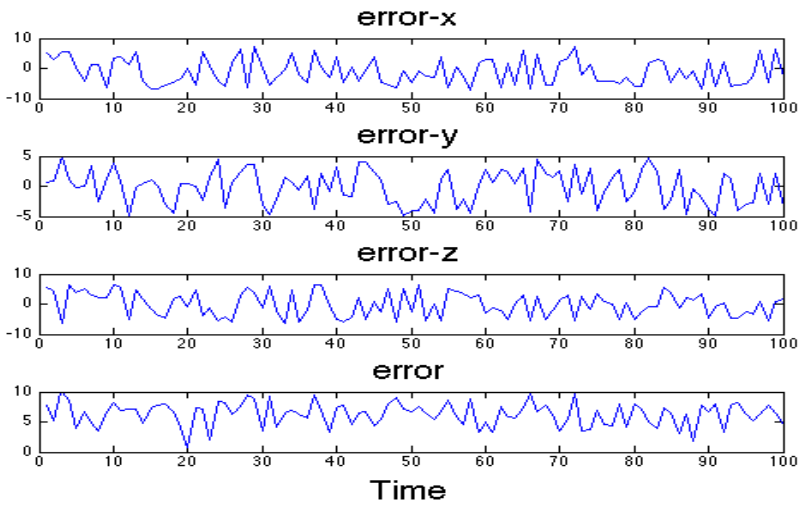

Figure 4.2: Antenna $ant(1, 2)$ navigation results

As an example, we also assume that antenna $ant(0, 0)$ position is $L(37.230^o, -80.414^o, 640)$ in Blacksburg, VA. Figure 4.2 shows the navigation results when using antenna $ant(1, 2)$ alone. The average navigation error is about 9.2 m, which means when using our simulated signals, the GPS receiver achieves similar positioning accuracy with real GPS signal. For the other eight antennas, we get similar position results, which we do not show here.

4.2 Interference simulation for smart antenna

As we discussed before, multiple antenna units are mainly used to enhance the GPS receiver anti-interference capability by applying some sophisticated signal processing algorithms. As with the stand alone antenna, when the interference model is enabled, each antenna unit receives the simulated GPS signal as well as the interference signals. Since the generation of the interference signal is quite similar with the descriptions in chapter 3, we will not discuss the interference signal generation here.

Suppose the jamming signal is $J(t)$, for each antenna $ant(i,j)$, the simulated signal can be expressed as:

$$s^{ant(i,j)}(t) = s_{rec}(t; P^{ant(i,j)}) + \alpha_{jam(i,j)} * J(t - \Delta t(i,j)) \tag{4.15}$$

where $\alpha_{jam(i,j)}$ is the signal free space loss, and $\Delta t(i,j)$ is time delay from jamming source to the antenna.

As an example, we also assume that there is some wide band interference source located at $L(37.141^o, -80.408^o, 2000)$ in Christiansburg, VA. The interference source's transmission power is about $20W$, and the signal bandwidth is about 3.8 MHz.

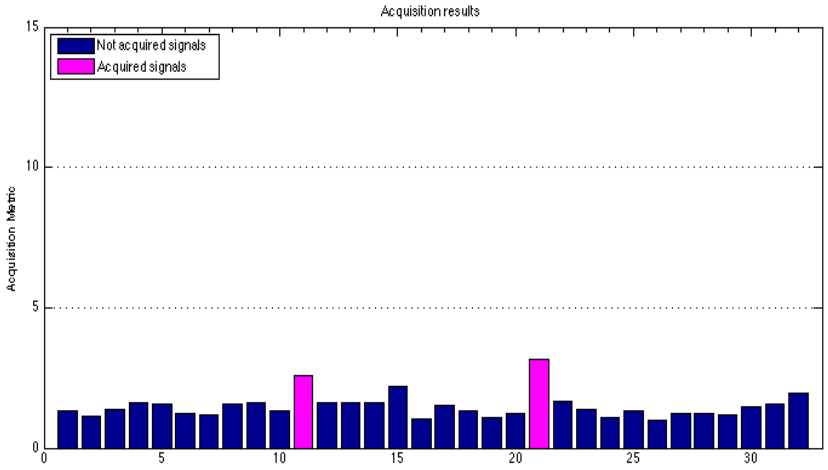

Figure 4.3: Antenna $ant(1,2)$ acquisition results

As shown in figure 4.3, when the wide band jamming signal is switched on, no single antenna unit in the smart antenna can acquire enough GPS satellites for position computing because of the existence of the strong wide band interference signals.

To further verify if the signal received by the smart antenna works correctly, we apply the power inversion (PI) algorithms [17] to mitigate the interference signals from the jamming source located in Christiansburg, VA. The PI algorithm tries to minimize the interference in

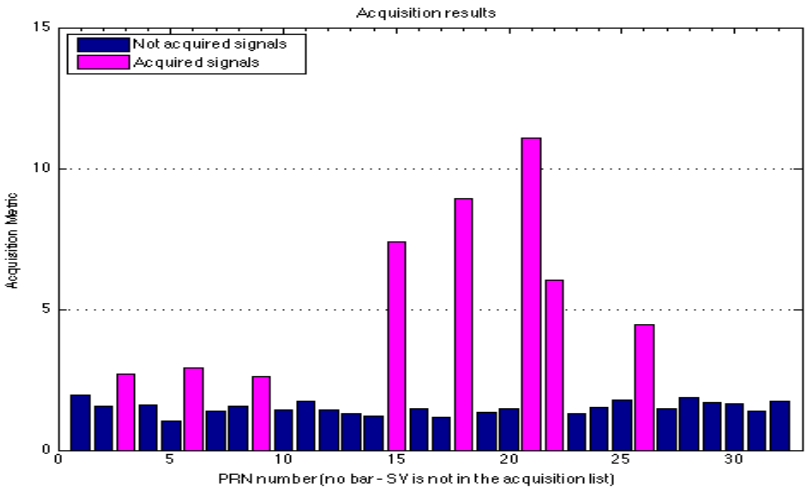

Figure 4.4: Acquisition results with PI algorithm

the direction of the strong jamming. In our example, we first use PI algorithm to process the nine units smart antenna GPS signals, and then input these processed GPS signals to the testing software defined receiver. As shown in figure 4.4, after applying the PI algorithm, the receiver can re-capture at least four satellites for positioning, which means that these simulated GPS signals for multiple antennas are generated correctly.

4.3 Summary

In this chapter, we use the planar smart antenna as an example to present the simulator's functionalities to generate GPS signals for multiple antennas simultaneously. The core problem of these functionalities is to compute each antenna's location in the Earth Coordinate System. We solve this problem through some linear transformations between coordinate systems. When given each antenna's location, the simulator can simulate clean as well as polluted GPS signals for that antenna like the stand alone antenna. The testing results show that our simulator is able to produce GPS signals very well for multiple antennas.

Chapter 5

Conclusion and future work

In this chapter, we draw our conclusion about our simulator, and then briefly give out our future work directions.

5.1 Conclusion

The GPS system dependent communication system has been increasingly deployed in nearly every corner of our daily lives. However, due to the intrinsic hole nature of GPS signals, GPS receivers are extremely prone to be interfered by some unintentional or intentional interference signals. During recent years, researchers are paying more attention to addressing the security issues in GPS receivers.

GPS simulator plays a critical role in developing and testing the GPS receivers. It provides control over the signals generated over the global test environment, so that testing can be conducted in well-controlled laboratory conditions. Using simulators facilitates several stages of research and product development, including requirements analysis, design and development, integration, production, maintenance, and support.

Unfortunately, the current commercial GPS simulators suffer the following important problems:

1. Not cost efficient.
   The simulator designers pay a lot of attention to modeling the extremely complicated error sources in GPS signals. These are actually unnecessary for some researchers, especially those who are focusing on the security issues in GPS receivers. Modeling those extremely complex error sources always means some powerful computation hardware resource is required in the simulator system, and hence a quite expensive simulator price is unavoidable.

2. Not security research oriented.
   Most of the current GPS signal simulators provide very little flexibility for the researchers to generate abnormal GPS signals, such as jamming, multi-path, and spoofing interference signals. However, these typical polluted GPS signals are actually of extreme value for some researchers. This is especially true because it is relatively easy to capture clean GPS signals, while it is quite difficult to capture the polluted GPS signals in our real world.

To address the problems about the GPS signal simulator, in this thesis, we design a software defined signal simulator using Matlab language (about 3200 lines of code). Our experimental results show that the simulator meets our design objectives. The functionalities of the simulator are summarized as follows:

1. The simulator is completely designed by software, which makes it cost efficient and flexible. The simulator users only need to provide some basic configuration parameters, such as antenna location, simulation time, interference model, etc. To generate different simulated GPS signals, the users only need to change the setting configuration files.

2. It is able to generate the simulated GPS signals for the stand alone antenna, and the simulated signals have the same positioning accuracy as the real GPS signals.

3. It provides the interface for the simulator users to generate GPS interference signals, such as jamming, multi-path, and spoofing. These features are critically important to the researchers who are concerned about the security issues of the GPS signals.

4. It can generate GPS signals for multiple antennas, simultaneously. In addition to generating the clean GPS signals, the simulator is also able to generate the typical polluted GPS signals for multiple antennas. Those features can facilitate researchers to develop and test sophisticated smart antenna algorithms. Another potential application area of those features is the wireless networks system, where tons of GPS receiver sensors are deployed.

5.2 Future work

The simulator we design in this thesis meets our research objectives, while there is still room for improvement. Our future work directions are summarized as follows:

1. Since we make some assumptions about the GPS system to reduce the design complexity, the navigation messages definition in the simulated GPS signals is not exactly the same with the real GPS system. In the near future, we are going to make the simulated signal have the same navigation messages definition with the real GPS signals. In this way, the simulator can be 100 percent compatible with the real GPS receivers.

2. Currently, the simulator can only generate GPS signals in L1 frequency band. Considering the fast development of the global navigation satellite system (GNSS), it is quite necessary to enhance the simulator's capability to generate more modern GNSS navigation signals, such as the GPS L2C[2], GLONASS civil signals.

3. We are going to optimize the simulator speed performance. The current speed performance of our simulator hardly meets the real-time testing requirements.

Bibliography

[1] A. Dempster, "How vulnerable is GPS?" *Transportation*, 2001.

[2] G. ICD, "Navstar GPS space segment/navigation user interfaces, interface specification," IS-GPS-200E, Tech. Rep., 2010.

[3] E. D. Kaplan and C. J. Hegarty, *Understanding GPS: principles and applications*. Artech house, 2005.

[4] G. Xie, "Principles of GPS and receiver design," *Publishing House of Electronics Industry, Beijing*, vol. 7, 2009.

[5] S. Ifune, "Global positioning system satellite signal simulator," Mar. 3 1992, US Patent 5,093,800.

[6] O. Michel, "Webotstm: Professional mobile robot simulation," *International Journal of Advanced Robotic Systems*, 2004.

[7] O. Julien, B. Zheng, L. Dong, and G. Lachapelle, "A complete software-based if GNSS signal generator for software receiver development," in *Long Beach: ION GNSS 17th International Technical Meeting of the Satellite Division*, 2004, pp. 2146–2157.

[8] B. M. Hannah, "Modelling and simulation of GPS multipath propagation," 2001.

[9] A. Brown, J. Redd, and M.-A. Hutton, "Simulating GPS signals - it doesn't have to be expensive," in *GPS World*, 2012.

[10] K. Borre, *A software-defined GPS and Galileo receiver: a single-frequency approach*. Springer, 2007.

[11] A. Pinker and C. Smith, "Vulnerability of the GPS signal to jamming," *GPS Solutions*, vol. 3, no. 2, pp. 19–27, 1999.

[12] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *ION GNSS*, 2005, pp. 13–16.

[13] F. Dovis, L. Musumeci, N. Linty, and M. Pini, "Recent trends in interference mitigation and spoofing detection," *International Journal of Embedded and Real-Time Communication Systems (IJERTCS)*, vol. 3, no. 3, pp. 1–17, 2012.

[14] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, 2012.

[15] W. Hedgecock, M. Maroti, J. Sallai, P. Volgyesi, and A. Ledeczi, "High-accuracy differential tracking of low-cost GPS receivers," *11th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys 2013). Taipei, Taiwan: ACM, Jun*, 2013.

[16] D. S. De Lorenzo, J. Gautier, J. Rife, P. Enge, and D. Akos, "Adaptive array processing for GPS interference rejection," in *Proceedings of the 18th International Technical Meeting of the Satellite Division of the Institute of Navigation*, 2005, pp. 618–627.

[17] D. Meng, Z. Feng, and M. Lu, "Anti-jamming with adaptive arrays utilizing power inversion algorithm," *Tsinghua Science & Technology*, vol. 13, no. 6, pp. 796–799, 2008.