GPS Signal and Position Authentication

Final Report

University of Minnesota Avionics Laboratory
Department of Aerospace Engineering & Mechanics
110 Union St, SE
Minneapolis, MN 55455
September 26, 2014

Authors:
Zhefeng Li
Demoz Gebre-Egziabher

*The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. The authors acknowledge the United States Department of Homeland Security for supporting the work reported here through the National Center for Border Security and Immigration under grant number 2008-ST-061-BS0002. However, any opinions, findings, conclusions or recommendations in this paper are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security.

Contents

List of Figures

List of Tables

Executive Summary

This report describes a position authentication system utilizing the white noise like GPS spreading codes as tamper proof watermarks. Position authentication as used in this report 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. This report also discusses an important implementation issue: Multiple false peaks caused by C/A power leakage which mask the detection of the watermark. Experimental results 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.

1 Introduction

This paper deals with the problem of position authentication. The term "position authentication" as discussed in this paper 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 commercial applications such as tamper-free shipment tracking and smart-border systems to enhance cargo inspection procedures will benefit from a position authentication system. Examples of the latter applications include some envisioned concepts of operation aimed at enhancing the safety and efficiency of commercial cargo shipment between the US, Canada and Mexico.

There are many commercial fleet and asset tracking systems available in the market, such as *FleetMatics* [2], *WirelessMatrix* [5], 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 travelling in an expected manner. This method of tracking is depicted graphically in Fig. 1.

The approach shown in Fig. 1 has at least two potential scenarios or fault modes which can lead to erroneous tracking of the 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 [8]). 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 [8] [6], 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 asset end but it cannot solve the report falsification problem at the monitoring center end.

The purpose of this paper is to examine the problem at the monitoring center. This paper 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 paper is based on the idea first presented in [10] and utilizes features of the GPS signal as tamper-proof watermarks to detect deceptive or erroneous position reports.

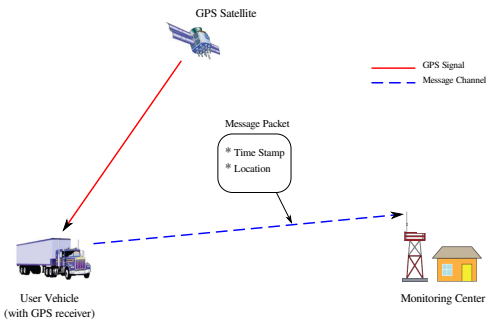

Figure 1: Typical asset tracking system

1.1 Using White Noise as a Watermark

The features for GPS position authentication should be very hard to reproduce and unique to different locations and time. In this case, the authentication process is reduced to detecting these features and checking if these features satisfy some constraints. The features are similar to the well designed watermarks to detect counterfeits.

The ideal white noise signal is a perfect watermark signal in the sense that it is impossible reproduce and predict. When the feature detection is performed, the signal to be checked is compared with a watermark template. To generate a white noise watermark template based on a mathematical model is impossible, so an alternative way is to get a real-time copy of this watermark signal from a trusted source.

Fig. 2 and Fig. 3 show the above idea would work. Fig. 2 is the architecture of the detection system. There is one transmitter T_x and two receivers (R_s and R_a) in the system. The task is to tell if a signal received at the receiver R_s is truly from T_x. R_a is the trusted source which gets a copy of the authentic signal $V_x(t)$ (i.e., the signal transmitted by T_x). R_a is established so that it can continuously and securely receive the signal from T_x. The snapshot signal $V_s(t)$ received at R_s is sent to the trusted place to compare with the signal $V_a(t)$ received at R_a.

The signals at T_x, R_a and R_s are depicted in Fig. 3. 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 a verification 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 [13]. 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 has a non-zero value. So the non-zero correlation means a match. In Fig. 3, 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. 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.

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

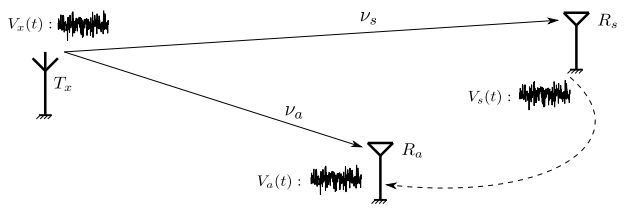

Figure 2: Architecture to detect a snapshot of a white noise

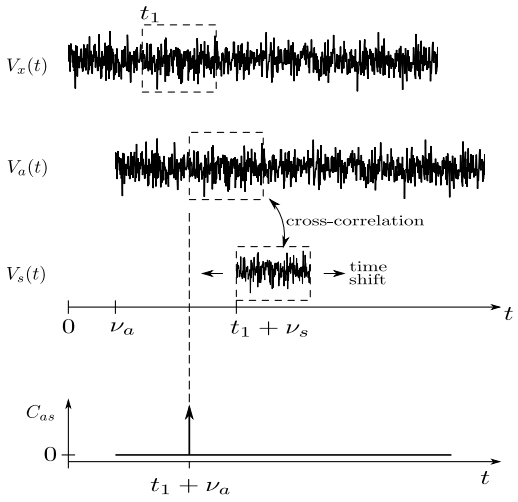

Figure 3: Signals of a white noise snapshot detection

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 Fig. 4, this watermark signal can be found inside the tracking loop quadrature signal $Q_1(t)$.

1.2 Prior Work

In [10] a method to authenticate whether a user is utilizing authentic GPS signal which is based on this watermark is introduced. The signal authentication method uses a segment of noisy P(Y) signal (not code) collected by a trusted user (called the authenticator) as a template. Another user's (called the supplicant) 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 means the GPS signal provided by the supplicant is false. A correlation peak that occurs earlier or later than predicted (based on the supplicant's reported position) indicates a false position report.

Fig. 5 is the architecture of the position authentication system described in this paper.

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

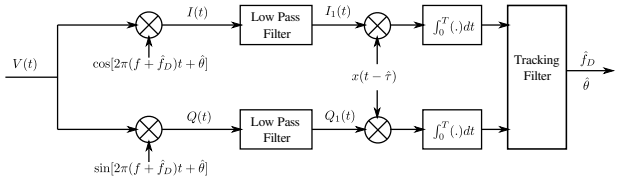

Figure 4: Watermark signal in a civilian receiver's tracking loop

the position message are transmitted to the authentication center by any data-link (e.g. cell phone data network, Wi-Fi, etc.).

The authentication station keeps tracking all the common satellites of the authenticator and the supplicant. 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.

1.3 Organization of the paper

The remainder of this paper describes the details of the authentication process and is organized as follows: In Section 2 we will discuss where the signals used for authentication are extracted within a GPS receiver. Then we will discuss the authentication autocorrelation function. This will lead to the problem we call "the C/A power leakage problem." How to deal with this problem is the subject of Section 3. In Section 4 we show how we can not only authenticate the signal but also calculate the position of the supplicant. In section 5, hardware developed to perform experimental validation is discussed. Concluding remarks close the paper. Two appendices are also included which provide detailed derivation of the peak detection function and the supplicant position calculation.

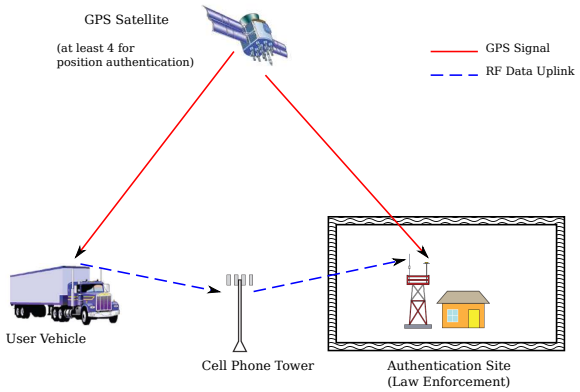

Figure 5: Architecture of position authentication system

2 Watermark Signal Detection

The watermark signal of interest is included in the signal $Q_1(t)$ shown in Fig. 4. But $Q_1(t)$ also has other components other than the watermark signal. Other signal components will 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 for 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 Fig. 4) signal in the authenticator's tracking loop is mathematically described as:

$$V^a_{1Q}(t) = \sqrt{2P^a_{c1}}Y_{D1}(t-\nu^a_1) + \sqrt{2P^a_{c2}}X_{D2}(t-\nu^a_2)\sin(2\pi\Delta f^a_{21}t + \Delta\theta^a_{21}) + \sqrt{2P^a_{y2}}Y_{D2}(t-\nu^a_2)\cos(2\pi\Delta f^a_{21}t + \Delta\theta^a_{21}) + n^a_Q(t) \quad (1)$$

where $n^a_Q(t)$ is the projected noise form the receiver noise $n^a(t)$ (see Appendix A) to the quadrature product. The other variables in this equation are defined as follows:

$x_i(t)$	The C/A spreading code
$y_i(t)$	The P(Y) spreading code
$D_i(t)$	The navigation message
$X_{Di}(t)$	$D_i(t)x_i(t)$
$Y_{Di}(t)$	$D_i(t)y_i(t)$
P^a_{ci}	The received C/A signal power for SVi
P^a_{yi}	The received P(Y) signal power SVi
ν^a_i	RF signal propagation delay SVi
Δf^a_i	The Doppler frequency SVi
$\Delta\theta^a_i$	The phase shift SVi
Δf^a_{ij}	$\Delta f^a_i - \Delta f^a_j$
$\Delta\theta^a_{ij}$	$\Delta\theta^a_i - \Delta\theta^a_j$

where the superscripts "a" and "s" denote "authenticator" and "supplicant" signals, respectively. The equations for the supplicant are the same as (1) where we replace the superscript "a" with "s."

Equation (1) is in Appendix A assuming that the tracking loop is locked. Now, the C/A signal of SV1 is wiped off and the P(Y) signal of SV1 is kept in the in-phase product. Because usually $\Delta f_{21} \neq 0$ and $\Delta\theta^a_{21} \neq 0$, there will be SV2's C/A signal residual and P(Y) signal residual in this SV1's quadrature product. The residual signals are modulated by a much lower frequency than the code chip rate. This low frequency sinusoidal signal is caused by the Doppler frequency difference between the SV1 and SV2. The P(Y) signal of SV1 does not have this low frequency component.

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

$$C_{_{1Q}}(\tau, T) = \frac{1}{T}\int_0^T V_{1Q}^a(t)V_{1Q}^s(t+\tau)\mathrm{d}t \tag{2}$$

Generally we only use a snapshot of the supplicant's signal of duration T. We also choose a snapshot signal from the authenticator with the same duration T. To use another snapshot of the authenticator signal, a different delay value τ is chosen. The variable τ denotes the relative delay of the authenticator's signal relative to the supplicant's signal. 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 $\frac{1}{T}\sqrt{P_{y_2}^a P_{y_2}^s}$.

Residuals from the signals of other satellites present in the quadrature products may also generate peaks when computing the cross-correlation defined by (2) above. The cross-correlation between different codes can be ignored because of the orthogonal property of different codes. The cross-correlation between SV2's signal residuals in $V_{_{1Q}}^s$ and $V_{_{1Q}}^s$, however, needs to be considered carefully. This is examined next.

2.0.1 P(Y) Residual Cross-correlation

The P(Y) residual signal is the third term in (1). In (2), the cross-correlation is only performed using a piece of the P(Y) signal (duration T). The partial correlation of the P(Y) code is different from the full length auto-correlation of one satellite's P(Y) code. The choice of this piece of signal is random, so we use the expectation of the cross-correlation rather than the cross-correlation itself. To simplify the analysis, we only consider the delay τ is only the integer times of the P(Y) chip duration T_c. That means $\tau = nT_c$, where $n = 0, 1, 2, 3....$ The reader is referred to Appendix A for a detailed derivation of the mathematical expression for this expectation of the cross correlation between two pieces of the P(Y) residual signal:

$$E\{C_{_{y2,y2}}(n, T)\} = \begin{cases} \frac{1}{T}\sqrt{P_{y_2}^a P_{y_2}^s}\left[\mathrm{sinc}(2\pi\Omega_u T) + \mathrm{sinc}(2\pi\Omega_b T)\right] E[\cos(\Psi_u)] & \text{if } n = 0 \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

where, for ease of writing, we have used the following auxiliary variables:

$$\begin{aligned} \Omega_u &= \Delta f_{21}^a + \Delta f_{21}^s \\ \Omega_b &= \Delta f_{21}^a - \Delta f_{21}^s \\ \Psi_u &= \Delta\theta_{21}^a - \delta\phi_1^a + 2\pi\Delta f_{21}^s\tau + \Delta\theta_{21}^s - \delta\phi_1^s \\ \Psi_b &= \Delta\theta_{21}^a - \delta\phi_1^a - 2\pi\Delta f_{21}^s\tau - \Delta\theta_{21}^s + \delta\phi_1^s \end{aligned} \tag{4}$$

Furthermore, $\mathrm{sinc}(x) = \frac{\sin(x)}{x}$.

From (3), we can find the conditions when the residuals, the SV2's signals in SV1's quadrature products, like or exhibit a correlation peak. If $\tau = 0$ or $n = 0$, the cross-correlation may generate a peak. It depends on the value of $\Omega_b T$ and $\Omega_u T$. If $\Omega_b T$ or $\Omega_u T = \frac{k}{2}$, where k=1, 2, 3, ... , then $\mathrm{sinc}(2\pi\Omega_b T) = 0$ or $\mathrm{sinc}(2\pi\Omega_u T) = 0$. There is no peak generated. If $\Omega_b T$ or $\Omega_u T \neq \frac{k}{2}$, then $\mathrm{sinc}(2\pi\Omega_b T) \neq 0$ or $\mathrm{sinc}(2\pi\Omega_u T) \neq 0$. In this situation, a false correlation peak is generated.

To mitigate the effect of the false peak, we can either choose T so that $\Omega_u T \gg \frac{1}{2}$ and $\Omega_b T \gg \frac{1}{2}$ or choose a bigger Ω_u and Ω_b. The maximum T is limited by the dynamics of

the authenticator and the supplicant. That means either we use longer snapshot to do the correlation or we choose the authenticator's location so that the distance between the authenticator and the supplicant is far enough. The worst scenario is when the authenticator and the supplicant are very close. In this case $\Delta f^s_{21} \approx \Delta f^a_{21}, \Omega_b = 0$, so $\text{sinc}(2\pi\Omega_b T)$ achieves its maximum value 1.

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 2 common satellites are in view. When there are more than 2 common satellites, there may have multiple P(Y) peaks. This is shown in Fig. 18 in Section 5.

2.0.2 C/A Residual

The fourth line in (1) is SV2's C/A signal residuals. When the correlation detection is performed as in (2), these two residuals may also generate C/A false peaks. The cross-correlation between two C/A signal residuals is

$$C_{x2,x2}(\tau, T) = \frac{2}{T}\sqrt{P^a_{x_2} P^s_{x_2}} \int_0^T X_{D2}(t) X_{D2}(t+\tau) \cos(2\pi\Delta f^a_{21} t + \Delta\theta^a_{21} - \delta\phi^a_1) \cos[2\pi\Delta f^s_{21}(t+\tau) + \Delta\theta^s_{21} - \delta\phi^s_1]\mathrm{d}t \quad (5)$$

The similar analysis for the $C_{x2,x2}(\tau, T)$ can be done as that for the $C_{y2,y2}(\tau, T)$. But the C/A code is different from the P(Y) code in that the C/A code is a short code which repeats every 1 ms, while the P(Y) code is a long code which repeats every week. The auto-correlation function of a C/A code [11] is a periodic function. Its period is 1 ms. In the absence of noise, the maximum value is 1 when $\tau = 0, 1, 2, ...,$ ms. C/A peaks may occur in a period of 1 ms when $\tau = 0, 1, 2, 3, ...,$ ms. It depends on the value of $\Omega_u T$ and $\Omega_b T$.

The correlation $C_{1Q}(\tau, T)$ to detect the P(Y) signal in SV1 is the superposition of $C_{y1,y1}(\tau, T)$, $C_{y2,y2}(\tau, T)$ and $C_{x2,x2}(\tau, T)$. That is,

$$C_{1Q}(\tau, T) = C_{y1,y1}(\tau, T) + C_{x2,x2}(\tau, T) + C_{y2,y2}(\tau, T) \quad (6)$$

Only the cross-correlation of SV1's P(Y) signal, $C_{y1,y1}(\tau, T)$ in (6), is the desired quantity. To detect the correct correlation peak, the effect of residual signals need to be mitigated. The method to eliminate the $C_{x2,x2}(\tau, T)$ is introduced in section 3.

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 are higher than the true peak. The C/A false peaks repeat in every 1 ms. If the C/A false peaks occur, they are greater than the true peak in both number and strength. With noise, it is hardly to identify the true peak from the correlation result corrupted by the C/A residuals.

In this section, a high-pass filter is introduced to address the problem. Simulation results are also listed to show the performance of this filter. Because the P(Y) code is unavailable to us, in the simulation we use P code instead to study the random characteristics of the

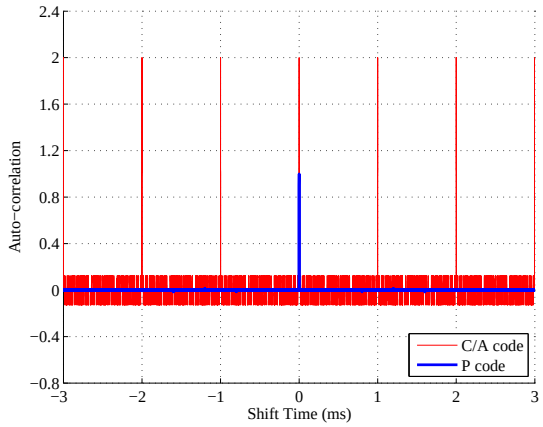

Figure 6: Auto-correlation of P codes and C/A code

watermark signal. This assumption is entirely correct. In Section 5, experimental results are listed to show this assumption is reasonable. Snapshots with 50 ms duration of PRN1's C/A code signal and PRN1's P code signal are used in the simulation.

The simulation result in Fig. 6 shows both the true peak (P code) and the false peaks (C/A code).

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 discussed above is that many match filters are needed. A simpler filter is proposed here 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 can be attenuated by one filter rather than to use separate match filters for different satellites. Fig. 7 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 Fig. 7. The high-pass filter only filter out the main lobe of the C/A signals. Because the spectrum of the C/A code signal and the spectrum of the P code signal are fully overlapped in $\pm$10.23 MHz, the high-pass filter also attenuates part of the P code energy. This degrades the auto-correlation peak of the P code. Even though the gain of the high-pass filter is the same for both the C/A code and the P code signals, this 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. The *false-peak rejection ratio* of the non-filtered signals is 0.5. Here we assume the worst case when C/A false peaks have the maximum amplitude as we discussed in the end of Section 2. The cut-off frequency of the high-pass filter is a parameter to be optimized to achieve a desired *false-peak rejection ratio*.

Fig. 8 is the comparison of the auto-correlation peak values using the filter in Fig. 7. The

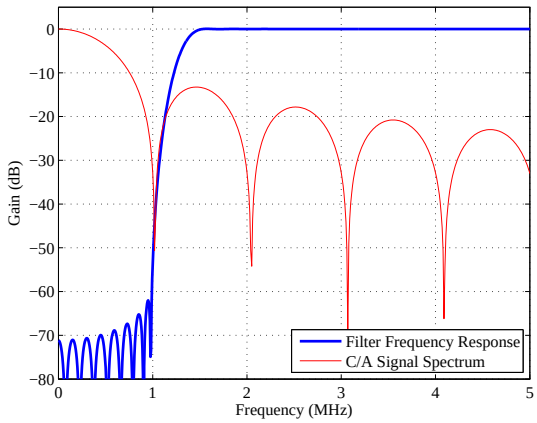

Figure 7: Frequency response of the notch filter

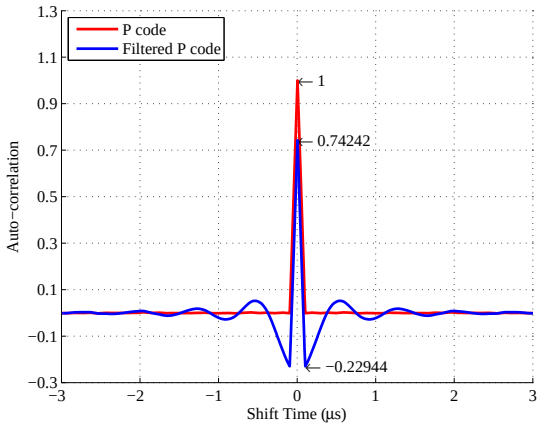

Figure 8: P code auto-correlation (filtered vs. non-filtered)

auto-correlation peak of the non-filtered P code is normalized to 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 Fig. 9. 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 Fig. 10. 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). 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 shows that one simpler high-pass filter rather than multiple match filters can be designed to achieve an acceptable *false-peak rejection ratio*.

4 Position Calculation

Consider the situation depicted in Fig. 11 where the authenticator and the supplicant have multiple common satellites in view. In this case, not only can we perform the *signal*

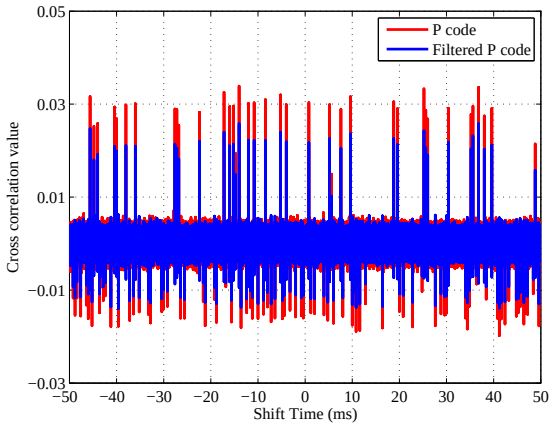

Figure 9: P code cross-correlation (filtered vs. non-filtered)

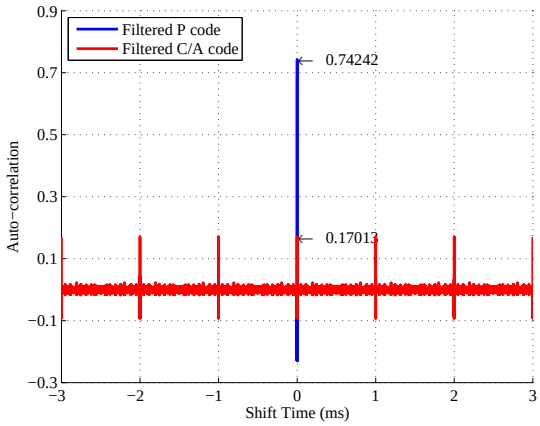

Figure 10: Auto-correlation of filtered codes

authentication (correlation detection described in Section 2) 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 of the supplicant is based on the P(Y) watermark signal rather than the supplicant's C/A signal. 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.

Fig. 12 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: SAT1, SAT2, SAT3 and SAT4. 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 SAT1 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 SAT2, SAT3 and SAT4 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

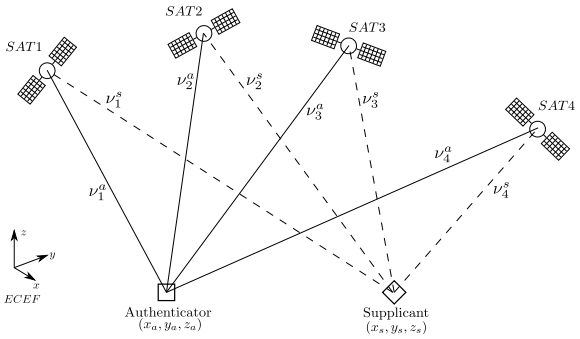

Figure 11: Positioning using watermark signal

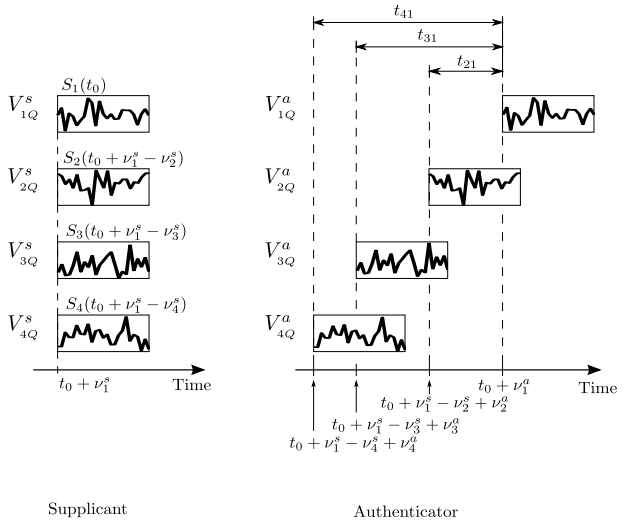

Figure 12: Relative time delays

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 Fig. 12 where a snapshot of the signal received from the supplicant's time $t_0 + \nu_1^s$ includes GPS signals from SAT1, SAT2, SAT3 and SAT4. 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 in the supplicant at time $t_0+\nu_1^s$ are $S_1(t_0)$, $S_2(t_0+\nu_1^s-\nu_2^s)$, $S_3(t_0+\nu_1^s-\nu_3^s)$ and $S_4(t_0+\nu_1^s-\nu_4^s)$. If this same snapshot of the signal at the supplicant is used to detect the matched watermark signals from SAT1, SAT2, SAT3 and SAT4 at the authenticator, the peaks time should occurs at $t_0 + \nu_1^a$, $t_0 + \nu_1^s - \nu_2^s + \nu_2^a$, $t_0 + \nu_1^s - \nu_3^s + \nu_3^a$ and $t_0 + \nu_1^s - \nu_4^s + \nu_4^a$.

Let t_{21} be the measured peak time delay from SAT2 to SAT1; let t_{31} be the measured peak time delay from SAT3 to SAT1; and let t_{41} be the measured peak time delay from SAT4 to SAT1. Then we have (7).

$$\begin{aligned} t_{21} &= t_0 + \nu_1^s - \nu_2^s + \nu_2^a - (t_0 + \nu_1^a) \\ t_{31} &= t_0 + \nu_1^s - \nu_3^s + \nu_3^a - (t_0 + \nu_1^a) \\ t_{41} &= t_0 + \nu_1^s - \nu_4^s + \nu_4^a - (t_0 + \nu_1^a) \end{aligned} \tag{7}$$

Equation (7) can be written as (8)

$$\begin{aligned} t_{21} &= (\nu_2^a - \nu_1^a) - (\nu_2^s - \nu_1^s) \\ t_{31} &= (\nu_3^a - \nu_1^a) - (\nu_3^s - \nu_1^s) \\ t_{41} &= (\nu_4^a - \nu_1^a) - (\nu_4^s - \nu_1^s) \end{aligned} \tag{8}$$

If the receiver has no noise, the travel time ν from a satellite to a receiver is

$$\nu = \frac{\rho}{c} + I + T \tag{9}$$

where ρ is the distance between the satellite and the receiver, c is speed of light, I is the ionospheric delay, T is the tropospheric delay.

Using (9), equation (8) can be rewritten as

$$\begin{aligned} t_{21} &= \frac{1}{c}\left[(\rho_2^a - \rho_1^a) - (\rho_2^s - \rho_1^s)\right] + (I_2^a - I_1^a) - (I_2^s - I_1^s) + (T_2^a - T_1^a) - (T_2^s - T_1^s) \\ t_{31} &= \frac{1}{c}\left[(\rho_3^a - \rho_1^a) - (\rho_3^s - \rho_1^s)\right] + (I_3^a - I_1^a) - (I_3^s - I_1^s) + (T_3^a - T_1^a) - (T_3^s - T_1^s) \\ t_{41} &= \frac{1}{c}\left[(\rho_4^a - \rho_1^a) - (\rho_4^s - \rho_1^s)\right] + (I_4^a - I_1^a) - (I_4^s - I_1^s) + (T_4^a - T_1^a) - (T_4^s - T_1^s) \end{aligned} \tag{10}$$

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

$$\chi_{ij} = (I_i^a - I_j^a) - (I_i^s - I_j^s) + (T_i^a - T_j^a) - (T_i^s - T_j^s) \tag{11}$$

then (10) can be written as

$$\begin{aligned} t_{21} &= \frac{1}{c}[(\rho_2^a - \rho_1^a) - (\rho_2^s - \rho_1^s)] + \chi_{21} \\ t_{31} &= \frac{1}{c}\left[(\rho_3^a - \rho_1^a) - (\rho_3^s - \rho_1^s)\right] + \chi_{31} \\ t_{41} &= \frac{1}{c}\left[(\rho_4^a - \rho_1^a) - (\rho_4^s - \rho_1^s)\right] + \chi_{41} \end{aligned} \tag{12}$$

In practice, the measurement always has noise. For example, the measured peak delay of t_{21} is

$$\hat{t}_{21} = t_{21} + \delta t_{21} \tag{13}$$

where $\delta t_{21}$is the noise in the measurement. This noise is caused by the clock error and signal alignment error. The peak time delay is only measured in a very short time, so only the short time stability of the supplicant's and the authenticator's clocks contribute to the measurement. When the signal from both the supplicant and the authenticator have noise, they lead to an offset (bias) in the peak detection time. We call this offset time as the alignment error. 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 shown in Fig. 13. So any measurement based on differencing the signals from the supplicant and the authenticator will have an error. This error is also included in the term δt_{21}. Increasing the sampling frequency minimizes this error.

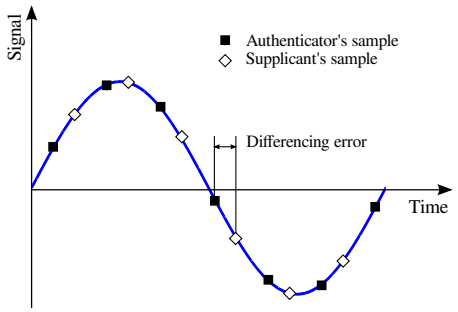

Figure 13: Clock differencing error

Referring to Fig. 11 again, suppose the authenticator's position (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_i^a is known. The positions of common satellites are also known to the authenticator. Rearranging (10) by moving the unknown variables to the left side and putting the measurements on the right side, we obtain

$$\begin{aligned} \rho_2^s - \rho_1^s &= \rho_2^a - \rho_1^a - ct_{21} + c\chi_{21} \\ \rho_3^s - \rho_1^s &= \rho_3^a - \rho_1^a - ct_{31} + c\chi_{31} \\ \rho_4^s - \rho_1^s &= \rho_4^a - \rho_1^a - ct_{41} + c\chi_{41} \end{aligned} \tag{14}$$

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

$$\rho_i^s = \sqrt{(x_i - x_s)^2 + (y_i - y_s)^2 + (z_i - z_s)^2} \tag{15}$$

Equation (14) is a system of three equations in three unknowns. The unknowns are the components of the supplicants position vector $\mathbf{r}_s = [x_s, y_s, z_s]^T$. This equation can be linearized and then solved using least squares techniques. When linearized (see Appendix B for details) the equations have the following form:

$$\mathbf{A}\delta\mathbf{r}_s = \delta\mathbf{m} \tag{16}$$

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

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

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

$$\begin{bmatrix} \delta m_1 \\ \delta m_1 \\ \delta m_3 \end{bmatrix} = \begin{bmatrix} \hat{\mathbf{e}}_2^T\delta\mathbf{r}_2 - \delta\rho_2^a + c\delta t_{21} - c\delta\chi_{21} - \hat{\mathbf{e}}_1^T\delta\mathbf{r}_1 + \delta\rho_1^a \\ \hat{\mathbf{e}}_3^T\delta\mathbf{r}_3 - \delta\rho_3^a + c\delta t_{31} - c\delta\chi_{31} - \hat{\mathbf{e}}_1^T\delta\mathbf{r}_1 + \delta\rho_1^a \\ \hat{\mathbf{e}}_4^T\delta\mathbf{r}_4 - \delta\rho_4^a + c\delta t_{41} - c\delta\chi_{41} - \hat{\mathbf{e}}_1^T\delta\mathbf{r}_1 + \delta\rho_1^a \end{bmatrix} \tag{17}$$

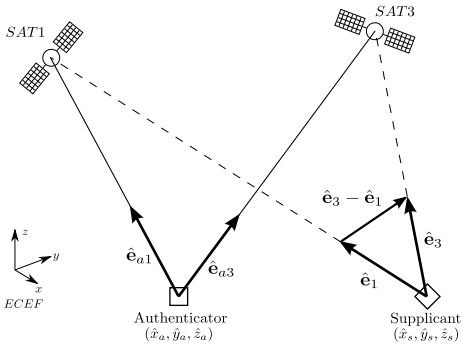

Figure 14: Line of sight vectors

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 (11)) and $\delta\rho_i^a$ is the measurement error of pseudorange ρ_i^a. As noted earlier, derivation of these equations is given in Appendix B. Fig. 14 is an example of LOS vectors used in the above equations.

Equation (16) is a standard form which can be solved by a weighted least squares(WLS) method. The solution is

$$\delta\mathbf{r}_s = (\mathbf{A}^T\mathbf{R}^{-1}\mathbf{A})^{-1}\mathbf{A}^T\mathbf{R}^{-1}\delta\mathbf{m} \tag{18}$$

where $\mathbf{R}$ is the covariance matrix of the measurement error vector $\delta\mathbf{m}$.

From (16) (18), we can see that the supplicant's position accuracy depends on both the geometry and the measurement errors.

4.1 Measurement Covariance Matrix R

The Authentication station is usually located at a fix position whose coordinates can be calibrated in a very high accuracy by surveillance systems. 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

$$\delta\rho_i^a = \mathbf{e}_{ai}^T\delta\mathbf{r}_i \tag{19}$$

For fix authentication station, (17) can be rewritten as

$$\delta\mathbf{m} = \begin{bmatrix} \delta m_1 \\ \delta m_1 \\ \delta m_3 \end{bmatrix} = \begin{bmatrix} \left(\hat{\mathbf{e}}_2^T - \mathbf{e}_{a2}^T\right)\delta\mathbf{r}_2 + c\delta t_{21} - c\delta\chi_{21} - \left(\hat{\mathbf{e}}_1^T - \mathbf{e}_{a1}^T\right)\delta\mathbf{r}_1 \\ \left(\hat{\mathbf{e}}_3^T - \mathbf{e}_{a3}^T\right)\delta\mathbf{r}_3 + c\delta t_{31} - c\delta\chi_{31} - \left(\hat{\mathbf{e}}_1^T - \mathbf{e}_{a1}^T\right)\delta\mathbf{r}_1 \\ \left(\hat{\mathbf{e}}_4^T - \mathbf{e}_{a4}^T\right)\delta\mathbf{r}_4 + c\delta t_{41} - c\delta\chi_{41} - \left(\hat{\mathbf{e}}_1^T - \mathbf{e}_{a1}^T\right)\delta\mathbf{r}_1 \end{bmatrix} \tag{20}$$

The errors in the measurement vector $\delta\mathbf{m}$ in (20) can be categorized into three groups based on the error mechanisms:

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	$\sigma_{\chi_{41}}$

Table 1: Variance of measurement error

1. satellite position error: $\delta\mathbf{r}_1$, $\delta\mathbf{r}_2$, $\delta\mathbf{r}_3$, $\delta\mathbf{r}_4$
2. peak delay error: δt_{21}, δt_{31}, δt_{41}
3. atmospheric parameter 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 parameter error is because the ionospheric model and the tropospheric model are not accurate enough.

The different error mechanisms make every error source listed above independent to others. Each error source can be described as a Gaussian random variable, so $\delta\mathbf{m}$ is a multi-dimensional Gaussian random vector in which each dimension is independent to others.

Using the symbols in Table 1, the covariance of the Gaussian random variable $\delta\mathbf{m}$ denoted $\mathbf{R}$ is given by

$$\mathbf{R} = E\left[\delta\mathbf{m}\delta\mathbf{m}^T\right] = \begin{bmatrix} \sigma_{m11}^2 & \sigma_{\mathbf{r}_1}^2 & \sigma_{\mathbf{r}_1}^2 \\ \sigma_{\mathbf{r}_1}^2 & \sigma_{m22}^2 & \sigma_{\mathbf{r}_1}^2 \\ \sigma_{\mathbf{r}_1}^2 & \sigma_{\mathbf{r}_1}^2 & \sigma_{m33}^2 \end{bmatrix} \tag{21}$$

where the diagonal items are

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

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

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

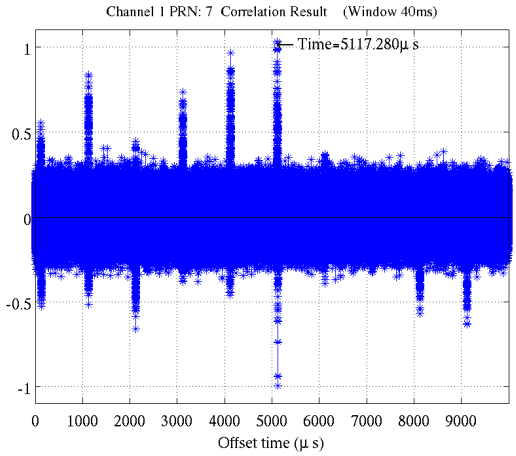

Figure 15: Correlation detection without high-pass filter

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.

The geometry matrix $\mathbf{A}$ has the similar function as the geometry matrix in a standard GPS receiver. The covariance matrix of the supplicant position error is

$$\text{cov}(\delta \mathbf{r}_s) = (\mathbf{A}^T \mathbf{R}^{-1} \mathbf{A})^{-1} \tag{22}$$

5 Experimental Validation

In what follows, we present experimental results validating the performance of the algorithms described earlier. The hardware used for these experiments is described in detail in the appendix to this report. First we present results that we can successfully deal with the C/A leakage problem using the high-pass filter described in Section 3. We perform a correlation between snippets of signal collected from the authenticator and a second USRP N210 software defined radio. Fig. 15 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 are not in the same amplitude. Fig. 16 show the correlation result using the same data snapshot as in Fig. 15. The difference is that Fig. 16 uses the high-pass filter 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 in Section 3.

Fig. 17 is a zoom in of the area around the peak in Fig. 16 to assess the accuracy of the peak detection. The method to calculate the "Expected Peak Time" in Fig. 17 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

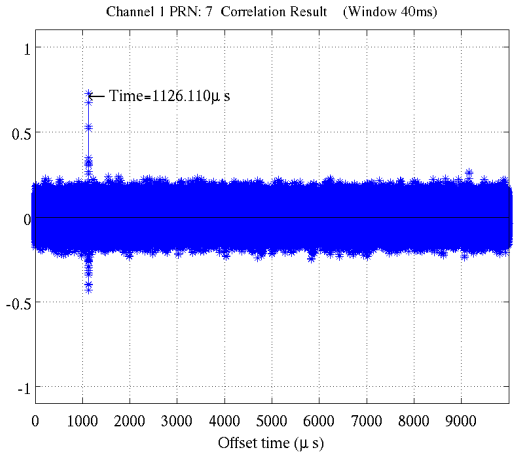

Figure 16: Correlation detection with high-pass filter

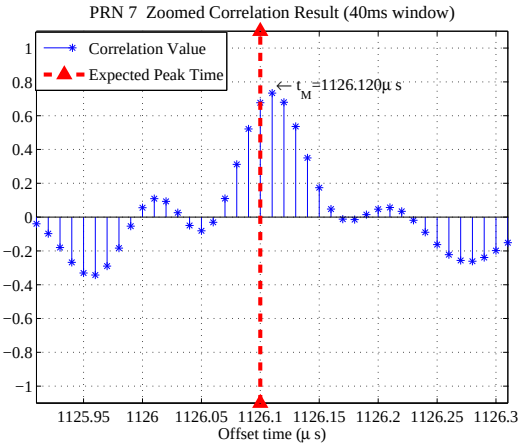

Figure 17: Correlation peak and expected peak time

are known. Referring back to (14), we rearrange it as

$$\begin{aligned} t_{21} - \chi_{21} &= \frac{1}{c}[(\rho_2^a - \rho_1^a) - (\rho_2^s - \rho_1^s)] \\ t_{31} - \chi_{31} &= \frac{1}{c}[(\rho_3^a - \rho_1^a) - (\rho_3^s - \rho_1^s)] \\ t_{41} - \chi_{41} &= \frac{1}{c}[(\rho_4^a - \rho_1^a) - (\rho_4^s - \rho_1^s)] \end{aligned} \tag{23}$$

The quantities on right side of (23) are all known. We calculate the right side and mark it as "Expected Peak Time" in Fig. 17. The left side is equivalent to the measured peak delay. Referring back to Fig. 15, we find that the peak time in Fig. 15 is wrong. This tell us that the peak with maximum value may not be the true peak if the C/A signal is not attenuated. Fig. 17 shows the error of the correlation peak is very small (less than 1 sampling interval).

Fig. 18 shows the P(Y) correlation peaks when there are more than one common satellites. Five P(Y) correlation peaks occur. Evey peak corresponds to one commone satellite. The relative time when these peaks occur constrained by the pseudorange differences. Table 2 shows the measured pseudorange difference using the C/A code. Comparing the delay time

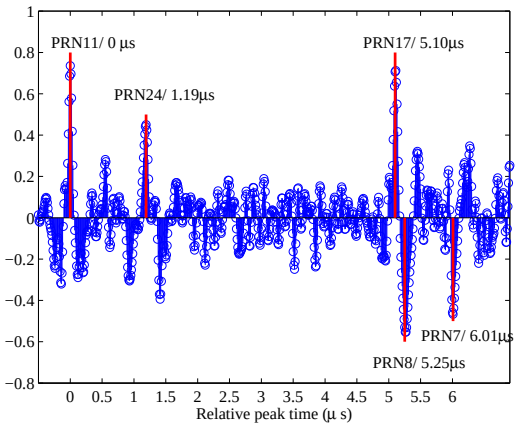

Figure 18: Delays between multiple P(Y) peaks

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

Table 2: Relative delays between multiple P(Y) peaks

in Table 2 and peak time in Fig. 18, we find that the peak time measurements from the Fig. 18 has very high accuracy.

Next we describe an experiment to validate the operation of the system as described earlier in the paper. In this experiment, the authenticator and the supplicant are 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 Fig. 19.

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

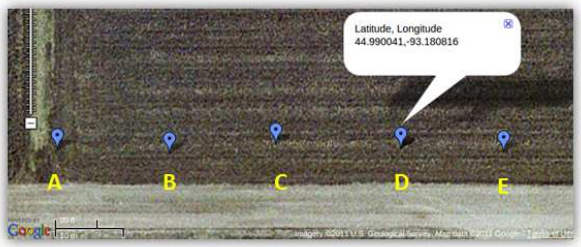

Figure 19: Five-point field test

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 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 3). That means the supplicant's raw IF signal has the watermark signal from every common satellite. 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 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 paper, 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 (13)) 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 3). Even though the position solution is not recalculated using the method described in Section 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.

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

Table 3: Five-Point position authentication results

6 Applications to Cargo Tracking

The GPS potion authentication system discussed above could be used to solve the two fault modes of typical commercial cargo/asset tracking systems discussed in Section 1. To use the authentication system, the commercial tracking system need to be updated. First, authentication stations as shown in Fig. 5 are setup to cover specific geographic regions. Second, the commercial GPS receivers on cargos or containers need to be updated to be capable to collect the GPS IF signal snapshot and to transmit this snapshot data back to the authentication station. The receivers on cargos or containers function as the supplicants discussed before. Supplicants also send back the real-time position calculated using the C/A code. When the authentication station receive the IF data snapshot and the C/A position, it recalculates an authentic postion using this snapshot. The reported C/A position is compared with the authentic position. If the difference between them is greater than a pre-defined range, the reported position is a fake position. That means a potential GPS signal spoofing or message tampering. The pre-defined position difference range is calculated based on the specifications of the false alarm rate and the miss detection rate.

The update of a commercial GPS receiver to a supplicant discussed above is not a very big modification. It only need to increase the sampling frequency of the A/D converter and to equip some buffer memory to temporarily store the snapshot data. The hardware cost can be greatly reduced with massive production, so that the increase of the supplicant's hardware cost can be ignored.

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.

One technical challenge to deploy the GPS position authentication station is the bandwidth of the data link between the supplicant and the authentication station. 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 capble to transmit this data size. If the 4G network is used, its bandwidth is wide enough to transmit this size of data. Further research can be conducted on reducing the sampling frequency and sampling resolution (4-bit in the experimental above) to reduce the bandwidth of the data transmission.

7 Conclusion

This paper described a GPS position authentication system. The authentication system has many potential applications where high credibility of a position report is required, such as cargo/asset tracking. The system detects a specific "watermark" signal in the broadcasted GPS signal to judge if a receiver uses 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 is discussed in the paper. A hardware platform which accomplishes this is 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 of this "watermark" signal.

In closing we note that before such a system is fielded its performance will have to be quantified in more precise terms. This quantification includes the rates of false alarm (i.e., concluding that a false position report has been made when in fact the report is authentic) and missed detection rates (i.e., a position report is judged to be authentic when in fact it is not).

Acknowledgment

The authors acknowledge 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. However, any opinions, findings, conclusions or recommendations in this paper are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security. The authors also acknowledge the useful suggestions provided by Dr. Sherman Lo and Dr. David J. De Lorenzo from the Stanford University GPS laboratory. The authors also acknowledge Prof. Tom Posbergh (Department of Electrical and Computer Engineering, University of Minnesota) for his support and help in FPGA code development.

A Derivation of Equation (3) in Section 2

The purpose of this appendix is to show how to derive the expressions for the cross-correlation function for the $Q_1(t)$ signals used in the authentication algorithm. Based on the parameter definitions in Section 2, the base band signal at the authenticator can be written

as

$$\begin{aligned} V^a(t) = &\sqrt{2P^a_{c_1}}X_{D1}(t-\nu^a_1)\cos(2\pi\Delta f^a_1 t + \Delta\theta^a_1) \\ &+ \sqrt{2P^a_{y_1}}Y_{D1}(t-\nu^a_1)\sin(2\pi\Delta f^a_1 t + \Delta\theta^a_1) \\ &+ \sqrt{2P^a_{c_2}}X_{D2}(t-\nu^a_2)\cos(2\pi\Delta f^a_2 t + \Delta\theta^a_2) \\ &+ \sqrt{2P^a_{y_2}}Y_{D2}(t-\nu^a_2)\sin(2\pi\Delta f^a_2 t + \Delta\theta^a_2) \\ &+ n^a(t) \end{aligned} \tag{24}$$

where $n^a(t)$ is the noise. The noise is mainly the thermal noise in the authenticator. 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 to eliminate 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 product and quadrature product. The quadrature product for SV1 at the authenticator is

$$\begin{aligned} V^a_{1Q}(t) &= V^a(t)\sin(2\pi\Delta\hat{f}^a_1 t + \Delta\hat{\theta}^a_1) \\ &= \sqrt{2P^a_{c_1}}X_{D1}(t-\nu^a_1)\sin\delta\phi^a_1 \\ &\quad + \sqrt{2P^a_{y_1}}Y_{D1}(t-\nu^a_1)\cos\delta\phi^a_1 \\ &\quad + \sqrt{2P^a_{c_2}}X_{D2}(t-\nu^a_2)\sin(2\pi\Delta f^a_{21}t + \Delta\theta^a_{21} - \delta\phi^a_1) \\ &\quad + \sqrt{2P^a_{y_2}}Y_{D2}(t-\nu^a_2)\cos(2\pi\Delta f^a_{21}t + \Delta\theta^a_{21} - \delta\phi^a_1) \\ &\quad + n^a_Q(t) \end{aligned} \tag{25}$$

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 (1) in Section 2 is obtained.

The in-phase product of the SV1 in the authenticator is

$$\begin{aligned} V^a_{1I}(t) &= V^a(t)\cos(2\pi\Delta\hat{f}^a_1 t + \Delta\hat{\theta}^a_1) \\ &= \sqrt{2P^a_{c_1}}X_{D1}(t-\nu^a_1)\cos\delta\phi^a_1 \\ &\quad + \sqrt{2P^a_{y_1}}Y_{D1}(t-\nu^a_1)\sin\delta\phi^a_1 \\ &\quad + \sqrt{2P^a_{c_2}}X_{D2}(t-\nu^a_2)\cos(2\pi\Delta f^a_{21}t + \Delta\theta^a_{21} - \delta\phi^a_1) \\ &\quad + \sqrt{2P^a_{y_2}}Y_{D2}(t-\nu^a_2)\sin(2\pi\Delta f^a_{21}t + \Delta\theta^a_{21} - \delta\phi^a_1) \\ &\quad + n^a_Q(t) \end{aligned} \tag{26}$$

where $n_I^a(t)$ is the projected noise form $n^a(t)$ to the in-phase product.

The base band signal at the supplicant, $V^s(t)$, and the quadrature product of SV1 in the supplicant, $V_{1Q}^s(t)$, are identical to $V^a(t)$ in (24) and $V_{1Q}^a(t)$ in (25), respectively, except the superscripts "a" are replaced by "s."

A.1 P(Y) Residual

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

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

where $n = 0, 1, 2, ...$, T_c is chip rate of the P(Y) code. Note that when $n = 0$, $\widetilde{Y}_2(t,n) \equiv 1$; when $n \neq 0$, $\widetilde{Y}_2(t,n)$ is another random sequence.

The correlation between the SV2's P(Y) residual signals is

$$C_{y2,y2}(n,T) = \frac{2}{T}\sqrt{P_{y_2}^a P_{y_2}^s}\int_0^T \widetilde{Y}_2(t,n)\cos(2\pi\Delta f_{21}^a t + \Delta\theta_{21}^a - \delta\phi_1^a) \cos[2\pi\Delta f_{21}^s(t+nT_c) + \Delta\theta_{21}^s - \delta\phi_1^s]\mathrm{d}t \tag{27}$$

Using the definitions of Ω_u, Ω_b, Ψ_u, Ψ_b in Section 2, Then

$$\begin{aligned} C_{y2,y2}(n,T) =& \frac{1}{T}\sqrt{P_{y_2}^a P_{y_2}^s}\int_0^T \widetilde{Y}_2(t,n)\cos(2\pi\Omega_u t + \Psi_u)\mathrm{d}t \\ &+ \frac{1}{T}\sqrt{P_{y_2}^a P_{y_2}^s}\int_0^T \widetilde{Y}_2(t,n)\cos(2\pi\Omega_b t + \Psi_b)\mathrm{d}t \end{aligned} \tag{28}$$

Define

$$\begin{aligned} C_{y2,y2}^+(n,T) &= \frac{1}{T}\int_0^T \widetilde{Y}_2(t,n)\cos(2\pi\Omega_u t + \Psi_u)\mathrm{d}t \\ C_{y2,y2}^-(n,T) &= \frac{1}{T}\int_0^T \widetilde{Y}_2(t,n)\cos(2\pi\Omega_s t + \Psi_s)\mathrm{d}t \end{aligned}$$

Write $C_{y2,y2}^+(\tau,T)$ and $C_{y2,y2}^-(\tau,T)$ in the complex form:

$$\begin{aligned} C_{y2,y2}^+(n,T) &= Re\left\{e^{j\Psi_u}\frac{1}{T}\int_0^T Y_{D2}(t)Y_{D2}(t-nT_c)e^{j2\pi\Omega_u t}\mathrm{d}t\right\} \\ C_{y2,y2}^-(n,T) &= Re\left\{e^{j\Psi_s}\frac{1}{T}\int_0^T Y_{D2}(t)Y_{D2}(t-nT_c)e^{j2\pi\Omega_s t}\mathrm{d}t\right\} \end{aligned}$$

According to [12], the expectations of $C_{y2,y2}^+(n,T)$ and $C_{y2,y2}^-(n,T)$ are

$$E\left\{C_{y2,y2}^+(n,T)\right\} = \overline{R}_{Y_2}(n,T)E\left\{Re\left\{e^{j(\pi\Omega_u T+\Psi_u)}\mathrm{sinc}(\pi\Omega_u T)\right\}\right\} \tag{29}$$

and

$$E\left\{C_{y2,y2}^-(n,T)\right\} = \overline{R}_{Y_2}(n,T)E\left\{Re\left\{e^{j(\pi\Omega_b T+\Psi_b)}\mathrm{sinc}(\pi\Omega_b T)\right\}\right\} \tag{30}$$

where

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

is the expectation (average) of the auto-correlation function of random selected a slice of the P(Y) sequence and $Re(.)$ is the operation to get the real part of a complex number . In (29) (30), we used the property that the random P(Y) sequence and random variables Ψ_u, Ψ_b are independent.

For the ideal white noise sequence,

$$\overline{R}_{Y}(n,T) = \begin{cases} 1 & \text{if } n=0 \\ 0 & \text{otherwise} \end{cases} \tag{31}$$

Equation (29)(30) are zeros when $n \neq 0$. When $n = 0$, using (4), Ψ_u and Ψ_b are

$$\begin{aligned} \Psi_u &= \Delta\theta_{21}^a - \delta\phi_1^a + \Delta\theta_{21}^s - \delta\phi_1^s \\ \Psi_b &= \Delta\theta_{21}^a - \delta\phi_1^a - \Delta\theta_{21}^s + \delta\phi_1^s \end{aligned} \tag{32}$$

Equation (32) is the phase tracking error. It can be treated as zero mean random variable with even probability distribution. That means $E[\sin(\Psi_u)] = 0$ and $E[\sin(\Psi_b)] = 0$. Then we can obtain

$$\begin{aligned} E[\cos(\Omega_u T + \Psi_u)] &= \cos(\Omega_u T)E(\Psi_u) \\ E[\cos(\Omega_b T + \Psi_b)] &= \cos(\Omega_b T)E(\Psi_b) \end{aligned} \tag{33}$$

Submitting (33), (31), (29) and (30) into (28), we obtain

$$E\{C_{y2,y2}(n,T)\} = \begin{cases} \frac{1}{T}\sqrt{P_{y2}^a P_{y2}^s}\left[\frac{\sin(2\pi\Omega_u T)}{\pi\Omega_u T} + \frac{\sin(2\pi\Omega_b T)}{\pi\Omega_b T}\right] E[\cos(\Psi_u)] & \text{if } n=0 \\ 0 & \text{otherwise} \end{cases} \tag{34}$$

Using the definition of $\mathrm{sinc}(x)$ in Section 2, we obtain(3) in Section 2.

B Derivation of Equation (16)

The purpose of this appendix is to provide the detailed derivation of the equation used to calculate the supplicant's position. This is (16) in Section 4. Starting with (14), we note that we have a system of equations with three unknowns. The three unknown variables (x_s, y_s, z_s) can be solved by using three equations.

When we solve (14), the only available values for the right sides are measurements with noise. The true value (x_s, y_s, z_s) is impossibly obtained from the solution of the equations. The solution is an estimate of the true value.

Let the noise of ρ_i^a is $\delta\rho_i^a$, the noise of t_{i1} is δt_{i1}, the atmospheric delay noise is χ_{i1}, the coordinate noise in ECEF is $(\delta x, \delta y, \delta z)$. The measurements are

$$\begin{aligned}
\hat{\rho}_i^a &= \rho_i^a + \delta\rho_i^a \\
\hat{t}_{i1} &= t_{i1} + \delta t_{i1} \\
\hat{\chi}_{i1} &= \chi_{i1} + \delta\chi_{i1} \\
\hat{x}_i &= x_i + \delta x_i \\
\hat{y}_i &= y_i + \delta y_i \\
\hat{z}_i &= z_i + \delta z_i
\end{aligned} \tag{35}$$

The estimate of the solution of (14) is $\hat{\mathbf{r}}_s(\hat{x}_s, \hat{y}_s, \hat{z}_s)$ which is obtain through the equation below

$$\begin{aligned}
\hat{\rho}_2^s - \hat{\rho}_1^s &= \hat{\rho}_2^a - \hat{\rho}_1^a - c\hat{t}_{21} + c\hat{\chi}_{21} \\
\hat{\rho}_3^s - \hat{\rho}_1^s &= \hat{\rho}_3^a - \hat{\rho}_1^a - c\hat{t}_{31} + c\hat{\chi}_{31} \\
\hat{\rho}_4^s - \hat{\rho}_1^s &= \hat{\rho}_4^a - \hat{\rho}_1^a - c\hat{t}_{41} + c\hat{\chi}_{41}
\end{aligned} \tag{36}$$

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 $i = 1, 2, 3, 4$.

Either the closed-form solution or the recursive solution using linearization [9] can be used to solve (36).

The error of the $\hat{\mathbf{r}}_s(\hat{x}_s, \hat{y}_s, \hat{z}_s)$ is caused by measurements errors. We are interested to find how the measurements errors propagates to the solution error. In (14), the left side, $\rho_i^s - \rho_1^s$, can be approximated using the Taylor series around the estimated value $\hat{\mathbf{r}}_s(\hat{x}_s, \hat{y}_s, \hat{z}_s)$ and measurements, $\hat{\mathbf{r}}_i(\hat{x}_i, \hat{y}_i, \hat{z}_i)$. For satellite $i = 2, 3, 4$,

$$\begin{aligned}
\rho_i^s - \rho_1^s = \hat{\rho}_i^s - \hat{\rho}_1^s
&- \left(\left.\frac{\partial \rho_i^s}{\partial x_s}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} - \left.\frac{\partial \rho_1^s}{\partial x_s}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \right) \delta x_s \\
&- \left(\left.\frac{\partial \rho_i^s}{\partial y_s}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} - \left.\frac{\partial \rho_1^s}{\partial y_s}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \right) \delta y_s \\
&- \left(\left.\frac{\partial \rho_i^s}{\partial z_s}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} - \left.\frac{\partial \rho_1^s}{\partial z_s}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \right) \delta z_s \\
&- \left.\frac{\partial \rho_i^s}{\partial x_i}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta x_i - \left.\frac{\partial \rho_i^s}{\partial y_i}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta y_i \\
&- \left.\frac{\partial \rho_i^s}{\partial z_i}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta z_i + \left.\frac{\partial \rho_1^s}{\partial x_1}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta x_1 \\
&+ \left.\frac{\partial \rho_1^s}{\partial y_1}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta y_1 + \left.\frac{\partial \rho_1^s}{\partial z_1}\right|_{(\hat{\mathbf{r}}_s, \hat{\mathbf{r}}_i, \hat{\mathbf{r}}_1)} \delta z_1 \\
&+ \mathcal{O}(\mathbf{r}^2)
\end{aligned} \tag{37}$$

where $\mathcal{O}(\mathbf{r}^2)$ is the high order terms. Because $\rho_i^s - \rho_1^s$ is expended using $\mathbf{r} = \hat{\mathbf{r}} - \delta\mathbf{r}$ defined in (35) rather than $\mathbf{r} = \hat{\mathbf{r}} + \delta\mathbf{r}$ as usual, the signs in all the error terms are different from the usual Taylor series.

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 ith 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 error vector as

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

the satellite position error vector as

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

Ignoring the higher order item in (37), the equation can be rewritten as

$$\rho_i^s - \rho_1^s = \hat{\rho}_i^s - \hat{\rho}_1^s + \left[\hat{\mathbf{e}}_i - \hat{\mathbf{e}}_1\right]^T \delta\mathbf{r}_s - \hat{\mathbf{e}}_i^T \delta\mathbf{r}_i + \hat{\mathbf{e}}_1^T \delta\mathbf{r}_1 \tag{38}$$

Substituting (14) (35) (36) into (38), we get

$$\left[\hat{\mathbf{e}}_i - \hat{\mathbf{e}}_1\right]^T \delta\mathbf{r}_s = \hat{\mathbf{e}}_i^T \delta\mathbf{r}_i - \hat{\mathbf{e}}_1^T \delta\mathbf{r}_1 - \delta\rho_i^a + \delta\rho_1^a + c\delta t_{i1} - c\delta\chi_{i1} \tag{39}$$

Using the definition of matrix $\mathbf{A}$, the measurement error vector $\delta\mathbf{m}$ in section 4, we obtain (16).

C Authenticator Hardware Description

In this appendix is a manual of sorts which describes two prototype receivers built to test the authentication algorithm and used in the validation experiments described earlier. In what follows, we first provide a description of the hardware and software developed as part of these prototypes.

D System Description

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 (12)) 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.

The authenticator designed for this work shown in Figure 20 and Figure 21 satisfies the above requirements. This authenticator integrates the RF front end and IF signal sampling. The authenticator is directly connected to the 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. A block diagram of the authenticator is shown in Figure 20.

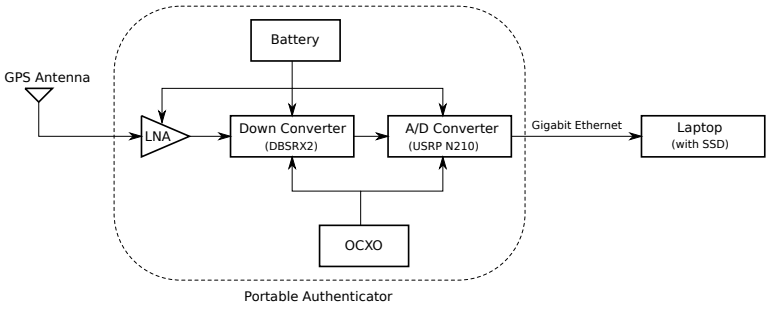

Figure 20: Schematic diagram of the authenticator receiver

Figure 21: Authenticator

The IF signal processing unit in the authenticator is based on USRP N210 software defined radio [1][4]. It offers the function of down converting, digitalization 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 [7] 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 20, the prototype receiver consists of one GPS antenna, two low noise amplifiers(LNA), one USRP2 [4] 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 [1] 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 [3]. 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 data processing. 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.

The next parts include detail structure analysis of analog and digital part based on the components data sheets and the source code.

D.1 Analog Signal Processing

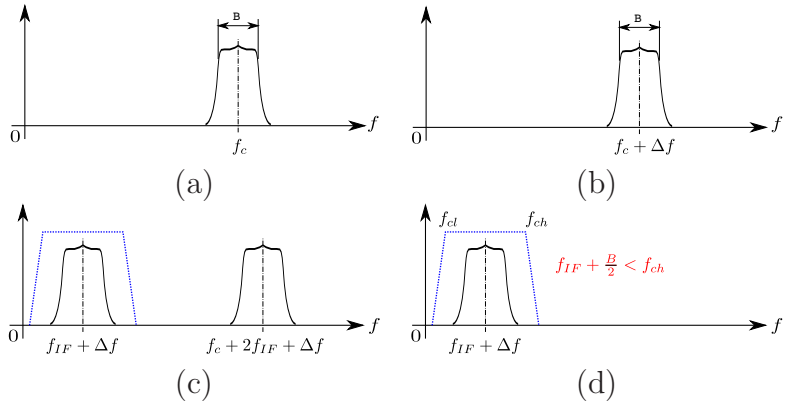

Figure 22: Spectrum change in the I/Q demodulator

Figure 22 lists the spectrum change before the output of the DBSRX board. Figure 22 (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 22 (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. This amplifiers ensure the signal has proper power level. After the mixers the spectrum of the signals are shown in 22 (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 22 (d) is the result signal spectrum at the output of the DBSRX board. In 22 (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 22 (d) is the 800Hz corner frequency of the high pass filter explained earlier.

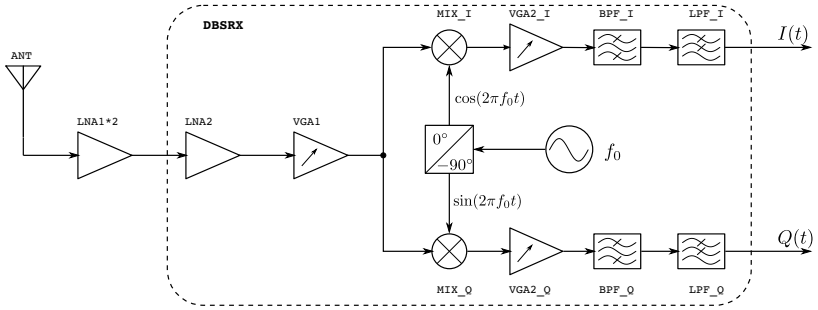

Figure 23: Analog signal processing diagram

Figure 23 shows the detail of the analog signal processing. The signal strength at the receiver's antenna is very weak (about -160dBm). It need 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 24.

The signal powers at different points are shown in Figure 25. By using two LNAs, the total noise figure of the analog part is only 2.2 dB which is dominated by the antenna. This

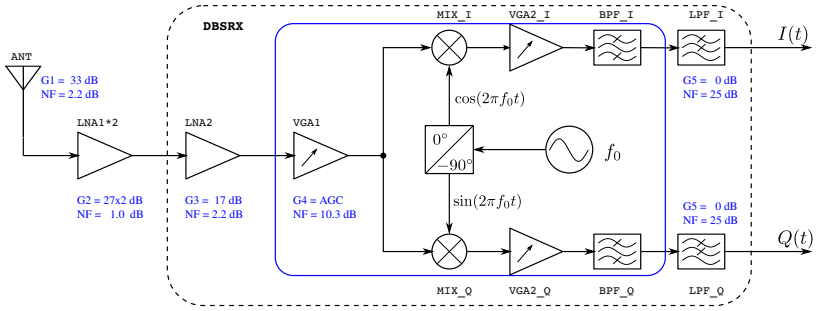

Figure 24: Gain assignment of the receiver

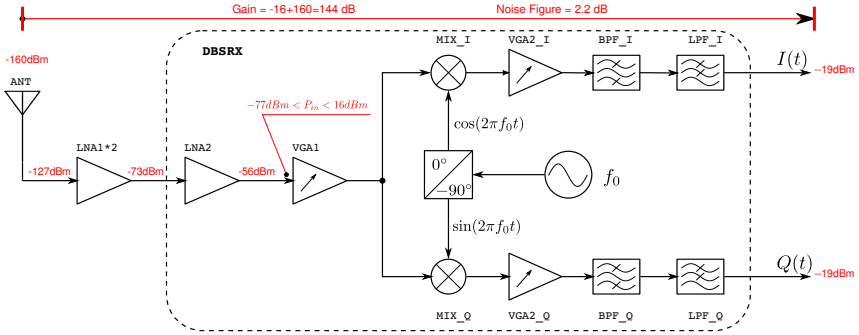

Figure 25: Signal power of the receiver

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 26 shows the mathematical signal expression of the analog processing part. The choice of the f_{IF} value will be explained in the later part.

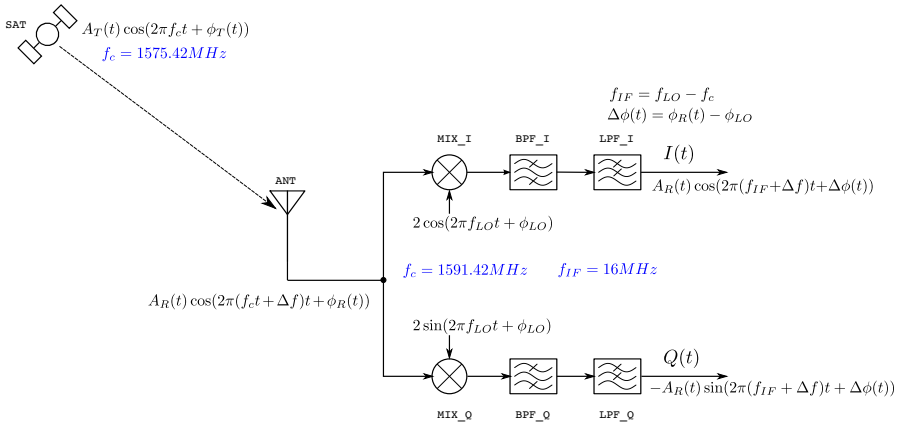

Figure 26: Mathematical signal expression of the analog part

D.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 is shown in

Figure 27. 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.

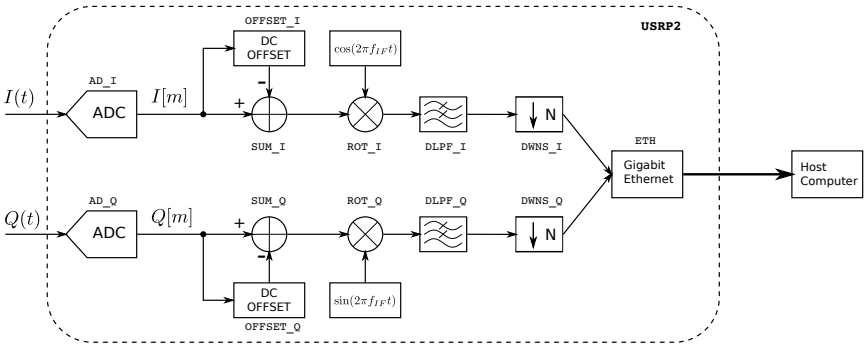

Figure 27: Digital signal processing diagram

The core in the DDC is a CORDIC (COordinate Rotation DIgital Computer) unit. The function of the CORDIC is shown in Figure 28. 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.

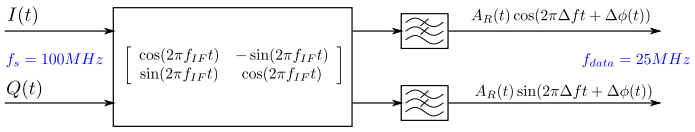

Figure 28: Mathematical expression of the digital signal processing

D.3 f_{IF} Selection

If the f_{IF} in Figure 22 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 22(d),

$$f_{IF} + \frac{B}{2} < f_{ch} \tag{40}$$

need to be satisfied to make sure the whole useful signal is not filtered out by the low pass filter. Figure 29 shows the sampling effect of the $Q(t)$ and $I(t)$ signal.

To avoid the overlapping, the condition in Equation (41) need to be satisfied.

$$\begin{aligned} B &< 2f_{IF} \\ B + 2f_{IF} &< f_s \end{aligned} \tag{41}$$

In this system f_s=100 MHz,B=25 MHz,f_{ch} =33MHz. Based on Equation (40) and (41) we can choose f_{IF}=16MHz.

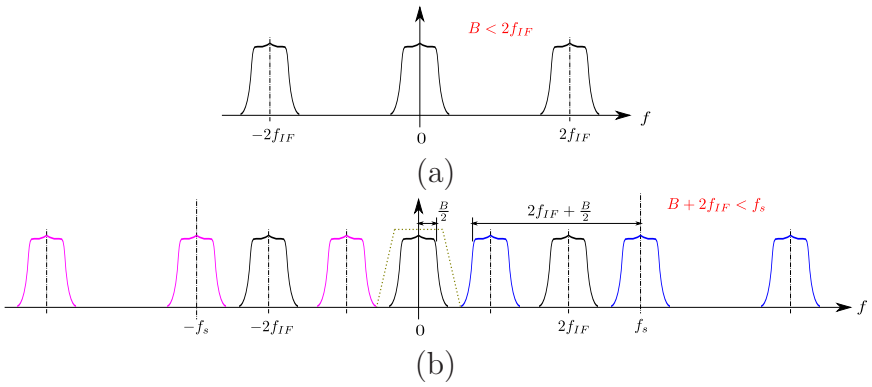

Figure 29: Spectrun chenge caused by sampling

D.4 Devices and Components

Most of the components and devices are purchased from commercial vendors as listed in Table 4. Figure 30 is a picture of these devices.

	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: Device list

References

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

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

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

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

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

[6] 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.

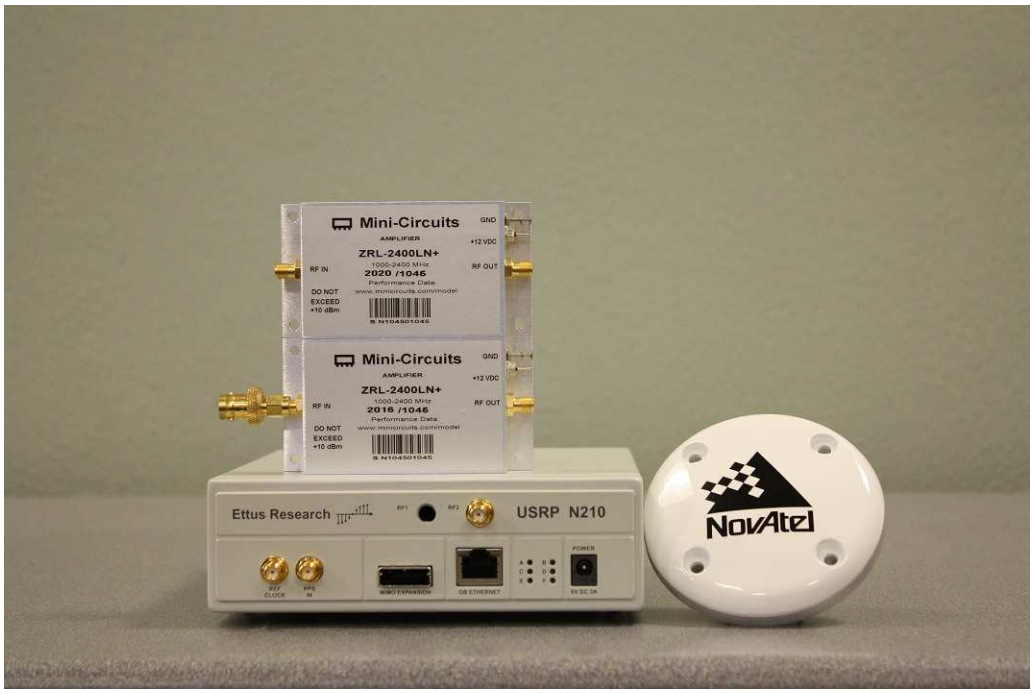

Figure 30: Photograph of Key Components of the GPS Authenticator

[7] 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.

[8] 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.

[9] Elliott D. Kaplan, Joseph L. Leva, Dennis Milbert, and Mike S. Pavloff. Fundamentals of satellite navigation. In Elliott D. Kaplan and Christopher J. Hegarty, editors, *Understanding GPS:principles and applications*, chapter 2, page 55. Artech House, Inc, Norwood, MA, second edition, 2006.

[10] 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.

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

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

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