Impact of evil waveforms on GBAS performance

Christophe Macabiau, Eric Chatre

Impact of Evil Waveforms on GBAS Performance

Christophe MACABIAU, CNS Research Laboratory of the ENAC
Eric CHATRE, STNA

ABSTRACT

Several types of failures can occur in the GPS satellites that transmit the ranging signals to the users. Among them, a specific type of failure in the signal generation process aboard the satellite may result in an anomalous waveform being transmitted, called an 'evil waveform'. Evil waveforms are GPS signals that have a distorted PRN code modulation waveform. The main impact is a rupture of the symmetry of the cross-correlation peak inside the tracking channel, therefore inducing a different measurement error for two receivers that would not have the same loops architecture. As a consequence, there is a potential for evil waveforms to induce large tracking errors of differential systems if left undetected. This paper aims at providing some insight on the behavior of specific ground monitoring techniques that were proposed for implementation.

I. INTRODUCTION

Several types of failures can occur in the GPS space segment designed to deliver the ranging signals to the users. Among the potential failures, a specific type of failure in the signal generation process aboard the satellite may result in an anomalous waveform being transmitted, called an 'evil waveform'. Such a failure was already observed in 1993 on a flying satellite, and an analysis of the causes of failures have led to the derivation of a mathematical model of these waveforms [1].

Evil waveforms are GPS signals that have a distorted PRN code modulation waveform. The deformation is modeled by a lead or a lag of the rising or falling edges of the modulation code, and/or by a second-order filtering of this waveform.

The main impact is a rupture of the symmetry of the cross-correlation peak inside the tracking channel, therefore inducing a different measurement error for two receivers that would not have the same loops architecture.

As a consequence, there is a potential for evil waveforms to induce large tracking errors of differential systems. Some international standardization forums, in RTCA or ICAO, encourage the development of adequate ground monitoring techniques and are on the way to impose constraints on the airborne receiver to make sure the differential tracking error does not exceed the required accuracy level.

Several propositions of ground monitoring techniques are currently discussed, and this paper is focused on the proposition made in [1].

II. EVIL WAVEFORM MODEL

The evil waveform is a GPS signal that has a distorted PRN code modulation waveform. The failure giving birth to an evil waveform occurs in the code modulation generation channel only, therefore the transmitted carrier is not affected. Two types of failure can occur that result in an evil waveform being radiated. A failure in the digital code chip generation module can alter the synchronization of some of the C/A code chip edges. A mismatch of the analog band-limiting filter can distort the physical waveform being transmitted.

As a consequence, the model proposed in [1] is a PRN signal affected by one or both of the following effects:

1. All the falling edges or all the rising edges of the code modulation are delayed or advanced by an amount of Δ seconds. If there is a lag, then Δ is positive, if there is a lead, Δ is negative. Δ is usually expressed in chips, as a multiple of the chip length T_c=1/1.023·10^6 s.
2. The modulation is filtered by a 2^{nd} order filter characterized by two parameters:
   - $\sigma=\delta\omega_n$ where δ is the damping factor and $\omega_n/2\pi$ is the frequency.
   - $F_d=\frac{\omega_n}{2\pi}\sqrt{1-\delta^2}$ is the resonant frequency.

   Usually, σ and F_d are expressed in MHz.

Several types of threat models are considered:

- Threat model A: this type of evil waveform contains only the lead/lag effect. In that case, σ=0, F_d=0 and the accepted range of values for Δ is: $-0.12\ T_c \le \Delta \le 0.12\ T_c$.
- Threat model B: this type of evil waveform contains only the 2^{nd} order filtering effect. Therefore, Δ=0 and the possible range of values for σ and F_d is: $0.8\ MHz \le \sigma \le 8.8\ MHz$, $4\ MHz \le F_d \le 17\ MHz$.
- Threat model C: this type of evil waveform contains both effects. The possible range of values is: $-0.12\ T_c \le \Delta \le 0.12\ T_c$, $0.8\ MHz \le \sigma \le 8.8\ MHz$, $7.3\ MHz \le F_d \le 13\ MHz$.

Figures 1,2,3 and 4 show examples of simulation of the effect of evil waveforms in the absence of RF front-end filter.

0-7803-5872-4/00/ $10.00 © 2000 IEEE

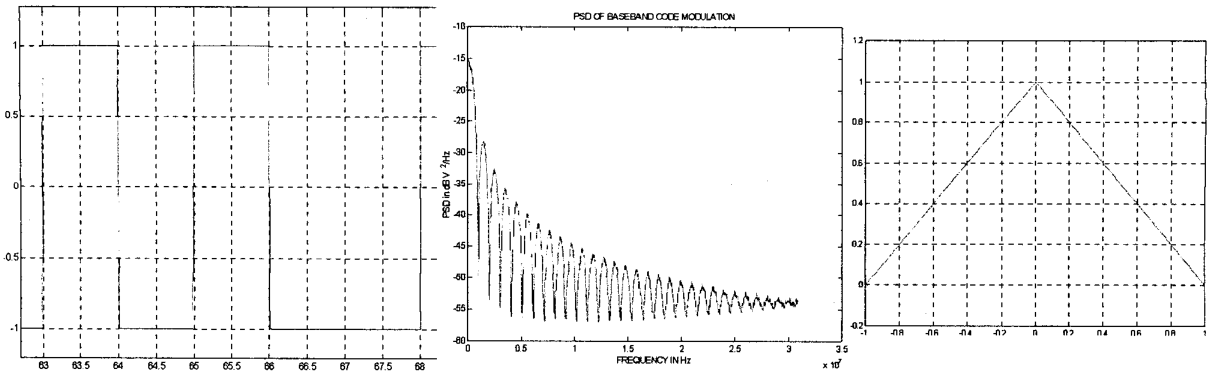

Figure 1: *Nominal C/A code (waveform, spectrum, cross-correlation)*

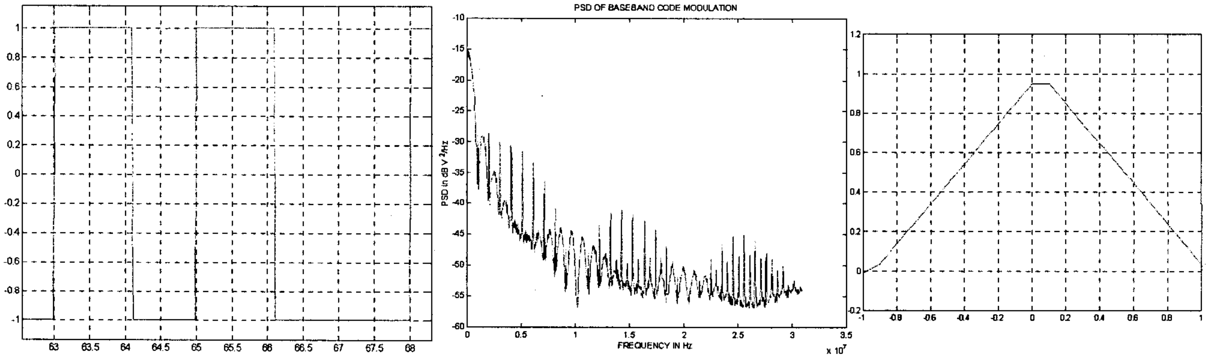

Figure 2: *Model A Evil Waveform: Δ=0.1 T_c*

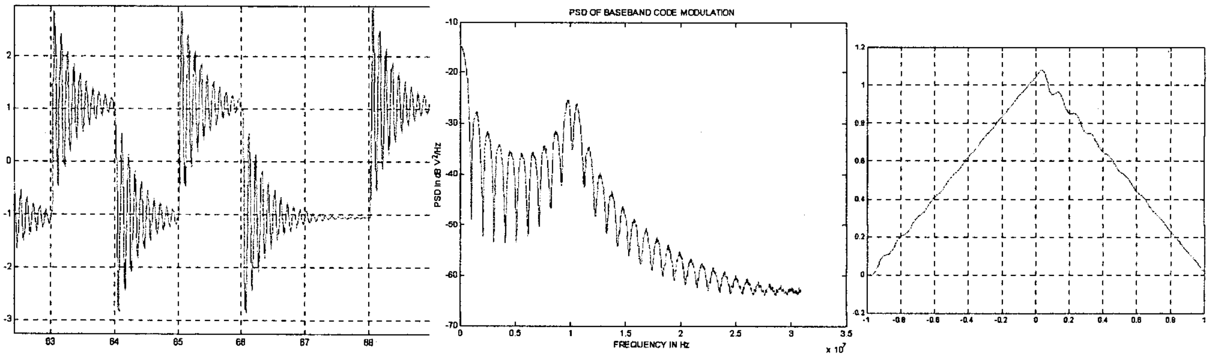

Figure 3: *Model B Evil Waveform: Δ=0, σ=3MHz, F_d=10 MHz.*

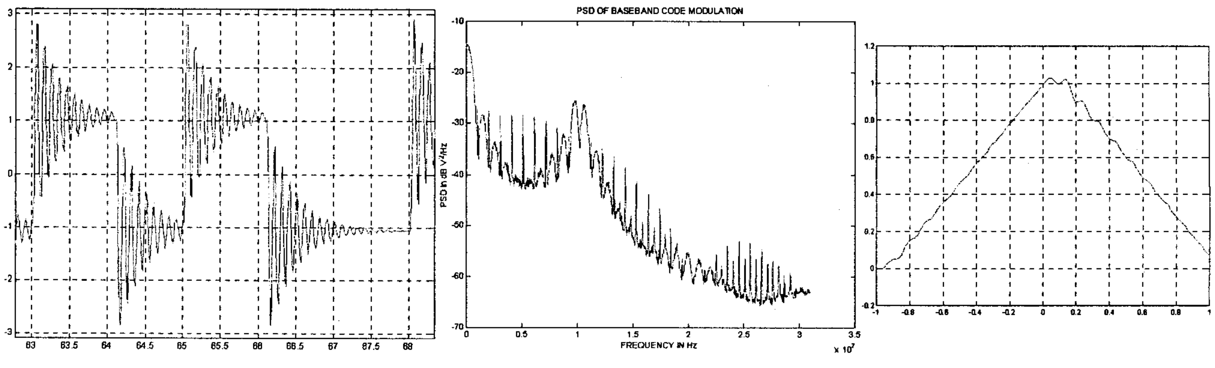

Figure 4: *Model C Evil Waveform: Δ=0.1 T_c, σ=3 MHz, F_d=10 MHz*

As we can see by comparing figure 1 and figure 2, model A evil waveforms add a periodic line spectrum to the nominal C/A code power spectrum density. This additive line spectrum has a $\sin(\pi f\Delta)/\pi f\Delta$ envelope. Moreover, model A evil waveforms raise the DC component of the code modulation by an amount close to $\Delta/2$ due to the near balance of 0s and 1s in each C/A code. As indicated in [1], the cross-correlation between model A evil waveforms and a nominal C/A code shifts the top section of the triangle, and introduces a plateau of width Δ.

As shown in figure 3, model B evil waveforms raise all the frequency components of the code spectrum located around F_d,. As a result, the cross-correlation function is also filtered by the 2nd order filter.

Model C evil waveforms are a combination of the lead/lag effect with the 2nd order filtering effect. Figure 4 shows the impact of this combination on the power spectrum density and on the cross-correlation function.

III. IMPACT OF EVIL WAVEFORMS ON GPS RECEIVER

The tracking errors due to evil waveforms depend on the exact characteristics of a receiver. First, the incoming signal is amplified, down-converted, filtered and converted to digital samples by the RF front-end. Then, this signal is sent to the tracking loops that try to generate local replicas of the incoming carrier and code modulation.

The amount of distortion conveyed by the evil waveform entering the tracking loops is determined by the RF front-end filter, that rejects out-of-band frequency components. The Delay Lock Loop (DLL) is designed to track nominal C/A codes having near-triangular cross correlation function, and is therefore misleaded by the deformations on the correlation values.

Therefore, the main parameters are:

- the transfer function of the RF front-end pre-correlation filter (bandwidth and group delay variations)
- the DLL discriminator function (value of the spacing between correlator outputs, form of the combination of these outputs)

As these parameters may vary considerably from one receiver to the other, the differential tracking error may be severely affected by the evil waveform.

IV. ANALYSIS OF SIGNAL QUALITY MONITORING TECHNIQUES

The techniques used to detect the presence of an evil waveform all tend to check whether the cross-correlation function significantly departs from the nominal triangular shape.

The signal quality monitoring (SQM) technique which is analyzed here is taken from [1] and consists in comparing the measurements made by three independent DLLs tracking the same satellite signal.

The chip spacings of these DLLs are 0.1 Tc, 0.15 Tc and 0.2 Tc. The difference between the 0.1 Tc and 0.15 Tc measurements, as well as the difference between the 0.2 Tc and 0.15 Tc measurements are compared to decision thresholds T_{test}. To assess the performance of the SQM during simulations, we compare these two test criteria with thresholds called the Minimum Detectable Errors (MDEs).

The test threshold T_{test} is determined as

$$T_{test} = K_{fa} \times \sigma_{test} \qquad (1)$$

where

- σ_{test} is the standard deviation of the test metrics
- K_{fa} is the expansion factor required to guarantee a specific false alarm probability

The MDEs are computed so that both the false alarm rate and the probability of missed detection are met:

$$MDE = (K_{fa} + K_{md})\sigma_{test} \qquad (2)$$

It is proposed in [2] that the probability of missed detection be set to 10^{-3}, inducing $K_{md}=3.09$, assuming the test metrics has a gaussian distribution. Similarly, a proposed allocation analysis in [2] concludes to a false alarm rate of $1.25 \cdot 10^{-8}$ when using a total of 8 parallel test metrics on measurements coming from 6 satellites correlated over 100s. Therefore, $K_{fa}=5.70$, and

$$MDE = 8.79 \times \sigma_{test} \qquad (3)$$

If no fault is detected by the SQM algorithm, then the pseudorange correction elaborated using the 0.1 Tc DLL measurement is sent to the airborne users.

V. SIMULATION OF THE GBAS DIFFERENTIAL TRACKING ERROR

Two software simulators implemented in MATLAB were used for this analysis. The first simulator is a complete GPS simulator, while the second one is a simplified GPS receiver simulator.

V.1 Complete GPS simulator

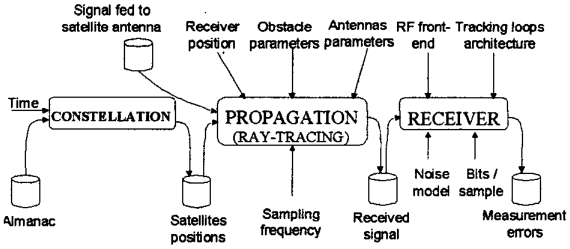

Figure 5: *Architecture of complete GPS simulator. For the analysis reported here, the propagation module was used in a simple mode, where it only outputs a GPS signal affected by the evil effects.*

As illustrated in figure 5, the complete GPS simulator is composed of three modules For the analysis reported here, only the last two modules were used.

- Signal generation module: generates the signal sensed by the antenna.
- Receiver module: simulates the signal processing operations performed by the GPS receiver on the incoming signal.

The simulator can be run in different modes, using different parameters values, enabling the user to:

- Generate a discrete evil waveform with any characteristics (Δ=lead/lag, σ=damping, F_d=system frequency).
- Simulate the effect of any RF front-end filter (brickwall, butterworth, chebychev, elliptic,...) with any double-sided bandwidth *BW2*.
- Plot the cross-correlation between the incoming and the local code.
- Determine the code tracking error of any DLL (dot-product, non-coherent E-L, HRC, ...) with any chip spacing.
- Simulate the operations of the ground monitoring unit (readings of correlator outputs, comparison with specified MDEs).
- Determine the differential code tracking error of the airborne receiver.

Due to the large number of operations performed by this simulator, its execution time is very long. Therefore, this simulator was only used as a reference during the development of the simplified GPS receiver simulator, and for the evaluation of the effect of quantization on the evil waveforms.

V.2 Simplified GPS receiver simulator

A simplified GPS receiver simulator was developed for this study, where the base signals are the cross-correlation functions between the pure C/A code and each of the evil waveform, depending on the evil parameter values. These functions are then filtered by the RF front-end filter, and they are finally used to determine the stable zero-crossing point of the discrimination function of the DLL, as presented in figure 6.

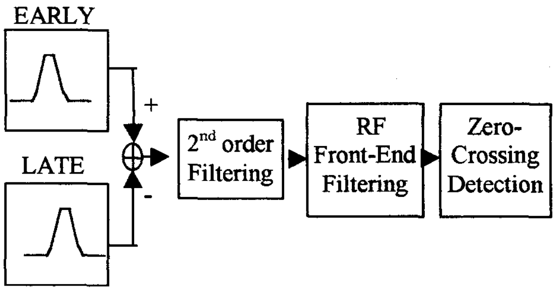

Figure 6: *Architecture of simplified GPS receiver simulator.*

Therefore, like the complete GPS simulation tool, this tool can also simulate the operations of the ground monitoring unit and determine the differential code tracking error of the airborne receiver.
As indicated previously, this simulator is very fast, therefore we used only this receiver to determine the results that are presented in this report, except the results concerning the quantization effect.

The simulator can be run in different modes, using different parameters values, enabling the user to:

- Generate a discrete evil waveform with any characteristics (Δ=lead/lag, σ=damping, F_d=system frequency).
- Simulate the effect of any RF front-end filter (brickwall, butterworth, chebychev, elliptic,...) with any double-sided bandwidth *BW2*.
- Plot the cross-correlation between the incoming and the local code.
- Determine the code tracking error of any DLL (dot-product, non-coherent E-L, HRC, ...) with any chip spacing.
- Simulate the operations of the ground monitoring unit (readings of correlator outputs, comparison with specified MDEs).

V.3 Simulation assumptions

1. The tracking errors are determined as the errors that cancel the discrimination function of a coherent Early-Late DLL.
Rationale: In this study, as we are interested only in the steady-state tracking errors, and not in the errors induced by transients due to the evil waveform we search for the errors that cancel the tension controlling the local oscillator. In addition, we chose to simulate ground and airborne receivers equipped with coherent Early-Late DLLs, as the model proposed in [1] does not reproduce any effect on the carrier phase.

2. The cross-correlation functions are generated with a sampling frequency which allows sufficient resolution of the zero-crossing point.

3. The RF front-end filter of the ground station receiver is modeled as a 6th order Butterworth filter with a double sided bandwidth of 16 MHz. The RF front-end filter of the airborne receiver is modeled as a 6th order Butterworth filter with a double sided bandwidth in [4MHz...20MHz].

4. The correlator outputs are assumed to be samples of the ideal evil waveform cross-correlation functions.
Rationale: To speed up the computations, it is easier to consider that the Integrate and Dump filters provide samples of an ideal cross-correlation function rather than to re-compute these values. Minor differences may appear due to the slight irregularities of the actual

cross-correlation functions outside of the $[-T_c;T_c]$ interval.

6. The measurements used by the ground station to monitor the signal quality are obtained from 3 independent loops set with chip spacings of (0.1 T_c, 0.15 T_c, 0.2 T_c).
Rationale: The ground station monitoring operations can also be performed with one DLL set to a unique chip spacing (0.1 T_c for example), and readings from multiple correlator outputs can be used to determine measurements at other spacings. In our previous analysis, we had shown that this second approach was less efficient for failure detection.

6. The ground station monitoring Minimum Detectable Errors (MDEs) are set accordingly to the chip spacings (1.62 m, 1.1 m)
Rationale: These MDEs were computed using the model presented in [2]. This model assumes the ground station has a Ground Accuracy Designator (GAD) 'B3'.

7. The pseudorange corrections transmitted by the ground station to the users are determined from the 0.1 T_c DLL.

An illustration of the data flow in the evaluation software is given in figure 7.

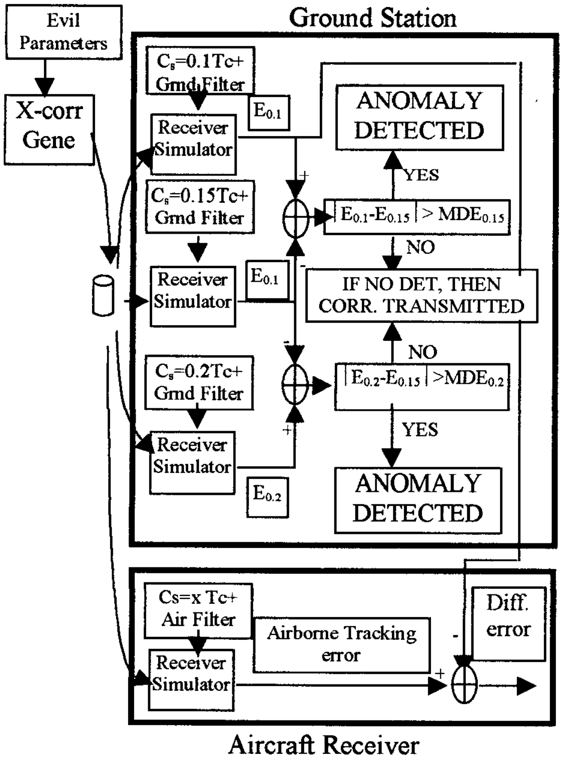

Figure 7: *Data flow in the simulator.*

VI. SIMULATION RESULTS

VI.1 Presentation of results

The results presented in this section are the worst-case airborne differential tracking errors for one particular threat model. These worst case errors are computed in the following way:

- For each parameter value in the threat model
    - Compute tracking errors at 0.1 T_c, 0.15 T_c and 0.2 T_c.
    - Compare difference of tracking errors at 0.15 T_c and 0.1 T_c with $MDE_{0.1}$
    - Compare difference of tracking errors at 0.2 T_c and 0.15 T_c with $MDE_{0.2}$
    - If any of the differences is larger than the corresponding MDE, then the anomaly is detected, and the pseudorange correction is not transmitted
    - If not, then the pseudorange correction is transmitted
        - For each RF filter bandwidth
            - For each chip spacing
                - Compute the tracking error
                - Compute the of the differential tracking error using the received correction
                - Determine the magnitude of the maximum differential tracking error observed up to now
            - End;
        - End;
    - End;
- End;
- Plot the magnitude of the maximum differential tracking error for all the evil waveforms in the threat model.

The current propositions of constraints for the airborne users would only allow receivers with the pairs of double sided bandwidth and chip spacings presented in table 1.

Region	3dB Pre-correlation Bandwidth, BW2	Average Correlator Spacing
1	0<BW≤7 MHz	0.045-1.1
2	7<BW≤16 MHz	0.045-0.21
3	16<BW≤20 MHz	0.045-0.12

Table 1: *Current proposition of constraints on allowed receiver designs.*

VI.2 Results for airborne Early-Late DLLs

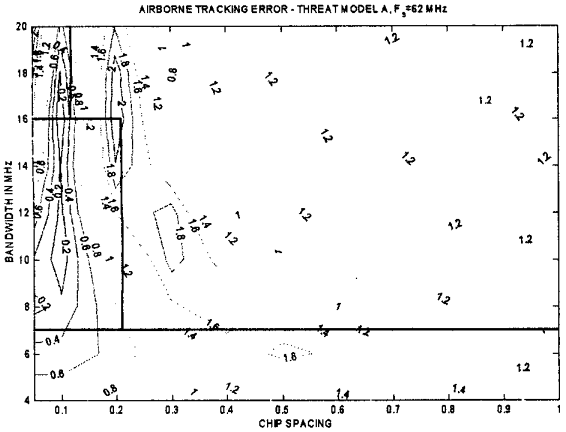

Figure 8: *Differential airborne tracking error induced by model A evil waveform with (0.1,0.15,0.2) SQM.*

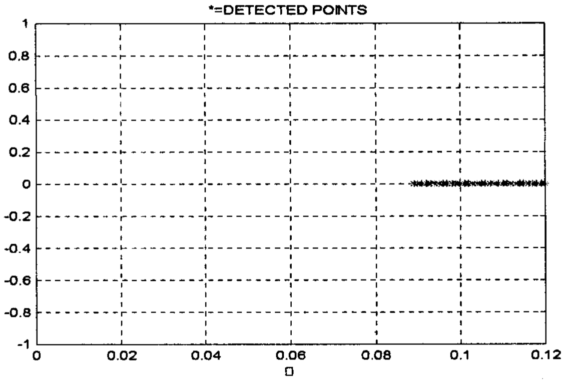

Figure 9: *Detection volume for model A evil waveform with (0.1,0.15,0.2) SQM.*

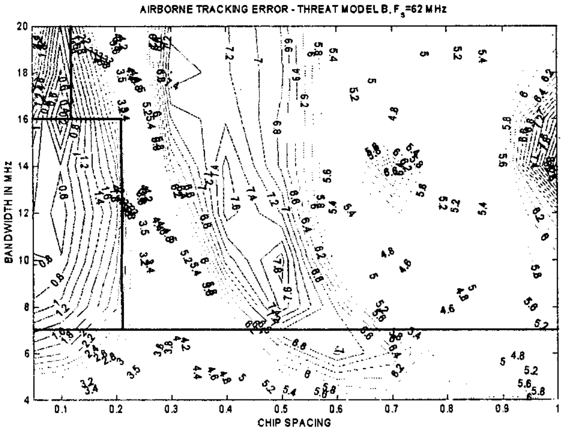

Figure 10: *Differential airborne tracking error for model B evil waveforms with (0.1,0.15,0.2) SQM.*

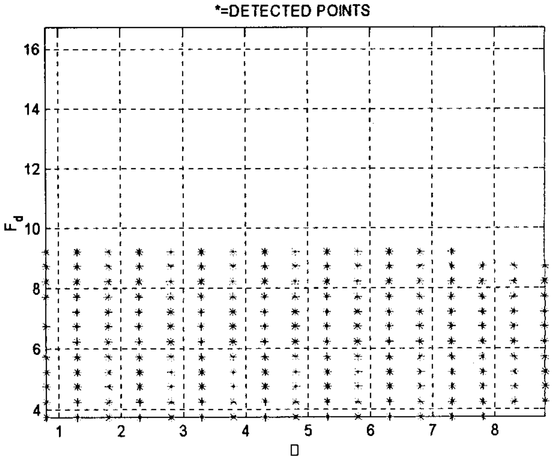

Figure 11: *Detection volume for model B evil waveforms with (0.1,0.15,0.2) SQM.*

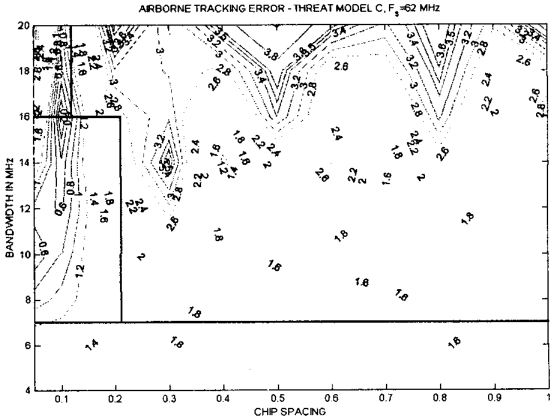

Figure 12: *Differential airborne tracking error for model C evil waveforms with (0.1,0.15,0.2) SQM.*

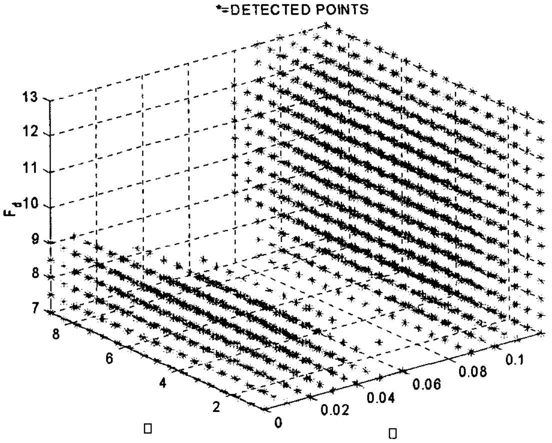

Figure 13: *Detection volume for model C evil waveforms with (0.1,0.15,0.2) SQM.*

VI.3 Analysis of results

The simulation results for model A show that the final tracking errors are acceptable in the three zones proposed for Early-Late DLLs.

For model B, the final differential airborne tracking error is too large, particularly in region 1. But these results are changed by modifying either the threat model exploration (density and starting point) or the sampling frequency. These differences are explained by the changing behaviour of the SQM depending on the simulation assumptions.
The acceptability of the three zones is therefore conditional to the assumptions.

For model C, the three zones are hardly acceptable due to marginal errors for narrow correlator spacings and wide bandwidths.

VII. EXISTENCE OF SINGULAR POINTS IN THE THREAT MODEL

When running simulations for model B, we noticed the extreme sensitivity of the SQM to the simulation assumptions, such as the sampling frequency, the density of the exploration, or the MDE values. To investigate this phenomenon, we plotted the decision criteria ($|E_{0.1}-E_{0.15}|$, $|E_{0.2}-E_{0.15}|$) of the SQM for model B. These figures were obtained with a ground filter modeled as a 6th order Butterworth filter with a double sided bandwidth of 16 MHz.

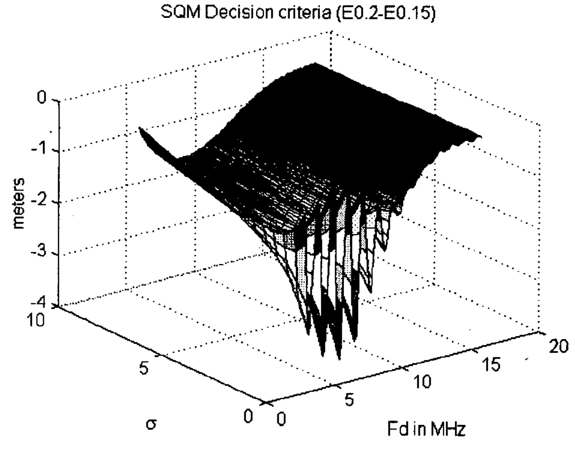

Figure 14: *Test criterion ($E_{0.2}$-$E_{0.15}$) as a function of σ and F_d for model B evil waveforms.*

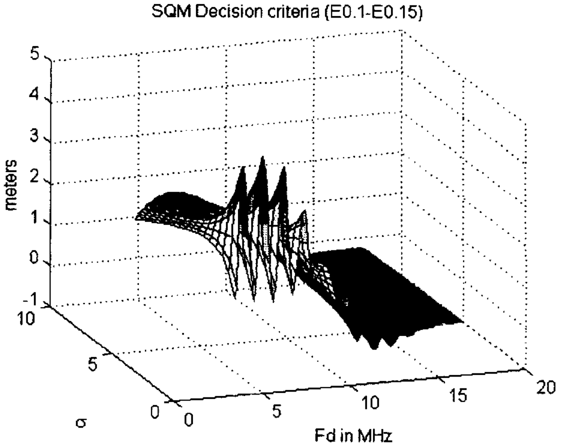

Figure 15: *Test criterion ($E_{0.1}$-$E_{0.15}$) as a function of σ and F_d for model B evil waveforms.*

We can see that for low values of σ and for F_d within the ground filter bandwidth, some large oscillations appear. This means that for small variations in F_d, the criteria may vary significantly. Therefore, depending on the threat model exploration (origin and density), the results can change dramatically.

Figure 16 presents the results obtained when using a very fine granularity to explore the threat space for σ=0.8 MHz. This shows that the test criteria present oscillations that come extremely close to the MDEs, inducing a very large susceptibility of the results to the simulation assumptions.

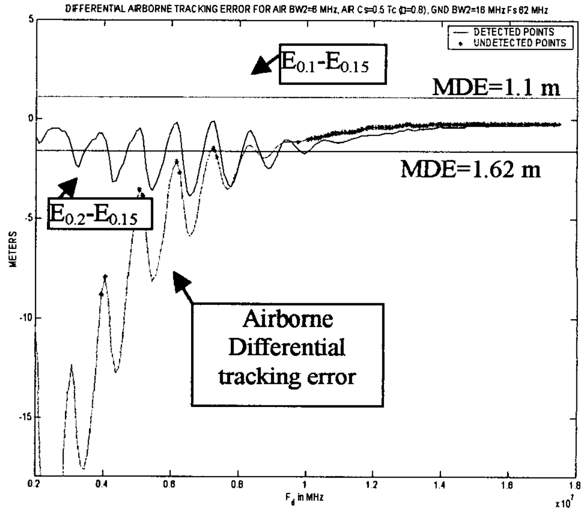

Figure 16: *Differential airborne tracking error and position of test criteria with respect to corresponding MDEs as a function of F_d for σ=0.8 MHz.*

VIII. CONCLUSION

The SQM analyzed here does not protect all the airborne users inside the proposed allowed regions, and other techniques have to be investigated.

This SQM is also characterized by an oscillation of its test criteria that induce a very high susceptibility of the results to the simulation assumptions.

As this SQM is not satisfying, work is now underway to propose new SQM techniques that would better protect the airborne users.

REFERENCES

[1] P. ENGE, E. PHELTS and A. MITELMAN, « Detecting Anomalous Signals from GPS Satellites », Global Navigation Satellite System Panel meeting, Toulouse October 18-29 1999, working paper 19.

[2] C. SHIVELY, M. BRENNER and P. KLINE, « Multiple Ground Tests Protecting Against Satellite Correlation Symmetry Faults in LAAS (Revision 3)», RTCA SC-159, 1999.