A Civilian GPS Position Authentication System

A DISSERTATION
SUBMITTED TO THE FACULTY OF THE GRADUATE SCHOOL
OF THE UNIVERSITY OF MINNESOTA
BY

Zhefeng Li

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
Doctor of Philosophy

Demoz Gebre-Egziabher

June, 2013

Acknowledgements

First and foremost, I would like to thank my advisor, Professor Demoz Gebre-Egziabher, for giving me the opportunity to work on this interesting research field. He gave me the most freedom in the research. His research attitude driven by his enthusiasm always inspires me to discover new areas. I would also like to thank him for the many valuable remarks and suggestions. Furthermore I would like to thank Professor Gary Balas for offering me the great opportunity to work in the UAV group. I would like to express my appreciation to Professor Peter Seiler and Professor Mihailo Jovanovic for their time spent on reading my dissertation and for their advices. I also owe great thanks to Professor Yiyuan Zhao and Professor Max Donath for their insightful comments as members of my Preliminary Oral Examination committee. I would like to thank Professor Tom Posbergh for his support and help in FPGA code development.

I would like to thank my colleagues in the navigation group, Zhiqiang Xing, Guijing Zhen, Susmita Bhattacharyya, Chen-chi Chu, F. Adhika Pradipta Lie, Hamid Mokhtarzadeh, Chandra Tjhai, for all the interesting discussions with them. I would also like to thank all my other friends who gave me great memories in all these years.

I would like to thank the United States Department of Homeland Security for supporting this work through the National Center for Border Security and Immigration under grant number 2008-ST-061-BS0002.

Last but not least, I would like to thank my parents: Zhengjian Li, Shenfeng Chen for their love and encourage without which this thesis would not have been possible.

Dedication

This work is dedicated to my father and mother

Abstract

A position authentication system utilizing the white noise like GPS spreading codes as tamper proof watermarks is developed. Position authentication as used here means the process of checking whether position reports made by a remote user are truthful and accurate. In the method proposed, a segment of the GPS signal collected by a trusted user (called the authenticator) is used as a template. Another user's (called the supplicant) GPS signal is compared with the template to judge if the user's position and time report is authentic. A pseudorandom noise sequence in the GPS signal (the P(Y) code) is used as a watermark in this process. An analysis to explain how noise affects the watermark signal detection is presented. This is done by casting the problem into a standard estimation and detection framework. A cross-correlator based watermark signal detector-estimator is constructed. This is different from the traditional match filter because the noisy template of the authenticator is used in this detector-estimator. The effect of the noisy template on the performance of the estimator is analyzed. An important practical implementation issue, namely, multiple false peaks caused by C/A power leakage which mask the detection of the watermark is analyzed. A method for suppressing these false peaks is developed. A pair of prototype receivers to validate this concept are constructed. Experimental results using these receivers show that the authentication method proposed can detect deceptive position report and the resolution of the position authentication is at or better than 15 meters. This method may also be used in other GNSS system, for example Galileo, by utilizing the encrypted Public Regulated Service signal as the watermark signal.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Overview

This thesis deals with the problem of position authentication. The term "position authentication" as discussed in this thesis is taken to mean the process of checking whether position reports made by a remote user are truthful (i.e., is the user where they say they are?) and accurate (i.e., in reality how close is remote user to the position they are reporting?). Many emergent aviation and commercial applications will benefit from a position authentication system. For example, in the future National Airspace System (NAS) of the United States known as NextGen [1], some air traffic control services will be based on aircraft using Global Navigation Satellite Systems (GNSS) such as the United States' GPS or the European Union's Galileo to determine their position. Then using a data-link such as ADS-B they will report their positions to air traffic control and other nearby aircraft. In this application an incorrect or false position report, regardless of whether it was intentional or malicious, can have severe consequences. Examples of commercial applications that would benefit from authentication are tamper-free shipping concepts aimed at enhancing the safety and efficiency of commercial cargo shipment across national borders.

There are many commercial fleet and asset tracking systems available in the market, such as *FleetMatics* [2], *WirelessMatrix* [3], etc. Most of these tracking systems depend on a GPS receiver installed on the cargo or asset to obtain a real-time location (and/or velocity) information. The location and the time when the asset was at a particular

location form the tracking message which is sent back to a monitoring center to verify if the asset is traveling in an expected manner.

Whether we are tracking cargo/asset or an airplane in the air traffic control system, this method of tracking can be depicted graphically as shown in Figure 1.1. The approach shown in Figure 1.1 is susceptible to at least two potential fault modes which can lead to erroneous tracking of the vehicle or asset. The first scenario occurs when an incorrect position solution is calculated as a result of GPS RF signal abnormalities (e.g. GPS signal spoofing [4]). The second scenario occurs when the correct position solution is calculated but the tracking message is tampered with during the transmission from the asset being tracked to the monitoring center. The first scenario is a falsification of the sensor and the second scenario is a falsification of the transmitted position report. In this paper we use the term "supplicant" and "authenticator", respectively to describe the entity making the position report and the entity validating the report. In [4] [5], the GPS signal spoofing is described and an in-line spoofing detector integrated with the GPS receiver is introduced as a solution for dealing with this challenge. The in-line detector can detect the sensor falsification described above at the supplicant end but it cannot solve the report falsification problem at the authenticator end.

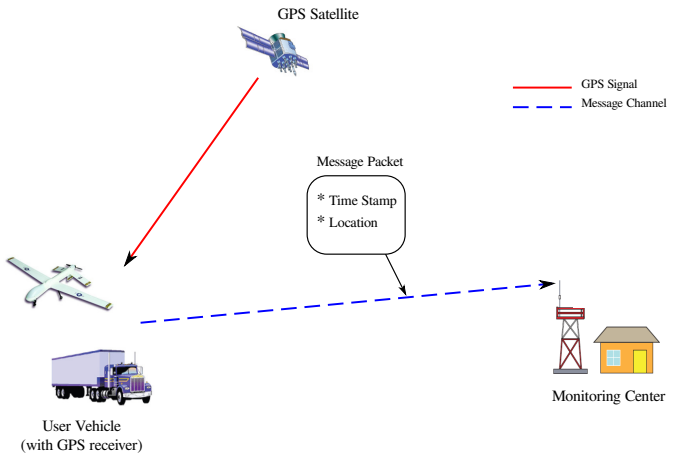

Figure 1.1: Typical asset tracking system

The purpose of this thesis is to examine the problem at the authenticator end. This thesis proposes an authentication system utilizing the white noise like spreading codes

of GPS to calculate an authentic position based on a snapshot of raw IF signal from the receiver. The system considered in this thesis is based on the idea first presented in [6] and utilizes features of the GPS signal as tamper-proof watermarks to detect deceptive or erroneous position reports.

1.2 Prior Research

In [7] a survey of various GNSS authentication methods is presented. In [6] a method to determine whether a user is utilizing authentic GPS signals based on the idea of a watermark is introduced. The method proposed uses a segment of noisy P(Y) signal (not code) collected by the authenticator as a template. The supplicant's GPS signal can be compared with the template signal to judge if the user's position and time reports are authentic. Correlating the supplicant's signal with the authenticator's copy of the signal recorded, yields a correlation peak which serves as a watermark. An absent correlation peak implies that the GPS signal provided by the supplicant is not genuine. This process is called *signal authentication*.

Relative to *position authentication*, a correlation peak that occurs earlier or later than predicted (based on the supplicant's reported position) indicates a false position report. The work in [5] identified some practical implementation challenges that must be addressed before the authentication approach outlined above can be practically implemented. The purpose of this thesis is, in part, to address these potential implementation issues. Most notably it discusses the so-called "C/A power leakage problem." Furthermore while [5] only addressed the sensor falsification problem, the work discussed here addresses the report falsification problem as well. It also provides a detailed exposition of the signal processing theory behind GPS authentication. That is, it provides a solid estimation theory grounding to the adhoc approach discussed in [6].

1.3 Problem Statement

There are other approaches proposed to deal with the GNSS authentication problem. One of them is to design a new GNSS signal structure where an authentication field is embedded. When the receiver receives the signal, it verifies if the authentication field

is true to decide whether the navigation message being used to calculate the position is genuine. However, this feature is not available in any of the existing GNSS systems. The European Union's Galileo has a plan to incorporate this authentication feature in its signal [8] but whether or not such a system will be fully deployed when the system becomes operational is unknown. There is also some GPS research suggesting that such an authentication field should be incorporated into the future GPS signals. However, there is no plan to deploy this proposed signal structure in the foreseeable future [6]. There are no published plans for the Russian Federation's GLONASS and the People's Republic of China's Beidou to implement this feature either. Thus, in the near future we can not expect a dedicated new GNSS signal to solve the authentication problem.

In view of the above, there is a need to design an authentication system that uses existing GPS signals. So the problem to be answered by this thesis is how do we do authentication using legacy signals of GPS? Furthermore can we make a system that will be backward compatible in future when new signals including authentication features are broadcast by GPS?

1.4 Thesis Contributions

This thesis develops a method for GPS position authentication based on the legacy L1 signal. To this end, this thesis makes the following contributions to the problem of GNSS position authentication:

1. It develops a method to mitigate the C/A power leakage problem in GPS L1 authentication. This problem is common for both the signal authentication and position authentication. Without this method, earlier proposed signal authentication methods can only reliably work when not more than one common satellite between the authenticator and the supplicant. It means that the authenticator and the supplicant have to be separated by a large distance. Using this method the authentication is able to authentic supplicants very close to the authenticator.

2. It develops a complementary position authentication method using the signal authentication measurements. Using the position authentication method, this system can tell not only if a supplicant's reported position is correct but also it

can calculate an authentic position even though the reported position is false or incorrect.

3. It develops a prototype GPS receiver suitable for the GPS position authentication problem. It is shown that using the developed receiver the accuracy of GPS position authentication are on the order of 15 meters or better.

4. It provides a rigorous analysis of factors that can affect the accuracy of the estimator used for the authentication problem. Stated differently, it provides the guideline to design optimal authenticators and supplicant for the GPS authenticator system.

1.5 Thesis Organization

The remainder of this thesis is organized as follows: Chapter 2 presents the theory behind GPS position authentication. It includes the characteristic of the watermark signal in GPS system, the C/A residual filter, the algorithm to calculate the authentic position using the signal authentication measurements. Chapter 3 provides a detailed analysis of the detection and estimation method used in authentication. It provides a systematic study of the detection and detection algorithm showing how various noises in the process affect the authentication results. To this end, the chapter first presents a model of the receiver noise. Next it develops a cross-correlator which is used to detect authentic GPS signals. The performance of this estimator-detector and the effect of various parameters have on the performances of the detection and estimation algorithm is discussed. In Chapter 4, results of experimental validation of the system is presented. This includes a description of the prototype receiver developed as part of this work. Finally, Chapter 5 summarizes the thesis findings and also provides recommendations for the future work.

Chapter 2

GPS Position and Time Authentication: Theory

This chapter describes the theory behind GPS position authentication. The idea of signal authentication and position authentication are first described. Next, the idea of using white noise sequences as watermarks is described. Then it is shown how the GPS P(Y) code can serve as a watermark. This is followed by a discussion of practical issues associated with detecting this watermark. Finally a method for position authentication is discussed.

2.1 Basics of Authentication

Signals used by a well-designed position authentication system should have features that are very hard to reproduce while simultaneously being able to uniquely encode a supplicant's location and time. In this case, the authentication process is reduced to detecting these features and checking if these features satisfy some constraints. These features are similar in function to the well-designed watermarks used to detect counterfeit currency.

A white noise process is a perfect watermark signal in the sense that it is impossible reproduce and predict.

A conceptual design of an authentication system that use a white noise process as a watermark is shown in Figure 2.1. Suppose we are interested in the detection of sensor falsification. In relation to Figure 2.1 this is the case where we are interested in knowing

whether the supplicant's receiver R_s is using a genuine signal from transmitter T_x and not an impostor (or spoofer) transmitter T_i. Receiver R_a is a trusted receiver that will perform the authentication. R_a is established so that it can continuously and securely receive the signal $V_x(t)$ from T_x.

The authentication process involves sending a snapshot of signal $V_s(t)$ received at R_s to the authenticator to compare it with the signal $V_a(t)$ received at R_a.

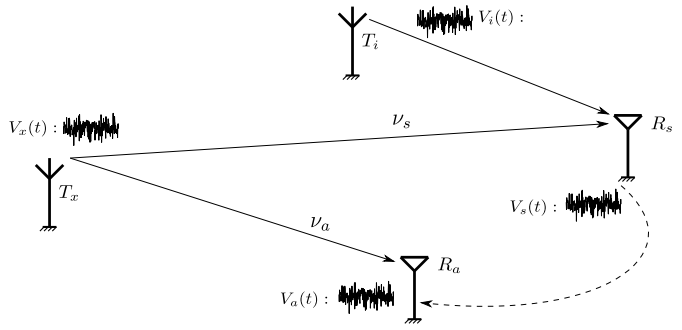

Figure 2.1: Architecture to detect a snapshot of a white noise

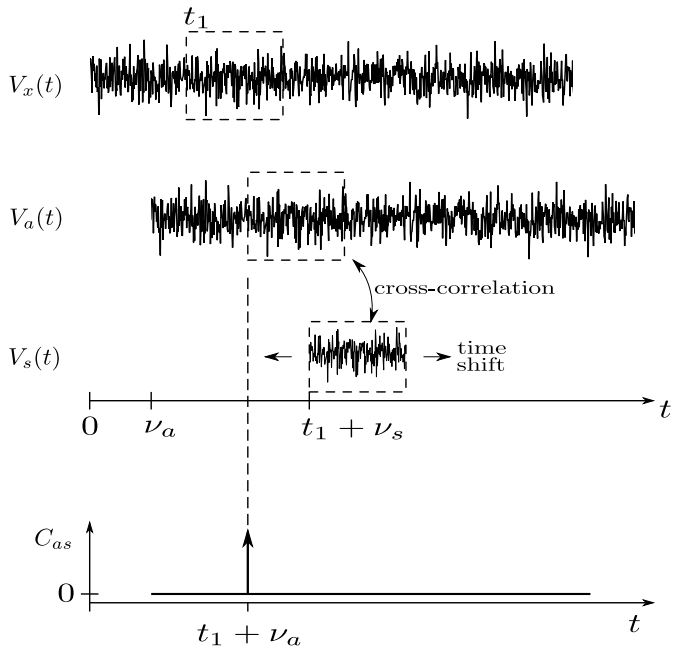

Figure 2.2: Signals of a white noise snapshot detection

Figure 2.2 shows how this works. We assume the transmitter and the receivers are ideal devices. That means there is no device noise in all the signals. The signal at R_a is a delayed version of signal transmitted from T_x. This delay ν_a is related to the distance between T_x and R_a. A snapshot signal as shown in the dashed box is transmitted at time t_1 from T_x. Because of the difference in traveling distances, this snapshot arrives at R_a and R_s at different times, $t_1 + \nu_a$ and $t_1 + \nu_s$, respectively. ν_s is the travel delay from T_x to R_s. Every time an authentication is performed, the snapshot signal from R_s is compared with a piece of the signal from R_a. If these two pieces of signal match, we can say the snapshot signal from R_s was truly transmitted from T_x. For the white noise signal, match detection is accomplished via a cross-correlation operation [9]. The cross-correlation between one white noise and any other signal is always zero. Only when the correlation is between the signal and its copy will the correlation have a non-zero value. In Figure 2.2, C_{as} is the cross-correlation between the snapshot from R_s and different pieces of signal from R_a. The time axis t denotes the start time of this selected piece from the signal of R_a. Note that the time when the correlation peak occurs provides additional information about the distance between R_a and R_s. The peak time $t_1 + \nu_a$ is before the snapshot time $t_1 + \nu_s$, so the distance between T_x and R_s is longer than the distance between T_x and R_a.

2.1.1 GPS Signal Watermarks

The RF carrier broadcasted by each GPS satellite is modulated by the Coarse Acquisition (C/A) code, which is known and can be processed by all users, and the encrypted P(Y) code, which can be decoded and used by Department of Defense (DoD) authorized users only. Both civilians and DoD authorized users see the same signal. To commercial GPS receivers the P(Y) code appears as noise. However, as discussed above, this noise can be used as a watermark which uniquely encodes locations and time. In a typical civilian GPS receiver's tracking loop as shown in Figure 2.3, this watermark signal can be found inside the tracking loop quadrature signal $Q_1(t)$.

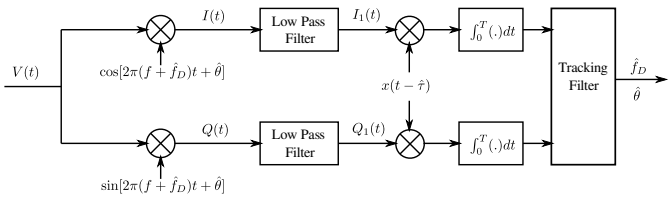

Figure 2.3: Watermark signal in a civilian receiver's tracking loop

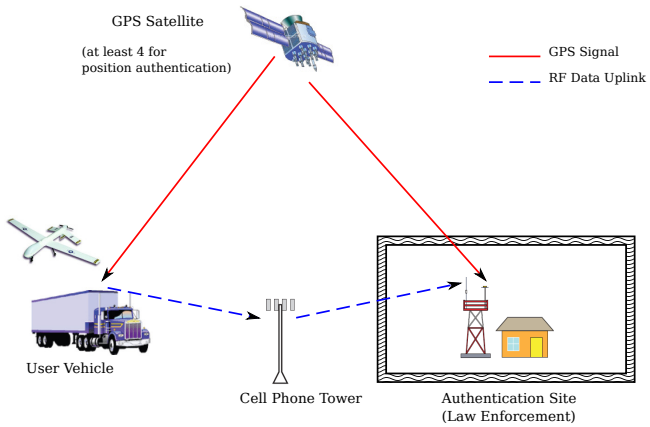

Figure 2.4: Architecture of position authentication system

2.2 Detecting the P(Y) Watermark Embedded

Figure 2.4 is the architecture of the position authentication system described in this thesis. In practice, we need a short snapshot of raw IF signal from the supplicant. This piece of the signal is the digitalized, down converted, IF signal before the tracking loops of a generic GPS receiver. Another information needed from the supplicant is the position solution and GPS time calculated by the supplicant using only the C/A signal. The raw IF signal and the position message are transmitted to the authenticator by a data-link such as a cell phone data network or a communication radio.

The authentication station keeps tracking all the common satellites the authenticator and the supplicant see. Every common satellite's watermark signal is obtained from its tracking loop. These watermark signals are stored into a signal database. Meanwhile the pseudorange between the authenticator and every satellite is also calculated and is stored into the same database.

When the authentication station receives the data from the supplicant, it converts the raw IF signal into the Q channel signals. In this step, the reported supplicant position is used to obtain the initial Doppler frequency and code shift of the raw IF signal. Then the supplicant's Q channel signal is used to perform the cross-correlation with the watermark signal in the database. If the correlation peak is found at the expected time, the supplicant's signal passes signal authentication test. By measuring the relative peak time of every common satellite, an authentic position can be obtained. The position authentication involves comparing the reported position of the supplicant to this calculated position. If the difference between two positions is in a pre-determined range, the reported position passes the position authentication.

The watermark signal of interest is embedded in the signal $Q_1(t)$ shown in Figure 2.3. The signal $Q_1(t)$ is the quadrature component of the signal being processed in a receiver tracking loop. The authentication process, in simple terms, involves performing a cross-correlation between a small snippet of $Q_1(t)$ from the supplicant with a history of $Q_1(t)$ saved by the authenticator. The $Q_1(t)$ signals from supplicant and authenticator must be carefully filtered because $Q_1(t)$ includes signals other than the watermark which affect the cross-correlation result between the $Q_1(t)$ signals from the authenticator and the supplicant. This effect is discussed in this section. To simplify the analysis, we assume that there are only two common visible satellites between the authenticator and the supplicant. The scenario where more than two common satellites are present is a simple extension of the results presented in this section.

The two common GPS satellites in view will be denoted as SVi where $i = 1, 2$. For SV1, the $Q_1(t)$ (in Figure 2.3) signal in the authenticator's tracking loop is mathematically described as:

$$\begin{aligned} V^a_{1Q}(t) =& \sqrt{2P^a_{y1}}Y_{D1}(t-\nu^a_1) + \sqrt{\frac{P^a_{c2}}{2}}X_{D2}(t-\nu^a_2)\sin\left[2\pi(\Delta f^a_2 + \Delta f^a_1)t + \Delta\theta^a_2 + \Delta\theta^a_1\right] \\ &- \sqrt{\frac{P^a_{c2}}{2}}X_{D2}(t-\nu^a_2)\sin\left[2\pi(\Delta f^a_2 - \Delta f^a_1)t + \Delta\theta^a_2 - \Delta\theta^a_1\right] \\ &+ \sqrt{\frac{P^a_{y2}}{2}}Y_{D2}(t-\nu^a_2)\cos\left[2\pi(\Delta f^a_2 - \Delta f^a_1)t + \Delta\theta^a_2 - \Delta\theta^a_1\right] \\ &- \sqrt{\frac{P^a_{y2}}{2}}Y_{D2}(t-\nu^a_2)\cos\left[2\pi(\Delta f^a_2 + \Delta f^a_1)t + \Delta\theta^a_2 + \Delta\theta^a_1\right] \\ &+ n^a_Q(t) \end{aligned} \tag{2.1}$$

where $n_Q^a(t)$ is the receiver noise $n^a(t)$ projected in the quadrature product (see Appendix A.1). The other variables in this equation are defined as follows where the superscripts "a" and "s" denote "authenticator" and "supplicant" signals, respectively. $x_i(t)$ is the C/A spreading code; $y_i(t)$ is the P(Y) spreading code; $D_i(t)$ is the navigation message; $X_{Di}(t)$ is $D_i(t)x_i(t)$; $Y_{Di}(t)$ is $D_i(t)y_i(t)$; P_{ci}^a is the received C/A signal power for SVi; P_{yi}^a is the received P(Y) signal power from SVi; ν_i^a is RF signal propagation delay for SVi; $\Delta f_i^a$is the Doppler frequency of SVi; $\Delta\theta_i^a$ is the phase shift of SVi. The equations for the supplicant are the same as (1) where we replace the superscript "a" with "s."

Now if we assume that the tracking loop is locked, then the C/A signal of SV1 is wiped off and, thus, absent in $Q_1(t)$. The P(Y) signal, however, will be present in $Q_1(t)$. Because usually $\Delta f_2^a \neq \Delta f_1^a$ and $\Delta\theta_2^a \neq \Delta\theta_1^a$, there will be other satellites' C/A and P(Y) signal residuals in this SV1 quadrature product. Furthermore, these residuals will be modulated by signals whose frequencies are functions of SV1 and SV2 Doppler. The frequency of this signal is much lower than the C/A and P(Y) code chipping rate.

If the authenticator and the supplicant have a common satellite, they both have the identical watermark signal in their quadrature products. The authenticator's version of the watermark is used as a template against which we compare the supplicant's watermark. We do this by first forming the cross-correlation between the authenticator and the supplicant signal

$$C_{1Q}(\tau, T) = \frac{1}{T}\int_0^T V_{1Q}^a(t)V_{1Q}^s(t-\tau)\mathrm{d}t \tag{2.2}$$

where T is the length of the signal snippet from the authenticator. The variable τ denotes the relative delay of the authenticator's signal relative to the supplicant's signal. If we substitute Equation (2.1) into Equation (2.2) and evaluate the integral, we find that $C_{1Q}(\tau, T)$ is the supperposition of three separate functions as shown below:

$$C_{1Q}(\tau, T) = C_{y1,y1}(\tau, T) + C_{x2,x2}(\tau, T) + C_{y2,y2}(\tau, T) \tag{2.3}$$

In this equation, $C_{y1,y1}(\tau, T)$ is the P(Y) code autocorrelation and its peak is the watermark we are looking for. If the supplicant signal includes the authentic GPS signal of common satellite SV1, $C_{1Q}(\tau, T)$ will have a peak at a specific delay value τ. The amplitude of this correlation peak is $\frac{1}{T}\sqrt{P_{y_2}^a P_{y_2}^s}$.

Our ability to detect the peak represented by $C_{y1,y1}(\tau, T)$, however, is tempered by the presence of the two false peaks $C_{x2,x2}(\tau, T)$ and $C_{y2,y2}(\tau, T)$ —SV2's P(Y) and C/A code autocorrelation functions, respectively. These functions are not necessarily equal to zero and unless we can remove them, they will interfere the authentication process. This is shown in Figure 2.5 which is a plot of $C_{1Q}(\tau, T)$ as a function of τ. In what follows, we will show why $C_{y2,y2}(\tau, T)$ (the P(Y) code false peak) and $C_{x2,x2}(\tau, T)$ (the C/A code false peak) are not always zero with a view to attenuating or eliminating their effect on $C_{1Q}(\tau, T)$.

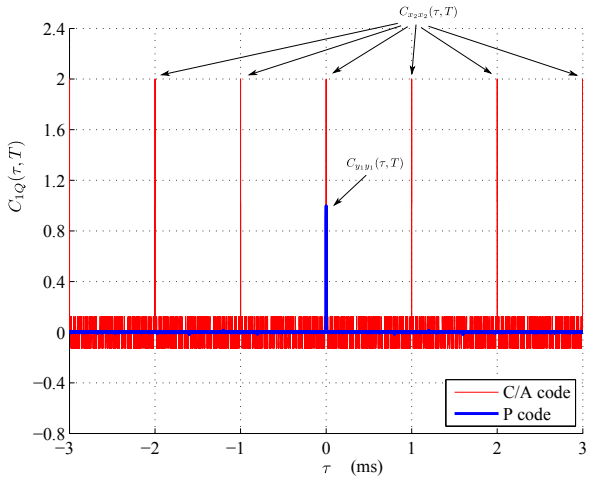

Figure 2.5: A plot of C_{1Q} as a function of τ

P(Y) False Peak $C_{y2,y2}(\tau, T)$

Recall that for the purpose of clarity we are assuming an idealized case where we are dealing with two satellites only and, thus, $C_{y2,y2}(\tau, T)$ represents the effect of only one other satellite. In reality we would be dealing with $\sum_{i=2}^{N} C_{y_i,y_i}$ where N is the total number of satellites in view. Furthermore, note that we are not dealing with the week long P(Y) code but a snippet of it. This means that the $C_{y2,y2}(\tau, T)$ is not the well known and understood P(Y) correlation function. That is, the partial correlation of the P(Y) code is different from the full length auto-correlation of one satellite's P(Y) code. Since the authenticator does not know in advance what portion of the P(Y) code

is transmitted from the supplicant, we treat the autocorrelation as a random variable and, thus, analyze its expectation. It can be shown that (see Appendix A.1 for details) the expectation of the cross correlation between two pieces of the P(Y) residual signal is given by:

$$E\{C_{y2,y2}(\tau,T)\} = \begin{cases} \frac{\sqrt{P^a_{y_2} P^s_{y_2}}}{4} \sum_{i=1}^{8} \text{sinc}(\pi\Omega_i T)\cos(\Psi_i) & \text{if } \tau = 0 \\ 0 & \text{otherwise} \end{cases} \tag{2.4}$$

where Ω_i and Ψ_i are given in Table A.1. Furthermore, $\text{sinc}(x) = \frac{\sin(x)}{x}$.

From Equation (2.4), we can identify the conditions when $C_{y2,y2}(n,T) \neq 0$. This occurs when $\tau = 0$, but $\sum_{i=1}^{8} \text{sinc}(\pi\Omega_i T)\cos(\Psi_i) \neq 0$. To minimize $C_{y2,y2}(\tau,T)$, we can either choose T so that $\Omega_i T \gg 1$ or choose bigger Ω_is. The maximum T is limited by the dynamics of the authenticator and the supplicant. Unless we are dealing with a static supplicant, T can not be longer than a few milliseconds. That means that the only degree of freedom we have then are Ω_i and Ψ_i. Examining the variables definition in Table A.2 we see that Ω_i and Ψ_i are functions of the GPS signal Doppler and phase shifts seen by the supplicant and authenticator. Thus by ensuring sufficient geographic separation between the two we can attenuate $C_{y2,y2}(\tau,T)$.

The ratio between the true peak and the false peak depends on the received power ratio. If $P^s_{y_2} P^a_{y_2} > P^s_{y_1} P^a_{y_1}$, the false peak may be greater than the true peak. The analysis above considers the scenario where two common satellites are in view. When there are more than two common satellites, there may be multiple P(Y) peaks. This will be discussed more later in the thesis.

C/A Code False Peak $C_{x2,x2}(\tau,T)$

It can be shown that the C/A code false peak is given by:

$$E\{C_{x2,x2}(\tau,T)\} = \begin{cases} \frac{\sqrt{P^a_{x_2} P^s_{x_2}}}{4} \sum_{i=1}^{8} \text{sinc}(\pi\Omega_i T)\cos(\Phi_i) & \text{if } \tau = 0 \\ 0 & \text{otherwise} \end{cases} \tag{2.5}$$

The auto-correlation function of a C/A code ($X_{D2}(t)$ in Equation (2.5) above) is a periodic function [10]. Its period is 1 ms and in the absence of noise, its maximum

value is 1 for $\tau = 0, 1, 2, ...,$ ms. This means that $C_{x2,x2}(\tau, T)$ will have periodic peaks. Unlike what was done for $C_{y2,y2}(\tau, T)$, however, we cannot rely on geometric separation between supplicant and authenticator to ensure that Ω_i and Φ_i assume values which make $C_{x2,x2}(\tau, T) = 0$. This is because the period of the C/A code is short (1 ms in time or 300m in space). This means that for a given pair of Ω_i and Φ_i, $C_{x2,x2}(\tau, T)$ peaks will occur for separation between supplicant and authenticator that are equal to integer multiplies of 300 meters. A practical way to deal with this problem of C/A signal strength "leaking" into V_{1Q} is to use a digital filter as discussed next.

2.3 C/A Residual Filter

The C/A signal energy in the GPS signal is about double the P(Y) signal energy ($P_{x_1} \approx 2P_{y_1}$). So the C/A false peaks $C_{x2,x2}(\tau, T)$ are higher than the P(Y) peak we are interested in detecting ($C_{y2,y2}(\tau, T)$). The C/A false peaks are greater in number as will and, thus, in the presence of noise, it is difficult to identify the true peak.

A high-pass filter is introduced as a practical way to address the problem and simulation results will show the performance of this filter. We resort to simulation because the P(Y) code is unavailable to us. In the simulation we use P code instead to study the random characteristics of the watermark signal. Experimental results presented later in the thesis confirm that conclusions derived from using the P code in designing this filter are valid.

Because the C/A code is known, a match filter can be designed for a GPS satellite to filter out its C/A signal from the Q channel signal (e.g.V^s_{1Q}, V^a_{1Q}) to be used for detection. In this way, one match filter is needed for every satellite in the common view of the authenticator and the supplicant. The drawback of the match filtering method is that many match filters (one for each SV) are needed. A simpler approach is to filter the C/A signal residual in the Q channel signal. In the frequency domain, the energy of the base band C/A signal is mainly (56%) in $\pm$1.023 MHz band, while the energy of the base band P code is spread over a wider band of$\pm$10.23 MHz band. A high-pass filter can be applied to V^a_{1Q} and V^a_{1Q} to filter out the signal energy in the $\pm$1.023 MHz band. In this way, all satellites' C/A signal energy is attenuated by one filter rather than separate match filters for different satellites.

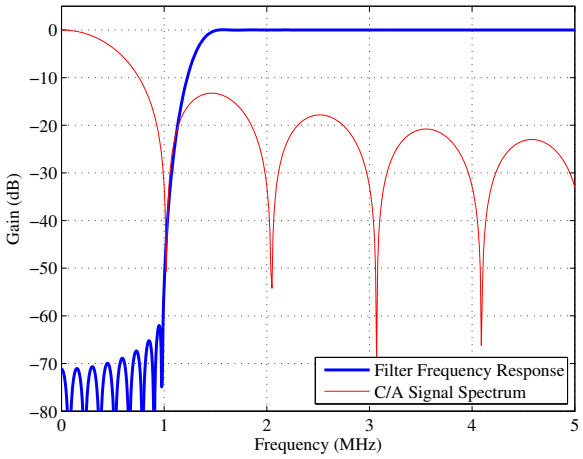

Figure 2.6: Frequency response of the notch filter

Figure 2.6 is the frequency response of a high-pass filter designed to filter out the C/A signal energy. The spectrum of the C/A signal is also plotted in Figure 2.6. The high-pass filter only filters out the main lobe of the C/A signals. Because the spectrum of the C/A and the P codes overlap in ±10.23 MHz band, the high-pass filter also attenuates part of the P code energy. This degrades the auto-correlation peak of the P code and can affect our ability to detect $C_{y1,y1}(\tau, T)$. This implies must be optimized in same way and a metric for determining its optimality must be defined. To this end note that even though the gain of the high-pass filter is the same for both the C/A code and the P code signals, its effect on their auto-correlation is different. That is because the percentage of the low frequency energy of the C/A code signal is much higher than that of the P code signal. The objective of the high-pass filter is to obtain the greatest *false-peak rejection ratio*. The *false-peak rejection ratio* is defined as the ratio between the peak value of P code auto-correlation and that of the C/A code auto-correlation. From Figure 2.5 we see that the *false-peak rejection ratio* of the non-filtered signals is 0.5. If we assume the worst case scenario (C/A false peaks have the maximum amplitude), then the cut-off frequency of the high-pass filter is a parameter to be optimized to achieve a desired *false-peak rejection ratio*.

Figure 2.7 is the comparison of the auto-correlation peak values using the filter in Figure 2.6. The auto-correlation peak of the non-filtered P code is normalized to

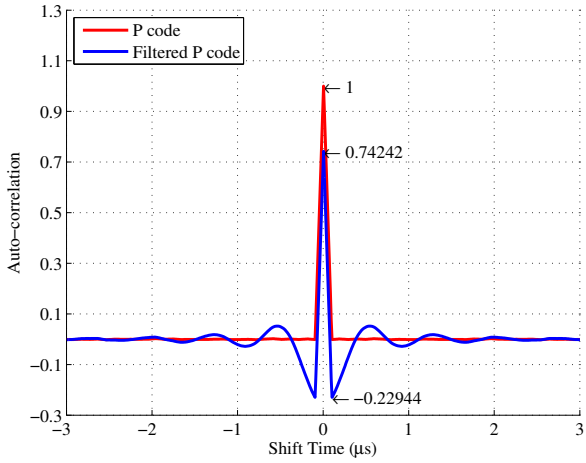

Figure 2.7: P code auto-correlation (filtered vs. non-filtered)

1. The peak of the filtered P code using the same scale is degraded by about 25%. The attenuation of the cross-correlation is shown in Figure 2.8. The cross-correlation amplitude of the filtered P code signal is also attenuated by about 25% compared with the non-filtered P code signal.The auto-correlation peak value of the filtered C/A code signal and that of the filtered P code signal is plotted in Figure 2.9. While the P code signal is attenuated by about 25%, the C/A code signal is attenuated by 91.5% (non-filtered C/A auto-correlation peak is 2). Thus, the *false-peak rejection ratio* is boosted from 0.5 to 4.36 by using the high-pass filter. The simulation results in this section show that one simple high-pass filter rather than multiple match filters can be designed to achieve an acceptable *false-peak rejection ratio*.

2.4 Position Calculation

Consider the situation depicted in Figure 2.10 where the authenticator and the supplicant have multiple common satellites in view. In this case, not only can we perform the *signal authentication* earlier described but also obtain an estimate of the pseudorange information from the authentication. Thus the authenticated pseudorange information can be further used to calculate the supplicant's position if we have at least three estimates of pseudoranges between the supplicant and GPS satellites. This position solution

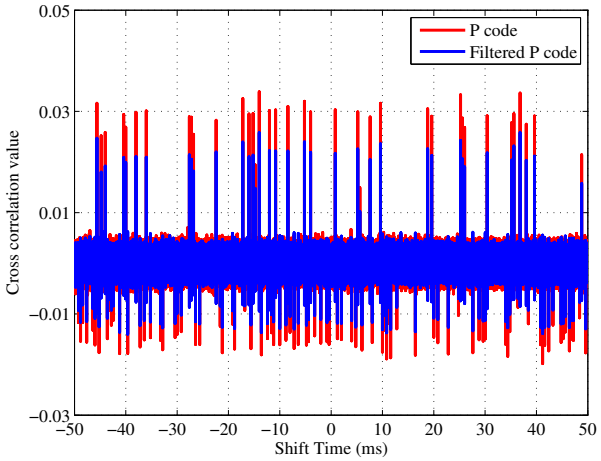

Figure 2.8: P code cross-correlation (filtered vs. non-filtered)

of the supplicant is based on the P(Y) watermark signal rather than the supplicant's C/A signal. Since it is based on the P(Y) watermark, this position solution must be an authentic solution. By comparing this authentic position with the reported position of the supplicant, we can authenticate the GPS position of the supplicant.

Figure 2.11 shows how the pseudorange information can be obtained during the signal authentication process. Let us assume that the authenticator and the supplicant have 4 common GPS satellites: SV1, SV2, SV3 and SV4. The signals transmitted from satellites at time t are $S_1(t), S_2(t), S_3(t)$, and $S_4(t)$, respectively. Suppose a signal broadcast by SV1 at time t_0 arrives at the supplicant at $t_0 + \nu_1^s$ where ν_1^s is the travel time of the signal. At the same time signals from SV2, SV3 and SV4 are received by the supplicant. Let us denote the travel time of these signals as ν_2^s, ν_3^s and ν_4^s, respectively. These same signals will be received at the authenticator. We will denote the travel times for the signals from satellite to authenticator as ν_1^a, ν_2^a, ν_3^a and ν_4^a.

The signal at a receiver's antenna is the superposition of the signals from all the satellites. This is shown in Figure 2.11 where a snapshot of the signal received by the supplicant at GPS time $t_0 + \nu_1^s$ includes GPS signals from SV1, SV2, SV3 and SV4. Note that even though the arrival times of these signal is the same, their transmit times (i.e., the time they were broadcast from the satellites) are different because the different ranges. Then signals received by the supplicant at GPS time $t_0 + \nu_1^s$ are

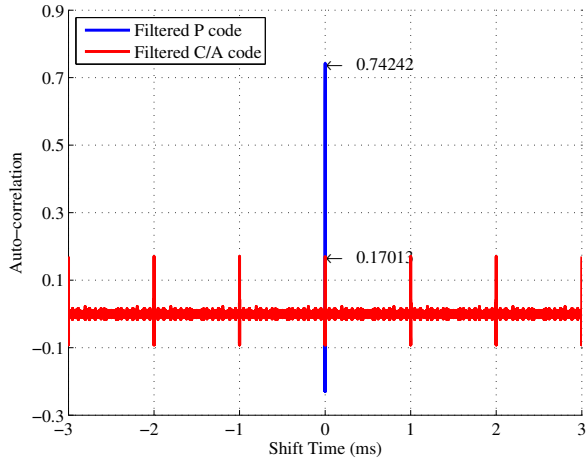

Figure 2.9: Auto-correlation of filtered codes

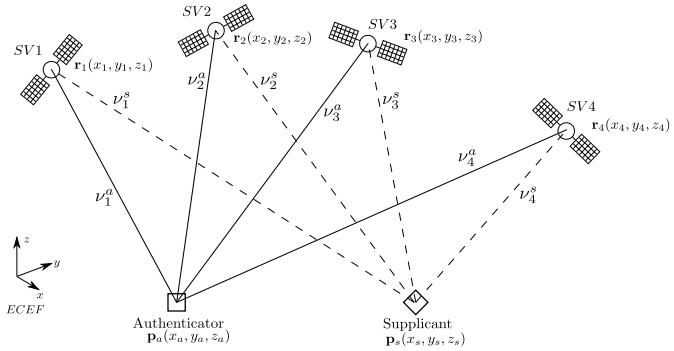

Figure 2.10: Positioning using watermark signal

$S_1(t_0)$, $S_2(t_0+\nu_1^s-\nu_2^s)$, $S_3(t_0+\nu_1^s-\nu_3^s)$ and $S_4(t_0+\nu_1^s-\nu_4^s)$. If these same snapshots of the signals at the supplicant are used to detect the matched watermark signals from SV1, SV2, SV3 and SV4 at the authenticator, the peaks time should occurs at GPS time $t_0+\nu_1^a$, $t_0+\nu_1^s-\nu_2^s+\nu_2^a$, $t_0+\nu_1^s-\nu_3^s+\nu_3^a$ and $t_0+\nu_1^s-\nu_4^s+\nu_4^a$.

Let t_{21} be the measured peak time delay between SV2 and SV1 measured at the authenticator. Similarly let t_{31} be the measured peak time delay between SV3 and SV1; and let t_{41} be the measured peak time delay between SV4 and SV1. Mathematically,

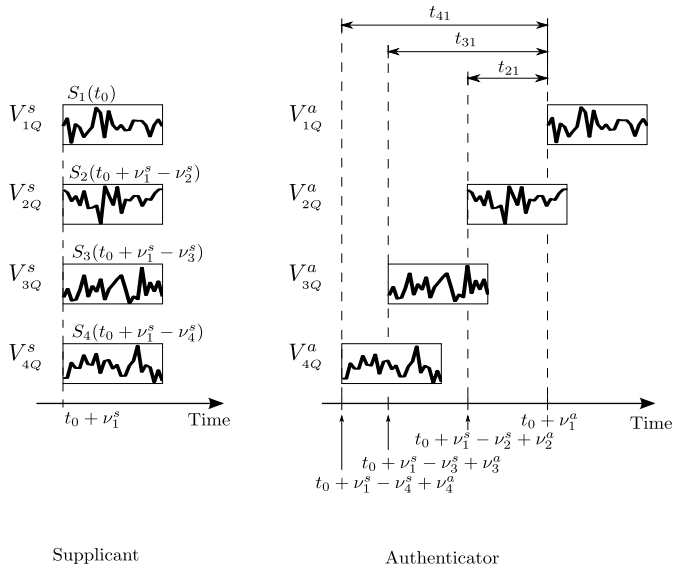

Figure 2.11: Relative time delays

these delays can be written as:

$$\begin{aligned} t_{21} &= t_0+\nu^s_1-\nu^s_2+\nu^a_2-(t_0+\nu^a_1) &&= (\nu^a_2-\nu^a_1)-(\nu^s_2-\nu^s_1) \\ t_{31} &= t_0+\nu^s_1-\nu^s_3+\nu^a_3-(t_0+\nu^a_1) &&= (\nu^a_3-\nu^a_1)-(\nu^s_3-\nu^s_1) \\ t_{41} &= t_0+\nu^s_1-\nu^s_4+\nu^a_4-(t_0+\nu^a_1) &&= (\nu^a_4-\nu^a_1)-(\nu^s_4-\nu^s_1) \end{aligned} \tag{2.6}$$

If the receiver has no noise, the travel time ν^i_k of a signal from a satellite k to a receiver i is

$$\nu^i_k = \frac{\rho^i_k}{c} + I^i_k + T^i_k \tag{2.7}$$

where ρ^i_k is the pseudorange between the k^{th}satellite and the i^{th} receiver, c is speed of light, I^i_k is the ionospheric delay between SV_k and i^{th} receiver; and T^i_k is the tropospheric delay between SV_k and the i^{th} receiver.

Using Equation (2.7), we can rewrite Equation (2.6) as

$$\begin{aligned} t_{21} &= \frac{1}{c}\left[(\rho^a_2-\rho^a_1)-(\rho^s_2-\rho^s_1)\right]+(I^a_2-I^a_1)-(I^s_2-I^s_1)+(T^a_2-T^a_1)-(T^s_2-T^s_1) \\ t_{31} &= \frac{1}{c}\left[(\rho^a_3-\rho^a_1)-(\rho^s_3-\rho^s_1)\right]+(I^a_3-I^a_1)-(I^s_3-I^s_1)+(T^a_3-T^a_1)-(T^s_3-T^s_1) \\ t_{41} &= \frac{1}{c}\left[(\rho^a_4-\rho^a_1)-(\rho^s_4-\rho^s_1)\right]+(I^a_4-I^a_1)-(I^s_4-I^s_1)+(T^a_4-T^a_1)-(T^s_4-T^s_1) \end{aligned} \tag{2.8}$$

Define the atmospheric correction item in the peak delay between satellite k and j as

$$\chi_{kj} = (I_k^a - I_j^a) - (I_k^s - I_j^s) + (T_k^a - T_j^a) - (T_k^s - T_j^s) \tag{2.9}$$

then Equation (2.8) can be written as

$$\begin{aligned} t_{21} &= \frac{1}{c}[(\rho_2^a - \rho_1^a) - (\rho_2^s - \rho_1^s)] + \chi_{21} \\ t_{31} &= \frac{1}{c}\left[(\rho_3^a - \rho_1^a) - (\rho_3^s - \rho_1^s)\right] + \chi_{31} \\ t_{41} &= \frac{1}{c}\left[(\rho_4^a - \rho_1^a) - (\rho_4^s - \rho_1^s)\right] + \chi_{41} \end{aligned} \tag{2.10}$$

In practice, the measurement of relative delays (i.e., t_{21}, t_{31} or t_{41}) always has noise. For example, the measured peak delay of t_{21} is

$$\hat{t}_{21} = t_{21} + \delta t_{21} \tag{2.11}$$

where δt_{21} is the noise in the measurement. This noise is caused by the clock error and signal alignment error. Since the peak time delay is only measured over a very short time interval, only the short time stability or noise of the supplicant's and the authenticator's clocks contribute to the measurement error. This noise leads to an offset (bias) in the peak detection time. We call this offset time as the *alignment error*.

In addition, the oscillators of the supplicant and authenticator receivers are not synchronized. This results in the supplicant's and the authenticator's reconstructions of the signal from the satellite being slightly different as depicted in Figure 2.12. So any measurement based on differencing the signals from the supplicant and the authenticator will have an additional error. We call this error the *signal reconstruction error* and is also included in the term δt_{21}. Increasing the sampling frequency minimizes this error.

Referring to Figure 2.10 again, suppose the authenticator's position $\mathbf{p}_a = (x_a,\, y_a,\, z_a)$ is known but the supplicant's position is unknown and needs to be determined. Because the actual position of the authenticator is known, each of the ρ_k^a is known. The positions of common satellites are also known to the authenticator. Rearranging Equation (2.10) by moving the unknown variables to the left side and putting the measurements on the

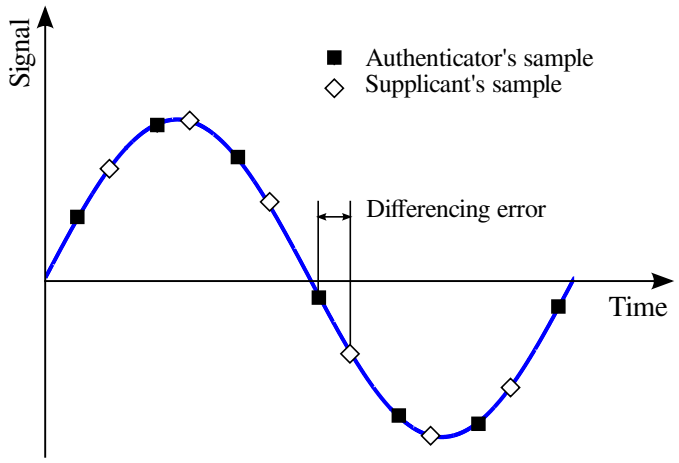

Figure 2.12: Clock differencing error

right side, we obtain

$$\begin{aligned}
\rho_2^s - \rho_1^s &= \rho_2^a - \rho_1^a - ct_{21} + c\chi_{21} \\
\rho_3^s - \rho_1^s &= \rho_3^a - \rho_1^a - ct_{31} + c\chi_{31} \\
\rho_4^s - \rho_1^s &= \rho_4^a - \rho_1^a - ct_{41} + c\chi_{41}
\end{aligned} \tag{2.12}$$

where ρ_i^s for $i = 1, 2, 3, 4$ is given by:

$$\rho_i^s = \sqrt{(x_i - x_s)^2 + (y_i - y_s)^2 + (z_i - z_s)^2} \tag{2.13}$$

Equation (2.12) is a system of three equations in three unknowns. The unknowns are the components of the supplicants position vector $\mathbf{p}_s = [x_s, y_s, z_s]^T$. This equation can be linearized and then solved using least squares techniques. When linearized (see Appendix B.1 for details) the equations have the following form:

$$\mathbf{A}\delta\mathbf{p}_s = \delta\mathbf{m} \tag{2.14}$$

where $\delta\mathbf{p}_s$ is given by $\delta\mathbf{p}_s = [\delta x_s, \delta y_s, \delta z_s]^T$, which is the estimation error of the supplicant's position. The matrix $\mathbf{A}$ is given by

$$\mathbf{A} = \begin{bmatrix} \hat{\mathbf{e}}_2^T - \hat{\mathbf{e}}_1^T \\ \hat{\mathbf{e}}_3^T - \hat{\mathbf{e}}_1^T \\ \hat{\mathbf{e}}_4^T - \hat{\mathbf{e}}_1^T \end{bmatrix} \tag{2.15}$$

where $\hat{\mathbf{e}}_i$ is the line of sight vector from the supplicant to the i^{th} satellite as depicted in Figure 2.13. Finally, the vector $\delta\mathbf{m}$ is given by:

$$\begin{bmatrix} \delta m_1 \\ \delta m_1 \\ \delta m_3 \end{bmatrix} = \begin{bmatrix} \hat{\mathbf{e}}_2^T \delta\mathbf{r}_2 - \delta\rho_2^a + c\delta t_{21} - c\delta\chi_{21} - \hat{\mathbf{e}}_1^T \delta\mathbf{r}_1 + \delta\rho_1^a \\ \hat{\mathbf{e}}_3^T \delta\mathbf{r}_3 - \delta\rho_3^a + c\delta t_{31} - c\delta\chi_{31} - \hat{\mathbf{e}}_1^T \delta\mathbf{r}_1 + \delta\rho_1^a \\ \hat{\mathbf{e}}_4^T \delta\mathbf{r}_4 - \delta\rho_4^a + c\delta t_{41} - c\delta\chi_{41} - \hat{\mathbf{e}}_1^T \delta\mathbf{r}_1 + \delta\rho_1^a \end{bmatrix} \tag{2.16}$$

where $\delta\mathbf{r}_i$ is the i^{th} satellite's position error, $\delta\chi_{ij}$ is the ionospheric error of χ_{ij} (defined in (2.9)) and $\delta\rho_i^a$ is the measurement error of pseudorange ρ_i^a.

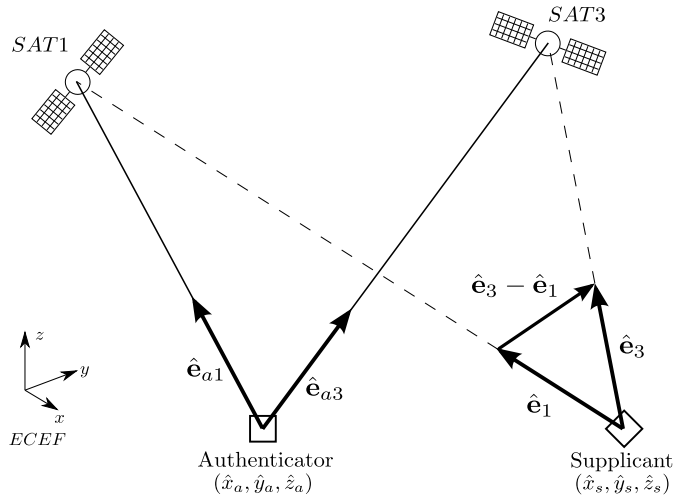

Figure 2.13: Line of sight vectors

Equation (2.14) is a standard form which can be solved by a weighted least squares (WLS) method. The solution is

$$\delta\mathbf{r}_s = (\mathbf{A}^T\mathbf{R}^{-1}\mathbf{A})^{-1}\mathbf{A}^T\mathbf{R}^{-1}\delta\mathbf{m} \tag{2.17}$$

where $\mathbf{R}$ is the covariance matrix of the measurement error vector $\delta\mathbf{m}$. From Equation (2.14) (2.17), we can see that the supplicant's position accuracy depends on both the geometry and the measurement errors.

2.4.1 Measurement Covariance Matrix R

The authentication station is usually located at a fixed position whose coordinates can be surveyed with a very high accuracy. As such, its position can be treated as error

free. Thus the error of the range from the authenticator to each satellite, $\delta\rho_i^a$, is only caused by the error of the satellite position. The range error is a projection from the satellite position error to the LOS between the satellite and the authenticator. If we define this LOS vector as

$$\mathbf{e}_{ai} = \begin{bmatrix} \frac{\hat{x}_i - x_a}{\hat{\rho}_i} & \frac{\hat{y}_i - y_a}{\hat{\rho}_i} & \frac{\hat{z}_i - z_a}{\hat{\rho}_i} \end{bmatrix}^T$$

then

$$\delta\rho_i^a = \mathbf{e}_{ai}^T \delta\mathbf{r}_i \tag{2.18}$$

For fix authentication station, Equation (2.16) can be rewritten as

$$\delta\mathbf{m} = \begin{bmatrix} \delta m_1 \\ \delta m_1 \\ \delta m_3 \end{bmatrix} = \begin{bmatrix} \left(\hat{\mathbf{e}}_2^T - \mathbf{e}_{a2}^T\right)\delta\mathbf{r}_2 + c\delta t_{21} - c\delta\chi_{21} - \left(\hat{\mathbf{e}}_1^T - \mathbf{e}_{a1}^T\right)\delta\mathbf{r}_1 \\ \left(\hat{\mathbf{e}}_3^T - \mathbf{e}_{a3}^T\right)\delta\mathbf{r}_3 + c\delta t_{31} - c\delta\chi_{31} - \left(\hat{\mathbf{e}}_1^T - \mathbf{e}_{a1}^T\right)\delta\mathbf{r}_1 \\ \left(\hat{\mathbf{e}}_4^T - \mathbf{e}_{a4}^T\right)\delta\mathbf{r}_4 + c\delta t_{41} - c\delta\chi_{41} - \left(\hat{\mathbf{e}}_1^T - \mathbf{e}_{a1}^T\right)\delta\mathbf{r}_1 \end{bmatrix} \tag{2.19}$$

The errors in the measurement vector $\delta\mathbf{m}$ in Equation (2.19) can be categorized into three groups based on the error mechanisms:

1. Satellite position error: $\delta\mathbf{r}_1$, $\delta\mathbf{r}_2$, $\delta\mathbf{r}_3$, $\delta\mathbf{r}_4$
2. Peak delay measurement error: δt_{21}, δt_{31}, δt_{41}
3. Atmospheric signal propagation delay error: $\delta\chi_{21}$, $\delta\chi_{31}$, $\delta\chi_{41}$

The difference between the broadcast ephemeris and the true ephemeris forms the satellite position error. The peak delay error is mainly caused by the noise in both the authenticator and the supplicant. The atmospheric propagation delay error is due to the fact that the ionospheric and tropospheric delay models used by the receivers are not perfect.

The three error mechanisms identified above are independent of each others. If each error source can be described as a Gaussian random variable, then $\delta\mathbf{m}$ is a Gaussian random vector whose covariance $\mathbf{R}$ is given by

$$\mathbf{R} = E\left[\delta\mathbf{m}\delta\mathbf{m}^T\right] = \begin{bmatrix} \sigma_{m11}^2 & \sigma_{\mathbf{r}_1}^2 & \sigma_{\mathbf{r}_1}^2 \\ \sigma_{\mathbf{r}_1}^2 & \sigma_{m22}^2 & \sigma_{\mathbf{r}_1}^2 \\ \sigma_{\mathbf{r}_1}^2 & \sigma_{\mathbf{r}_1}^2 & \sigma_{m33}^2 \end{bmatrix} \tag{2.20}$$

Table 2.1: Variance of measurement error

Error	Variance
SAT 1 position	$\sigma_{\mathbf{r}_1}$
SAT 2 position	$\sigma_{\mathbf{r}_2}$
SAT 3 position	$\sigma_{\mathbf{r}_3}$
SAT 4 position	$\sigma_{\mathbf{r}_4}$
SAT 2 to SAT 1 peak delay	$\sigma_{t_{21}}$
SAT 3 to SAT 1 peak delay	$\sigma_{t_{31}}$
SAT 4 to SAT 1 peak delay	$\sigma_{t_{41}}$
SAT 2 to SAT 1 atmospheric delay	$\sigma_{\chi_{21}}$
SAT 3 to SAT 1 atmospheric delay	$\sigma_{\chi_{31}}$
SAT 4 to SAT 1 atmospheric delay	$\sigma_{\chi_{41}}$

where the symbols defined in Table 2.1 are used and the diagonal terms are given by

$$\sigma_{m11}^2 = \sigma_{\mathbf{r}_2}^2 + \sigma_{\mathbf{r}_1}^2 + \sigma_{t_{21}}^2 + \sigma_{\chi_{21}}^2$$
$$\sigma_{m22}^2 = \sigma_{\mathbf{r}_3}^2 + \sigma_{\mathbf{r}_1}^2 + \sigma_{t_{31}}^2 + \sigma_{\chi_{31}}^2$$
$$\sigma_{m33}^2 = \sigma_{\mathbf{r}_4}^2 + \sigma_{\mathbf{r}_1}^2 + \sigma_{t_{41}}^2 + \sigma_{\chi_{41}}^2$$

The satellite position error variances are the variances of projected range errors rather the original position error. For example

$$\sigma_{\mathbf{r}_1}^2 = E\left\{\left[\left(\hat{\mathbf{e}}_1^T - \mathbf{e}_{a1}^T\right)\delta\mathbf{r}_1\right]^2\right\}$$

The variances of peak delay errors are also converted into range unit by multiplying the speed of light. For example

$$\sigma_{t_{21}}^2 = E\left\{[c\delta t_{21}]^2\right\}$$

where $E\{.\}$ is the expectation operator. Finally, since the geometry matrix $\mathbf{A}$ has the similar function as the geometry matrix in a standard GPS position estimation problem, we can write the covariance matrix of the supplicant position error (as computed by the authenticator) as

$$\text{cov}(\delta\mathbf{r}_s) = (\mathbf{A}^T\mathbf{R}^{-1}\mathbf{A})^{-1} \tag{2.21}$$

2.5 Summary

The theory of the GPS position authentication was presented in this chapter. The position authentication method proposed in this chapter extended the capability of earlier proposed signal authentication method by introducing a high pass filter to mitigate the C/A multiple-peak problem so that the signal authentication method can be used when the authenticator and the supplicant are located in close proximity of each other. Furthermore, the relative delays of the watermark signals were used as measurements to calculate an authentic GPS position. It was shown that the position calculation method is mathematically similar to other GNSS relative positioning methods. The error sources of this positioning method were discussed. Most of these errors, such as atmospheric error, clock error, etc., have been discussed widely in the GPS literature. However, the error of the relative delay is unique to this position authentication method. This error is of the shift time estimation accuracy which will be discussed in next chapter.

Chapter 3

Authentication Performance Analysis

The algorithm used for signal and position authentication described in Chapter 2 are affected by noise. In this chapter the effect of noise on the algorithm developed in Chapter 2 is examined. In particular, we develop the framework required for assessing the accuracy of the position authentication and the false alarm rate of the signal authentication process. The accuracy and false alarm rate are key performance metrics used in any position system where high reliability is required.

3.1 Noise Sources in GPS Receiver Front End

The noise sources that affect the performance of a GPS receiver with respect to authentication can be cataloged into two major groups. The first one is the signals broadcast from the satellites other than the satellite which is tracking by the tracking loop. For a civilian GPS receiver only the C/A code signal is used, thus the P(Y) signal from the same satellite is a noise. Another noise type is thermal noise. The thermal noises include the antenna noises and thermal noises inside the receiver. Some of the antenna noise is caused by the thermal motion of the atoms around the antenna. The remainder of the thermal noise inside the GPS receiver include the amplifier noise and cable noise. The noise inside the GPS receiver is mostly contributed by the RF front end. This will be shown later.

To understand how big the various noise component in the RF front end of a GPS receiver are, we analyze a typical configuration of a GPS receiver as an example. Fig. 3.1 is the block diagram of a GPS RF front end which features a typical two-stage low noise amplifier (LNA) structure. In Figure 3.1 S is the signal from the satellite we are processing, N_a is the antenna noise, N_{L_1} is the noise of cable 1, N_{G_1} is the amplifier noise of Low Noise Amplifier # 1 or LNA1, N_{L_2} is the noise of cable 2 and N_{G_2} is the amplifier noise of LNA2. The thermal noise is usually referred to as the noise temperature and, thus, which has the unit of temperature. In Figure 3.1, T_a, T_{L_1}, T_{G_1}, T_{L_2} and T_{G_2} are the corresponding noise temperatures. The signal and noise before the antenna are converted to the signals appear at the output terminal of the GPS antenna, which are S and N_a.

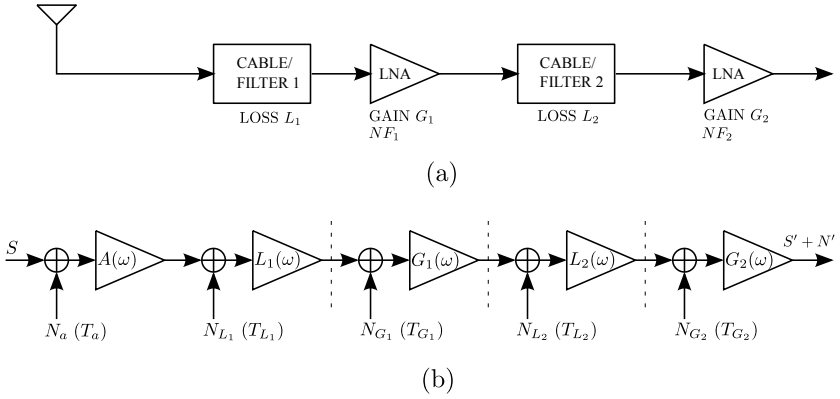

Figure 3.1: Noise sources in GPS receiver front end

The typical gains of the components are $G1 = 33dB$ and $G_2 = 27dB$. The typical losses of the components are $L_1 = 1.1dB$ and $L2 = 4.1dB$. The noise figures are $NF_1 = 2.2dB$ and $NF_2 = 2.5dB$. Because we convert the signal before the antenna into signal at the antenna terminal, the antenna gain $A = 1$ or $A = 0dB$. The ω in Figure 3.1 is used to indicate that the gain of every component varies at different frequencies. For GPS receivers, these components can be modeled as bandpass filters. In this example, we simply assume they have the same bandwidth which is 24 MHz. Using the parameters above, the powers of different noises sources are listed in Table 3.1.

Table 3.1: Input power of noise source (BW=24 MHz)

Source	Noise Figure (dB)	Noise Temperature (K)	PSD (dBW/Hz)	Power (dBW)
Antenna (N_a)		100	-208.6	-134.8
Cable1 (N_{L1})	1.1	29	-214.0	-140.2
LNA1 (N_{G1})	2.2	190	-205.8	-132.0
Cable2 (N_{L2})	4.1	455	-202.1	-128.3
LNA2 (N_{G2})	2.5	226	-205.1	-131.3

Table 3.2 lists the noise powers measured at the output of the RF front end. Table 3.2 shows that the contribution of the amplifier and cable after the first stage LNA is very small. Thus we can ignore their noise contribution and consider them as noiseless amplifiers. Figure 3.2 graphically shows the energy ratios of different sources at the output of RF front end. The energy of the signal to be tracked by the GPS receiver is less than 0.3%. The antenna noise and cable noise contribute about $\frac{1}{3}$ of the total energy. The internal thermal noise contributes about $\frac{2}{3}$ of the total noise energy.

Table 3.2: Power at output of RF front end (BW=24 MHz)

Source	Symbol	Gain	Power (dBW)	Percentage %
Antenna	P'_{N_a}	$\frac{G_1G_2}{L_1L_2}$	-80.0	26.67
Cable1	$P'_{N_{L1}}$	$\frac{G_1G_2}{L_1L_2}$	-85.4	7.69
LNA1	$P'_{N_{G1}}$	$\frac{G_1G_2}{L_2}$	-76.1	65.46
Cable2	$P'_{N_{L2}}$	$\frac{G_2}{L_2}$	-105.4	0.08
LNA2	$P'_{N_{G2}}$	G_2	-104.3	0.1

From Figure 3.1, we can see that the GPS signal and the antenna noise share the same signal path. However, the internal thermal noise has a shorter signal path compared with the GPS signal. Based on these facts above, Figure 3.1 can be simplified. Figure 3.3 shows a simplified block diagram of the GPS RF front end. The amplifiers and cables after the first stage LNA are ignored. This simplified block diagram will ease

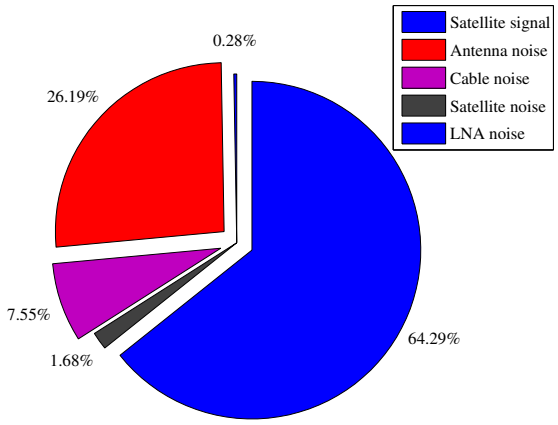

Figure 3.2: Signal and noise energy distribution at output of RF front end

the performance analyses of the detection and estimation algorithms which are at the heart of the authentication problem.

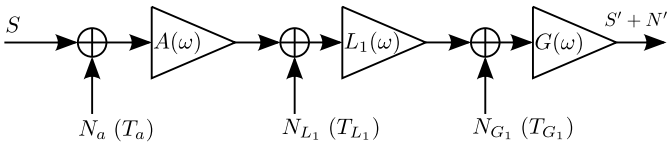

Figure 3.3: Simplified noise sources in GPS receiver front end

3.2 Distribution of Receiver Noise at Baseband

In the section above, the main noise sources in the GPS receiver were identified. They were antenna noise and internal thermal noise. This section discusses the distribution of the signal at base band output. It also discusses the stationarity of the signal at this point in the receiver.

The signals processed by the watermark detector used in Chapter 2 are depicted in Figure 3.4. Signal $p(t)$ is the watermark signal from a specific GPS satellite. It is received at the antennas of two GPS receivers which are an authenticator and a supplicant. Signals $n_a(t)$ and $n_s(t)$, at the end of the LNA, are the noise signals discussed in Section

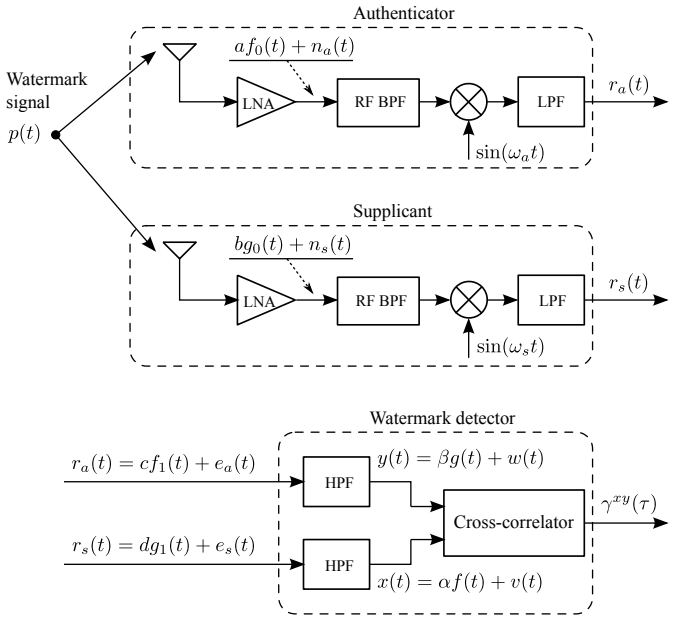

Figure 3.4: Signals of watermark detector

3.1. Signal $f_0(t)$ is the filtered form of signal $p(t)$ at the output of the authenticator's LNA. Signal $g_0(t)$ is the filtered form of signal $p(t)$ at the output of the supplicant's LNA. a and b are two scalars which represent the amplitude of watermark signals when the noise signal $n_a(t)$ and $n_s(t)$ are normalized to unit variance noise signals. The energy of the watermark signal is very small compared with the noise signal and, thus, a and b are very small. The majority in the noise signal $n_a(t)$ or $n_s(t)$ are thermal noises of the antenna and the LNA. This thermal noise can be modeled as a narrow-band Gaussian random process [11][12][13]. Other satellites' watermark signals and channel noise also appear in the noise signal $n_a(t)$ or $n_s(t)$, but their energy is so small that they can be ignored. The distributions of $n_a(t)$ and $n_s(t)$ are mainly determined by the thermal noise. Thus we can approximately model $n_a(t)$ and $n_s(t)$ as a narrow-band Gaussian random processes. Their bandwidths are determined by the bandwidth of antenna and the LNA that they pass through. In Figure 3.4, the ω_a and ω_s are the operation frequencies of the down-converters in the authenticator and the supplicant, respectively. These frequencies are very close to the center carrier frequency of the GPS L1 band, which is 1575.42 MHz.

The energy of the thermal noise is mainly determined by the temperature. In a short period, the energy of the thermal noise does not change appreciably since the change in temperature is a very slow process. In the GPS position authentication system, the duration of the data needed is about 10 ms to 100 ms. In this time scale, the thermal noise can be treated as a stationary random process. In summary, we will approximately model noise signal $n_a(t)$ and $n_s(t)$ as narrow-band Gaussian random processes which are also wide-sense-stationary (WSS).

The down-converters in Figure 3.4 do not change the distributions and the stationarity of the noise signals. To demonstrate this consider the noise signal $n_a(t)$ in Figure 3.4. The narrow-band noise can be expressed by two independent base-band random processes [11][12]. The Gaussian WSS random process $n_a(t)$ can be expressed in the form

$$n_a(t) = i_a(t)\cos(\omega_c t) - q_a(t)\sin(\omega_c t) \tag{3.1}$$

where ω_c is the center frequency of the narrow-band noise, $i_a(t)$ and $q_a(t)$ are two independent base-band Gaussian WSS random processes. The variances of $n_a(t)$, $i_a(t)$ and $q_a(t)$ are the same, i.e. $\sigma^2_{n_a} = \sigma^2_{i_a} = \sigma^2_{q_a}$. When the carrier tracking loop is locked, we have $\omega_a = \omega_c$ in the down-converter . After the noise $n_a(t)$ passes the down-converter, we get the signal below

$$\begin{aligned}[af_0(t) + n_a(t)]\sin(\omega_a t) = af_0(t)\sin(\omega_a t) \\ + \frac{1}{2}i_a(t)\sin(2\omega_c t) - \frac{1}{2}q_a(t) - \frac{1}{2}q_a(t)\sin(2\omega_c t)\end{aligned} \tag{3.2}$$

When the signal in Equation (3.2) passes the low-pass filter (LBP in Figure 3.4), the $2\omega_a$ components are filtered out. Thus we have the output of the low-pass filter

$$r_a(t) = af_0(t)\sin(\omega_a t) - \frac{1}{2}q_a(t) \tag{3.3}$$

There are no carrier signals in $r_a(t)$. Thus Equation (3.3) represents the base band signal fed to the watermark detector. Denoting the base band watermark signal as $f_1(t)$ and base band noise signal as $e_a(t)$, we have $cf_1(t) = af_0(t)\sin(\omega_a t)$ and $e_a(t) = -\frac{1}{2}q_a(t)$. Thus, the noise component of $r_a(t)$ in Figure 3.4 is a stationary random process as described in Equation (3.1).

In the watermark detector the two base band signals, $r_a(t)$ and $r_s(t)$, first past a high-pass filter as discussed in Chapter 2. We denote these two base band signal as $x(t)$ and $y(t)$ of the authenticator and the supplicant, respectively. They have watermark signal components, $f(t)$ and $g(t)$, and noise component, $u(t)$ and $v(t)$. The high-pass filters are linear time-invariant filters. Thus when a WSS Gaussian random process is filtered by the HPF, the resulting random process is still a WSS Gaussian. We can conclude that the noise components $u(t)$ and $v(t)$ in Figure 3.4 can be approximated as WSS Gaussian random processes.

To show the approximation above is reasonable, a real data set is analyzed. This real data set is quadrature signal component at the output of the tracking loops. It is equivalent to the signal $r_a(t)$ or $r_s(t)$ in Figure 3.4. The duration of the data used is 10 ms and this data set has 10^6 samples. The histogram is shown in Figure 3.5. The quantile of this data set versus a standard normal distribution is plotted in Figure 3.6. These two figures shows that the distribution of this data set can be treated as a Gaussian process within $\pm 3.5\sigma$, where σ is the standard derivation. It means that about 99.953% samples satisfies the Gaussian distribution. Note that this real data includes both the thermal noise component and very weak watermark signal. Thus we can say that the effect of the watermark signal on the distribution of the noise signal can be ignored.

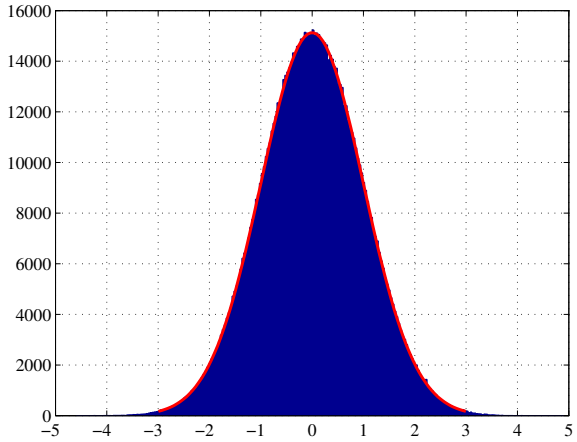

Figure 3.5: Histogram of quadrature signal

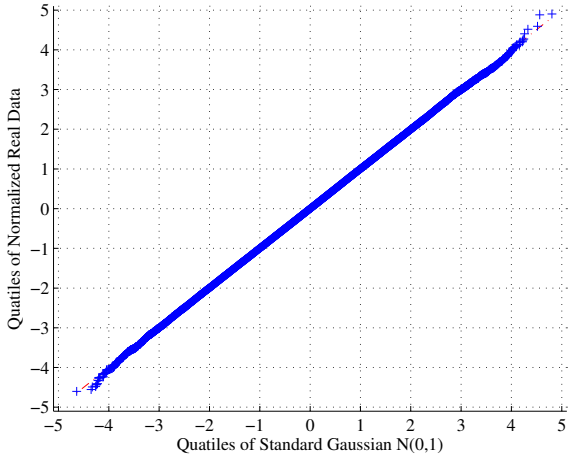

Figure 3.6: Quantiles of quadrature signal

The thermal noises, which are the majority of the noise component, in authenticator and supplicant receivers are independent because these two receiver do not share any common devices and they are in different environment. Thus we can say that the noise processes $u(t)$ and $v(t)$ in Figure 3.4 are independent. The watermark signal is generated by the GPS satellite, so it is also independent from both $u(t)$ and $v(t)$.

3.3 Measuring Shift Time

The term "shift time" as used in this section means the difference between the traveling times of the watermark signal from one GPS satellite to the authenticator and the supplicant. Because the distances between the satellite and the two GPS receivers are different, the traveling time are also different. In this section, the structure of the estimator used for determining traveling time is discussed and its performance is analyzed.

As discussed in Chapter 2, in the GPS position authentication system we use two measured signal sequences to estimate the shift time. They are the quadrature signals in the GPS receiver tracking loop as shown in Figure 2.3. Both signals include the watermark signal and noise signals. These two signals are $x(t)$ and $y(t)$ and are shown in Figure 3.4. The $x(t)$ and $y(t)$ in Figure 3.4 assumes that the watermark signals $f_1(t)$

and $g_1(t)$ arrive at the watermark detector without time difference. When the shift time is considered, we have

$$\begin{aligned} x(t) &= \alpha f(t) + v(t) \\ y(t) &= \beta g(t - t_d) + u(t) \end{aligned} \tag{3.4}$$

where t_d is the shift time. If the arrival time of the watermark at the supplicant is t_s and the arrival time of the watermark signal at the authenticator is t_a, then $t_d = t_s - t_a$. The objective of the shift estimator is to estimate t_d when two measurements $x(t)$ and $y(t)$ are available. The difficulty in designing an estimator is that we have no waveform information about the watermark signal $p(t)$ shown in Figure 3.4. Thus we have no information about the signals $f(t)$ and $g(t)$ other than the fact that one is a delayed and noisy replica of the other. For the P(Y) signal $p(t)$ we know that it is a pseudorandom signal and its auto-correlation function (ACF) is available.

For the the conventional arrival time estimation problem [14], the match filter is an optimal estimator. The match filter is optimal in the sense of both minimum variance and maximum likelihood. The match filter used for a known signal is a cross-correlator. It takes two signals as the inputs. One input signal is the known deterministic signal called template and the other signal is a noisy measurement which includes the known signal and noise. For the GPS position authentication system, we can not implement this optimal match filter because we have no waveform information of the watermark signal. Stated differently, we do not have a noise-free template.

Appendix D tries to utilize the maximum likelihood principle to construct an estimator for the GPS position authentication system. It shows that the cross-correlator between two measurement sequences $x(n)$ and $y(n)$ is not the optimal estimator for shift time in the maximum likelihood sense. Even though suboptimal the cross-correlator between two measurement sequences will perform well if the number of samples is very big. While from the perspective of seeking an engineering solution, the performance of this direct cross-correlator is worth exploring. In the remainder of this section, we will use another approach to construct an estimator. This approach first discusses the method to measure the shift time when there is no noise in two measurement sequences. This noiseless method is a transformation from two functions to a scalar variable which is the shift time. In other word, we first seek a discriminator for measuring shift time.

Then we consider the scenario when both of the measurements have noises to see how the discriminator is affected by the noises. Further the performance of this estimator is evaluated to determine how the noise parameters are related to the estimate accuracy.

3.3.1 Measuring Shift Time without Noises

A widely used method to measure the shift time between a binary value random sequence and its delayed copy is cross-correlation[9, 15]. For example, $s(n)$ is a random sequence with possible values 0 or 1. Its delayed copy is $z(n) = s(n - n_0)$, where n_0 is the delay time or the shift time. The cross-correlation between two sequences is

$$R(m) = \sum_{n=-\infty}^{+\infty} s(n)z(n+m) \tag{3.5}$$

$R(m)$ achieves its maximum only when $m = n_0$. Thus the shift time can be measured by finding the peak of the cross-correlator. The time (or shift) where the peak occurs is the shift time. Because $z(n)$ is a delayed version of the original signal $s(n)$, Equation (3.5) is the auto-correlation function (ACF) of the sequence $s(n)$.

The GPS P(Y) sequence is a pseudorandom binary sequence with value -1 or +1. Its auto-correlation function [16] is

$$R_p(\tau) = \begin{cases} \frac{\tau}{T_c} + 1 & \text{if } -T_c < \tau < 0 \\ -\frac{\tau}{T_c} + 1 & \text{if } 0 < \tau < T_c \\ 0 & \text{otherwise} \end{cases} \tag{3.6}$$

where τ is the delay time and T_c is the duration of a single P(Y) chip. For the P(Y) signal $T_c = \frac{1}{10.23e6} \approx 97.75\ ns$. The shape of this auto-correlation function is a triangle.

When there is no noise, the auto-correlation function can be used to measure the shift time of a P(Y) sequence based on the discussion above. In reality where noise presents in the measurement, we can still construct the auto-correlation of the P(Y) signal and then try to measure the shift time by detecting the peak of the auto-correlation function. The problem with this approach, however, is that the auto-correlation is corrupted by certain noise and, thus, the accuracy of the shift time estimate is degraded. This effect of noise was alluded too earlier in this thesis in relation to the direct cross-correlator

used in Chapter 2. Figure 4.13 shows the result of this direct cross-correlator where the auto-correlation function peak is distorted.

In addition to the peak, there is a noise floor in the direct cross-correlation. This noise corrupts the auto-correlation function and further degrade the shift time accuracy. In what follows the reason why the auto-correlation function is distorted will be examined closely. The characteristics of the noise floor will be discussed next. As a prelude to these discussions, the details of the sample cross-correlator used in Chapter 2 will now be discussed.

3.3.2 Sample Cross-correlator

The cross-correlation between two zero mean WSS random process $X(t)$ and $Y(t)$ is defined as

$$\gamma_{xy}(\tau) = E[X(t)Y(t+\tau)] \tag{3.7}$$

In practice, it is difficult to calculate the cross-correlation using (3.7) because it is a stochastic function of signals whose density function may be unknown. In practice, the sample cross-correlation method shown in Figure 3.7 is used to estimate the $\gamma_{xy}(\tau)$, using finite number of signal samples [17].

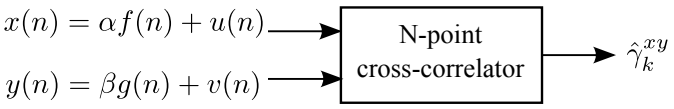

Figure 3.7: Sample cross-correlator

The sample cross-correlation between x_n and y_n using N samples is given by

$$\hat{\gamma}_k^{xy} = \frac{1}{N}\sum_{n=1}^{N} x_n y_{n+k} \tag{3.8}$$

which is the output of the sample correlator in Figure 3.7. Because the sample cross-correlation defined above is a function of random variables, for a specific lag value k, $\hat{\gamma}_k^{xy}$ is also a random variable. Thus, a sequence of lags, $\hat{\gamma}_k^{xy}$ constructs a random process.

Figure 3.8 graphically shows the signal samples used in (3.8). The N-point x_n signal snapshot is the noisy template. We want to find a signal piece, which is also of length

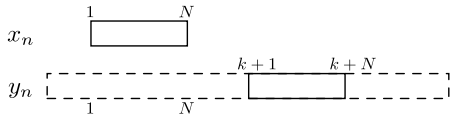

Figure 3.8: Signal samples for the correlator

N, in y_n so that these two pieces mostly match each other. The signal piece in y_n is depicted as a solid line box in Figure 3.8.

For simplicity, we express signals in the vector form. Four basic signal components, f_n, g_n, u_n and v_n in Figure 3.7, can be represented in the vector form. That is,

$$\begin{aligned}
\mathbf{f} &= [f_1 \ f_2 \ f_3 \ \cdots \ f_N]^T \\
\mathbf{g} &= [g_1 \ g_2 \ g_3 \ \cdots \ g_N]^T \\
\mathbf{u} &= [u_1 \ u_2 \ u_3 \ \cdots \ u_N]^T \\
\mathbf{v} &= [v_1 \ v_2 \ v_3 \ \cdots \ v_N]^T
\end{aligned} \tag{3.9}$$

For a given lag k, the samples of signals x_n and y_n (started from index k+1) can also be written in the vector form as

$$\begin{aligned}
\mathbf{x} &= [x_1 \ x_2 \ x_3 \ \cdots \ x_N]^T \\
\mathbf{y}_k &= [y_{1+k} \ y_{2+k} \ y_{3+k} \ \cdots \ y_{N+k}]^T
\end{aligned} \tag{3.10}$$

Signals in Figure 3.7 (Equation (3.4)) can be written as

$$\begin{aligned}
\mathbf{x} &= \alpha\mathbf{f} + \mathbf{u} \\
\mathbf{y}_k &= \beta\mathbf{g}_k + \mathbf{v}_k
\end{aligned} \tag{3.11}$$

Thus the vector form of the sample correlation in (3.8) is

$$\hat{\gamma}_k^{xy} = \frac{1}{N}\mathbf{x}^T\mathbf{y}_k = \frac{1}{N}\langle \mathbf{x}, \mathbf{y}_k \rangle \tag{3.12}$$

where $\langle \cdot, \cdot \rangle$ is the inner product operator.

Since the inner product operator is a linear operator, Equation (3.12) can be written as

$$\hat{\gamma}_k^{xy} = \alpha\beta\frac{\langle \mathbf{f}, \mathbf{g}_k \rangle}{N} + \alpha\frac{\langle \mathbf{f}, \mathbf{v}_k \rangle}{N} + \beta\frac{\langle \mathbf{u}, \mathbf{g}_k \rangle}{N} + \frac{\langle \mathbf{u}, \mathbf{v}_k \rangle}{N} \tag{3.13}$$

Similarly as Equation (3.8) and (3.12), we define the sample cross-correlations between signals f_n, g_n, u_n and v_n. For example, the sample cross-correlation between f_n and v_n is

$$\hat{\gamma}_k^{fv} = \frac{1}{N}\mathbf{f}^T\mathbf{v}_k = \frac{\langle \mathbf{f}, \mathbf{v}_k \rangle}{N} \tag{3.14}$$

The $\hat{\gamma}_k^{ug}$ and $\hat{\gamma}_k^{uv}$ have the similar definition except that the superscripts denotes the different signals. The sample cross-correlation between the signal f_n and g_n is defined as

$$\hat{\gamma}_k^{fg} = \frac{1}{N}\mathbf{f}^T\mathbf{g}_k = \frac{\langle \mathbf{f}, \mathbf{g}_k \rangle}{N} \tag{3.15}$$

Now we define the sample cross-correlation error as

$$\delta_{\gamma_k^{fg}} = \hat{\gamma}_k^{fg} - \gamma_k^{fg} \tag{3.16}$$

The nature of this error has a direct impact on how well we can estimate delay time. As such, this error will be discussed more detail in Section 3.3.6. In the mean time, note that Equation (3.12) can be written as

$$\begin{aligned} \hat{\gamma}_k^{xy} &= \alpha\beta\hat{\gamma}_k^{fg} + \alpha\hat{\gamma}_k^{fv} + \beta\hat{\gamma}_k^{ug} + \hat{\gamma}_k^{uv} \\ &= \alpha\beta\gamma_k^{fg} + \alpha\beta\delta_{\gamma_k^{fg}} + \alpha\hat{\gamma}_k^{fv} + \beta\hat{\gamma}_k^{ug} + \hat{\gamma}_k^{uv} \end{aligned} \tag{3.17}$$

Equation (3.17) can be interpreted in two ways. The first way is to treat the output of the sample cross-correlator as a new random process, i.e. $\hat{\gamma}_k^{xy}$. This random process is the linear combination of a deterministic signal γ_k^{fg} and other random processes: $\delta_{\gamma_k^{fg}}$, $\hat{\gamma}_k^{fv}$, $\hat{\gamma}_k^{ug}$ and $\hat{\gamma}_k^{uv}$. In this perspective of the signal, Equation (3.17) shows that $\hat{\gamma}_k^{xy}$ is a summation of a deterministic signal and a noise signal. This deterministic signal component, $\alpha\beta\gamma_k^{fg}$, is what we want to detect. The noise component is the difference between $\hat{\gamma}_k^{xy}$ and the wanted quantity $\alpha\beta\gamma_k^{fg}$. If we define this noise component as

$$\begin{aligned} \Delta\hat{\gamma}_k^{xy} &= \hat{\gamma}_k^{xy} - \alpha\beta\gamma_k^{fg} \\ &= \alpha\beta\delta_{\gamma_k^{fg}} + \alpha\hat{\gamma}_k^{sv} + \beta\hat{\gamma}_k^{us} + \hat{\gamma}_k^{uv} \end{aligned} \tag{3.18}$$

then as shown in Appendix C.2 the four random variables on the right of Equation (3.18) are independent of each other. Thus the variance of the error signal is the sum of the variances of four random components. This is shown in Equation (C.34).

The second way to interpret Equation (3.17) is to treat the sample cross-correlator as an estimator. The expectation of this estimator is $\alpha\beta\gamma_k^{fg}$ as shown in Appendix C.1. This appendix also shows that this estimator is an unbiased estimator. The variance of the estimator is discussed in Appendix C.2.

Note the cross-correlator in Equation (3.8), (3.12) and (3.14) are different from the general unbiased N-sample cross-correlator as defined in [17]. This is because the sample cross-correlator in this application always has N effective samples for every lag k. It is shown in Figure 3.8. For the general correlator defined in the same way as (3.8), however, the total effective number of samples is N. For most of the general correlation operation, the signal need to be zero padded. This is why the general correlator define as (3.8) is biased.

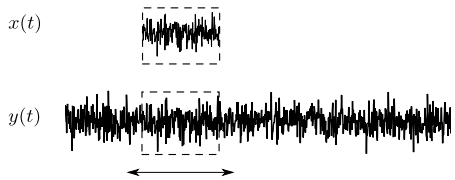

Figure 3.9: Input signals to the correlator

3.3.3 Characteristics of the Noise Floor

The noise components defined in Equation (3.18) represent the noise floor in Figure 4.13. Typical values of α and β are listed in Table C.1 where it is shown that the maximum possible values of α^2, β^2 and $\alpha\beta$ is less than 1% (bandwidth is 12MHz and C/N_0 is 50 dB-Hz). Appendix C.2 also shows that the energy of the first three items in Equation (3.18) is very small. Thus $\hat{\gamma}_k^{uv}$ is the major power contributor of the noise floor and in what follows the other three components in Equation (3.18) can be ignored. This engineering approximation is reasonable, which is shown by the simulation results in Section 3.3.5. In [18] it was shown that all the components in Equation (3.18), $\hat{\gamma}_k^{xy}$, $\delta_{\gamma_k^{fg}}$, $\hat{\gamma}_k^{fv}$, $\hat{\gamma}_k^{ug}$ and $\hat{\gamma}_k^{uv}$, are approximately Gaussian distributed when the number of the samples, N, is fairly large. For the GPS position authentication system, the typical value of N is greater than 10^6. The Gaussian approximation is valid in the application discussed in this thesis. Thus the distribution of the noise floor of $\hat{\gamma}_k^{xy}$ can be approximated as Gaussian.

To describe a Gaussian random process, only its mean and covariance need to be characterized. The mean of the noise floor, or approximately $\hat{\gamma}_k^{uv}$, is zero because the receiver noise u and v are also zero mean random processes. This has been shown in Appendix C.2. Then we only need to characterize the covariance of the noise floor.

Both the frequency domain approach and the time domain approach are performed to obtain the characteristics of the noise floor. The frequency domain approach is presented here and the time domain approach is presented in Appendix C.2. In the frequency domain approach we will first seek its power spectral density. Then by taking the inverse Fourier transformation, the covariance or auto-correlation function can be obtained.

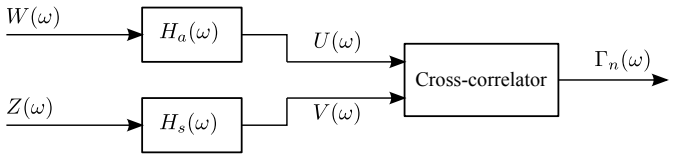

Figure 3.10: Simplified noise model

The most widely used method to describe a WSS Gaussian random process is to represent it as the output of a causal linear time invariant (LTI) filter driven by a white Gaussian noise [19]. In this thesis we also use this method to model the base band receiver noise. The white noise signal is called the exciting noise which is a unit variance Gaussian random process. And the filter is called the noise model filter. For the two receivers, the authenticator and the supplicant, their exciting noises are independent. In the frequency domain, the cross-correlator can be depicted as the simplified block diagram shown in Figure 3.10. $H_a(\omega)$ and $H_s(\omega)$ are the frequency responses of the noise model filters of the authenticator and the supplicant, respectively. For a power signal, such as a noise process, its Fourier transform does not exist. But the Fourier transform of a piece of noise signal exists because it is an energy limited signal. In Figure 3.10, the variables $W(\omega)$ and $Z(\omega)$ represent the Fourier transform of a piece of the exciting noise realization of the authentication and the supplicant, respectively. $U(\omega)$ and $V(\omega)$ represent the Fourier transform of the base band receiver noise pieces of the authenticator and the supplicant; $\Gamma_n(\omega)$ represents the Fourier transform of the piece of the noise floor; The impulse responses of the LTI filters are $h_a(n)$ and $h_s(n)$ for

the authenticator and the supplicant, respectively. Then we have

$$\begin{aligned} U(\omega) &= H_a(\omega)W(\omega) \\ V(\omega) &= H_s(\omega)Z(\omega) \end{aligned} \tag{3.19}$$

The cross-correlation operation can be written in the frequency domain as

$$\Gamma_n(\omega) = \frac{U(\omega)V^*(\omega)}{N} \tag{3.20}$$

where $*$ is the complex conjugate operator and N is the number of samples of every piece of the noise. Substituting Equation (3.19) into (3.20), we obtain

$$\Gamma_n(\omega) = \frac{H_a(\omega)H_s^*(\omega)W(\omega)Z^*(\omega)}{N} \tag{3.21}$$

The power spectral density of the noise floor is

$$\begin{aligned} \mathcal{P}_{nn}(\omega) &= \frac{\Gamma_n(\omega)\Gamma_n^*(\omega)}{N} \\ &= \frac{H_a(\omega)H_s^*(\omega)H_a^*(\omega)H_s(\omega)W(\omega)W^*(\omega)Z(\omega)Z^*(\omega)}{N^3} \end{aligned} \tag{3.22}$$

Because the exciting noises are unit variance, we have $W(\omega)W^*(\omega) = N$ and $Z(\omega)Z^*(\omega) = N$. Then Equation (3.22) becomes

$$\mathcal{P}_{nn}(\omega) = \frac{H_a(\omega)H_s^*(\omega)H_a^*(\omega)H_s(\omega)}{N} \tag{3.23}$$

By taking the inverse Fourier transform, the auto-correlation function of the noise floor is

$$\begin{aligned} \gamma_n(\tau) &= \mathcal{F}^{-1}\{\mathcal{P}_\gamma(\omega)\} \\ &= \frac{h_a(\tau) * h_s(\tau) * h_s(-\tau) * h_a(-\tau)}{N} \\ &= \frac{\gamma_a(\tau) * \gamma_s(\tau)}{N} \end{aligned} \tag{3.24}$$

where $\gamma_a(\tau)$ and $\gamma_s(\tau)$ are the auto-correlation functions of the receiver noises, i.e. $U(\omega)$ and $V(\omega)$ in Figure 3.10, respectively. Equation (3.24) shows that the auto-correlation function of the noise floor is proportional to the convolution between two auto-correlation functions, the ACF of the authenticator noise and that of the supplicant

noise. Thus, once we have the noise models of two receiver, the covariance of the noise floor is determined by Equation (3.24).

If the noises, $U(\omega)$ and $V(\omega)$, are normalized, Equation becomes

$$\gamma_n(\tau) = \frac{\rho_a(\tau) * \rho_s(\tau)}{N} \tag{3.25}$$

where $\rho_a(\tau)$ and $\rho_s(\tau)$ are the auto-correlation coefficient of the receiver noises, i.e. $U(\omega)$ and $V(\omega)$, respectively.

Appendix C.2 shows that the auto-correlation function of the sample cross-correlation between two independent colored random process $u(n)$ and $v(n)$ can be calculated using the below equation

$$\mathrm{cov}(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}) \approx \frac{K_l^{uv}}{N} \tag{3.26}$$

where

$$K_l^{uv} = \rho_0^u \rho_l^v + 2\sum_{i=1}^{M} \rho_i^u \rho_{i+l}^v \tag{3.27}$$

and ρ_i^u and ρ_i^v are the auto-correlation coefficient of the unit variance receiver noises of the authenticator and the supplicant, respectively. Equation (3.27) can be rewritten as

$$\begin{aligned} K_l^{uv} &= \rho_0^u \rho_l^v + 2\sum_{i=1}^{M} \rho_i^u \rho_{i+l}^v \\ &= \rho_i^u * \rho_i^v \end{aligned} \tag{3.28}$$

where $*$ is the convolution operator. Substituting Equation (3.28) into Equation (3.26), we have

$$\mathrm{cov}(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}) \approx \frac{\rho_i^u * \rho_i^v}{N} \tag{3.29}$$

Comparing Equation (3.29) and (3.25), we find they are identical. This shows that the results obtained using time domain approach and the frequency domain approach are the same.

Equation (3.29) shows that the covariance decreases when the number of the samples increases. It also shows that another component, $\rho_i^u * \rho_i^v$, are independent from the

number of samples. This component is determined by the characteristics of the noise model filters. This is validated later as shown in Figure 3.18.

A zero mean WSS Gaussian random process is uniquely determined by the covariance of the process. Based on the analysis above, the characteristics of the noise floor is determined by the noise filters models of the authenticator and the supplicant. Thus these filter models play an very important role in the performance analysis of the GPS position authentication system. Accordingly, in what follows how the noise models of the authenticator and the supplicant can be abstracted from real data by using system identification methods is discussed.

3.3.4 ARMA Models of the Receiver Noises

One approach to obtain filter parameters is to use the original design files of the receiver from which the filter parameters can be calculated. This is impractical, however, as this reference is proprietary. The alternative approach to find the parameters is the system identification method. For two prototype GPS receivers (authenticator and supplicant) developed and used in the work reported in this thesis (see Chapter 4) the system identification method was used to find an approximated filter model.

The base band signal $r_a(t)$ and $r_s(t)$ in Figure 3.4 are identified by determining the Autoregressive Moving Average (ARMA) parameters that yields a good fit. The details of this determination are not included here as it can be found in [20] and [21]. Instead what we will do here is to show results of the performance of the ARMA models.

To this end, the results are shown in Figure 3.11 through Figure 3.14. Figure 3.11 and Figure 3.12 are the frequency response of the identified models. The dashed line shows the equivalent noise bandwidth of the front-end. In the original design, components was chosen to have the bandwidth about 12 MHz, which can cover the bandwidth of P(Y) signal. But for the assembled receivers in the test, the actual bandwidths are less than the original designed bandwidths. The real data used in this paper is sampled in 100 MHz, so the time interval between two samples is 10 ns.

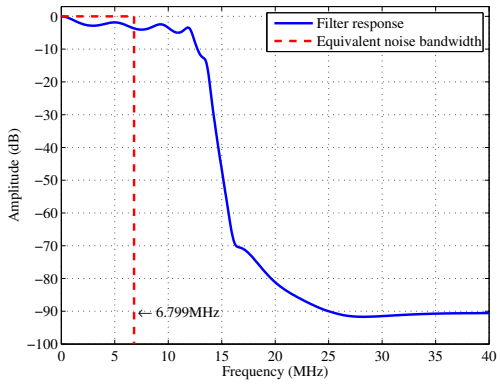

Figure 3.11: Frequency response of authenticator's RF front end filter

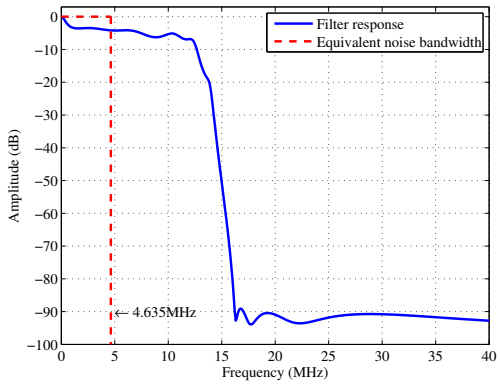

Figure 3.12: Frequency response of supplicant's RF front end filter

Figure 3.13 and Figure 3.14 are the calculated auto-correlation functions of the authenticator and supplicant's noises.

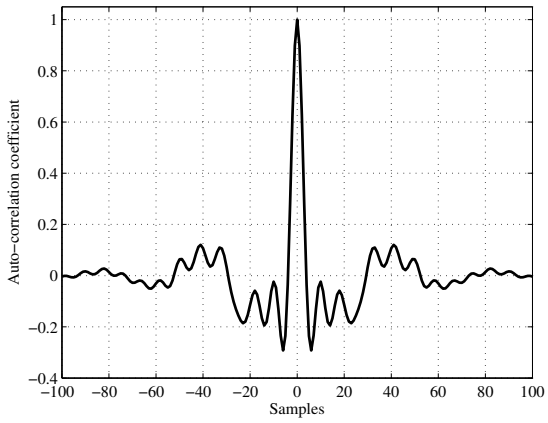

Figure 3.13: Auto-correlation coefficient of authenticator's noise

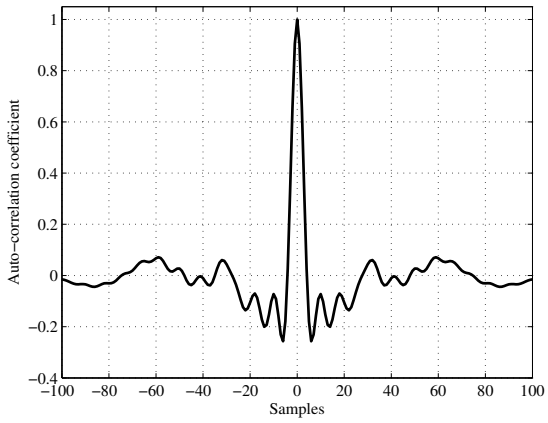

Figure 3.14: Auto-correlation coefficient of supplicant's noise

3.3.5 Validation of Method to Calculate Noise Parameters

To validate the method of calculating the covariance of the noise floor, both the simulation data and real data collected by the receivers are used. For the validation using simulation data, two independent white noise sequences are generated. These two sequences are fed to the noise models, of the authenticator and the supplicant, obtained in Section 3.3.4. The outputs at two noise models are further fed to a sample cross-correlator. At the output of the sample cross-correlator, a new noise sequence is generated. This sequence is the simulated noise floor. A predicted results is generated using the Equation (3.26). Figure 3.15 shows the results of the simulated variance of the noise floor and predicted variance of the noise floor. The error between these two variances are shown in Figure 3.16. They show that the Equation (3.26) is valid and can precisely predict the variance of the noise floor using the noise models of the authenticator and the supplicant. The sampling frequency is 100M Hz in both the simulation and real data validation.

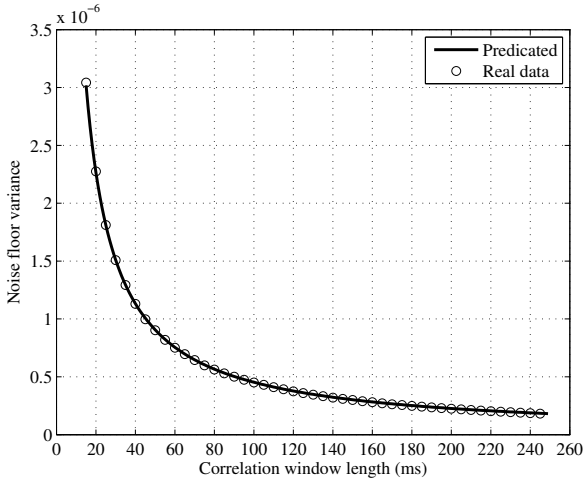

Figure 3.15: Noise floor variance comparison

Further, the real data collected using two GPS receivers are used to calculate the covariance of the noise floor. The real data here is the base band signal and noise at the end of the tracking loop (Q component). This is equivalent to the signal $r_a(t)$ and $r_s(t)$ in Figure 3.4. Then the high pass filter to mitigate the effect of multiple peak

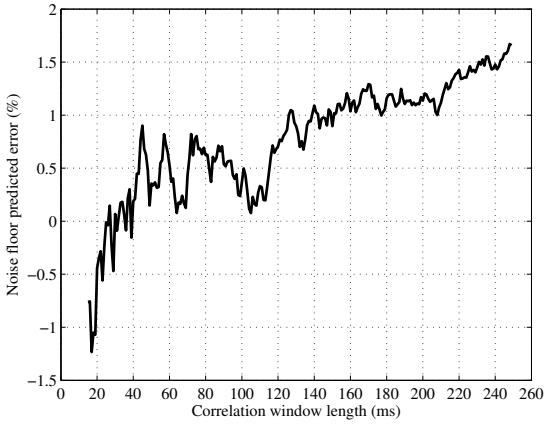

Figure 3.16: Noise floor variance prediction error

problem is applied to the Q component signal. The same sample cross-correlator is used to generate the noise floor. The results are plotted in Figure 3.17.

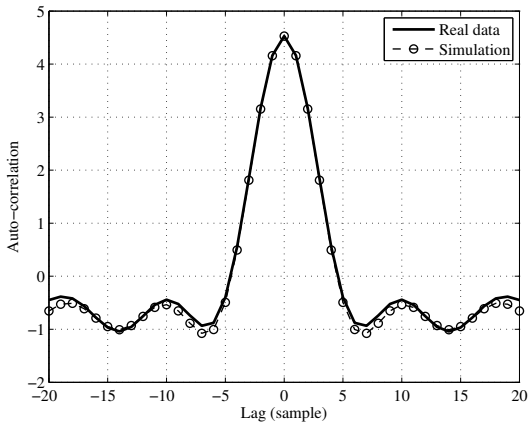

Figure 3.17: Noise floor covariance of simulation and real data

Figure 3.18 shows the auto-correlation coefficient of the real data noise floor when different numbers of samples, N, are used. It shows that even though the number of samples changes, the auto-correlation coefficients do not change, which is also shown in Equation (3.26).

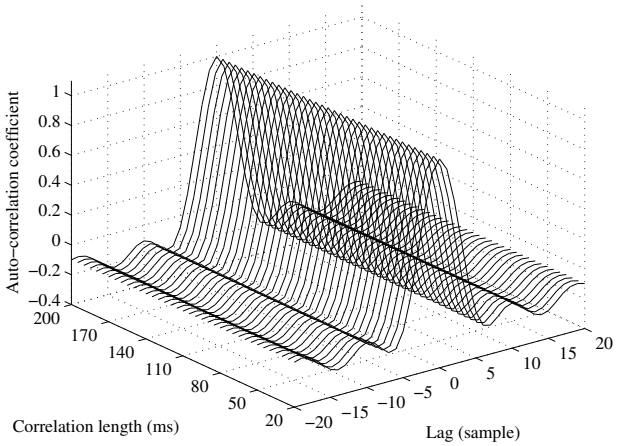

Figure 3.18: Noise floor auto-correlation coefficient of different correlation lengths

The distribution of the noise floor is also validated. Figure 3.19 is the histogram of the real data noise floor. Figure 3.20 is the quantile plot of the real data noise floor. Both shows that the distribution of the noise floor can be approximated as Gaussian. The quantile plot shows that this approximation is valid in the range of $\pm 4\sigma$, which is equivalent to say that more than 99.99% of the samples in the noise floor satisfy the Gaussian distribution.

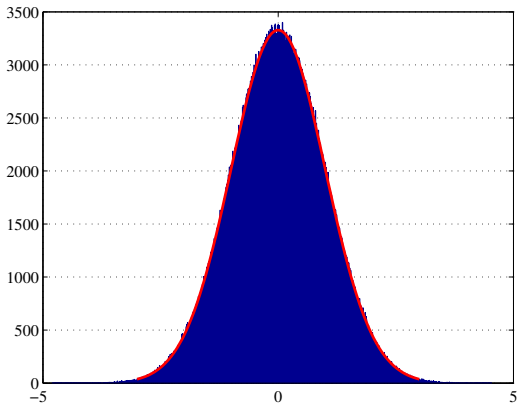

Figure 3.19: Histogram of the cross-correlation noise floor

Note that in the real data validation above, the real data noise floor includes not

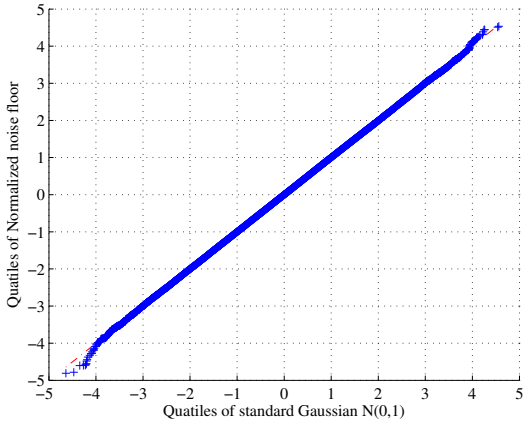

Figure 3.20: Quantiles of the cross-correlation noise floor

Table 3.3: Simulation of variance prediction

Variance name	Prediction formula	Predicted variance	Variance in simulation	Error
$\sigma^2_{\hat{\gamma}^{uv}}$	K_0^{uv}/N	9.058340e-07	8.934964e-07	1.362%
$\beta^2\sigma^2_{\hat{\gamma}^{us}}$	$\beta^2 K_0^{us}/N$	1.471657e-08	1.476298e-08	-0.315%
$\alpha^2\sigma^2_{\hat{\gamma}^{sv}}$	$\alpha^2 K_0^{sv}/N$	8.498176e-09	8.484985e-09	0.155%
$\sigma^2_{\hat{\gamma}^{xy}}$		9.290488e-07	9.167062e-07	1.328%

only the cross-correlation between the two receiver noise ($\hat{\gamma}_k^{xy}$) but also other three items in Equation (3.18). Table 3.3 lists the simulated variances and predicted variances of all the components in Equation (3.18). The parameters used in the simulation are: $N = 5000000$, $\alpha = 0.088884$, $\beta = 0.121610$. The simulation results here and in the next section show that these three items contribute very small energy to the noise floor.

3.3.6 Deterministic Component of Sample Cross-correlator Output

As discussed in Section 3.3.2, the output of the sample correlator can be considered as a deterministic signal plus a Gaussian random noise. This deterministic signal is the cross-correlation between two filtered watermark signals in two receivers, the authenticator and the supplicant. This section discusses the cross-correlation of the watermark signal and its error if it is estimated using a sample cross-correlator. Referring back to (3.17), the cross-correlation is $\alpha\beta\gamma_k^{fg}$ and its error is $\alpha\beta\delta_{\gamma_k^{fg}}$.

The signal paths for the watermark signal and the thermal noise are different as discussed in Section 3.1. Thus we can not use the noise model for the thermal noise to model filters in the watermark's path. Further, the filters in two receivers are not the same. Then two receivers' watermark signals at the input of the cross-correlator are different even though they are from the same source, P(Y) signal from one GPS satellite. In Figure 3.4, $f(t)$ and $g(t)$ are used to distinguish them. Figure 3.21 shows the simplified signal model for the watermark signals. $Q_a(\omega)$ and $Q_s(\omega)$ are the frequency response of the filters in the watermark signal paths of the authenticator and the supplicant, respectively. $P(\omega)$ is the Fourier transform of the P(Y) signal before the GPS antennas. $\Gamma_s(\omega)$ is the Fourier transform of the signal at the output of the sample cross-correlator. Similarly as in Section 3.3.3, the Fourier transform is applied on finite measurement with length of N.

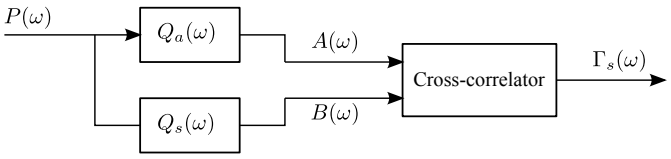

Figure 3.21: Simplified signal model

We have the following equations for the signals in Figure 3.21

$$\begin{aligned} A(\omega) &= Q_a(\omega)P(\omega) \\ B(\omega) &= Q_s(\omega)P(\omega) \end{aligned} \tag{3.30}$$

Then

$$\begin{aligned}\Gamma_s(\omega) &= \frac{A(\omega)B^*(\omega)}{N} \\ &= \frac{Q_a(\omega)P(\omega)Q_s^*(\omega)P^*(\omega)}{N} \\ &= Q_a(\omega)Q_s^*(\omega)S_{pp}(\omega) \end{aligned} \tag{3.31}$$

where $S_{pp}(\omega) = \frac{P(\omega)P^*(\omega)}{N}$ is the power spectral density of the P(Y) signal before the GPS antennas. In the time domain, the output signal at the end of the cross-correlator is the inverse Fourier transform of Equation (3.30). That is

$$\gamma_{xy}(\tau) = q_a(\tau) * q_s(-\tau) * \gamma_p(\tau) \tag{3.32}$$

where $q_a(\tau)$, $q_s(\tau)$ are the impulse responses of watermark filters in the authenticator and the supplicant, respectively; $\gamma_p(\tau)$ is the auto-correlation function of the P(Y) signal as shown in Equation (3.6). Even though the P(Y) signal is a random sequence, the cross-correlation of two filtered P(Y) signal is a deterministic signal.

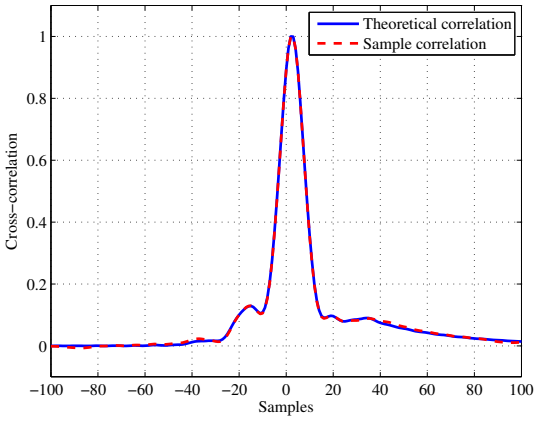

Figure 3.22: cross-correlations comparison

The error of the estimator is very small when the number of samples are very large. Figure 3.22 is a simulation which compares two cross-correlations. The theoretical correlation in Figure 3.22 is calculated using Equation (3.32). Figure 3.23 is the difference between the two correlations in Figure 3.22. It shows that the error is very small. Further, this error, $\alpha\beta\delta_{\gamma_k^{fg}}$, is multiplied by a very small value $\alpha\beta$. Thus the effect of this item in Equation (3.18) can be ignored.

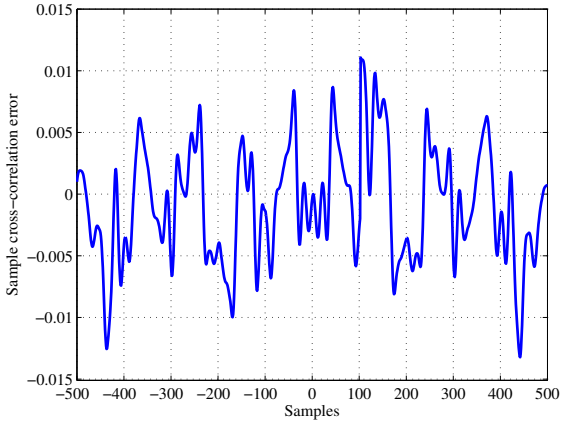

Figure 3.23: Error of filtered P code sample cross-correlation

3.3.7 Accuracy: Shift Time Estimator

After the deterministic component and the noise at the output of the sample cross-correlator has been determined, an estimator can be constructed and the performance of the estimator can be evaluated.

As discussed in Section 3.3.1, the shift time can be measured by finding the time when the maximum value of the auto-correlation happens if there is no noise. For the GPS position authentication system, if there is no noise, the method to measure the shift time is to find the maximum value of the cross-correlation between two watermark signals in the two GPS receivers. It is because the filters of the P(Y) signal in two receivers are different. With noises in the input of sample cross-correlator, the output of the cross-correlator includes not only the cross-correlation also the noise floor. Thus the task to measure the shift time of the watermark signal is converted to measure the shift time of the cross-correlation of the watermark signals in the output of the sample cross-correlator. The cross-correlation of the watermark signals is a deterministic signal as discussed in Section 3.3.6. And the covariance of the noise floor is known once we know the noise models of two receivers. Thus measuring the shift time of the cross-correlation between two watermark signals is the problem of estimating a deterministic signal from a colored WSS Gaussian noise with known covariance.

With the conversion above, we can use a simplified notation to describe the shift

time estimation problem. Note that we are assuming the P(Y) signal is received at both the authenticator and the supplicant. Thus this is only an estimation problem. To determine if the watermark signal is received or not is the detection problem discussed later. The mathematical description of the estimation is below: We have a measurement sequence $z(n)$ which includes a deterministic signal $s(n-n_0)$ and a noise $w(n)$. That is

$$z(n) = s(n - n_0) + w(n) \tag{3.33}$$

where the shift time n_0 is to be estimated. Comparing Equation (3.33) with Equation (3.17) and (3.18), we have $s(n - n_0) = \alpha\beta\hat{\gamma}_k^{fg}$, $w(n) = \Delta\hat{\gamma}_k^{xy}$. The product $\alpha\beta$ in $s(n - n_0) = \alpha\beta\hat{\gamma}_k^{fg}$ is known because they can be calculated using the C/N_0 values which are available for civilian GPS receivers. The noise $w(n)$ is a WSS colored Gaussian random process with the covariance described in Equation (3.29).

The estimator to solve Equation (3.33) is a match filter which is discussed in [14, 22]. The match filter for a white Gaussian noise is

$$\sum_{n=n_0}^{n_0+N-1} z(n)s(n - n_0) \tag{3.34}$$

which is also a cross-correlator between the measurement $z(n)$ and the template signal $s(n)$. When the noise $w(n)$ is a colored Gaussian noise sequence, it needs to be pre-whitened before the match filter in Equation (3.34) can be applied [22]. The pre-whitening filter does not change the performance of the estimator.

The whitening filter can be found using Equation (3.22) and (3.24). With the PSD of a colored WSS Gaussian noise, whitening is equivalent to do the spectral factorization of the PSD [23]. If the filters $H_a(\omega)$ and $H_s(\omega)$ in Equation (3.22) are minimum phase filters, the inverse of them exist. Denoting the inverse filters as $H_a^{-1}(\omega)$ and $H_s^{-1}(\omega)$, the whitening filter is $H_a^{-1}(\omega)H_s^{-1}(\omega)$. For the physical filters in the GPS receivers, they are usually minimum phase filters. If there are delay components in the receiver, we can remove the delay components when we model the receiver noise model so that $H_a(\omega)$ and $H_s(\omega)$ are minimum phase filters. Removing the delay component will introduce bias to the shift time estimate. But this bias is a constant for all the satellites. Since we use relative delays to calculate the authentic position as described in Section 2.4, this constant bias does not affect the positioning method used in the GPS position authentication system.

By pre-whitening the measurement $z(n)$ using the whitening filter $H_a^{-1}(\omega)H_s^{-1}(\omega)$ we have the new signal

$$z_1(n) = s_1(n - n_0) + w_1(n) \tag{3.35}$$

where $w_1(n)$ is a WSS white Gaussian random process and $s_1(n) = s(n) * h_m^{-1}(n) * h_s^{-1}(n)$ is the signal after $s(n)$ passes through the filter $H_a^{-1}(\omega)H_s^{-1}(\omega)$. Then the match filter for Equation (3.35) is

$$\sum_{n=n_0}^{n_0+N-1} z_1(n)s_1(n - n_0) \tag{3.36}$$

Appendix D shows that the cross-correlation

$$\frac{\mathbf{y}_2\mathbf{G}\mathbf{x}}{N} = \frac{\left(\mathbf{V}_{aM}\mathbf{y}_2\right)^T \left(\mathbf{H}_s^{-1}\mathbf{x}\right)}{N} \tag{3.37}$$

is an asymptotic maximum likelihood estimator (MLE) when the number of the samples tends to infinity. $\mathbf{V}_{aM}$ and $\mathbf{H}_s^{-1}$ are whitening filters to whiten the base band noise in the authenticator and the supplicant, respectively. Both the estimator in this section and the estimator in Appendix D use the whitening filters. The difference is where in the signal chain the whitening filters are. The estimator in Appendix D uses two separate filters before the sample cross-correlator while the estimator in this Section cascades two whitening filters together and applies them at the end of the sample cross-correlator. The total performance of two estimator are the same.

If the filters of the noise path and the watermark path are the same, i.e. $H_a(\omega) = Q_a(\omega)$ and $H_s(\omega) = Q_s(\omega)$, $s_1(n)$ is converted back to the auto-correlation function of the P(Y) signal.

The performance of the estimator has been discussed in [14]. The match filter in Equation (3.35) is optimal in the sense of both minimum variance and maximum likelihood. It is unbiased estimator. The error of the estimate is Gaussian distributed and the variance of this error achieves the Cramer-Rao Lower Bound (CRLB). The CRLB of the estimator in Equation (3.35) is given by

$$\sigma_{\hat{n}_0}^2 \geq \frac{\sigma_{w_1}^2}{f_s \int_0^{+\infty} \left(\frac{\mathrm{d}s_1(t)}{\mathrm{d}t}\right)^2 \mathrm{d}t} \tag{3.38}$$

where $\sigma_{w_1}^2$ is the variance of the noise w_1 in Equation (3.35), f_s is the sampling frequency. Equation (3.38) shows that sampling frequency and filters in the receivers affect the accuracy of the shift time estimate. Another factor which affects the accuracy is the number of the samples. As shown in Equation (3.29), the variance of $w_1(n)$ will decrease with increasing N.

The filters in the receiver affect the variance by changing the shape of $s_1(t)$. The amplitude of the signal also affects the variance. In these parameters, the effect of the filters is implicit. To see how other explicit parameters are related to the accuracy of the shift time, we simplify the problem by assuming filters in both the authenticator and the supplicant are all pass filters. In this situation, $s_1(t)$ is proportional to the auto-correlation function of the P code as shown in Equation (3.6). That is,

$$\frac{\mathrm{d}s_1(t)}{\mathrm{d}t} = \begin{cases} 0 & \text{if } t < -T_p \\ \frac{\sqrt{\alpha\beta}}{T_p} & \text{if } -T_p \le t < 0 \\ -\frac{\sqrt{\alpha\beta}}{T_p} & \text{if } 0 \le t < T_p \\ 0 & \text{if } t \ge T_p \end{cases} \tag{3.39}$$

where T_p is the duration of one chip of P(Y) code. Further we get

$$\int_0^{+\infty} \left(\frac{\mathrm{d}s_1(t)}{\mathrm{d}t}\right)^2 \mathrm{d}t = \frac{2\alpha\beta}{T_p} \tag{3.40}$$

Then Equation (3.35) can be simplified as

$$\sigma_{\hat{n}_0}^2 \ge \frac{1}{f_s f_p N \alpha\beta} \tag{3.41}$$

where f_p is the chip rate of the P(Y) signal, N is the number of samples. The typical values of them are: $\alpha\beta$ =0.0042, N=5e6, f_s=100 MHz and f_p=10.23 MHz. Substituting these values into Equation (3.41), we have $\sigma_{\hat{n}_0} \ge$ 2.16e-10 second. This value is obtained in an extreme condition. The filters in the receiver make the signal $s_1(t)$ much smoother than the triangular auto-correlation function of the P(Y) signal. But the variance bound shows that we are able to achieve the accuracy of the shift time within one sample period (10 ns for 100MHz sampling frequency). When the models of the filters are available, the detail analysis can be performed using Equation (3.38).

3.4 False Alarm Rate: Watermark Detector

With the same problem description in Section 3.3.7, the detection of the watermark signal is discussed in this section. From the perspective of detection theory, this is a classical unknown arrival time problem [24].

We denote $\mathcal{H}_0$ as the hypothesis that the supplicant does not receive the P(Y) signal, and denote $\mathcal{H}_1$ as the hypothesis that the supplicant receives the P(Y) signal. Now Equation (3.35) can be cast into the detection problem as

$$\begin{aligned} \mathcal{H}_0 &: z_1(n) = w_1(n) \\ \mathcal{H}_1 &: z_1(n) = s_1(n - n_0) + w_1(n) \end{aligned} \tag{3.42}$$

A generalized likelihood ratio test (GLRT) is given as a detector in [24] to address this type of problem. The test statistics is given by

$$T(\mathbf{z}_1) = \sum_{n=\hat{n}_0}^{\hat{n}_0+N-1} z_1(n)s_1(n - \hat{n}_0) \tag{3.43}$$

where $\mathbf{z}_1$ is the vector form of the pre-whitened signal given in Equation (3.35). We decide $\mathcal{H}_1$ if

$$T(\mathbf{z}_1) \geq \gamma \tag{3.44}$$

where γ is the threshold value based on the required false alarm rate. If the threshold is exceeded, we declare that the watermark signal is detected; otherwise we declare that there is only noise. Comparing the test statistic, Equation (3.43), with the match filter in Equation (3.35), we can see that they are the same. Therefore the whole detection process can be described as follows: First the measured signal $z_1(n)$ is cross-correlated with the signal $s_1(n)$. When the maximum value is found, we take this delay time as $\hat{n}_0$. Then the maximum value is compared with the threshold γ. If it exceeds the threshold, we declare that the watermark signal exists in the supplicant RF snapshot.

The threshold γ is determined by the distribution of the test statistic $T(\mathbf{z}_1)$. The test statistic in Equation (3.43) can be written as

$$T(\mathbf{z}_1) = \max_{n_0} \sum_{n=n_0}^{n_0+N-1} z_1(n)s_1(n - n_0) \tag{3.45}$$

From Equation (3.45), we can see that we need to determine the maximum of correlated Gaussian random numbers to determine the PDF of $T(\mathbf{z}_1)$. There is no closed form to express the distribution of this maximum problem. Numerical method such as Monte Carlo simulation can be used to get the distribution of the test statistic. Then the threshold value γ can be determined.

3.5 Effect of the Sampling Frequency Difference

Up to this point, an implicit assumption has been that the sampling frequencies of the authenticator and the supplicant are the same. In reality, it is impossible for the two sampling frequencies to be the same because of the clock bias. This section examine how this difference affects the estimation and detection performance.

When the sampling frequencies are different, the digitized signal sampled by a higher frequency is compressed compared with the signal sampled by a lower frequency, when two digitized signals are aligned sample by sample. This is equivalent to introducing an additional Doppler frequency into the signal. The effect of the Doppler frequency on an ambiguity function is discussed in [25]. Similar to the ambiguity function, we can expect that the deterministic component, $\alpha\beta\hat{\gamma}_k^{fg}$, in Equation (3.17) decreases when the sampling frequencies are different.

The results below shows how sensitive the deterministic component is to the sampling frequency difference. Figure 3.24 shows that the authenticator has a sampling frequency, F_s= 100.010696 MHz, which is different from the sampling frequency of the supplicant. For the authenticator, if we assume the sampling frequency is 100MHz, we have the clock bias from the GPS position solution. It is in the unit of length. The error of the receiver sampling clock (the vertical axis) increases in a linear relationship with the time (the horizontal axis). The slope of the fitted line is the frequency error of the sampling clock. If the correct sampling frequency (100010696.2 Hz) is used to solve the GPS position and time solution, the clock error does not change with time. We can do the same process of the supplicant. The sampling frequency of the supplicant, F_s= 100.001761 MHz, is shown in Figure 3.25. The frequency difference is 8935 Hz. The relative difference is 89 ppm.

Figure 3.26 shows the cross-correlation peak value when the number of the samples

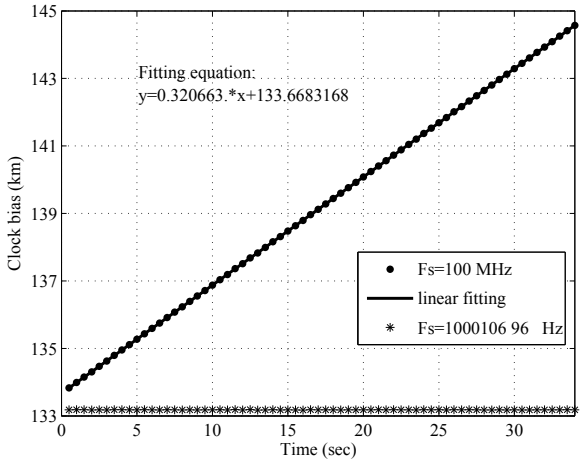

Figure 3.24: Clock bias of authenticator

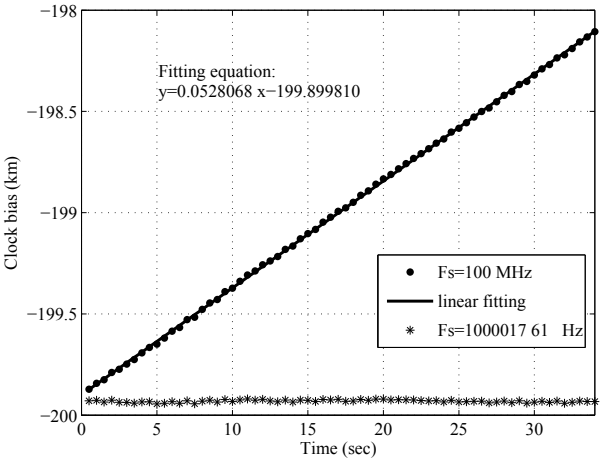

Figure 3.25: Clock bias of supplicant

used for correlation changes. The longer the cross-correlation length, the greater the drop of the peak. When the cross-correlation length is large, the mismatch between the two watermark signals becomes bigger.

As discussed before, the effect of the sampling frequency difference is the same as the Doppler frequency in the signal. It is also has the same effect as if through the chip rate of the P(Y) changed. In Figure 3.26, the dashed line is from a simulation. In this simulation the chip rate of P code is changed corresponded to the sampling frequency difference. When the amplitudes of the P code signals also match that of the real data, we get the same pattern of the peak change. This simulation shows that the effect of sampling frequency difference is analogous to the effect of chip rate change of the auto-correlation function of the P code.

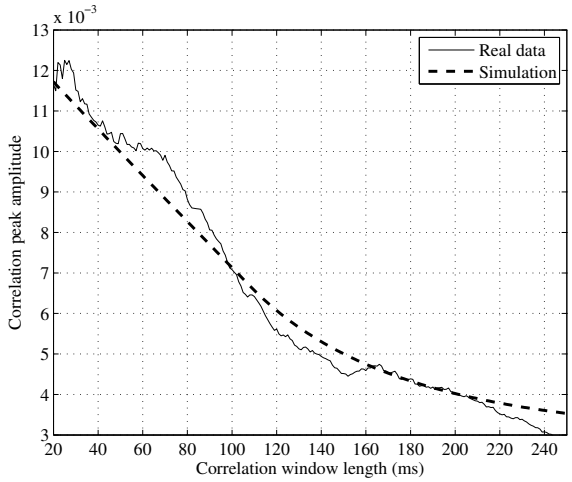

Figure 3.26: Correction peaks affected by chip rate difference (PRN 7)

3.6 Summary

It was shown that the shift time can be estimated using a cross-correlator based estimator. Even though this estimator is suboptimal, it is feasible to obtain a satisfactory accuracy by increasing the number of samples used in the calculation. The shift time measurement problem was cast into a standard framework to estimate a deterministic signal in a colored Gaussian noise using some reasonable engineering approximations. The accuracy of the estimator and the false alarm rate are both affected by the filters in the signal paths of the authenticator and the supplicant. The parameters of these filters can be tuned to obtain the optimal performance of the shift time estimation. Another approach to improve the accuracy of the shift time estimate is to increase the signal length of the cross-correlation. But this approach has a practical limitation which is the clock bias of the receivers. Increasing the signal-to-noise ratio of the authenticator has direct effect on improving the accuracy of the estimation. In the next chapter, the idea from Chapter 2 and 3 are used to realize a prototype authentication system.

Chapter 4

Experimental Validation

In this chapter we discuss the design of two prototype receivers built to test the authentication algorithm described in Chapter 2. Experimental validation to confirm the findings of Chapter 2 and Chapter 3 are then presented. We first provide a description of the hardware and software developed as part of these prototypes. The purpose of this description is to help other investigators to replicate our hardware design and signal processing algorithms. Then we describe a field test performed to validate the system performance.

4.1 Requirements for Authentication Receivers

The receiver used in the authentication system must have features normally not found in current standard GNSS receivers. First, it must have a RF front end with a large bandwidth. The authentication method uses the P(Y) signal as the watermark to do the authentication. The RF front-end bandwidth of the authenticator, therefore, should be greater than 20.46 MHz. Furthermore, it must be coupled with a GPS antenna with a bandwidth of at least ± 10 MHz. Secondly, the RF front end must have low noise.The authentication method use a noisy P(Y) piece at the authenticator as a template to detect if that P(Y) piece exists in the supplicant's raw IF signal. So the detection is very sensitive to the noise in both the authenticator and the supplicant. Thus, the authenticator should be designed to have less noise than the supplicant receiver. Finally, it must have high data bandwidth. This is because the positioning accuracy depends

on the accuracy of the differential pseudorange measurement (Equation (2.10)) which is determined from time difference measurements. The accuracy of this time difference depends on the sampling frequency used to digitize the IF signal. High sampling frequency means high data bandwidth after the sampling.

4.2 System Description

The authenticator designed for this work shown schematically in Figure 4.1 satisfies the above requirements.

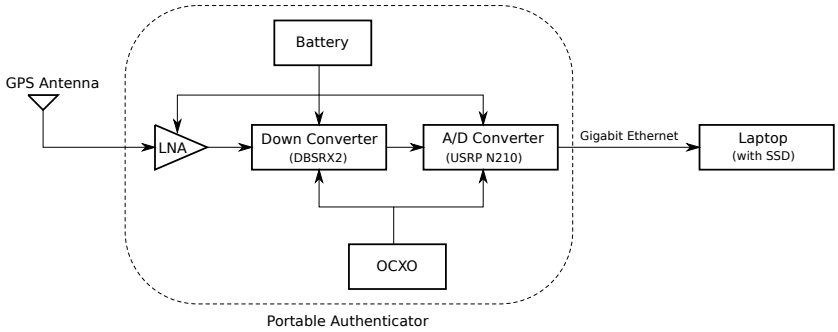

Figure 4.1: Schematic diagram of the authenticator receiver

The system built on the USRP2 software defined radio. The radio and antenna are shown in Figure 4.2.

Figure 4.2: Devices to assemble prototype

Most of the components and devices are purchased from commercial vendors as listed in Table 4.2. The components in Figure 4.2 are packaged into the final system shown

	Name	Part No	Qty.	Vendor
1	USRP2	USRP2-PKG	2	Ettus
2	Daughter Board	DBSRX2	2	Ettus
3	MIMO Cable	MIMO-Cable	1	Ettus
4	LNA	ZRL-2400LN+	4	MiniCircuits
5	GPS Antenna	ANT-35C1GA-TW-N	2	Navtech GPS
6	Power Supply	675-MB12-1.7A	2	Mouser
7	SSD Hard Disk	SSDSA2MH120G2K5	1	Newegg

Table 4.1: Device list

in Figure 4.3. This authenticator integrates the RF front end and IF signal sampling. The authenticator is directly connected to an active GPS antenna. The RF front end supplies the power to the antenna. The RF signal from the antenna is amplified by the Low Noise Amplifier (LNA) before it is down converted to the IF signal. The IF signal is digitized by the analog to digital (A/D) converter. Then the digital IF signal is transmitted to the computer through the Gigabit Ethernet connection.

Figure 4.3: A prototype authenticator receiver

The IF signal processing unit in the authenticator is based on USRP N210 software

defined radio [26, 27]. It offers the function of down converting, digitization and data transmission. The firmware and FPGA configuration in the USRP N210 are modified to integrate a software automatic gain control (AGC) and to increase the data transmission efficiency. The sampling frequency is 100MHz and the effective resolution of the A/D is 6 bits. The maximum data bandwidth is limited by the Gigabit Ethernet. The authenticator integrates an optional power source in the form of a battery which can power the system for up to 4 hours at full load.

The software to process the IF data is written in the Matlab where the SoftGNSS software [28] is used to get a C/A code solution. The watermark signals are also obtained from the SoftGNSS with some modifications of the original scripts.

As shown in Figure 4.1, the prototype receiver consists of one GPS antenna, two low noise amplifiers(LNA), one USRP2 [27] motherboard, one receiver daughter board, one Laptop and power suppliers. The RF signal received at the GPS antenna is amplified by two cascaded LNAs. The amplified RF signal is fed to the DBSRX [26] daughter board to convert to IF band. The DBSRX board also does the I/Q demodulation. The output signals from the DBSRX board include the in phase component $I(t)$ and the quadrature component $Q(t)$. The USRP2 mother board converters the input analog signal into digital signal at first. A digital down converter (DDC) is implemented after the A/D converter to eliminate the IF signal. The digital signal after the DDC can also be decimated to a lower sampling frequency so that the sampling data can be transmitted in a low data rate. The USRP2 use the Ethernet connection to communicate with a host computer. Both the control commands and the sampling data are transmitted in this Gigabit Ethernet port. After the sampling data is received by the Laptop, it is saved to a file for the post processing. Traditional spinning hard disk can not handle the high streaming speed of the sampling data so a solid state disk (SSD) is used to record the data stream.

USRP2 is a hardware development platform for the open source project GNU Radio [29]. It is dedicated to the software defined radio (SDR). Using USRP2 platform to construct the recorder has a few advantages. The fist advantage is that the source codes for the embedded system and the host computer are completely open source. The second advantage is that the USRP2 has a high speed expansion port. This port is a MIMO (multiple input multiple output) synchronization bus. Data up to 200MB/sec

and synchronization clock can be transmitted through this port. Using this port, two USRP2 radios can be synchronized into a master-slave network to do more complex processing. This port can also be used to group more than 2 USRP2 into a network with a HUB. The third advantage is that it is cheaper than other SDR platforms. The fourth advantage is that the USRP2 has rich FPGA resource for customized functions. The manufacturer of the FPGA is Xilinx.

The receiver daughter board DBSRX is a zero IF I/Q demodulator. It can directly convert a RF signal into baseband signals $I(t)$ and $Q(t)$ without any IF component. However, in this application the output signal from DBSRX still has the IF component. This is determined by the GPS signal characteristics and the zero IF receivers' characteristics. The advantage of zero IF receivers is its simple structure with only one stage. But the leakage energy from the local oscillator to the RF input will turn to a DC signal at the output of the receiver. Thus the suitable application field of the zero IF receiver is where baseband signal has no DC component such voice signal. To overcome this, most zero IF receivers has a high pass filter at its output. After this high pass filter the output signal has only little DC component which can be treated as error in the post processing of data. The DBSRX board has a 800Hz high pass filter. Both the GPS C/A code signal and the P(Y) signal have DC components. Thus we can not use zero IF structure for the GPS signal recorder.

4.2.1 Analog Signal Processing

Figure 4.4 lists the spectrum change before the output of the DBSRX board. Figure 4.4 (a) is the signal at the antenna of one GPS satellite. Its center frequency is the carrier frequency f_c of GPS L1 band. When the signal arrives at the receiver's antenna, it has a Doppler shift Δf as shown in 4.4 (b). The signal after the receiver's antenna is amplified by two LNAa and a variable gain amplifier (VGA) before the mixers MIX_I and MIX_Q. These amplifiers ensure the signal has proper power level. After the mixers the spectrum of the signals are shown in 4.4 (c). It has a desired component centered at $f_{IF} + \Delta f$ and a undesired component centered at $f_c + 2f_{IF} + \Delta f$. The undesired part is filtered by a low pass filter. The signal shown in 4.4 (d) is the resulting signal spectrum at the output of the DBSRX board. In 4.4 (d) the f_{ch} is the corner frequency of the low pass filter. It can be programmed from 4MHz to 33MHz. The f_{cl} in 4.4 (d)

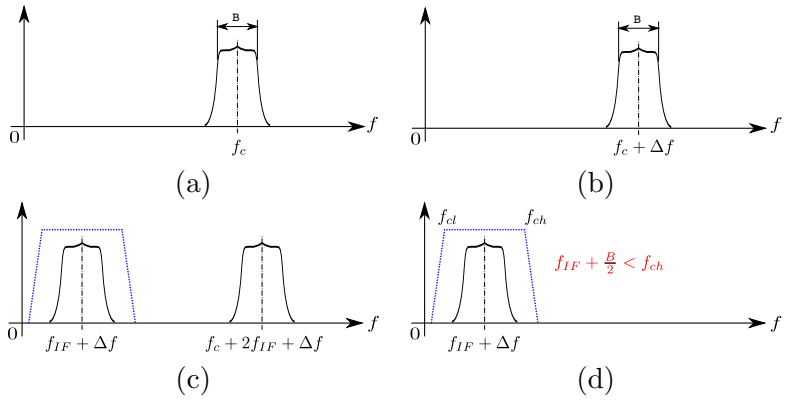

Figure 4.4: Spectrum change in the I/Q demodulator

is the 800Hz corner frequency of the high pass filter explained earlier.

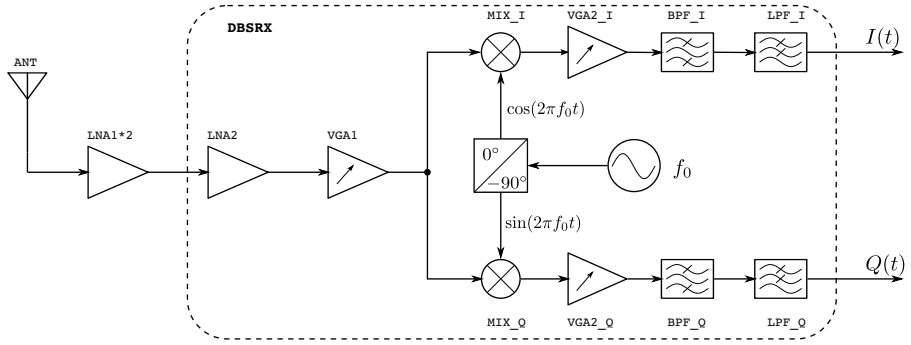

Figure 4.5: Analog signal processing diagram

Figure 4.5 shows the detail of the analog signal processing. The signal strength at the receiver's antenna is very weak (about -160dBm). It needs to be amplified to satisfy the input power requirement of the mixer. The mixer requires an input power above -77dBm to generate the full scale output at the output pins of the DBSRX. The gain assignment is shown in Figure 4.6.

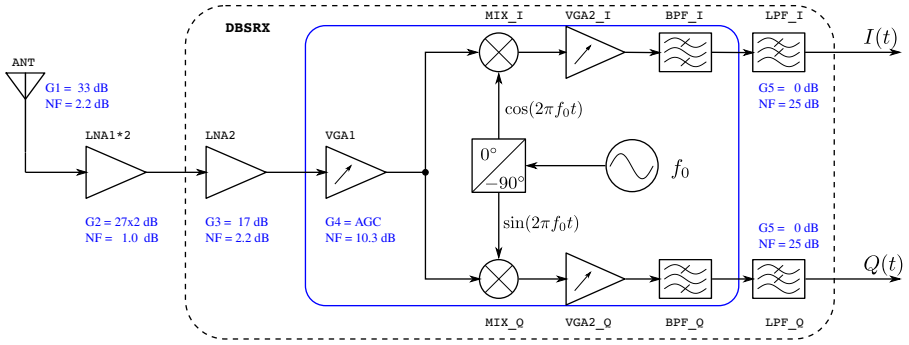

Figure 4.6: Gain assignment of the receiver

The signal powers at different points are shown in Figure 4.7. By using two LNAs, the total noise figure of the analog part is only 2.2 dB which is dominated by the antenna. This means that the SNRs of $I(t)$ and $Q(t)$ only increase 2.2 dB compared to the SNR of the signal at the receiver.

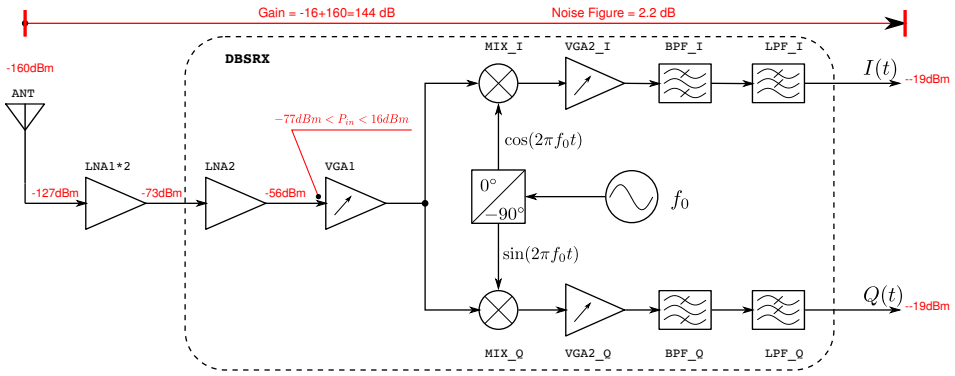

Figure 4.7: Signal power of the receiver

Figure 4.8 provides the mathematical expression of the signal as it processed from antenna down the analog processing part of the receiver. The choice of the f_{IF} value will be explained in later.

4.2.2 Digital Signal Processing

The $I(t)$ and $Q(t)$ are fed to 2 A/D converters inside the USRP2 mother board. The sampling frequency of two clock synchronized A/D converter is $f_s = 100MHz$ which is the maximum sampling frequency of the A/Ds. The detail structure of the digital part

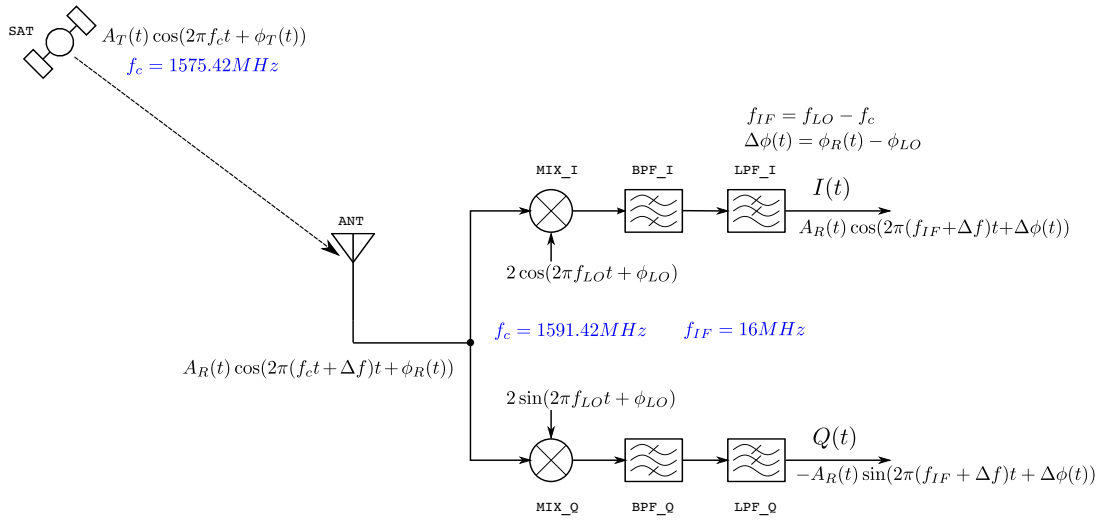

Figure 4.8: Mathematical signal expression of the analog part

is shown in Figure 4.9. A digital down converter (DDC) is immediately after the A/D to eliminate the IF component. The DDC includes a DC offset correction component. This will correct some DC offset caused by the gain mismatches and phase mismatches in the previous analog processing unit. The DC offset correction component is mainly an integrator.

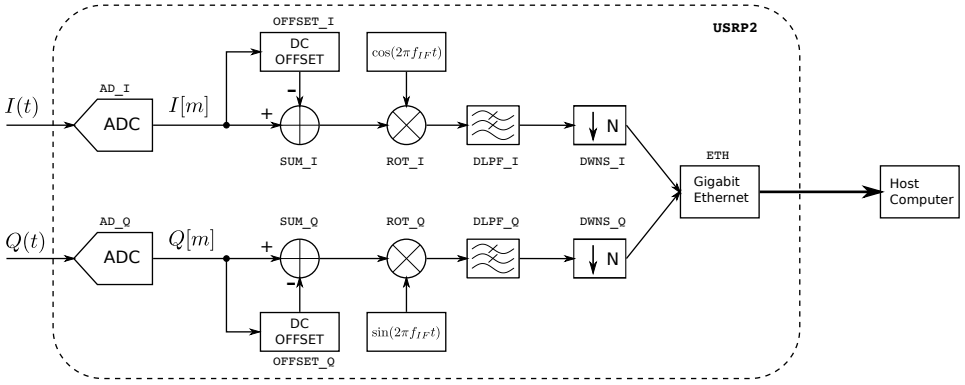

Figure 4.9: Digital signal processing diagram

The core in the DDC is a CORDIC (COordinate Rotation DIgital Computer) unit. The function of the CORDIC is shown in Figure 4.10. It rotates a vector $\begin{bmatrix} I(t) & Q(t) \end{bmatrix}$ by an angle of $2\pi f_{IF}t$. This process eliminate the IF components in $I(t)$ and $Q(t)$. The

advantage of the CORDIC is that it only uses addition and shift operations. This makes it very suitable for implementing in FPGAs. It is also very efficient in computation.

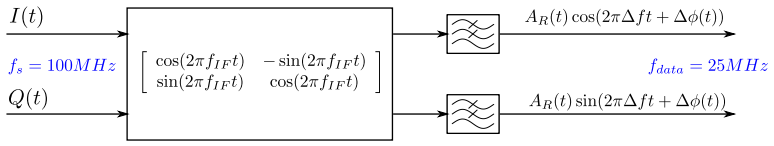

Figure 4.10: Mathematical expression of the digital signal processing

4.2.3 f_{IF} Selection

If the f_{IF} in Figure 4.4 is improper, the spectrum overlapping might happen. The overlaps happen in the mixer and the A/D converter. Once the overlapping occurs, the sampled digital signal does not represent the original baseband signal. To avoid the spectrum overlapping, some constraints need to be satisfied in the system. In Figure 4.4(d),

$$f_{IF} + \frac{B}{2} < f_{ch} \tag{4.1}$$

need to be satisfied to make sure the whole useful signal is not filtered out by the low pass filter. Figure 4.11 shows the sampling effect of the $Q(t)$ and $I(t)$ signal.

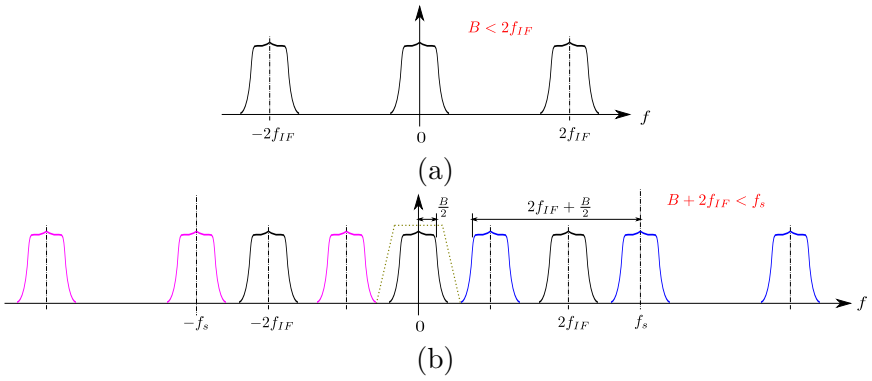

Figure 4.11: Spectrun chenge caused by sampling

To avoid the overlapping, the condition in Equation (4.2) need to be satisfied.

$$\begin{aligned} B &< 2f_{IF} \\ B + 2f_{IF} &< f_s \end{aligned} \tag{4.2}$$

In this system f_s=100 MHz,B=25 MHz,f_{ch} =33MHz. Based on Equation (4.1) and (4.2) we can choose f_{IF}=16MHz.

4.3 Experimental Validation

First we present results that shows that we can successfully deal with the C/A leakage problem using the high-pass filter described earlier. We perform a correlation between snippets of signal collected from the authenticator and a second USRP N210 software defined radio. Figure 4.12 is the correlation result without the high-pass filter. The periodic peaks in the result have a period of 1 ms and are a graphic representation of the C/A leakage problem. Because the noise, these peaks do not have the same amplitude. Figure 4.13 shows the correlation result using the same data snapshot as in Figure 4.12 where the high-pass filter is used to attenuate the false peaks caused by the C/A signal residual. Only one peak appears in this result as expected and, thus, confirms the analysis given earlier in this thesis.

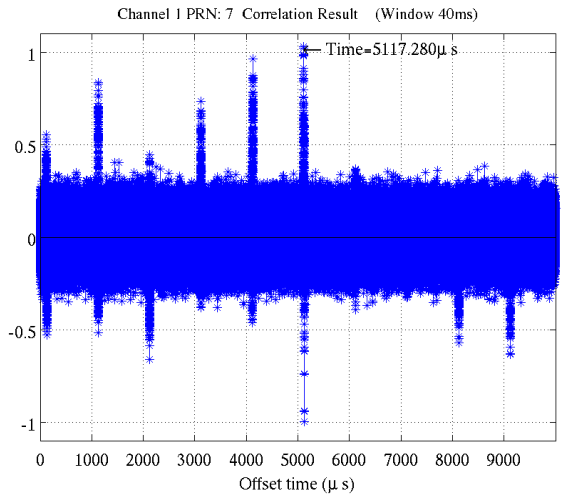

Figure 4.12: Correlation detection without high-pass filter

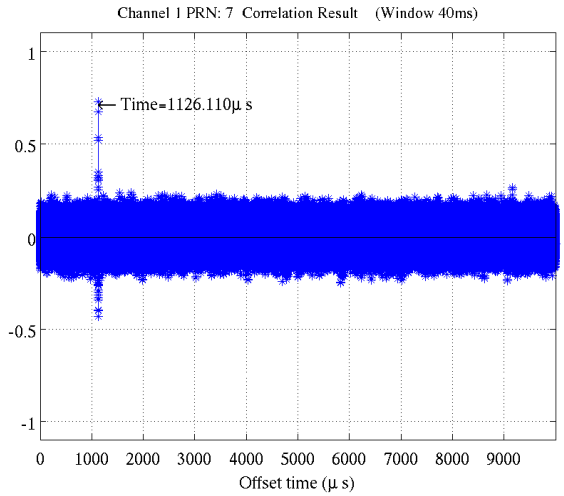

Figure 4.13: Correlation detection with high-pass filter

Figure 4.14 is a zoom in of the area around the peak in Figure 4.13 to assess the accuracy of the peak detection. The method to calculate the "Expected Peak Time" in Figure 4.14 is described below. The true positions of the supplicant and the authenticator are both known in the experiment. So the pseudoranges from both the supplicant and the authenticator to GPS satellites are known. Referring back to Equation (2.12), we rearrange it as

$$\begin{aligned} t_{21} - \chi_{21} &= \frac{1}{c}[(\rho_2^a - \rho_1^a) - (\rho_2^s - \rho_1^s)] \\ t_{31} - \chi_{31} &= \frac{1}{c}[(\rho_3^a - \rho_1^a) - (\rho_3^s - \rho_1^s)] \\ t_{41} - \chi_{41} &= \frac{1}{c}[(\rho_4^a - \rho_1^a) - (\rho_4^s - \rho_1^s)] \end{aligned} \tag{4.3}$$

The quantities on right side of Equation (4.3) are all known and are to calculate the "Expected Peak Time" in Figure 4.14. The left side is equivalent to the measured peak time.

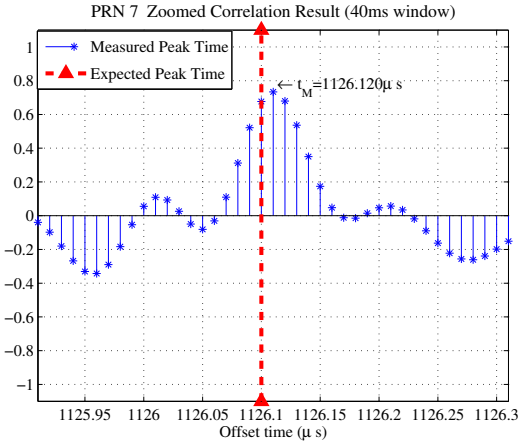

Figure 4.14: Measured peak time and expected peak time

It is interesting to note that in the absence of the C/A code high pass filter, not only do we have multiple peaks but the largest peak may be the incorrect peak. This can be seen in Figure 4.12 where the largest peal occurs at $t = 5117.280\mu s$. The correct peak at $t = 1126.120\mu s$ is smaller than the false peak at $t = 5117.280\mu s$.

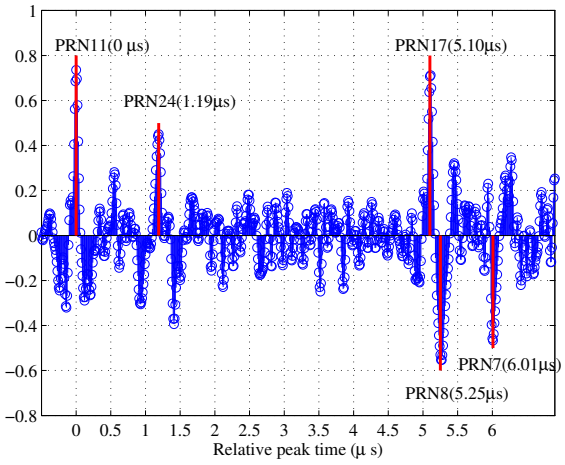

Figure 4.15: Delays between multiple P(Y) peaks

Figure 4.15 shows the P(Y) correlation peaks when there are several common satellites in view. Five P(Y) correlation peaks are shown where each peak corresponds to one common satellite. The time difference between these peaks is constrained by and must

be consistent with the pseudorange double differences given in Equation (2.12). The second column in Table 4.2 shows the measured pseudorange double difference using the C/A code. The third column lists this difference in time units. Comparing the values in the third column with those obtained from the P(Y) peak difference given in Figure 4.15 shows that the P(Y) peak time measurements have a very high accuracy.

Table 4.2: Relative delays between multiple P(Y) peaks

Satellite	$\Delta\rho$ **(m)**	Δt (μs)
i	$\rho_{11} - \rho_i$	$\Delta\rho/c$
PRN 11	0	0
PRN 24	358	1.19
PRN 17	1530	5.10
PRN 8	1576	5.26
PRN 7	1802	6.07

Next we describe an experiment to validate the operation of the system in an operational scenario similar to those described in the introduction of this thesis. We refer to this scenario as the Five Point Test and has the authenticator and the supplicant separated by about 1 mile. The location of the authenticator is fixed. The supplicant is then sequentially placed at five points along a straight line. The distance between two adjacent points is about 15 meters. The supplicant is in a open space so that there are a sufficient number of satellites in view and multi-path, if any, is minimal. The locations of the 5 test points are shown in Figure 4.16.

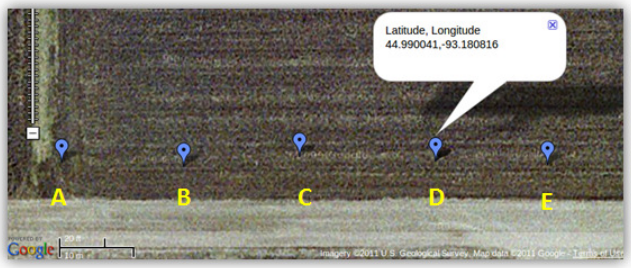

Figure 4.16: Five-point field test

The first step of the five-point test was to place the supplicant at point A and collect

a 40 ms snippet of data. This data was then processed by the authenticator to determine if: (1) The signal contained the water mark (signal authentication) (2) The supplicant is actually at the position coordinates that they say they are (position authentication). Then the supplicant is moved to point B. However, in this instance, the supplicant reports that it is still located at point A. That is, they make a false position report. Thus, if an authentication test is performed on the RF data collected from point B, it will pass the signal authentication test (i.e., check for the watermark) but should fail the position authentication test. This is repeated for the remaining positions (C through E) where at each point the supplicant reports that they are located a point A. That is, the supplicant continues to make a false position report.

In this experiment, we have five common satellites between the supplicant (at all the test points A to E) and the authenticator. The results of the five-point test are summarized in Table 4.3. If we can detect a strong peak for every common satellite, we say this point passes the signal authentication test (and note "Yes" in second column of Table 4.3). That means the supplicant's raw IF signal has the watermark signal from every common satellite, implying that authentic GPS signals and not a spoofer's signal are being used by the supplicant. Next, we perform the position authentication test. This test tries to determine whether the supplicant is at the position they claim to be. In essence this test consists of calculating the time where the correlation peak between supplicant and authenticator's signal occurs based on the supplicant position report. Then this time is compared to the peak time observed from the data transmitted by the supplicant. If there is a mismatch between the peak times, this is an indication of an incorrect or false position report. In this instance we note that the supplicant has failed the position authentication test and mark "No" in the third column of Table 4.3.

If a failure of the position authentication test occurs, a third test is performed. This test consists of determining the position of the supplicant using the data in the RF snippet. Then a determination is made whether the calculated position matches the position coordinates of the points from which the report was made. We note that in practice this last test cannot be performed because the authenticator will not have access to the true position coordinates of the supplicant. In the test performed for this thesis, we do have access to the supplicants true location. The point of performing this third test is to demonstrate the resolution capability of the authenticator. That

is, can we detect a position falsification less than some threshold? In this case, since the reporting points are separated by 15 meters, we will be determining whether the resolution of the authenticator is better than 15 meters. The third test is performed by comparing the measured peak delays (i.e., the $\hat{t}_{ij}$ in Equation (2.11)) with the expected peak delays. The expected peak delay are obtained by using the supplicant's true positions to calculate the pseudorange differences. For every common satellite, if a strong correlation peak is detected at the expected time, we denote that it passes the measurement test (and note "Yes" in fourth column of Table 4.3). Even though the position solution is not recalculated using the method described in Section 2.4, we still can conclude that correct position solution can be obtained because the measurements match the true position.

The five-point test result shows that even though the wrong positions of points (B,C,D,E) are reported, the authenticator can detect the inconsistency between the reported position and the raw IF data. Furthermore, since the distance between two adjacent points is 15 meters, this implies that resolution of the position authentication is at or better than 15 meters.

Table 4.3: Five-point position authentication results

Location	**Successful Signal Authentication?**	**Successful Position Authentication?**	**Successful Delay Measuring?**
A	Yes	Yes	Yes
B	Yes	No	Yes
C	Yes	No	Yes
D	Yes	No	Yes
E	Yes	No	Yes

4.4 Summary

This chapter described the design and construction of a pair of prototype receivers to test the GPS position authentication method developed in this thesis. The receiver are constructed from COTS hardware. Experiments to validate the performance of the prototype system was also described. The experiments show that the signal and position authentication methods developed in Chapter 2 and 3 are sound. While it was shown

that the position falsification greater than 15 m was detected, it is obvious that the resolution (based on Chapter 3 analysis) can be better than this.

Chapter 5

Conclusion and Future Research

5.1 Summary

This thesis described a GPS position authentication system. The authentication system has many potential applications where high credibility of a position report is required in application such as traffic control or cargo/asset tracking. The system detects a specific "watermark" signal in the broadcasted GPS signal to judge if a receiver is using the authentic GPS signal. The differences of the "watermark" signal travel times is constrained by the positions of the GPS satellites and the receiver. A method to calculate an authentic position using this constraint was developed. A hardware platform which accomplishes this was developed using a software defined radio. Experimental results demonstrates that this authentication methodology is sound and has a resolution better than 15 m.

This method can also be used in other GNSS system provided that watermark signals can be found. For example, in the Galileo system, the encrypted Public Regulated Service (PRS) signal is a candidate for this "watermark" signal.

The structure and the performance of the detector-estimator were presented. To achieve high positioning accuracy, low noise receiver is very important. The characteristics of the filters in the receiver affect the detection and estimation performance. The receivers can and should be optimized to help improve the detection and estimation performance.

5.2 Recommendations

The detection performance, such as the miss detection rate and the false alarm rate, are crucial for the authentication. Currently, the distribution of test statistic is hard to express in a simple closed form. Both numerical and theoretical methods are needed to obtain the distribution. Once the distribution is obtained, the miss detection rate and false alarm rate can be calculated. Efficient ways of doing this will be important before such system can be fielded.

The accuracy of the shift time estimate was discussed in this thesis. Note that the shift time is the measurement to calculate the position solution. Thus, for the accuracy of the authentic position, the error propagation from the delay time to the final position solution need to be studied. In this situation, the satellite geometry also affect the position accuracy.

One technical challenge to deploying the GPS position authentication station has to do with how to geographically distribute authentication sites. Typically an authentication station can cover an area with a radius about 100 to 200 miles. So the cost of the authentication station is also affordable. How to choose the locations of the authentication stations to optimize the position accuracy and to offer maximum coverage is a very useful topic that needs further study.

One of the challenges that limits the application of this system is the communication bandwidth. Transmitting raw RF signal through data channel is expensive. Based on the experimental results shown above, a 40 ms snapshot is about 2 MB which is about the size of a typical picture file on the Internet. The 3G cell phone network is capable to transmit this data size. If the 4G network is used, its bandwidth is wide enough to transmit this size of data. To lower the cost, either the data compression method or the detection method using less data samples need to be studied. For the detector/estimator, the question that needs to be answered is what the least data requirement is to achieve a giving performance.

References

[1] Nextgen. http://www.faa.gov/news/fact_sheets/news_story.cfm?newsid=8145.

[2] FleetMatics. http://www.fleetmatics.com/.

[3] WirelessMatrix. http://www.wirelessmatrix.com/.

[4] Todd E. Humphreys, Brent M. Ledvina, and Paul Y. Montgomery. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In *Proceedings of the 2009 International Technical Meeting of The Institute of Navigation*, Disney's Paradise Pier Hotel, Anaheim, CA, January26–28 2009.

[5] William J. Bencze, Bryan Galusha, Brent M. Ledvina, and Isaac Miller. An in-line anti-spoofing device for legency civil GPS receivers. In *Proceedings of the 2010 International Technical Meeting of The Institute of Navigation*, Catamaran Resort Hotel, San Diego, CA, January25–27 2010.

[6] Sherman Lo, David De Lorenzo, Per Enge, Dennis Akos, and Paul Bradley. Signal authentication: A secure civil GNSS for today. *Inside GNSS*, pages 30–39, September/October 2009.

[7] Scott Logan. Spoofs, proofs & jamming: Towards a sound national policy for civil location and time assurance. *Inside GNSS*, pages 42–53, September/October 2012.

[8] Galilie. http://ec.europa.eu/dgs/energy_transport/galileo/doc/galilei_brochure.pdf.

[9] Dilip V. Sarwate and Michael B. Pursley. Crosscorrelation properties of pseudorandom and related sequences. *Proceedings of the IEEE*, 68(5):593–619, May 1980.

[10] Pratap Misra and Per Enge. *Global Positioning System: Signals, Measurements, and Performance*, page 389. Ganga-Jamuna Press, Lincoln, Massachusetts, 2006.

[11] A. J. Van Dierendonck. GPS receivers. In Bradford W. Parkinson and James J. Spikler, editors, *Global Positioning System:Theory and Applications*, chapter 8. AIAA, Inc, Washington, DC, 1996.

[12] Mischa Schwartz. *Information Transmission, Modulation, and Noise*, chapter 6, pages 464–470. McGraw-Hill, New York, fourth edition, 2006.

[13] Philip F. Panter. *Modulation, noise, and spectral analysis: applied to information transmission*. Mc Graw-Hill, New York, 1965.

[14] Steven M. Kay. *Fundamentals of Statistical Signal Processing: Estimation Theory*, volume 1. Prentice Hall PTR, Upper Saddle River, New Jersey, 1993.

[15] Paul A. Wintz and Edgar J. Luecke. Performance of optimum and suboptimum synchronizers. *IEEE Transactions of Communication Technology*, com-17(3):380–389, 1969.

[16] Pratap Misra and Per Enge. *Global Positioning System: Signals, Measurements, and Performance*, page 357. Ganga-Jamuna Press, Lincoln, Massachusetts, 2006.

[17] Wayne A. Fuller. *Introduction to Statistical Time Series*, chapter 6. John Wiley & Sons, New York, second edition, 2006.

[18] R. L. Anderson. Distribution of the serial correlation coefficient. *The Annals of Mathematical Statisctics*, 13(1):1–13, March 1942.

[19] Peter J. Brockwell and Richard A. Davis. *Time Series: Theory and Methods*. Springer-Verlag, New York, 1987.

[20] Pieter Eykhoff. *System Identification: Parameter and State Estimation*. John Wiley & Sons, New York, 1974.

[21] Lennart Ljung. *System Identification: Theory for the User*. Prentice Hall, Upper Saddle River, NJ, second edition, 1999.

[22] Harry L. Van Trees. *Detection, Estimation, and Modulation Theory.* John Willey & Sons, New York, 2001.

[23] John F. Claerbout. *Fundamentals of Geophysical Data Processing.* Blackwell Scientific Publications, Boston Massachusetts, 1985.

[24] Steven M. Kay. *Fundamentals of Statistical Signal Processing: Detection Theory*, volume 2. Prentice Hall PTR, Upper Saddle River, New Jersey, 1993.

[25] Pratap Misra and Per Enge. *Global Positioning System: Signals, Measurements, and Performance*, page 448. Ganga-Jamuna Press, Lincoln, Massachusetts, 2006.

[26] DBSRX2 receiver daughter board. https://www.ettus.com/product/details/DBSRX2.

[27] USRP N210 software defined radio. https://www.ettus.com/product/details/UN210-KIT.

[28] K. Borre, D. Akos, N. Bertelsen, P. Rinder, and S. Jensen. *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach.* Birkhäauser, Boston, Mass, USA, 2007.

[29] GNURadio. http://gnuradio.org/.

[30] O. D. Anderson. *Time Series Analysis and Forecasting: The Box-Jenkins approach.* Butterworths, London ; Boston, 1976.

[31] M. S. Bartlett. On the theoretical specification and sampling properties of autocorrelated time-series. *Supplement to the Journal of the Royal Statistical Society*, 8(1):27–41, 1946.

Appendix A

Multiple-peak conditions

A.1 Derivation of Equation (2.3)

The purpose of this appendix is to show how to derive the expressions for the cross-correlation $C_{1Q}(\tau, T)$ given by Equation (2.2) and its components given by Equation (2.4) and (2.5). Based on the parameter definitions in Section 2.2, the base band signal at the authenticator can be written as

$$\begin{aligned} V^a(t) = & \sqrt{2P^a_{c_1}} X_{D1}(t-\nu^a_1)\cos(2\pi\Delta f^a_1 t + \Delta\theta^a_1) \\ & + \sqrt{2P^a_{y_1}} Y_{D1}(t-\nu^a_1)\sin(2\pi\Delta f^a_1 t + \Delta\theta^a_1) \\ & + \sqrt{2P^a_{c_2}} X_{D2}(t-\nu^a_2)\cos(2\pi\Delta f^a_2 t + \Delta\theta^a_2) \\ & + \sqrt{2P^a_{y_2}} Y_{D2}(t-\nu^a_2)\sin(2\pi\Delta f^a_2 t + \Delta\theta^a_2) \\ & + n^a(t) \end{aligned} \tag{A.1}$$

where $n^a(t)$ is the noise. The noise is mainly the thermal noise in the authenticator receiver. We are only interested the signals from the common satellites. Thus, signals from other satellites can be treated as added noise on the signals for SV1 and SV2. They can be treated simply as white noise and included in the term $n^a(t)$.

For every satellite visible, there is a carrier tracking loop which eliminates this satellite's Doppler frequency Δf and phase difference $\Delta\theta$. The tracking loop generates two estimated values $\Delta\hat{f}$, $\Delta\hat{\theta}$ of the true Δf and $\Delta\theta$. The base band signal $V^a(t)$ is multiplied by a pair of orthogonal sinusoidal signals $\cos(2\pi\Delta\hat{f}t + \Delta\hat{\theta})$ and $\sin(2\pi\Delta\hat{f}t + \Delta\hat{\theta})$

to wipe off the Doppler frequency and the phase difference. The products of the multiplication are called in-phase and quadrature products, respectively. The quadrature product for SV1 at the authenticator is

$$\begin{aligned}
V^a_{1Q}(t) &= V^a(t)\sin(2\pi\Delta\hat{f}^a_1 t + \Delta\hat{\theta}^a_1) \\
&= -\sqrt{2P^a_{c_1}}X_{D1}(t-\nu^a_1)\sin\delta\phi^a_1 \\
&\quad + \sqrt{2P^a_{y_1}}Y_{D1}(t-\nu^a_1)\cos\delta\phi^a_1 \\
&\quad + \sqrt{\frac{P^a_{c_2}}{2}}X_{D2}(t-\nu^a_2)\sin\left[2\pi(\Delta f^a_2+\Delta f^a_1)t + (\Delta\theta^a_2+\Delta\theta^a_1) - \delta\phi^a_1)\right] \\
&\quad - \sqrt{\frac{P^a_{c_2}}{2}}X_{D2}(t-\nu^a_2)\sin\left[2\pi(\Delta f^a_2-\Delta f^a_1)t + (\Delta\theta^a_2-\Delta\theta^a_1) + \delta\phi^a_1)\right] \\
&\quad + \sqrt{\frac{P^a_{y_2}}{2}}Y_{D2}(t-\nu^a_2)\cos\left[2\pi(\Delta f^a_2-\Delta f^a_1)t + (\Delta\theta^a_2-\Delta\theta^a_1) + \delta\phi^a_1\right] \\
&\quad - \sqrt{\frac{P^a_{y_2}}{2}}Y_{D2}(t-\nu^a_2)\cos\left[2\pi(\Delta f^a_2+\Delta f^a_1)t + (\Delta\theta^a_2+\Delta\theta^a_1) - \delta\phi^a_1)\right] \\
&\quad + n^a_Q(t)
\end{aligned} \tag{A.2}$$

where $n^a_Q(t)$ is the portion of $n^a(t)$ projected into the quadrature product. The phase tracking error

$$\delta\phi^a_1 = 2\pi(\Delta f^a_1 - \Delta\hat{f}^a_1)t + \Delta\theta^a_1 - \Delta\hat{\theta}^a_1$$

When the carrier tracking loop is locked, the phase tracking error is usually less than 10°. This implies that $\delta\phi^a_1 \approx 0$ and, thus, Equation (2.1) is obtained. In the analysis below, we will ignore this tracking error, that means $\Delta f^a_1 = \Delta\hat{f}^a_1$ and $\Delta\theta^a_1 = \Delta\hat{\theta}^a_1$.

The base band signal at the supplicant, $V^s(t)$, and the quadrature product of SV1 in the supplicant, $V^s_{1Q}(t)$, are identical to $V^a(t)$ in Equation (A.1) and $V^a_{1Q}(t)$ in Equation (A.2), respectively, except the superscripts "a" are replaced by "s."

A.2 Derivation of Equation (2.4)

First we define the product of the SV2's P(Y) code and its delayed version as

$$\widetilde{Y}_2(t,\tau) \triangleq Y_{D2}(t)Y_{D2}(t-\tau)$$

where τ is the delay time.

When the tracking error is small, the correlation between the SV2's P(Y) residual signals is

$$\begin{aligned} C_{y2,y2}(\tau,T) =& \frac{\sqrt{P^a_{y_2} P^s_{y_2}}}{2T} \int_0^T \widetilde{Y}_2(t,\tau)\{\cos\left[2\pi(\Delta f^a_2 - \Delta f^a_1)t + \Delta\theta^a_2 - \Delta\theta^a_1\right] \\ & - \cos\left[2\pi(\Delta f^a_2 + \Delta f^a_1)t + \Delta\theta^a_2 + \Delta\theta^a_1\right]\} \\ & \{\cos\left[2\pi(\Delta f^s_2 - \Delta f^s_1)(t-\tau) + \Delta\theta^s_2 - \Delta\theta^s_1\right] \\ & - \cos\left[2\pi(\Delta f^s_2 + \Delta f^s_1)(t-\tau) + \Delta\theta^s_2 + \Delta\theta^s_1\right]\}\mathrm{d}t \end{aligned} \tag{A.3}$$

Equation (A.3) can be written in the below form

$$C_{y2,y2}(\tau,T) = \frac{\sqrt{P^a_{y_2} P^s_{y_2}}}{4T} \int_0^T \widetilde{Y}_2(t,\tau) \sum_{i=1}^{8} \cos(2\pi\Omega_i t + \Phi_i)\mathrm{d}t \tag{A.4}$$

where Ω_i and Φ_i are given in Table A.1.

Table A.1: Ω_i and Φ_i

i	Ω_i	Φ_i
1	$f^a_2 - f^a_1 + f^s_2 - f^s_1$	$\theta^a_2 - \theta^a_1 + \theta^s_2 - \theta^s_1 - 2\pi(f^s_2 - f^s_1)\tau$
2	$f^a_2 - f^a_1 - f^s_2 + f^s_1$	$\theta^a_2 - \theta^a_1 - \theta^s_2 + \theta^s_1 + 2\pi(f^s_2 - f^s_1)\tau$
3	$f^a_2 - f^a_1 + f^s_2 + f^s_1$	$\theta^a_2 - \theta^a_1 + \theta^s_2 + \theta^s_1 - 2\pi(f^s_2 + f^s_1)\tau + \pi$
4	$f^a_2 - f^a_1 - f^s_2 - f^s_1$	$\theta^a_2 - \theta^a_1 - \theta^s_2 - \theta^s_1 + 2\pi(f^s_2 + f^s_1)\tau + \pi$
5	$f^a_2 + f^a_1 + f^s_2 - f^s_1$	$\theta^a_2 + \theta^a_1 + \theta^s_2 - \theta^s_1 - 2\pi(f^s_2 - f^s_1)\tau + \pi$
6	$f^a_2 + f^a_1 - f^s_2 + f^s_1$	$\theta^a_2 - \theta^a_1 - \theta^s_2 + \theta^s_1 - 2\pi(f^s_2 - f^s_1)\tau + \pi$
7	$f^a_2 + f^a_1 + f^s_2 + f^s_1$	$\theta^a_2 + \theta^a_1 + \theta^s_2 + \theta^s_1 - 2\pi(f^s_2 + f^s_1)\tau$
8	$f^a_2 + f^a_1 - f^s_2 - f^s_1$	$\theta^a_2 - \theta^a_1 - \theta^s_2 - \theta^s_1 - 2\pi(f^s_2 + f^s_1)\tau$

The expectations of $C_{y2,y2}(\tau, T)$ are given by

$$
\begin{aligned}
& E\left\{C_{y2,y2}(\tau,T)\right\} \\
&= \overline{R}_{Y2}(\tau,T)\frac{\sqrt{P_{y_2}^a P_{y_2}^s}}{4T}\int_0^T \sum_{i=1}^{8}\cos(2\pi\Omega_i t+\Phi_i)\mathrm{d}t \\
&= \overline{R}_{Y2}(\tau,T)\frac{\sqrt{P_{y_2}^a P_{y_2}^s}}{4T}\sum_{i=1}^{8}\int_0^T \cos(2\pi\Omega_i t+\Phi_i)\mathrm{d}t \\
&= \overline{R}_{Y2}(\tau,T)\frac{\sqrt{P_{y_2}^a P_{y_2}^s}}{4T}\sum_{i=1}^{8}\int_{-\frac{T}{2}}^{\frac{T}{2}} \cos[2\pi\Omega_i(t-\frac{T}{2})+\Phi_i)\mathrm{d}t \\
&= \overline{R}_{Y2}(\tau,T)\frac{\sqrt{P_{y_2}^a P_{y_2}^s}}{4T}\sum_{i=1}^{8}\frac{\sin(2\pi\Omega_i t+\Phi_i-\pi\Omega_i T)}{2\pi\Omega_i}\Bigg|_{-\frac{T}{2}}^{\frac{T}{2}} \\
&= \overline{R}_{Y2}(\tau,T)\frac{\sqrt{P_{y_2}^a P_{y_2}^s}}{4}\sum_{i=1}^{8}\frac{\sin(\pi\Omega_i T+\Phi_i-\pi\Omega_i T)+\sin(\pi\Omega_i T-\Phi_i+\pi\Omega_i T)}{2\pi\Omega_i T} \\
&= \overline{R}_{Y2}(\tau,T)\frac{\sqrt{P_{y_2}^a P_{y_2}^s}}{4}\sum_{i=1}^{8}\frac{2\sin(\pi\Omega_i T)\cos(\Phi_i-\pi\Omega_i T)}{2\pi\Omega_i T} \\
&= \overline{R}_{Y2}(\tau,T)\frac{\sqrt{P_{y_2}^a P_{y_2}^s}}{4}\sum_{i=1}^{8}\frac{\sin(\pi\Omega_i T)}{\pi\Omega_i T}\cos(\Phi_i-\pi\Omega_i T) \\
&= \overline{R}_{Y2}(\tau,T)\frac{\sqrt{P_{y_2}^a P_{y_2}^s}}{4}\sum_{i=1}^{8}\mathrm{sinc}(\pi\Omega_i T)\cos(\Phi_i-\pi\Omega_i T)
\end{aligned}
\tag{A.5}
$$

where

$$\overline{R}_{Y2}(\tau,T) = E\left\{\frac{1}{T}\int_0^T Y_{D2}(t)Y_{D2}(t-\tau)\mathrm{d}t\right\}$$

is the expectation (average) of the auto-correlation function of a randomly selected snippet the P(Y) sequence.

For the ideal white noise sequence,

$$\overline{R}_{Y}(\tau,T) = \begin{cases} 1 & \text{if } \tau = 0 \\ 0 & \text{otherwise} \end{cases} \tag{A.6}$$

Equation (A.5) is zero when $\tau \neq 0$. When $\tau = 0$, we get

$$E\left\{C_{y2,y2}(0,T)\right\} = \frac{\sqrt{P_{y_2}^a P_{y_2}^s}}{4}\sum_{i=1}^{8}\mathrm{sinc}(\pi\Omega_i T)\cos(\Psi_i) \tag{A.7}$$

Table A.2: Ω_i, and Θ_i

i	Ω_i	Ψ_i	Θ_i
1	$f_2^a - f_1^a + f_2^s - f_1^s$	$\theta_2^a - \theta_1^a + \theta_2^s - \theta_1^s - \pi\Omega_i T + \pi$	
2	$f_2^a - f_1^a - f_2^s + f_1^s$	$\theta_2^a - \theta_1^a - \theta_2^s + \theta_1^s - \pi\Omega_i T$	
3	$f_2^a - f_1^a + f_2^s + f_1^s$	$\theta_2^a - \theta_1^a + \theta_2^s + \theta_1^s - \pi\Omega_i T$	
4	$f_2^a - f_1^a - f_2^s - f_1^s$	$\theta_2^a - \theta_1^a - \theta_2^s - \theta_1^s - \pi\Omega_i T + \pi$	
5	$f_2^a + f_1^a + f_2^s - f_1^s$	$\theta_2^a + \theta_1^a + \theta_2^s - \theta_1^s - \pi\Omega_i T$	
6	$f_2^a + f_1^a - f_2^s + f_1^s$	$\theta_2^a - \theta_1^a - \theta_2^s + \theta_1^s - \pi\Omega_i T + \pi$	
7	$f_2^a + f_1^a + f_2^s + f_1^s$	$\theta_2^a + \theta_1^a + \theta_2^s + \theta_1^s - \pi\Omega_i T + \pi$	
8	$f_2^a + f_1^a - f_2^s - f_1^s$	$\theta_2^a - \theta_1^a - \theta_2^s - \theta_1^s - \pi\Omega_i T$	

where Ψ_i is given in Table A.2.

Based on the derevation above, we obtain the expectation of $C_{y2,y2}$:

$$E\{C_{y2,y2}(\tau,T)\} = \begin{cases} \frac{\sqrt{P_{y_2}^a P_{y_2}^s}}{4} \sum_{i=1}^{8} \text{sinc}(\pi\Omega_i T)\cos(\Psi_i) & \text{if } \tau = 0 \\ 0 & \text{otherwise} \end{cases} \tag{A.8}$$

Following a similar apparoach, we obtain the following for the expectation of $C_{x2,x2}$:

$$E\{C_{x2,x2}(\tau,T)\} = \begin{cases} \frac{\sqrt{P_{x_2}^a P_{x_2}^s}}{4} \sum_{i=1}^{8} \text{sinc}(\pi\Omega_i T)\cos(\Phi_i) & \text{if } \tau = 0 \\ 0 & \text{otherwise} \end{cases} \tag{A.9}$$

where Φ_i is given in Table A.2.

Appendix B

Linearization of Position Calculation

B.1 Derivation of Equation (2.14)

The purpose of this appendix is to provide the detailed derivation of Equation (2.14). Starting with Equation (2.12), we note that we have a system of equations with three unknowns x_s, y_s and z_s. When we solve Equation (2.12), the only available values for the right sides are measurements with noise. Thus all we can do is generate an estimate of the true value. The noisy measurements are given by:

$$\begin{aligned} \hat{\rho}_i^a &= \rho_i^a + \delta\rho_i^a \\ \hat{t}_{i1} &= t_{i1} + \delta t_{i1} \\ \hat{\chi}_{i1} &= \chi_{i1} + \delta\chi_{i1} \\ \hat{x}_i &= x_i + \delta x_i \\ \hat{y}_i &= y_i + \delta y_i \\ \hat{z}_i &= z_i + \delta z_i \end{aligned} \tag{B.1}$$

Substituting these into Equation (2.12) gives

$$\begin{aligned}
\hat{\rho}_2^s - \hat{\rho}_1^s &= \hat{\rho}_2^a - \hat{\rho}_1^a - c\hat{t}_{21} + c\hat{\chi}_{21} \\
\hat{\rho}_3^s - \hat{\rho}_1^s &= \hat{\rho}_3^a - \hat{\rho}_1^a - c\hat{t}_{31} + c\hat{\chi}_{31} \\
\hat{\rho}_4^s - \hat{\rho}_1^s &= \hat{\rho}_4^a - \hat{\rho}_1^a - c\hat{t}_{41} + c\hat{\chi}_{41}
\end{aligned} \tag{B.2}$$

where

$$\hat{\rho}_i^s = \sqrt{(\hat{x}_i - \hat{x}_s)^2 + (\hat{y}_i - \hat{y}_s)^2 + (\hat{z}_i - \hat{z}_s)^2}$$

for common satellites $i = 1, 2, 3, 4$.

The supplicant's position estimate, $\hat{\mathbf{p}}_s(\hat{x}_s, \hat{y}_s, \hat{z}_s)$, can be determined by linearizing and solving Equation (B.2).

In Equation (B.2) the left side, $\rho_i^s - \rho_1^s$, can be linearized using a Taylor series around the estimated value $\hat{\mathbf{p}}_s(\hat{x}_s, \hat{y}_s, \hat{z}_s)$ and measurements, $\hat{\mathbf{r}}_i(\hat{x}_i, \hat{y}_i, \hat{z}_i)$, for satellite $i = 2, 3, 4$. That is,

$$\begin{aligned}
\rho_i^s - \rho_1^s = \hat{\rho}_i^s - \hat{\rho}_1^s
&- \left(\left.\frac{\partial \rho_i^s}{\partial x_s}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} - \left.\frac{\partial \rho_1^s}{\partial x_s}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \right) \delta x_s \\
&- \left(\left.\frac{\partial \rho_i^s}{\partial y_s}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} - \left.\frac{\partial \rho_1^s}{\partial y_s}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \right) \delta y_s \\
&- \left(\left.\frac{\partial \rho_i^s}{\partial z_s}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} - \left.\frac{\partial \rho_1^s}{\partial z_s}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \right) \delta z_s \\
&- \left.\frac{\partial \rho_i^s}{\partial x_i}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta x_i - \left.\frac{\partial \rho_i^s}{\partial y_i}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta y_i \\
&- \left.\frac{\partial \rho_i^s}{\partial z_i}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta z_i + \left.\frac{\partial \rho_1^s}{\partial x_1}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta x_1 \\
&+ \left.\frac{\partial \rho_1^s}{\partial y_1}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta y_1 + \left.\frac{\partial \rho_1^s}{\partial z_1}\right|_{(\hat{\mathbf{p}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta z_1 \\
&+ \mathcal{O}(\mathbf{r}^2)
\end{aligned} \tag{B.3}$$

where $\mathcal{O}(\mathbf{r}^2)$ represents the higher order terms. Because $\rho_i^s - \rho_1^s$ is expanded using $\mathbf{r} = \hat{\mathbf{r}} - \delta\mathbf{r}$ as defined in Equation (B.1) rather than $\mathbf{r} = \hat{\mathbf{r}} + \delta\mathbf{r}$ as is done typically, the signs in all the error terms are different from the usual Taylor series expansion.

If we define the Line of Sight (LOS) vector from the estimated position $(\hat{x}_s, \hat{y}_s, \hat{z}_s)$ of the supplicant to the i^{th} satellite as

$$\hat{\mathbf{e}}_i = \begin{bmatrix} \frac{\hat{x}_i - \hat{x}_s}{\hat{\rho}_i} & \frac{\hat{y}_i - \hat{y}_s}{\hat{\rho}_i} & \frac{\hat{z}_i - \hat{z}_s}{\hat{\rho}_i} \end{bmatrix}^T$$

and the supplicant position error vector as

$$\delta\mathbf{p}_s = \begin{bmatrix} \delta x_s & \delta y_s & \delta z_s \end{bmatrix}^T$$

, and the satellite position error vector as

$$\delta\mathbf{r}_i = \begin{bmatrix} \delta x_i & \delta y_i & \delta z_i \end{bmatrix}^T$$

then ignoring the higher order item in Equation (B.3) we can write

$$\rho_i^s - \rho_1^s = \hat{\rho}_i^s - \hat{\rho}_1^s + \left[\hat{\mathbf{e}}_i - \hat{\mathbf{e}}_1\right]^T \delta\mathbf{p}_s - \hat{\mathbf{e}}_i^T \delta\mathbf{r}_i + \hat{\mathbf{e}}_1^T \delta\mathbf{r}_1 \tag{B.4}$$

Substituting Equation (2.12), (B.1) and (B.2) into Equation (B.4), we get

$$\left[\hat{\mathbf{e}}_i - \hat{\mathbf{e}}_1\right]^T \delta\mathbf{p}_s = \hat{\mathbf{e}}_i^T \delta\mathbf{r}_i - \hat{\mathbf{e}}_1^T \delta\mathbf{r}_1 - \delta\rho_i^a + \delta\rho_1^a + c\delta t_{i1} - c\delta\chi_{i1} \tag{B.5}$$

Using the definition of matrix $\mathbf{A}$ given in Equation (2.15) and the measurement error vector $\delta\mathbf{m}$ in Equation (2.16), we obtain the linear system defined by Equation (2.14).

Appendix C

Sample Cross-correlator mean and variance

C.1 Expectation of Sample Cross-correlation

This appendix discusses the expectation value of the sample cross-corrletor defined in (3.8).

The expectation of $\hat{\gamma}^{xy}$ is

$$E\left[\hat{\gamma}_k^{xy}\right] = E\left[\frac{1}{N}\sum_{n=1}^{N} x_n y_{n+k}\right] = \frac{1}{N}\sum_{n=1}^{N} E\left(x_n y_{n+k}\right) \tag{C.1}$$

where $E(.)$ is the operation to get the expectation value of a random variable.

Following the signal description in (3.4), the sum of expectations in (C.1) is

$$\begin{aligned}\sum_{n=1}^{N} E\left(x_n y_{n+k}\right) = \alpha\beta \sum_{n=1}^{N} E\left(f_n g_{n+k}\right) \\ + \alpha \sum_{n=1}^{N} E\left(f_n v_{n+k}\right) \\ + \beta \sum_{n=1}^{N} E\left(u_n g_{n+k}\right) \\ + \sum_{n=1}^{N} E\left(u_n v_{n+k}\right)\end{aligned} \tag{C.2}$$

The last three items in (C.2) are all zeros since u_n, v_n f_n and g_n are independent to each other and they are zero mean. So

$$\sum_{n=1}^{N} E\left(x_n y_{n+k}\right) = \alpha\beta \sum_{n=1}^{N} E\left(f_n g_{n+k}\right) = \alpha\beta \sum_{n=1}^{N} \gamma_k^{fg}$$
$$= N\alpha\beta\gamma_k^{fg} \tag{C.3}$$

Substituting (C.3) into (C.1), we get

$$E\left[\hat{\gamma}_k^{xy}\right] = \alpha\beta\gamma_k^{fg} \tag{C.4}$$

Equation (C.4) shows that the sample cross-correlator defined in (3.8) is an unbiased estimator of $\alpha\beta\gamma_k^{fg}$.

C.2 Covariance of Sample Cross-correlation

The output of the sample cross-correlator in Figure 3.7 is an estimation of the true value $\alpha\beta\gamma_k^{fg}$ rather than the true cross-correlation. The covariance of estimator is discussed in this appendix to evalaute the error performance of the estimator. This appendix first discusses the covariance of the sample cross-correlation between two independent random process. Then it discusses the covariance of $\hat{\gamma}_k^{xy}$.

C.2.1 Covariance between two independent random processes

The random processes u_n and v_n are two independent WSS Gaussian random processes as discussed in Section 3.2. We assumes that the statistical parameters of the signals u_n and v_n are known. For example, their auto-correlation functions are available. Next we discuss how to calculate the covariance of the sample cross-correlation using these auto-correlation functions.

Because u_n and v_n are independent and they are both zero means, the cross-correlation between them is zero. That is

$$\gamma_k^{uv} = \mathrm{cov}(u, v) = 0 \tag{C.5}$$

The covariance of the sample cross-correlation between u_n and v_n is

$$\begin{aligned}\operatorname{cov}\left(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}\right) &= E\left[\left(\hat{\gamma}_k^{uv} - \gamma_k^{uv}\right)\left(\hat{\gamma}_{k+l}^{uv} - \gamma_{k+l}^{uv}\right)\right] \\ &= E\left(\hat{\gamma}_k^{uv}\hat{\gamma}_{k+l}^{uv}\right) \end{aligned} \tag{C.6}$$

Referring the sample cross-correlation of $\hat{\gamma}_k^{xy}$ defined in (3.8), for $\hat{\gamma}_k^{uv}$, we have

$$\begin{aligned} E\left(\hat{\gamma}_k^{uv}\hat{\gamma}_{k+l}^{uv}\right) &= \frac{1}{N^2} E\left(\sum_{n=1}^{N} u_n v_{n+k} \sum_{m=1}^{N} u_m v_{m+k}\right) \\ &= \frac{1}{N^2}\sum_{n=1}^{N}\sum_{m=1}^{N} E\left(u_n u_m\right) E\left(v_{n+k} v_{m+k}\right) \end{aligned} \tag{C.7}$$

where we use the property that u_n and v_n are independent.

The processes u_n and $v_n$are all WSS random processes. For a WSS random process, its auto-covariance is a function of the lag time. For example,

$$\begin{aligned} E\left(u_n u_m\right) &= \gamma_{m-n}^{u} \\ E\left(v_{n+k} v_{m+k+l}\right) &= \gamma_{m-n+l}^{v} \end{aligned} \tag{C.8}$$

Substituting (C.8) and (C.6) into (C.7), we have

$$\operatorname{cov}(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}) = \frac{1}{N^2}\sum_{n=1}^{N}\sum_{m=1}^{N}\left[\gamma_{m-n}^{u}\gamma_{m-n+l}^{v}\right] \tag{C.9}$$

Because $\gamma_k^u = \rho_k^u$ and $\gamma_k^v = \rho_k^v$ which are stated in Section 3.3.2, equation (C.9) can be written as

$$\operatorname{cov}(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}) = \frac{1}{N^2}\sum_{n=1}^{N}\sum_{m=1}^{N}\left[\rho_{m-n}^{u}\rho_{m-n+l}^{v}\right] \tag{C.10}$$

The double summation in (C.10) is the sum of all the elements of the N-by-N Toeplitz matrix

$$\begin{pmatrix} \rho_0^u\rho_l^v & \rho_1^u\rho_{l+1}^v & \cdots & \rho_{N-1}^u\rho_{l+N-1}^v \\ \rho_1^u\rho_{l+1}^v & \rho_0^u\rho_l^v & \cdots & \rho_{N-2}^u\rho_{l+N-2}^v \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{N-1}^u\rho_{l+N-1}^v & \rho_{N-2}^u\rho_{l+N-2}^v & \cdots & \rho_0^u\rho_l^v \end{pmatrix} \tag{C.11}$$

Equation (C.10) can be written as

$$\mathrm{cov}(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}) = \frac{1}{N^2}\left[N\rho_0^u\rho_l^v + 2\sum_{i=1}^{N}(N-i)\rho_i^u\rho_{i+l}^v\right] \tag{C.12}$$

The random processes u_n and v_n are not very narrow band processes, so $\rho_i^u \to 0$ and $\rho_i^v \to 0$ when $i \to \pm\infty$. There is a minimal index M satisfies the condition that $\rho_i^u = 0$ and $\rho_i^v = 0$ when $i > M$. Usually $M \ll N$, then most of the elements in the matrix $C(l)$ of (C.11) are zeros. This greatly reduces the computational operations of (C.12). Then (C.12) can be simplified as

$$\mathrm{cov}(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}) = \frac{1}{N^2}\left[N\rho_0^u\rho_l^v + 2\sum_{i=1}^{M}(N-i)\rho_i^u\rho_{i+l}^v\right] \tag{C.13}$$

Equation (C.13) can be further written as

$$\begin{aligned}
&\mathrm{cov}(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}) \\
&= \frac{1}{N^2}\left[N\rho_0^u\rho_l^v + 2\sum_{i=1}^{M}(N-i)\rho_i^u\rho_{i+l}^v\right] \\
&= \frac{1}{N^2}\left[N\rho_0^u\rho_l^v + 2N\sum_{i=1}^{M}\rho_i^u\rho_{i+l}^v - 2\sum_{p=1}^{M} i\rho_i^u\rho_{i+l}^v\right] \\
&= \frac{1}{N}\left[\rho_0^u\rho_l^v + 2\sum_{i=1}^{M}\rho_i^u\rho_{i+l}^v - \frac{2}{N}\sum_{i=1}^{M} i\rho_i^u\rho_{i+l}^v\right]
\end{aligned} \tag{C.14}$$

Usually the points of the samples N is very big so that

$$\frac{2}{N}\sum_{i=1}^{M} i\rho_i^u\rho_i^v \approx 0 \tag{C.15}$$

Then (C.14) can be approximated as

$$\mathrm{cov}(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}) \approx \frac{1}{N}\left[\rho_0^u\rho_l^v + 2\sum_{i=1}^{M}\rho_i^u\rho_{i+l}^v\right] \tag{C.16}$$

The auto-correlations are independent of the points of sample correlation. We define

$$K_l^{uv} = \rho_0^u\rho_l^v + 2\sum_{i=1}^{M}\rho_i^u\rho_{i+l}^v \tag{C.17}$$

With known ρ_i^u and ρ_{i+l}^v information, K_l^{uv} can be pre-calculated. Then (C.16) can be written as

$$\mathrm{cov}(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}) \approx \frac{K_l^{uv}}{N} \tag{C.18}$$

C.2.2 Covariance of $\hat{\gamma}_k^{xy}$

The covariance of the sample cross-correlation between two samples at index k and $k+l$ is

$$\mathrm{cov}(\hat{\gamma}_k^{xy}, \hat{\gamma}_{k+l}^{xy}) = E\left[\left(\hat{\gamma}_k^{xy} - \alpha\beta\gamma_k^{fg}\right)\left(\hat{\gamma}_{k+l}^{xy} - \alpha\beta\gamma_{k+l}^{fg}\right)\right] \tag{C.19}$$

where the expectation expression (C.4) is used.

Substituting (3.18), the error of the sample cross-correlator, into (C.19), we have

$$\mathrm{cov}(\hat{\gamma}_k^{xy}, \hat{\gamma}_{k+l}^{xy}) = E\left(\Delta\hat{\gamma}_k^{xy}\Delta\hat{\gamma}_{k+l}^{xy}\right) \tag{C.20}$$

Then we will show that error signal, $\Delta\hat{\gamma}_k^{xy}$, is a linear combination of four uncorrelated processes. Each of these process is a sample cross-correlation. Thus the covariance of the error signal is the linear combination of the four covariances.

The error signal defined in (3.18) is rewritten below

$$\Delta\hat{\gamma}_k^{xy} = \alpha\beta\delta_{\gamma_k^{fg}} + \alpha\hat{\gamma}_k^{fv} + \beta\hat{\gamma}_k^{ug} + \hat{\gamma}_k^{uv} \tag{C.21}$$

where $\delta_{\gamma_k^{fg}}$, $\hat{\gamma}_k^{fv}$, $\hat{\gamma}_k^{ug}$ and $\hat{\gamma}_k^{uv}$ are four processes to be shown uncorrelated.

We first show that two processes $\hat{\gamma}_k^{fv}$ and $\hat{\gamma}_{k+l}^{ug}$ are uncorrelated.

$$\begin{aligned} E\left(\hat{\gamma}_k^{fv}\hat{\gamma}_{k+l}^{ug}\right) &= \frac{1}{N^2}E\left(\sum_{n=1}^{N} f_n v_{n+k} \sum_{m=1}^{N} u_m g_{m+k}\right) \\ &= \frac{1}{N^2}\sum_{n=1}^{N}\sum_{m=1}^{N} E\left(f_n g_{m+k} v_{n+k} u_m\right) \end{aligned} \tag{C.22}$$

Because u_n and v_n are independent and each of them is also independent to signals f_n and g_n, thus

$$\begin{aligned} E\left(\hat{\gamma}_k^{fv}\hat{\gamma}_{k+l}^{ug}\right) &= \frac{1}{N^2}\sum_{n=1}^{N}\sum_{m=1}^{N} E\left(f_n g_{m+k}\right) E\left(v_{n+k}u_m\right) \\ &= \frac{1}{N^2}\sum_{n=1}^{N}\sum_{m=1}^{N} E\left(f_n g_{m+k}\right) E\left(v_{n+k}\right) E\left(u_m\right) \\ &= 0 \end{aligned} \tag{C.23}$$

The means of random variables $\hat{\gamma}_k^{fv}$ and $\hat{\gamma}_k^{ug}$ are zeros. Thus we have

$$E\left(\hat{\gamma}_k^{fv}\hat{\gamma}_{k+l}^{ug}\right) = \mathrm{cov}\left(\hat{\gamma}_k^{fv}, \hat{\gamma}_{k+l}^{ug}\right) = 0 \tag{C.24}$$

It means that the random variables $\hat{\gamma}_k^{fv}$ and $\hat{\gamma}_{k+l}^{ug}$ are uncorrelated.

We can further show that the processes $\delta_{\gamma_k^{fg}}$, $\hat{\gamma}_k^{fv}$, $\hat{\gamma}_k^{ug}$ and $\hat{\gamma}_k^{uv}$ are uncorrelated to each other by following the same approach shown above.

Based on the uncorrelated conclusion, we have

$$\begin{aligned} E\left(\Delta\hat{\gamma}_k^{xy}\Delta\hat{\gamma}_{k+l}^{xy}\right) = \alpha\beta E\left(\delta_{\gamma_k^{fg}}\delta_{\gamma_{k+l}^{fg}}\right) + \alpha^2 E\left(\hat{\gamma}_k^{fv}\hat{\gamma}_{k+l}^{fv}\right) \\ + \beta^2 E\left(\hat{\gamma}_k^{ug}\hat{\gamma}_{k+l}^{ug}\right) + E\left(\hat{\gamma}_k^{uv}\hat{\gamma}_{k+l}^{uv}\right) \end{aligned} \tag{C.25}$$

It is easy to show that $\Delta\hat{\gamma}_k^{xy}$ is a zero mean process, i.e. $E\left(\Delta\hat{\gamma}_k^{xy}\right) = 0$. Thus

$$E\left(\Delta\hat{\gamma}_k^{xy}\Delta\hat{\gamma}_{k+l}^{xy}\right) = \mathrm{cov}\left(\Delta\hat{\gamma}_k^{xy}, \Delta\hat{\gamma}_{k+l}^{xy}\right) \tag{C.26}$$

Because $\delta_{\gamma_k^{fg}}$, $\hat{\gamma}_k^{fv}$, $\hat{\gamma}_k^{ug}$ and $\hat{\gamma}_k^{uv}$ are zero mean processes, we have

$$\begin{aligned} \mathrm{cov}\left(\Delta\hat{\gamma}_k^{xy}, \Delta\hat{\gamma}_{k+l}^{xy}\right) = \alpha\beta\mathrm{cov}\left(\delta_{\gamma_k^{fg}}, \delta_{\gamma_{k+l}^{fg}}\right) \\ + \alpha^2\mathrm{cov}\left(\hat{\gamma}_k^{fv}, \hat{\gamma}_{k+l}^{fv}\right) \\ + \beta^2\mathrm{cov}\left(\hat{\gamma}_k^{ug}, \hat{\gamma}_{k+l}^{ug}\right) \\ + \mathrm{cov}\left(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}\right) \end{aligned} \tag{C.27}$$

Equation (C.27) shows that the total covariance, $\mathrm{cov}(\Delta\hat{\gamma}_k^{xy}, \Delta\hat{\gamma}_{k+l}^{xy})$, is the weighted sum of the covariances of sub-signals. These sub-signals are $\delta_{\gamma_k^{fg}}$, $\hat{\gamma}_k^{fv}$, $\hat{\gamma}_k^{ug}$ and $\hat{\gamma}_k^{uv}$.

For other sub-signals in (C.27), we can do the same derivations and get

$$\begin{aligned}
\mathrm{cov}(\hat{\gamma}_k^{fv}, \hat{\gamma}_{k+l}^{fv}) &\approx \frac{K_l^{fv}}{N} \\
\mathrm{cov}(\hat{\gamma}_k^{ug}, \hat{\gamma}_{k+l}^{ug}) &\approx \frac{K_l^{ug}}{N} \\
\mathrm{cov}(\hat{\gamma}_k^{fg}, \hat{\gamma}_{k+l}^{fg}) &\approx \frac{K_l^{fg}}{N}
\end{aligned} \tag{C.28}$$

where K_l^{fv}, K_l^{ug} and K_l^{fg} have the similar definitions as in (C.17) except that the subscripts represent the lags and the superscripts represent signals.

Substituting (C.18) (C.28) into (C.27), we get

$$\begin{aligned}
\mathrm{cov}(\Delta\hat{\gamma}_k^{xy}, \Delta\hat{\gamma}_{k+l}^{xy}) \approx \frac{1}{N} \Big(& \alpha\beta K_l^{fg} + \alpha^2 K_l^{fv} \\
& + \beta^2 K_l^{ug} + K_l^{uv} \Big)
\end{aligned} \tag{C.29}$$

For the GPS signal, the range of α^2 or β^2 is about $0.00002 \sim 0.05$ which depends on the C/N_0 and the bandwidth of the RF front-end. Table C.1 gives some typical values of the SNR (or α^2, β^2) values. Based on the Table C.1, the first three items in (C.27) and (C.29) can be ignored because α^2 and β^2 are very small. Equation (C.27) becomes

$$\mathrm{cov}(\hat{\gamma}_k^{xy}, \hat{\gamma}_{k+l}^{xy}) \approx \mathrm{cov}(\hat{\gamma}_k^{uv}, \hat{\gamma}_{k+l}^{uv}) \tag{C.30}$$

A simulation result is given in Section 3.3.5 to show this approximation is reasonable.

When the approximation in (C.30) is used, the method to calculate $\mathrm{cov}(\hat{\gamma}_k^{xy}, \hat{\gamma}_{k+l}^{xy})$ is

$$\mathrm{cov}(\Delta\hat{\gamma}_k^{xy}, \Delta\hat{\gamma}_{k+l}^{xy}) \approx \frac{K_l^{uv}}{N} \tag{C.31}$$

The variance is a particular case of covariance when the lag is zero. When $l = 0$, equation (C.16) is the variance of $\hat{\gamma}_k^{uv}$. This variance can be written as

$$\begin{aligned}
\sigma^2_{\hat{\gamma}_k^{uv}} &= \mathrm{cov}(\hat{\gamma}_k^{uv}, \hat{\gamma}_k^{uv}) \\
&= \frac{1}{N}\left[1 + 2\sum_{i=1}^{M} \rho_i^u \rho_i^v\right] \\
&\approx \frac{K_0^{uv}}{N}
\end{aligned} \tag{C.32}$$

Table C.1: Typical values of α^2 and β^2

C/N_0 (dB-Hz)	Double-sided bandwidth (MHz)	SNR (dB)	α^2 or β^2
30	2	-33	1 / 1995
45	2	-18	1 / 63
50	2	-13	1 / 19
30	12	-40.8	1 / 12023
45	12	-25.8	1 / 380
50	12	-20.8	1 / 120
30	20	-43	1 / 19953
45	20	-28	1 / 631
50	20	-23	1 / 199

If u_n and v_n are the same processes, i.e. $v(n) = u(n)$, equation (C.32) gives the same result which is described in [30] [31]. It is the variance of the sample autocorrelation function of $u(n)$

$$\sigma^2_{\hat{\gamma}^u_k} \approx \frac{1}{N}\left[1 + 2\sum_{i=1}^{M}(\rho^u_i)^2\right] \tag{C.33}$$

Similar as (C.27), the variance of $\hat{\gamma}^{xy}_k$, $\sigma^2_{\hat{\gamma}^{xy}_k}$, can also be written as a weighted sum of sub-signals variances. This expression is shown in (C.34).

$$\sigma^2_{\hat{\gamma}^{xy}_k} = \alpha\beta\sigma^2_{\delta_{\gamma^{fg}_k}} + \alpha^2\sigma^2_{\hat{\gamma}^{fv}_k} + \beta^2\sigma^2_{\hat{\gamma}^{ug}_k} + \sigma^2_{\hat{\gamma}^{uv}_k} \tag{C.34}$$

Based on the above discussion, we noted that all the covariances and variances discussed in this appendix do not depend on the index k. That means the generated processes $\hat{\gamma}^{xy}_k$, $\delta_{\gamma^{fg}_k}$, $\hat{\gamma}^{fv}_k$, $\hat{\gamma}^{ug}_k$ and $\hat{\gamma}^{uv}_k$ are all wide-sense-stationary (WSS) processes.

[18] shows that $\hat{\gamma}^{xy}_k$, $\delta_{\gamma^{fg}_k}$, $\hat{\gamma}^{fv}_k$, $\hat{\gamma}^{ug}_k$ and $\hat{\gamma}^{uv}_k$ are approximately Gaussian distributed when the number of the samples, N, is farely large.

Appendix D

MLE Estimate of Shift Time

In this Appendix, an estimator for the watermark signal shift time between the authenticator and the supplicant will be sought using the maximum likelihood principle. As will be shown, if an error-free template of the P(Y) code was available, the maximum likelihood estimator (MLE) of $\hat{n}_0$ will be nothing more than the maximum of the cross-correlation between the two signals. However, when a noise corrupted P(Y) code is used (as is the case in actual practice), the resulting estimator is biased. Fortunately, as will be shown, the bias can be made arbitrarily small by a judicious selection of the template's length. To this end, first, the simplified signal and noise model is presented. Then the maximum likelihood principle is applied to this model to establish an estimator.

In the authentication process, there are two measurement signals which are from two GPS receivers: the authenticator and the supplicant. We call the signal from the supplicant $x(n)$ and call the signal from the authenticator $y(n)$. Both $x(n)$ and $y(n)$ can be modeled as output signals at the end of the receiver's filters. For simplicity, for the moment, we assume the GPS signal and the thermal noises share the same filters.

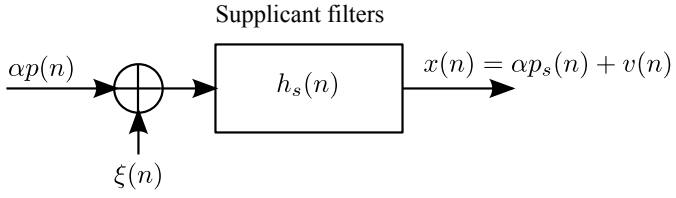

Figure D.1: Simplified signal model for supplicant

The input signals of the filters include a piece of the P(Y) signal $p(n)$ and white noise. As depicted in Figure D.1, $x(n)$ can be expressed as

$$x(n) = \alpha p_s(n) + v(n) \tag{D.1}$$

where $p_s(n)$ is the filtered signal of $p(n)$, $v(n)$ is the filtered white noise, and $\alpha \geq 0$ is a scalar to represent the amplitude of the filtered P(Y) signal. When $p(n)$ is not received at the supplicant, $\alpha = 0$.

Similarly signal $y(n)$ depicted in Figure D.2 can be expressed as

$$y(n) = \beta p_{1a}(n) + w(n) \tag{D.2}$$

where $p_a(n)$ is the filtered signal of $p_1(n)$, $w(n)$ is another filtered signal equal to $h_a(n) * \eta(n)$, and $\beta > 0$ is a scalar to represent the amplitude of the filtered P(Y) signal. The two source of white noises in $x(n)$ and $y(n)$ are independent and thus $w(n)$ and $v(n)$ are also independent.

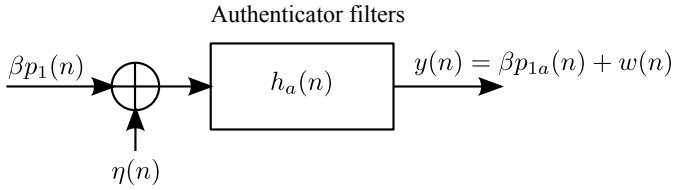

Figure D.2: Simplified signal model for authenticator

In Figure D.2, the GPS signal is $p_1(n)$ rather than $p(n)$. $p_1(n)$ can be expressed as

$$p_1(n) = \begin{cases} 0 & 0 \leq n < n_0 \\ p(n - n_0) & n_0 \leq n < M + n_0 \\ 0 & M + n_0 \leq n < N \end{cases}$$

where n_0 is the delay between signal $x(n)$ and $y(n)$, M is the length of signal $p(n)$ (it is also the length of $x(n)$), and N is the length of signal $y(n)$. The signal $p_1(n)$ is a zero-padded, delayed version of signal $p(n)$. This is because the lengths of $x(n)$ and $y(n)$ available for the authentication process are different. The supplicant is only able to send a short piece of signal to the authentication station because of the limited communication bandwidth. Thus the length of signal $x(n)$ can not be very long. On

the other hand the digitized GPS signal at the authenticator can buffered, thus a long history of this signal is available. Because of the distances from the GPS satellite to the supplicant and the authenticator are different, the arrival times of signal $p(n)$ are also different. The difference between two arrival times is what is called the shift time. Denote the arrival time at the authenticator as t_a and the arrival time at the supplicate as t_s. Then the shift time is

$$t_d = t_s - t_a \tag{D.3}$$

Thus at certain delay time t_d, embedded in the signal $p_1(n)$ is a copy of signal $p(n)$. For the discrete signal, $t_d = n_0 T_s$, where T_s is the sampling frequency. At other samples where $p_1(n)$ does not include $p(n)$, $p_1(n)$ is zero. In Figure D.2, if only a noise-free copy of $p(n)$ passes through the authenticator filters, the output signal will be $p_a(n)$, which has the same length as signal $p_s(n)$.

Figure D.3 shows a M-point long $x(n)$ and a N-point long $y(n)$ (M $\ll$ N) signals, respectively. There is a piece of P(Y) signal of length M in the signal $x(n)$ when the supplicant receives the authentic GPS signal. At some shift point, n_0 as shown in Figure D.3, the same piece of P(Y) signal is in $y(n)$. The task of the shift estimator is to estimate n_0 based on the available measurement signals $x(n)$ and $y(n)$.

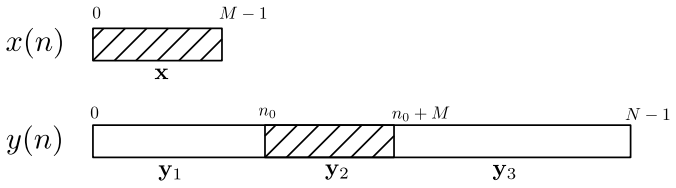

Figure D.3: Measurement sequences for estimator

The sequence $x(n)$ and $y(n)$ can be expressed in the vector form. As shown in Figure D.3, $x(n)$ is expressed as a $M \times 1$ vector $\mathbf{x}$ and $y(n)$ is expressed as $\mathbf{y} = [\mathbf{y}_1^T\ \mathbf{y}_2^T\ \mathbf{y}_3^T]^T$. The lengths of vectors $\mathbf{y}_1$, $\mathbf{y}_2$ and $\mathbf{y}_3$ are n_0, M and $N - M - n_0$, respectively. The vectors $\mathbf{x}$ and $\mathbf{y}$ are multi-dimensional random variables. The mean of $\mathbf{x}$ is $\alpha \mathbf{p}_s$, where $\mathbf{p}_s$ is the vector form of $p_s(n)$ in (D.1). The mean of $\mathbf{y}$ is $\beta \mathbf{p}_{1a} = \beta[\mathbf{0_1}^T\ \mathbf{p}_a^T\ \mathbf{0_2}^T]^T$, where $\mathbf{p}_a$ is the vector form of $p_a(n)$ and $\mathbf{0_1}$, $\mathbf{0_2}$ are zero vectors with length n_0 and $N - M - n_0$.

The noise signals $v(n)$ and $w(n)$ are zero-mean stationary Gaussian random processes as discussed in Section 3.1. In signals $x(n)$ and $y(n)$, $p_{1a}(n)$ and $p_s(n)$ are deterministic signals. The random components in $x(n)$ and $y(n)$ are $v(n)$ and $w(n)$. Thus the pdf of $\mathbf{y}$ can be written as

$$p(\mathbf{y}; n_0) = \frac{1}{(2\pi)^{\frac{N}{2}}[\det(\mathbf{\Sigma}_w)]^{\frac{1}{2}}} \exp\left[-\frac{1}{2}(\mathbf{y} - \beta\mathbf{p}_{1a})^T \mathbf{\Sigma}_w^{-1}(\mathbf{y} - \beta\mathbf{p}_{1a})\right] \tag{D.4}$$

where $\mathbf{\Sigma}_w$ is the covariance matrix of the random vector $\mathbf{w}$. Equation (D.4) is a function of shift time n_0.

When the filters in the authenticator and the supplicant are minimum-phase filters, their inverse filters are also stable and causal. The covariance matrix can be related to the filter impulse response. We take the authenticator filters as the example. The covariance matrix can be written as

$$\mathbf{\Sigma}_w = \mathbf{H}_a \mathbf{H}_a^T \tag{D.5}$$

In Equation (D.5), $\mathbf{H}_a$ is the transform matrix of the convolution operation.

$$\mathbf{H}_a = \begin{pmatrix} h_a(0) & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ h_a(1) & h_a(0) & \cdots & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ h_a(K) & h_a(K-1) & \cdots & h_a(0) & 0 & \cdots & 0 & 0 \\ 0 & h_a(K) & \cdots & h_a(1) & h_a(0) & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & h_a(K) & h_a(K-1) & \cdots & h_a(0) & 0 \\ 0 & 0 & \cdots & 0 & h_a(K) & \cdots & h_a(1) & h_a(0) \end{pmatrix} \tag{D.6}$$

which is a $N \times N$ matrix and the impulse response $h_a(n)$ has a length of $K + 1$. $\mathbf{H}_a$ is a lower triangular Toeplitz matrix. When the filter $h_a(n)$ is a minimum-phase filter, its inverse filter can be found. Any linear time-invariant filter can be approximated as a finite-impulse-response (FIR) filter when its order is high enough. Thus we can also write the transform matrix of the inverse filter into another triangular Toeplitz matrix. Denote this transform matrix as $\mathbf{V}_a$.

Referring back to Figure D.2, we can express $\mathbf{w}$ in the matrix form as

$$\mathbf{w} = \mathbf{H}_a \boldsymbol{\eta} \tag{D.7}$$

where $\boldsymbol{\eta}$ is the vector form of signal $\eta(n)$ in Figure D.2. When $\eta(n)$ is a unit variance zero-mean white noise, its covariance matrix is $\mathbf{I}$. Then we have Equation (D.5). Based on the description above, we also have

$$\boldsymbol{\eta} = \mathbf{V}_a \mathbf{w} \tag{D.8}$$

The inverse filter is a whitening filter which converts the color noise signal into a white noise.

From Equation (D.8), we can calculate the covariance matrix of $\boldsymbol{\eta}$,

$$\begin{aligned} \boldsymbol{\Sigma}_\eta &= E\{\boldsymbol{\eta}\boldsymbol{\eta}^T\} \\ &= E\{\mathbf{V}_a \mathbf{w}\mathbf{w}^T \mathbf{V}_a^T\} \\ &= \mathbf{V}_a E\{\mathbf{w}\mathbf{w}^T\} \mathbf{V}_a^T \\ &= \mathbf{V}_a \Sigma_w \mathbf{V}_a^T \\ &= \mathbf{I} \end{aligned} \tag{D.9}$$

Then we have

$$\boldsymbol{\Sigma}_w^{-1} = \mathbf{V}_a^T \mathbf{V}_a \tag{D.10}$$

Equation (D.10) has the same form as Equation (D.5), thus $\boldsymbol{\Sigma}_w^{-1}$ is a symmetric Toeplitz matrix. When the dimension of $\boldsymbol{\Sigma}_w^{-1}$ is large enough (i.e. $n_0 \gg K$, $M \gg K$ and $(N - M - n_0) \gg K$, the matrix $\boldsymbol{\Sigma}_w^{-1}$ can be written in the block matrix as

$$\boldsymbol{\Sigma}_w^{-1} = \begin{pmatrix} \mathbf{C}_1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{C}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{C}_3 \end{pmatrix} \tag{D.11}$$

where the dimension of $\mathbf{C}_1$ is $n_0 \times n_0$, the dimension of $\mathbf{C}_2$ is $M \times M$ and the dimension of $\mathbf{C}_3$ is $(N - M - n_0) \times (N - M - n_0)$.

Note that the determinant of $\mathbf{H}_a$ is $[h_a(0)]^N$, further the determinant of $\boldsymbol{\Sigma}$ is

$$\det(\boldsymbol{\Sigma}) = \det(\mathbf{H}_a \mathbf{H}_a^T) = [\det(\mathbf{H}_a)]^2 \tag{D.12}$$

$$= [h_a(0)]^{2N} \tag{D.13}$$

Thus the Equation (D.4) can written as

$$p(\mathbf{y}; n_0) = \frac{1}{[2\pi h_a^2(0)]^{\frac{N}{2}}} \exp\left[-\frac{1}{2}(\mathbf{y} - \beta\mathbf{p}_{1a})^T \mathbf{\Sigma}_w^{-1}(\mathbf{y} - \beta\mathbf{p}_{1a})\right] \tag{D.14}$$

The maximum likelihood estimate [14] of n_0 is that value of n_0 that maximize $p(\mathbf{y}; n_0)$ in Equation (D.4) for a given observed $\mathbf{y}$. Because $\left[2\pi h_a^2(0)\right]^{\frac{N}{2}}$ does not depend on the parameter n_0 and $(\mathbf{y} - \beta\mathbf{p}_{1a})^T \mathbf{\Sigma}_w^{-1}(\mathbf{y} - \beta\mathbf{p}_{1a}) \geq 0$, maximizing $p(\mathbf{y}; n_0)$ is equivalent to minimizing $(\mathbf{y} - \beta\mathbf{p}_{1a})^T \mathbf{\Sigma}_w^{-1}(\mathbf{y} - \beta\mathbf{p}_{1a})$. Thus, the maximum likelihood estimate of n_0 is

$$\hat{n}_0 = \arg\min_{n_0}(\mathbf{y} - \beta\mathbf{p}_{1a})^T \mathbf{\Sigma}_w^{-1}(\mathbf{y} - \beta\mathbf{p}_{1a}) \tag{D.15}$$

The cost function in Equation (D.15) can be written as

$$\begin{aligned} L(n_0) &= (\mathbf{y} - \beta\mathbf{p}_{1a})^T \mathbf{\Sigma}_w^{-1}(\mathbf{y} - \beta\mathbf{p}_{1a}) \\ &= \mathbf{y}^T \mathbf{\Sigma}_w^{-1}\mathbf{y} + \beta^2 \mathbf{p}_{1a}^T \mathbf{\Sigma}_w^{-1}\mathbf{p}_{1a} - 2\mathbf{y}^T \mathbf{\Sigma}_w^{-1}\mathbf{p}_{1a} \end{aligned} \tag{D.16}$$

Substituting Equation (D.11) into Equation (D.16), we obtain

$$L(n_0) \approx \mathbf{y}^T \mathbf{\Sigma}_w^{-1}\mathbf{y} + \beta^2 \mathbf{p}_a^T \mathbf{C}_2 \mathbf{p}_a - 2\mathbf{y}_2^T \mathbf{C}_2 \mathbf{p}_a \tag{D.17}$$

The first two items in Equation (D.17) reflect the signal energies of the observed $\mathbf{y}$ and the filtered P(Y) signal. They do not change with n_0 once an observation of $\mathbf{y}$ is captured. Thus

$$\begin{aligned} \hat{n}_0 &= \arg\min_{n_0} L(n_0) \\ &= \arg\max_{n_0} \mathbf{y}_2^T \mathbf{C}_2 \mathbf{p}_a \end{aligned} \tag{D.18}$$

When the length of signal $x(n)$, M, is much longer than the order of the whitening filter, the matrix $\mathbf{C}_2$ can also be written in a form similar to Equation (D.10) or

$$\mathbf{C}_2 = \mathbf{V}_{aM}^T \mathbf{V}_{aM} \tag{D.19}$$

where $\mathbf{V}_{aM}$ is the $M \times M$ transform matrix of the whitening filter. Thus Equation (D.18) can be written as

$$\begin{aligned} \hat{n}_0 &= \arg\max_{n_0} \mathbf{y}_2^T \mathbf{C}_2 \mathbf{p}_a \\ &= \arg\max_{n_0} \mathbf{y}_2^T \mathbf{V}_{aM}^T \mathbf{V}_{aM} \mathbf{p}_a \\ &= \arg\max_{n_0} (\mathbf{V}_{aM}\mathbf{y}_2)^T (\mathbf{V}_{aM}\mathbf{p}_a) \end{aligned} \tag{D.20}$$

Equation (D.18) shows that the MLE of the shift time n_0 is found using a cross-correlation operation. The two input signals in the cross-correlation first pass through the same whitening filter, i.e $\mathbf{V}_{aM}$. The inputs to the whitening filter are different. The first input/source signal, $\mathbf{p}_a$, is the filtered P(Y) code. The other input/source signal, $\mathbf{y}_2$, is a piece of observed signal at the authenticator. The whitened template signal is cross-correlated with all possible whitened measured signals at the authenticator. Then the estimate of shift time, $\hat{n}_0$, is the shift when the cross-correlation achieves its maximum.

For the GPS position authentication system, the P(Y) signal is unknown. Thus we can not directly use the cross-correlator in Equation (D.20). The only available signal is a noisy P(Y) signal, $x(n)$, which is the measurement at the supplicant. The effect of using this noisy signal as the template to estimate n_0 is discussed next.

Referring backing to Equation (D.1) and using the vector form, we obtain

$$\mathbf{p}_s = \frac{1}{\alpha}(\mathbf{x} - \mathbf{v}) \tag{D.21}$$

The vector $\mathbf{p}_s$ is the filtered signal of the P(Y) signal $p(n)$ through the supplicant filters. The impulse response of suppliant filters is $h_s(n)$ as shown in Figure D.1. Then we have

$$\mathbf{p}_s = \mathbf{H}_s\mathbf{p} \tag{D.22}$$

where $\mathbf{p}$ is the vector form of signal $p(n)$ and $\mathbf{H}_s$ is the transform matrix of $h_s(n)$. Substituting Equation (D.22) into Equation (D.21), we have

$$\mathbf{p} = \frac{1}{\alpha}\mathbf{H}_s^{-1}(\mathbf{x} - \mathbf{v}) \tag{D.23}$$

Substituting Equation (D.23) into Equation (D.20), we have

$$\begin{aligned}
\hat{n}_0 &= \arg\max_{n_0}(\mathbf{V}_{aM}\mathbf{y}_2)^T(\mathbf{V}_{aM}\mathbf{p}_a) \\
&= \arg\max_{n_0}(\mathbf{V}_{aM}\mathbf{y}_2)^T(\mathbf{p}) \\
&= \arg\max_{n_0}(\mathbf{V}_{aM}\mathbf{y}_2)^T(\frac{1}{\alpha}\mathbf{H}_s^{-1}(\mathbf{x} - \mathbf{v})) \\
&= \arg\max_{n_0}\left[(\mathbf{V}_{aM}\mathbf{y}_2)^T\left(\mathbf{H}_s^{-1}\mathbf{x}\right) - (\mathbf{V}_{aM}\mathbf{y}_2)^T\left(\mathbf{H}_s^{-1}\mathbf{v}\right)\right]
\end{aligned} \tag{D.24}$$

This is equivalent to maximizing the cost function

$$\begin{aligned} L_1(n_0) &= \frac{(\mathbf{V}_{aM}\mathbf{y}_2)^T\left(\mathbf{H}_s^{-1}\mathbf{x}\right)}{N} - \frac{(\mathbf{V}_{aM}\mathbf{y}_2)^T\left(\mathbf{H}_s^{-1}\mathbf{v}\right)}{N} \\ &= \frac{\mathbf{y}_2^T\mathbf{G}\mathbf{x}}{N} - \frac{\mathbf{y}_2^T\mathbf{G}\mathbf{v}}{N} \end{aligned} \tag{D.25}$$

where $\mathbf{G} = \mathbf{V}_{aM}\mathbf{H}_s^{-1}$.

Because we have only measurements $\mathbf{x}$ and $\mathbf{y}$, the best estimate we can generate is to find $\hat{n}_0$ by maximizing the first term in Equation (D.25). It is obviously not the MLE of n_0 because the second term varies for different time shifts. Note that both terms in Equation (D.25) are sample cross-correlations. The noise $\mathbf{v}$ is independent of both $\mathbf{p}_a$ and $\mathbf{w}$ in the measurement $\mathbf{y}$. Thus when the number of cross-correlation samples, M, is sufficiently large, the second term in Equation (D.25) is close to zero and can be ignored. That means as M$\rightarrow \infty$ the cross-correlation between $\mathbf{x}$ and $\mathbf{y}$, i.e $\frac{\mathbf{y}_2^T\mathbf{G}\mathbf{x}}{N}$ is asymptotic to the MLE.

In summary, it has been shown that the cross-correlation between two measurement $\mathbf{x}$ and $\mathbf{y}$, i.e $\frac{\mathbf{y}_2^T\mathbf{G}\mathbf{x}}{N}$, is not the MLE of time shift n_0. However, if the number of samples used to compute the cross-correlation is sufficiently large, the estimate $\hat{n}_0$ will approach the MLE estimate.