Estimation of ICAO Threat Model Parameters For Operational GPS Satellites

Alexander M. Mitelman, Dennis M. Akos, Samuel P. Pullen, Per K. Enge, *Stanford University*

BIOGRAPHY

Alexander Mitelman is a Ph.D. candidate in the Department of Electrical Engineering at Stanford University. As a member of the GPS Laboratory, his research is focused on local area differential GPS design, signal analysis, and applications. Mr. Mitelman received his S.B. in Electrical Engineering from the Massachusetts Institute of Technology in 1993 and his M.S. in Electrical Engineering from Stanford University in 1995.

Dr. Dennis M. Akos completed the Ph.D. degree in Electrical Engineering at Ohio University within the Avionics Engineering Center. He has since served as a faculty member with Luleå Technical University, Sweden, and is currently a Research Associate with the GPS Laboratory at Stanford University.

Dr. Sam Pullen received his Ph.D. in Aeronautics and Astronautics from Stanford University in 1996. Since graduating, Dr. Pullen has served as Research Associate and as Technical Manager at Stanford, where he has supported GPS Local Area Augmentation System (LAAS) and Wide Area Augmentation System (WAAS) research and development and is now the LAAS project leader. His work in these fields and his support of the Johns Hopkins University Applied Physics Laboratory (JHU/APL) GPS Risk Assessment earned him the ION Early Achievement Award in 1999.

Dr. Per Enge is a Professor of Aeronautics and Astronautics at Stanford University. He received his B.S. in Electrical Engineering from the University of Massachusetts at Amherst in 1975, and his M.S. and Ph.D., both in Electrical Engineering, from the University of Illinois at Urbana-Champaign in 1979 and 1983. Professor Enge's research focuses on the design of navigation systems which satisfy stringent requirements with respect to accuracy, integrity (truthfulness), time availability, and continuity.

ABSTRACT

The ICAO Second Order Step threat model defines a class of signal deformations that present a potential integrity threat to GPS-based aircraft landing systems such as the Local Area Augmentation System (LAAS). The Signal Quality Monitoring (SQM) component of LAAS must have its detection thresholds set at a level which ensures both the required level of safety in the presence of such deformations (integrity) and uninterrupted service under nominal conditions (continuity).

The determination and validation of appropriate SQM thresholds requires a detailed understanding of nominal GPS constellation performance. This paper explores the measured performance of healthy satellites in the context of the ICAO threat model. By making direct measurements of the waveforms in the time domain (as opposed to the correlation domain, as is done in conventional receivers), we demonstrate consistent trends among satellites in Block II-A and Block II-R, and overbound all measured satellite signals with waveforms from the ICAO model threat space.

INTRODUCTION

A key component of the Local Area Augmentation System (LAAS) is the Signal Quality Monitor (SQM). This system component is tasked with identifying satellites whose signals are sufficiently deformed to cause hazardously misleading information (HMI) to be provided to airborne users. At the same time, the SQM must not be so sensitive to minor, non-hazardous signal deformations – such as those caused by receiver thermal noise, small atmospheric variations, and so on – as to impair the usefulness of the overall landing system due to frequent disruptions of service. Detailed, quantitative specifications for LAAS integrity and continuity are provided in [1].

The ability to correctly identify HMI while simultaneously providing adequate continuity is strongly dependent on the detection thresholds in a given SQM. In order to provide a quantitative framework for this aspect of SQM analysis, and also to place reasonable bounds on the (otherwise arbitrarily large) space of possible signal deformations, the International Civil Aviation Organization (ICAO) adopted the Second-Order Step (2OS) threat model. This model mathematically describes a class of signal anomalies in the time domain using three simple parameters, and defines a threat space over which any candidate SQM must meet the competing requirements for integrity and continuity. The model itself, along with some historical context and motivation, is described in [2].

Direct testing for 2OS waveforms in the time domain is challenging because a conventional GPS antenna, even one with a significantly directional radiation pattern such as the Multipath Limiting Antenna (MLA) [3][4], still does not have enough gain to bring the raw GPS waveform above the ambient noise floor. This is simply a consequence of the fact that such an antenna must be able to see an appreciable portion of the celestial sphere, which implies a relatively large beamwidth. For example, an antenna with a hemispherical pattern (3 dBic at zenith) yields a received C/A code signal whose peak spectral density is roughly 11.9 dB below the ambient noise floor under typical conditions [5]. As a result, conventional GPS receivers operate in the correlation domain and never see raw C/A code waveforms directly.

For the purposes of validating the ICAO model, however, it is useful to have a detailed picture of the C/A code signal in the time domain, before correlation. In this paper, we present a method for collecting and analyzing these raw GPS signals directly, and describe solutions to several problems that are specific to time domain processing. We then use this method to estimate ICAO Threat Model B (analog anomaly) parameters for several operational GPS satellites.

EXPERIMENTAL SETUP

This section contains a basic description of the equipment used to gather raw GPS data. All data were gathered during September, 2001, at Camp Parks Communications Annex in Dublin, CA. The receive chain consisted of a steerable, high-gain L-band antenna (18 m diameter, 45 dB gain), a low-loss waveguide, and a 50 dB low-noise amplifier. The equivalent noise temperature of the entire RF chain was approximately $150\,°\mathrm{K}$.

The output of the RF chain was fed into an Agilent 89600 Vector Signal Analyzer (VSA). The VSA performs down-conversion and synchronous in-phase and quadrature sampling, and has a signal bandwidth of 36 MHz. The resulting I and Q points were generated at a nominal sample rate of 46.08 MHz each and fed into Matlab for post-processing.

ANALYSIS OF EXPERIMENTAL ERRORS

This section provides a mathematical description of the data collection process and the most significant error sources involved. In particular, we describe the relationship between the various errors due to Doppler shift, local oscillator (LO) and sampling clock errors on the VSA, and the residual frequency error exhibited by raw data prior to post-processing.

In general, raw GPS signals received by a terrestrial user include errors due to the receiver's clock and Doppler shift. In the case of a conventional antenna/receiver, these errors are largely corrected by normal GPS processing, and are invisible to the user. Data gathered with the experimental setup described above, however, still contain these errors because the "receiver" in this case is a blind, non-GPS-aware downconverter. It is therefore necessary to remove these errors in post-processing.

Viewed mathematically, the GPS signal has two main components, the coarse acquisition signal, $C(t)$, and the precise signal, $P(t)$. These signals are nominally modulated in quadrature onto a carrier at $f_{L_1} = 1575.42\,\mathrm{MHz}$ to form the signal transmitted by a GPS satellite:

$$G_\mathrm{t}(t) = C(t)\cos(2\pi f_{L_1}t) + P(t)\sin(2\pi f_{L_1}t) \qquad (1)$$

where we have ignored the 50 Hz navigation data signal for simplicity. It does not affect the rest of this analysis.

The received GPS signal is stretched or compressed in time as a function of Doppler shift. Defining the quantity $k_d = 1 - f_\mathrm{Dop}/f_{L_1}$, we can rewrite equation (1) to describe the signal received by a stationary antenna on the ground as

$$
\begin{aligned}
G_\mathrm{r}(t) \;=\; & C(t/k_d)\cos(2\pi f_{L_1}t/k_d) + \\
& P(t/k_d)\sin(2\pi f_{L_1}t/k_d)
\end{aligned}
\qquad (2)
$$

and this is the signal that arrives at the RF input of the VSA. For completeness, we will keep both C/A code and P code in the derivation initially, although the balance of this analysis concerns the C/A code only.

The analyzer contains an internal 10 MHz oven-controlled crystal oscillator (OCXO) frequency reference from which the LO and sampling clocks are generated using a pair of fractional-M/N synthesizers. This implies that any errors in the two clocks are related by a fixed, rational number (the ratio of the two synthesizer coefficients), which is computed below.

For convenience, we will assume that the analyzer's true LO frequency differs from f_{L_1} by some fixed amount f_{VSA}, and that its phase with respect to the carrier of the incoming signal is ϕ. Defining the quantity $k_v = 1 - f_{\text{VSA}}/f_{L_1}$ to be consistent with earlier notation, the mixdown term can then be written in complex form as

$$
\begin{aligned}
L_{\text{c}}(t) &= \exp(j(2\pi(f_{L_1} + f_{\text{VSA}})t + \phi)) \\
&\approx \exp(j(2\pi f_{L_1} t/k_v + \phi)) \quad\quad (3)
\end{aligned}
$$

where we have made the approximation $1 + x \approx 1/(1 - x)$ for small values of x. (For the 89600 VSA, the quantity f_{VSA}/f_{L_1} is on the order of 2×10^{-7} or smaller.) Finally, the sampling clock that drives the ADC can be described as

$$
s(t) = \sum_{n=-\infty}^{\infty} \delta(t - nT_s) = \frac{1}{T_s}\text{III}(t/T_s) \quad\quad (4)
$$

where the actual sampling period is numerically related to the LO clock error by

$$
T_s = \frac{1}{f_s} = \frac{M}{f_{L_1} + f_{\text{VSA}}} \approx \frac{M k_v}{f_{L_1}} \quad\quad (5)
$$

and M is a rational number representing the ratio of the two fractional synthesizer coefficients. In our setup, the nominal frequency span is 36 MHz and $M = 1575.42\,\text{MHz}/(1.28 \cdot 36\,\text{MHz}) = 26257/768$ exactly.

Combining equations (1)-(3) yields an expression describing the initial continuous-time downconversion to (almost) DC. Expanding the exponential, applying trigonometric identities for the products of sinusoids, discarding the terms containing $2\pi f_{L_1}(1/k_d + 1/k_v)$ to account for anti-alias filtering, and defining $f_x = f_{L_1}(1/k_d - 1/k_v)$ for compactness yields

$$
\begin{aligned}
G_{\text{d}}(t) &= G_{\text{r}}(t)L_{\text{c}}(t) \\
&= \frac{1}{2}\left[C(t/k_d)\cos(2\pi f_x t - \phi) + \right.\\
&\qquad \left. P(t/k_d)\sin(2\pi f_x t - \phi)\right] - \\
&\quad \frac{j}{2}\left[C(t/k_d)\sin(2\pi f_x t - \phi) - \right.\\
&\qquad \left. P(t/k_d)\cos(2\pi f_x t - \phi)\right] \quad\quad (6)
\end{aligned}
$$

as a continuous-time (complex) representation of the downconverted signal.

Strictly speaking, the VSA actually performs a two-step downconversion slightly different from the process described above. Specifically, the first mixdown and filtering step occurs in the continuous-time domain, resulting in a signal spectrum centered at an intermediate frequency (IF) of 70 MHz. The remainder of the downconversion is performed by sampling the IF signal at 92.16 MHz, which effectively aliases the spectrum to baseband. (The sampling rate, though less than twice the IF center frequency, nonetheless satisfies the Nyquist sampling criterion

because the IF signal is bandlimited to 36 MHz by filtering.) This downconversion technique, known as *bandpass sampling*, is discussed in [6]. For simplicity, however, we model all the continuous-time operations first and account for the sampling in the last step of this derivation. Because each step represents a linear operation, changing the order of the steps does not affect the end result.

Equation (6) suggests that the raw measurements should exhibit both phase error and residual frequency modulation. This is consistent with the plots of the raw (uncorrected) data shown in Figures 1 and 3. Ordinarily, a Costas loop or some other automated processing would be used to correct for these errors, particularly with long data sets. The loop would also need to be modified to output its best frequency estimate over the length of the data set, because these values are required to perform the averaging step described in the next section. In this experiment, however, the data snapshots are only 100 msec long, so the errors are essentially constant throughout the length of the sets. Thus the process of removing the errors can simply be done manually. We now consider these errors one at a time.

The phase error is relatively simple to remove, for two reasons. First, the error is fixed throughout the entire data set; that is, in the absence of any residual frequency error, the phase relationship between the I and Q channels remains constant throughout the data set. Second, the phase term can be estimated without knowing the frequency term if we look near the very beginning of the data, where $\exp(-j(2\pi f t + \phi)) \approx \exp(-j\phi)$ for very small values of t. A plot of raw I and Q samples, shown in Figure 1, exhibits this non-zero initial phase error even for very small values of t. (The non-zero residual frequency modulation, on the other hand, is not visible in this plot because the accumulation of phase is negligible over this small time span.)

To estimate the phase term, the raw complex data in Figure 1 are multiplied by $\exp(-j\phi)$, where ϕ is varied until the C/A code and P code appear cleanly split between the I and Q channels at the very beginning of the data set. The results of this phase correction are shown in Figure 2.

Next we consider the residual frequency modulation. Although the phase correction in the preceding step ensures a clean C/A code on the in-phase channel at the start of the data set, the phase error resurfaces if we look at a sufficiently long chunk of data, as shown in Figure 3 (only the C/A code is plotted).

This error is removed by multiplying the phase-corrected data by a complex spectral shift term of the form $\exp(j2\pi(-f_{\text{res}})t)$. As with the phase correction, the parameter f_{res} is varied manually until the clean split in the first step remains throughout the entire length of the data
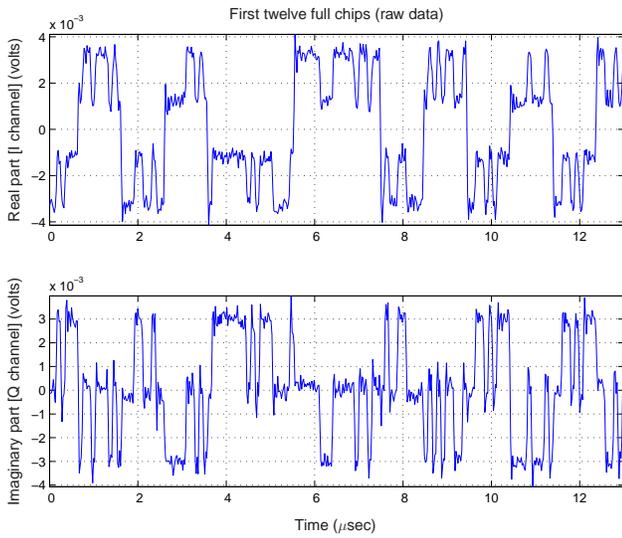
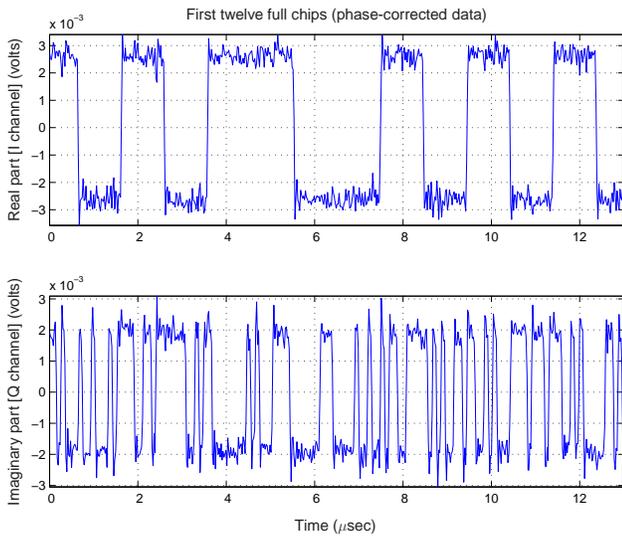**Figure 1:** Raw (uncorrected) data

Figure 2: Phase-corrected data

set. This removes any residual modulation (which occurs due to the cumulative, but initially uncorrected, effects of Doppler shift and errors in LO frequency). The results of this process are shown in Figure 4.

Mathematically, the real part of the resulting signal is the I channel:

$$
\begin{aligned}
I(t) &= \mathrm{Re}[G_d(t)e^{j2\pi(-f_{\mathrm{res}})t}] \\
&= \tfrac{1}{2}C(t/k_d)\cos(2\pi(f_x + f_{\mathrm{res}})t) + \\
&\quad \tfrac{1}{2}P(t/k_d)\sin(2\pi(f_x + f_{\mathrm{res}})t) \qquad (7)
\end{aligned}
$$

and the imaginary part is the Q channel:

$$
Q(t) = \mathrm{Im}[G_d(t)e^{j2\pi(-f_{\mathrm{res}})t}]
$$

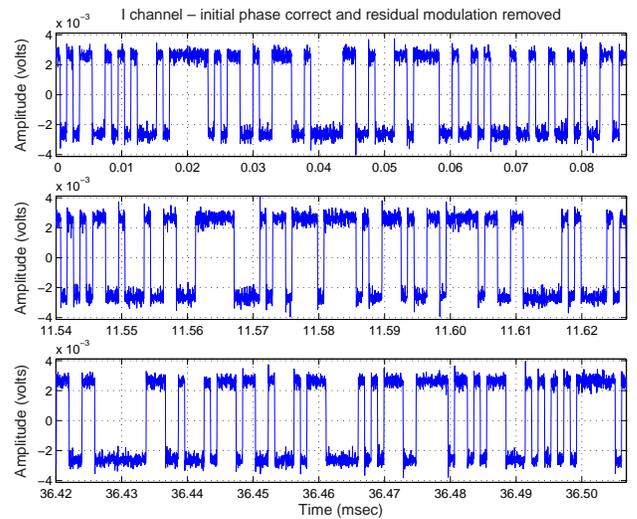**Figure 3:** Non-zero residual modulation

Figure 4: Residual modulation removed

$$
\begin{aligned}
&= -\tfrac{1}{2}C(t/k_d)\sin(2\pi(f_x + f_{\mathrm{res}})t) + \\
&\quad \tfrac{1}{2}P(t/k_d)\cos(2\pi(f_x + f_{\mathrm{res}})t) \qquad (8)
\end{aligned}
$$

The process described above is equivalent to setting the residual frequency term so that

$$
f_{\mathrm{res}} = -f_x = f_{\mathrm{VSA}} - f_{\mathrm{Dop}} \qquad (9)
$$

which gives $I(t) = \tfrac{1}{2}C(t/k_d)$ and $Q(t) = \tfrac{1}{2}P(t/k_d)$. In other words, determining f_{res} in this way results in pure C/A code on the I channel and pure P code on the Q channel, with no residual modulation. This mathematical result is reflected in the error-corrected data shown in Figure 4. It is also worth noting that the two components of the residual frequency term appear in equation (9) as an algebraic sum (difference), implying that the two effects – LO error

on the VSA and non-zero Doppler on the satellite signal – are *indistinguishable* in the continuous-time domain.

Finally, we come to the sampling step described in equations (4) and (5). First, we note that for an arbitrary periodic function $x(t)$ with a period T_x, the function $x(t/a)$ has a period aT_x. Thus the downconverted C/A code on the I channel, $C(t/k_d)$, has an epoch period of $T_e = (1 \text{ msec})k_d$ and a chipping interval (or quasi-period, since the code is pseudorandom) of $T_c = (1 \text{ msec}/1023)k_d = T_e/1023$. Assuming f_{res} has been determined as described in equation (9), the number of points per epoch is simply the ratio of the actual epoch and sample periods:

$$
\begin{aligned}
N_e &= \frac{T_e}{T_s} \\
&= \frac{(1 \text{ msec})(1 - f_{\text{Dop}}/f_{L_1})f_{L_1}}{(M)(1 - f_{\text{VSA}}/f_{L_1})} \\
&\approx (\frac{1 \text{ msec}}{M})(1 - \frac{f_{\text{Dop}}}{f_{L_1}})(1 + \frac{f_{\text{VSA}}}{f_{L_1}})f_{L_1} \\
&\approx (\frac{1 \text{ msec}}{M})(1 + \frac{f_{\text{VSA}} - f_{\text{Dop}}}{f_{L_1}})f_{L_1} \\
&= (\frac{1 \text{ msec}}{M})(f_{L_1} + f_{\text{res}}) \\
&= 46080 + \frac{(1 \text{ msec})f_{\text{res}}}{M} \qquad (10)
\end{aligned}
$$

where we have again used the approximation $1/(1 - x) \approx 1 + x$ for small values of x and discarded the second-order term in the fourth line. Similarly, the number of points per chip is $N_c = N_e/1023$.

This result indicates that the errors due to satellite Doppler shift and VSA sampling clock error are lumped together, just as in the residual frequency modulation term described in equation (9). Thus the two effects are numerically *indistinguishable* in the discrete-time post-processing step as well.

DATA AVERAGING

Regardless of the signal-to-noise ratio provided by the receiving antenna, raw satellite data will invariably contain some amount of noise. This effect can be reduced by averaging over multiple C/A code epochs, taking advantage of the periodicity of the signal to preserve detail. The exact amount of averaging required depends on several system-specific parameters, including antenna gain and system noise figure.

In order to perform this noise reduction without also averaging (or "blurring") the underlying features in the waveform, the data must be resampled to ensure an integral number of samples per epoch (or even per chip). Since the features in question may be quite small in the case of

nominally healthy satellites – perhaps close to the limits of the VSA's accuracy – this averaging must be performed as accurately as possible, including compensation for local clock errors and Doppler.

Fortunately, the analysis in the previous section indicates that the frequency error found in the raw data, f_{res}, neatly encapsulates all the information necessary to perform the resampling correctly. The desired downsampling ratio is

$$
R = \frac{46080 + \lfloor (1 \text{ msec})f_{\text{res}}/M \rfloor}{46080 + (1 \text{ msec})f_{\text{res}}/M}
$$

and yields an integral number of points per epoch. This ratio is plotted as a function of f_{res} in Figure 5. It is worth
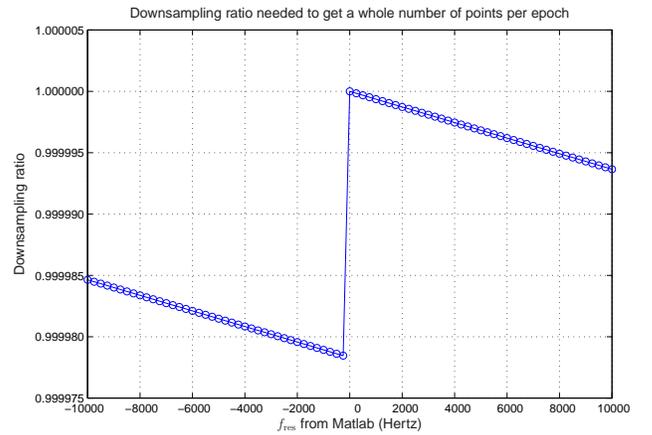

Figure 5: Downsampling ratio versus f_{res}

noting that although R is very close to unity, the error incurred by neglecting the resampling step can be significant. For example, if resampling is ignored for a 100 msec data set with $f_{\text{res}} = 2$ kHz, the first sample point in each C/A code epoch drifts by approximately 127 nsec (one-eighth of a chip) with respect to start of the underlying epoch over the length of the data set. This is more than enough to obscure fine detail in the averaged waveform. The benefit of careful resampling is illustrated in Figure 6. The significant blurring at the C/A code symbol edges on the top trace suggests that fine detail just after those edges will be lost if the resampling is not performed.

With the data properly resampled, it is possible to average together multiple epochs (accounting for any navigation bit flips that occur within the set) without significantly distorting the underlying C/A code waveform. The application of this averaging strategy to experimental data is demonstrated in the next section.
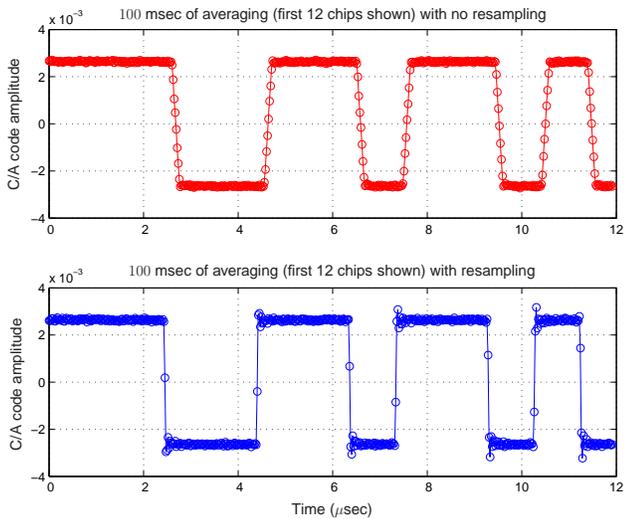
Figure 6: Effects of resampling ($f_{\text{res}} = -2533.2$ Hz)

EXPERIMENTAL RESULTS

In this section, we apply the methods described above to data from several nominally healthy GPS satellites.

Figure 7 shows the noise-averaged C/A code edge transitions for several satellites from Blocks II-A and II-R, along with the step response of the VSA (measured with a 5 nsec edge input) for reference.
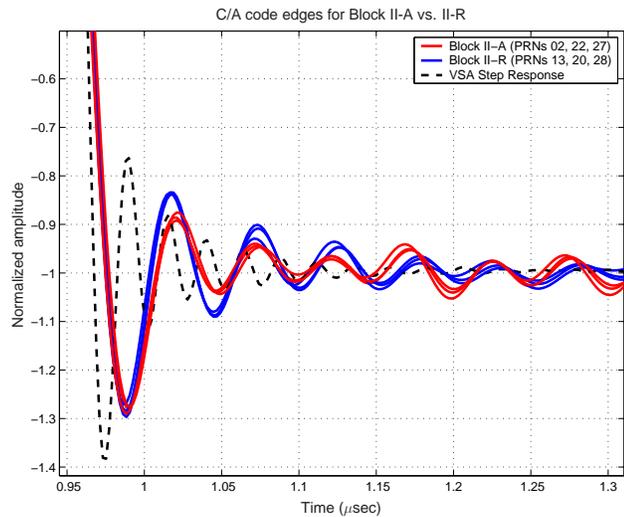

Figure 7: Healthy satellite C/A code edges (zoomed)

This plot suggests several observations. First, nominally healthy satellites really do exhibit a small amount of oscillatory ringing at the edges of the C/A code. This ringing is distinct from imperfections in the measurement setup, since the damped oscillation frequency is substantially dif-

ferent than that of the instrument's step response and the settling time is measurably longer. Second, the waveforms appear to be fairly consistent within a satellite block. Third, slight differences exist between Block II-A and II-R satellites: while the initial overshoot is approximately identical for both, the II-R waveforms appear to have a slightly larger amplitude on the next few oscillation cycles than their II-A counterparts, while their settling time appears to be shorter.

Finally, we consider the measured Block II-A and II-R signals in the context of the ICAO 2OS model. In general, there are three main transient characteristics to consider: ringing frequency, settling time, and maximum overshoot. Because this analysis specifically examines the analog failure mode (Threat Model B), however, only two degrees of freedom are available. In the case of a true two-pole system, this would be sufficient, since only two of these characteristics would be mathematically independent. One possible curve fit for the aggregate waveforms (II-A and II-R), chosen to best match the frequency of oscillation and settling time (first seven half-cycles), is shown in Figure 8.
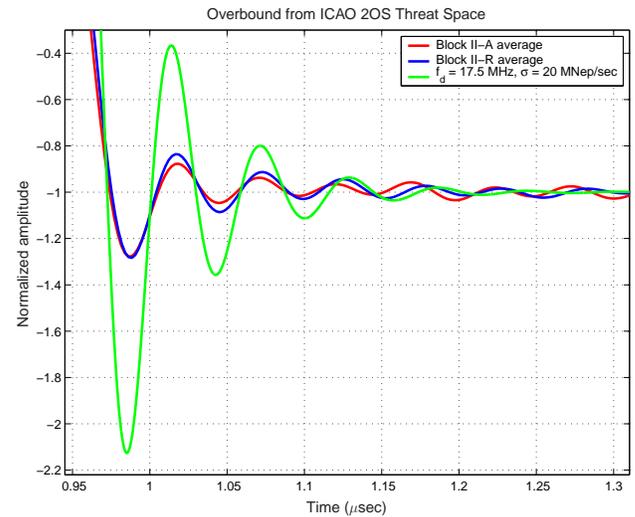

Figure 8: Approximate overbound from ICAO threat space

The proposed 2OS curve is clearly a fairly conservative overbound. This is to be expected, since the 2OS model implicitly assumes a single dominant failure mode; a healthy GPS satellite, on the other hand, is a highly complex system, so under nominal conditions it is not surprising that the waveforms require more than two poles to describe them.

Using the approach described in [7], contour plots for standard early-late and double-delta correlators are shown in Figures 9 and 10, respectively. These plots assume a ground reference station with 16 MHz front-end bandwidth and a tracking pair spacing of 0.1 chip. The allowable regions of operation for LAAS are enclosed by heavy black lines. From the plots, the worst-case undetected pseudor-
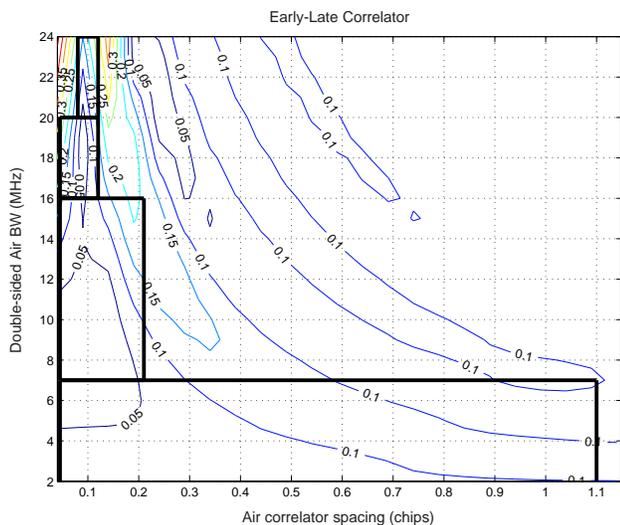
Figure 9: Worst-case pseudorange error (early-late)

ange error corresponding to the Threat Model B parameters proposed in Figure 8 ($f_d \approx 17.5$ MHz, $\sigma \approx 20$ MNep/sec) is approximately 33 cm for the standard early-late correlator configuration (for a user receiver with 20 MHz, 0.04 chips) and 18 cm for the double-delta configuration (for a user receiver with 7 MHz, 0.44 chips, and $\Delta_{\text{narrow}} = 0.44$).

For more typical airborne receiver designs, however, the error is much smaller. For example, a receiver with a 0.1 chip correlator spacing and 12 MHz front-end bandwidth experiences errors of approximately 4 cm and 10 cm, respectively, for the early-late and double-delta cases. Since the 2OS waveform is a conservative overbound, the real worst-case errors experienced by users due to the nominal deformations shown above will be smaller still.
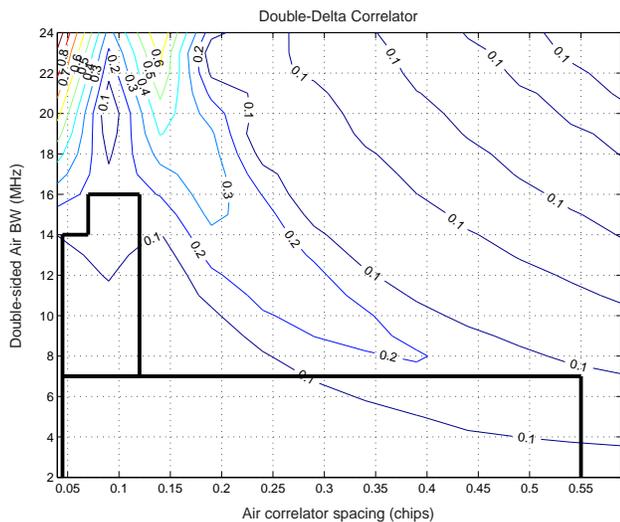

Figure 10: Worst-case pseudorange error (double-delta)

CONCLUSION

Gathering raw GPS data in the time domain is a useful tool in designing and evaluating SQM detection thresholds. Time averaging to reduce noise can significantly improve the ability to identify small artifacts in the data, but several corrections need to be applied to the data prior to averaging. Specifically, the phase error between the in-phase and quadrature components and any residual frequency modulation (due to local clock errors and satellite Doppler) must be identified and removed. This information must then be used to resample the data to an integral number of sample points per epoch. It is not necessary, however, to know either the exact Doppler shift, the precise LO frequency, or the precise sampling rate the time of measurement; all of these errors can be lumped together into a single quantity, to be identified in post-processing.

The overbounding of processed data from healthy satellites with waveforms from the ICAO 2OS threat space is conservative, because nominal satellite signals are more complex than what a simple two-pole model can describe. The resulting signal deformations and differential pseudorange errors are small enough that existing SQM thresholds do not need to be inflated significantly to account for nominal performance variations in Block II-A or II-R satellites.

Future work in this area will include exploration of Threat Model A (digital failure mode), which will leverage much of the work presented in this paper. It may also be possible to more accurately characterize the step response of the data-gathering equipment and to correct for it, explicitly, in post-processing.

ACKNOWLEDGMENTS

References

[1] *Specification: Performance Type One Local Area Augmentation System Ground Facility.* U.S. Federal Aviation Administration, Washington, D.C., FAA-E-2937A, April 17, 2002. (Retrieved on October 1, 2002, from http://gps.faa.gov/Library/Data/LAAS/LGF2937A.PDF)

[2] Enge, P., R. Phelts and A. Mitelman, "Detecting Anomalous Signals from GPS Satellites," Working Paper 19, Global Navigation Satellite System Panel meeting, Toulouse, France, October 18-29, 1999.

[3] Braasch, M., "Optimum Antenna Design for DGPS Ground Reference Stations," Proceedings of the Institute of Navigation ION GPS-94, Salt Lake City, UT, September 1994.

[4] Thornberg, D., *et. al.*, "The LAAS Integrated Multipath Limiting Antenna (IMLA)," Proceedings of the Institute of Navigation ION GPS-2002, Portland, OR, September 2002.

[5] Parkinson, B. and J. Spilker, Jr., eds. *Global Positioning System: Theory and Applications I,* Progress in Astronautics and Aeronautics, vol. 163, pp. 88-90, AIAA, Washington, D.C., 1996.

[6] Misra, P., and P. Enge, *Global Positioning System: Signals, Measurements, and Performance,* pp. 325-331, Ganga-Jamuna Press, Lincoln, MA, 2001.

[7] Phelts, R., *Multicorrelator Techniques For Robust Mitigation of Threats To GPS Signal Quality,* Ph.D. Thesis, Stanford University, Stanford, CA, 2001.