Processing Technique and Performance of the Observation of Evil Waveform in the Chip Domain

Paul Thevenon[(1)], Jean-Baptiste Pagot[(1)], Olivier Julien[(1)], Quentin Tessier[(1)]

[(1)]Ecole Nationale de l'Aviation Civile (ENAC)
7 avenue Edouard Belin – CS 54005
31055 Toulouse Cedex 4 – FRANCE
Email: thevenon@recherche.enac.fr, pagot@recherche.enac.fr, ojulien@recherche.enac.fr, tessier@recherche.enac.fr

ABSTRACT
This paper focuses on the Chip Domain Observable, a particular observation of the GNSS signal that is done in the time-domain, directly on the digitized samples at the output of the RF front-end of a GNSS receiver. With such observable, it is possible to observe in details the average chip transitions of the received GNSS signal, and to monitor some anomalies affecting the signal. This observable is obtained through a particular signal processing technique, which is presented in details in the paper. Then, a particular type of signal deformation, called the Evil Waveforms and modelled by the ICAO, is applied to this observable. The paper gives the analytical expression of each ICAO Threat Model observed by the Chip Domain Observable, as well as the measurement noise affecting the observation, in function of the receiving conditions and some signal processing parameters. This work may serve in the future to investigate some novel signal quality monitors, working in the time domain, rather than in the correlation domain.

INTRODUCTION
The basic principle of GNSS signal processing assumes that the received signal is undistorted. For example, a code delay lock loop aims at equaling an early and a late correlator in order to find the location of the prompt correlator, which should correspond to the maximum of the correlation function of the GNSS signal, which is then turned into a pseudo-range measurement. This assumes that the correlation peak has a triangular shape. However, in reality, the received signal is affected by distortions, for example due to some incorrect behavior of the signal generation payload onboard GNSS satellite (also called Evil Waveform) or due to the local environment of the receiving antenna which may create multipath. Both effects are translated into deformation of the correlation function, which in turn creates some error on the pseudo-range measurements and the subsequent position.
In order to detect or mitigate errors coming from signal distortion, a family of signal processing techniques has been derived, usually based on the monitoring of the correlation function of the received signal thanks to multiple correlators. The correlation function is therefore observed at different delays, and combinations of different correlators permit to detect anomalies on the correlation function such as asymmetry or slope change. Such multi-correlator techniques are used in high integrity systems, for example Ground-Based Augmentation System, in order to detect an Evil Waveform and exclude a potentially failing ranging source [7]. Another application is the detection of multipath for receivers roaming in urban environment, in order to either exclude some measurements and improve the overall quality of the position solution, or to estimate the multipath parameters and mitigate their impact [5][1].
More recently, signal deformation monitoring has turned to the observation of the signal in the time domain, rather than in the correlation domain. Indeed, by observing the signal in the time domain, thanks to the particular properties of GNSS signals (recalled in [3]) and adequate signal processing, it is possible to observe the chip transitions with high fidelity. This observation is believed to be used by Novatel under the name of Vision Correlator.

The aim of this paper, and resulting structure, is to detail the advantages of the Chip Domain Observable (CDO), to explain what signal processing steps are required for CDO computation, to illustrate the use of this technique on the Evil Waveform monitoring for GPS L1 C/A, and finally to detail the accuracy of such observation, in terms of standard deviation of the observed CDO values.

DESCRIPTION OF THE CHIP DOMAIN OBSERVABLE
The Chip Domain Observable (CDO) is a measurement of the GNSS signal that permits to observe the average GNSS chip transition, and possible distortions affecting the GNSS signal, in the time domain. An 'average' chip transition is obtained by superimposing every transition of a given type (e.g. rising edge) during a chosen time window called the integration time, in order to average out the noise affecting the initial digitized samples of the GNSS signal.
In the end, the CDO will consist of a vector of chosen length, and each element will correspond to the average signal amplitude at a relative delay around a given transition type. The CDO can be formalized using the following notations:

- CDO_k is the k-th value of the signal amplitude in the k-th delay bin
- τ_k is the k-th instant relative to a transition type, expressed in fraction of chips. This delay corresponds to the center of the k-th delay bin.
- $\Delta\tau$ is the delay bin width, expressed in fraction of chips. It corresponds to the time resolution with which the transition is observed.

- N_{bins} is the number of delay bins, on which the CDO is computed. Therefore, it is the length of both vectors $\{CDO_k\}$ and $\{\tau_k\}$. The delay bin width $\Delta\tau$ is related to the number of bins N_{bins} and the chip duration T_c through the formula $\Delta\tau = T_c/N_{bins}$.
- Finally, the CDO is computed only for a given type of transition. There may be therefore 4 different types of CDO: rising (0→1), falling (1→0), lower level (0→0) and upper level (1→1). Since the principle of the timing measurement done by a GNSS receiver is to synchronize with the transitions of the PRN code, only the first two types of transitions will usually be studied.

In this paper, the delay bins are regularly spaced. However, in the general case, the bins could be arbitrarily placed on the chip transition.

Examples of CDO can be found in Figure 4 at the end of this paper.

Usually, the signal distortion is observed indirectly through the correlation function that is computed within the receiver [7]. Observing the signal in the time domain level has several advantages, compared to the observation in the correlation domain:

- the resolution of the CDO benefits from the high sampling frequency at the output of the RF front-end, while multi-correlator techniques require a specific and cumbersome correlation processing for each observed point of the correlation function. Recall that the sampling frequency at the RF front-end output can reach more than 100 MHz.
- additionally the CDO resolution can still be increased noticing that the bins frequency is independent from the sampling frequency. This resolution increase is not done thanks to an interpolation process, but because if the sampling frequency is not a multiple of code rate, digitized signal samples over a long period (e.g. 1s) will correspond to a large number of positions on or around the chip transition.
- the noise affecting the CDO is white noise that has a lower correlation time due to the RF filter bandwidth (up to 24 MHz), while the noise affecting a correlation function observation is correlated by multiplication by the local code replica (1.023 MHz for L1 C/A). This may have advantages when estimating certain parameters from the CDO.
- the CDO permits to observe independently different types of chip transitions. For example, it is possible to observe separately some anomalies on the rising chip transitions and on the falling chip transitions, which is not possible on the correlation function.
- it will be demonstrated that the signal to noise ratio of the CDO can be increased by lengthening the integration time. It is therefore possible to reach any desired signal to noise ratio. Note that this can also be done on the correlation function, by averaging correlator outputs over a longer duration.

Some limitations of the CDO compared to the correlation function observation are:

- the CDO is less related to the actual tracking process done by a receiver. It is therefore more difficult to relate the impact of an anomaly observed on the CDO, on the pseudo-range measurement. This is less true for the correlation function, since it is directly used for the computation of the pseudo-range measurement. So additional analysis may be required to assess the impact of CDO anomaly on the user measurements.
- The signal to noise ratio of this observation is lower than the one for the correlation function. This is due to the fact that only one type of transition is used for the accumulation of the signal and averaging of the noise. There will be typically a factor 4 between the SNR of both types of observation. However, as it is possible to extend the averaging period, this issue could be tackled by extending the integration time of the CDO processing.
- Specific signal processing techniques must be implemented in the receiver to produce the CDO, while correlation is already available is the nominal working of a receiver.

SIGNAL PROCESSING TECHNIQUE TO OBTAIN THE CHIP DOMAIN OBSERVABLE

Overview of the signal processing steps

Figure 1 shows the different steps required to compute the CDO. The first step, noted (1) in the Figure, of the processing is the actual digitization of the signal by the receiver's RF front-end. The second step (2) is to estimate the signal parameters by conventional tracking loops (DLL and PLL). Then, these signal parameters are re-used for the processing of the same digitized samples that were used and stored for the estimation. The third step (3) consists in correcting the samples by the Doppler and phase estimates. The fourth step (4) puts a time-stamp on each sample, using the estimated Doppler and delay. Finally, the samples are accumulated in delay bins over a chosen duration (5). The rest of this section will detail each step of the processing.

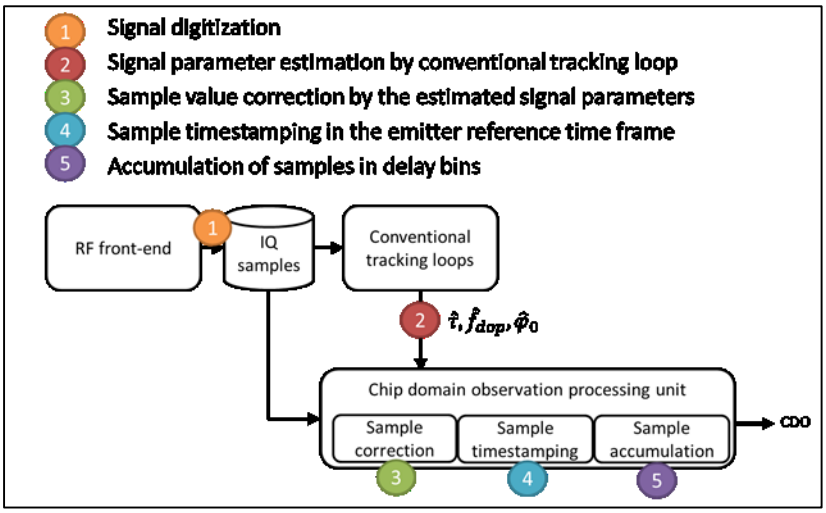

Figure 1 – Signal processing steps to obtain the Chip Domain Observable

Signal digitization

The model of the signal received by a ground antenna is:

$$s(t) = c(t-\tau, f_{dop}).d(t-\tau, f_{dop}).\exp(j2\pi f_{dop}t + j\varphi_0) \quad \text{Eq. 1}$$

Where f_{dop} is the Doppler frequency affecting the (carrier) signal, in Hz
τ is the delay affecting the signal, in seconds
φ_0 is the initial carrier phase offset, in radians
$c(t, f_{dop})$ is the PRN chip sequence affected by a Doppler f_{dop} at time t
$\mathrm{d}(t, f_{dop})$ is the data sequence affected by a Doppler f_{dop} at time t

In the following, we will ignore the effect of the data sequence, by assuming that the receiver is able to demodulate the navigation message and to correct it so that $d(t, f_{dop}) = 1$.

It is useful to further detail the expression of $c(t, f_{dop})$. Without Doppler offset, the chip sequence expression would be:

$$c(t, f_{dop}=0) = \sum_{p=-\infty}^{+\infty} \sum_{k=0}^{L-1} c_k \,.\, Rect_{T_c}(t - kT_c - pLT_c) \quad \text{Eq. 2}$$

Where c_k is the value of the k-th chip of the PRN code,
T_c is the chip duration in seconds
L is the number of chips in the PRN code. For L1, L = 1023.
$Rect_{T_c}(t) = \begin{cases} 1 & \text{for } t \in [0, T_c] \\ 0 & \text{elsewhere} \end{cases}$ It is the rectangle function corresponding to the BPSK modulation with a chip rate of $1/T_c$

In case of the presence of a Doppler offset, we have to use the modified chip duration after application of the Doppler offset.

$$T_c' = \frac{T_c}{1 + f_{dop}/f_c} \quad \text{Eq. 3}$$

Where f_{dop} is the Doppler frequency affecting the carrier frequency, in Hz.
f_c is the carrier frequency in Hz. For example, for L1, f_c = 1575.42 MHz and for L5, f_c = 1176.45 MHz
T_c' is the chip duration affected by the Doppler effect.

So in the end, the model for the received signal (without noise) is:

$$s(t) = \sum_{p=-\infty}^{+\infty} \sum_{k=0}^{L-1} c_k \,.\, Rect_{T_c'}(t - \tau - kT_c' - pLT_c').\exp(j2\pi f_{dop}t + j\varphi_0) \quad \text{Eq. 4}$$

Finally, this signal is sampled at a frequency f_s, giving the following expression of each sample:

$$s_n = s\left(\frac{n}{f_s}\right) = \sum_{p=-\infty}^{+\infty} \sum_{k=1}^{L} c_k \,.\, Rect_{T_c'}\left(\frac{n}{f_s} - \tau - kT_c' - pLT_c'\right).\exp\left(j\frac{2\pi f_{dop} n}{f_s} + j\varphi_0\right) \quad \text{Eq. 5}$$

This is the formulation of an undistorted signal. It can be augmented by adding the RF front-end filter and/or the different signal distortion (e.g. EWF) under study.

Signal parameter estimation by conventional tracking loop

To obtain the CDO, it is necessary to have access to the signal main parameters: PRN number, delay τ, carrier Doppler offset f_{dop}, initial phase offset φ_0.

These parameters can be estimated thanks to a conventional GNSS tracking loop. These tracking processes are well described in many reference books or courses on GNSS signal processing and will not be described in details. The output of this processing step is the computation of signal parameter estimates: $\hat{\tau}$, $\hat{f}_d$, $\hat{\varphi}_0$.

The parameters are re-used to process the digitized samples of the received signal collected before the correlation process.

Sample value correction by the estimated signal parameters

The sample values are affected by a phase shift, due to the initial phase φ_0 and by the Doppler effect f_{dop} on the carrier. The operation to compensate for these effects is:

$$s_n^{corr} = s_n . \exp\left(-j\frac{2\pi\hat{f}_{dop}n}{f_s} - j\hat{\varphi}_0\right) \quad \text{Eq. 6}$$

Sample time-stamping in the emitter reference time frame

For the time stamping of the samples, the estimated delay $\hat{\tau}$ and Doppler frequency $\hat{f}_{dop}$ are used. The received signal is sampled with a sampling frequency f_s. However, the received signal is affected by a Doppler. Therefore, the instant of emission in the emitter time scale are emitted with a Doppler-corrected sampling frequency $f_s' = f_s(1 - f_{dop}/f_c)$.

Additionally, the time of reception of the samples are affected by the delay τ.

Therefore, the time-stamp in the emitter time scale of the n-th received sample is determined by the following formula:

$$\tau_n = \frac{n}{f_s'} - \hat{\tau} = \frac{n}{f_s(1 - \hat{f}_{dop}/f_c)} - \hat{\tau} \quad \text{Eq. 7}$$

Accumulation of samples in delay bins

The corrected samples are associated to a given delay bin based on their time-stamp. Only the samples belonging to the studied transition type will be accumulated. Let us focus on the rising transition type, and let us call τ_m^{rise} the theoretical delay of the m-th rising transition in our PRN.

Each time stamp can be expressed relatively to the theoretical delay of a transition, by subtracting τ_m^{rise} to τ_n. Then, we decide to allocate a sample to a delay bin if the relative time stamp to the transition delay falls into a delay bin.

$s_k^{bin} = \{s_n^{corr}\}$, for all samples verifying the following condition on their time-stamp:

$\tau_n - \tau_m^{rise} \in \left[\tau_k^{bin} - \frac{\Delta\tau}{2}, \tau_k^{bin} + \frac{\Delta\tau}{2}\right]$, for all values of m (ie for all rising transitions).

After distributing the different samples in the delay bin, the mean of all sample values is done, to obtain the CDO.

$$CDO_k = mean\left(s_k^{bin}\right) \quad \text{Eq. 8}$$

Consideration of the integration time

A final parameter of the CDO technique is the integration time T_{int}. This time corresponds to the duration over which the signal is accumulated in the delay bins before doing the average. Usually, this time is a multiple of code periods.

If the integration time is longer than the conventional tracking loop update interval, then for each tracking update, a different value of $\hat{\tau}$, $\hat{f}_{dop}$ and $\hat{\varphi}_0$ will be used on the samples used for tracking.

For example, if the integration time $T_{int} = 40$ ms and our tracking loop update interval is 20 ms, then a first set of signal parameters will be used on the first half of the samples, and then the second set of signal parameters will be used on the second half of the samples.

MODEL OF AN EVIL WAVEFORM IN THE CHIP DOMAIN

Introduction to Evil Waveform models

Evil Waveforms (EWF) are signal distortions that are caused by a satellite anomaly. The first (and only) EWF occurred in 1993, on GPS satellite SVN19. Such distortion creates some error on the pseudo-range measurement, without the receiver loosing track of the affected satellite. This pseudo-range error is then propagated in the position domain, with vertical errors up to 8m, as reported in [2]. This kind of pseudo-range error is not eliminated through differential corrections, if the reference receiver and the rover receiver have different parameters (mainly pre-correlation bandwidth, discriminator type and correlator spacing). Therefore, ICAO has required the monitoring of this threat for high-integrity systems such as SBAS and GBAS, and defined a Threat Model [4].

The ICAO Threat Model identifies 3 types of anomalies on the L1 C/A signal that can lead to errors on the pseudo-range.

- Threat Model A consists of a systematic lag or lead, called Δ in the instant of the falling edge of a PRN chip. It corresponds to an anomaly in the digital part of the signal generation unit.
- Threat Model B consists of some ringing effects that would be created in the analog part of the signal generation unit. These ringings are modelled by assuming that the PRN signal goes through a 2nd order linear system,

characterized by 2 parameters: the damping frequency f_d and the damping factor σ. More precisely, the unit step response of such system is given by Eq. 9.

$$e(t) = \begin{cases} 0 & \text{for } t \leq 0 \\ 1 - e^{-\sigma t}\left[\cos(2\pi f_d t) + \frac{\sigma}{2\pi f_d}\sin(2\pi f_d t)\right] & \text{for } t \geq 0 \end{cases} \quad \text{Eq. 9}$$

- Finally Threat Model C is a combination of both analog and digital distortions.

The range of the Threat Model parameters is given in Table 1.

Table 1 – Threat Model parameter range [4]

	Δ (chip)	σ (MNepers/s)	f_d (MHz)
TM A	[-0.12 ; 0.12]	-	-
TM B	-	[0.8 ; 8.8]	[4 ; 17]
TM C	[-0.12 ; 0.12]	[0.8 ; 8.8]	[7.3 ; 13]

The goal of this section is to provide an analytical model of the impact of the ICAO threat model applied to the CDO. The following models are valid for the infinite bandwidth and noise-free case.

Digital Failure Model (Threat Model A)

For the TM-A model, the modelling of the CDO is fairly simple. The rising transition will not be modified. The falling transition is delayed by the value Δ. This can be put into equations:

$$CDO_{TM-A}^{rising}(t) = \begin{cases} 0 & \text{for } -T_c/2 \leq t \leq 0 \\ 1 & \text{for } 0 \leq t \leq T_c/2 \end{cases} \text{ and } CDO_{TM-A}^{falling}(t) = \begin{cases} 0 & \text{for } -T_c/2 \leq t \leq \Delta \\ 1 & \text{for } \Delta \leq t \leq T_c/2 \end{cases} \quad \text{Eq. 10}$$

Note that this equation is valid for values of Δ below 0.5 chips.

Analog Failure Model (Threat Model B)

[4] provides the response to a unit step of the 2nd order linear filter used to model a TM-B. This expression can be used directly for the modelling of the impact of TM-B on the CDO. This section will only focus on the rising transition type (0→1), but similar approach can be taken for the falling transition type (1→0).

Let us consider all 4 chip-long subsequence ending by a rising transition: 0001, 1001, 0101, 1101. Indeed, for some low values of the damping factor σ, the ringing effect will last more than one chip. This is why the described approach considers transitions occurring well before the considered rising transition. For each transition, it is possible to use the unit step response expression that is given in [4] and recalled in Eq. 9.

$$\begin{aligned} \text{for } 0001, \quad & s_1(t) = -e(t+3T_c) && && +2e(t) \\ \text{for } 1001, \quad & s_2(t) = +e(t+3T_c) && -2e(t+2T_c) && +2e(t) \\ \text{for } 0101, \quad & s_3(t) = -e(t+3T_c) && +2e(t+2T_c) && -2e(t+T_c) && +2e(t) \\ \text{for } 1101, \quad & s_4(t) = +e(t+3T_c) && && -2e(t+T_c) && +2e(t) \end{aligned} \quad \text{Eq. 11}$$

In the CDO processing, an average over an integer number of code period is done to obtain the value at each delay bin. Therefore, the resulting CDO is the average of all signal $s_k(t)$ for the different subsequence, weighted by the number of occurrence of this particular subsequence type present in the particular PRN code:

$$CDO_{TM-B}^{rising}(t) = \frac{n_1.s_1(t) + n_2.s_2(t) + n_3.s_3(t) + n_4.s_4(t)}{n_1 + n_2 + n_3 + n_4} \quad \text{Eq. 12}$$

Where n_k corresponds to the number of the subsequence in the particular PRN.

An analysis of the PRN codes 1 to 32 used by GPS has been done to count the number of subsequences assessed in each PRN and is shown in Figure 2.

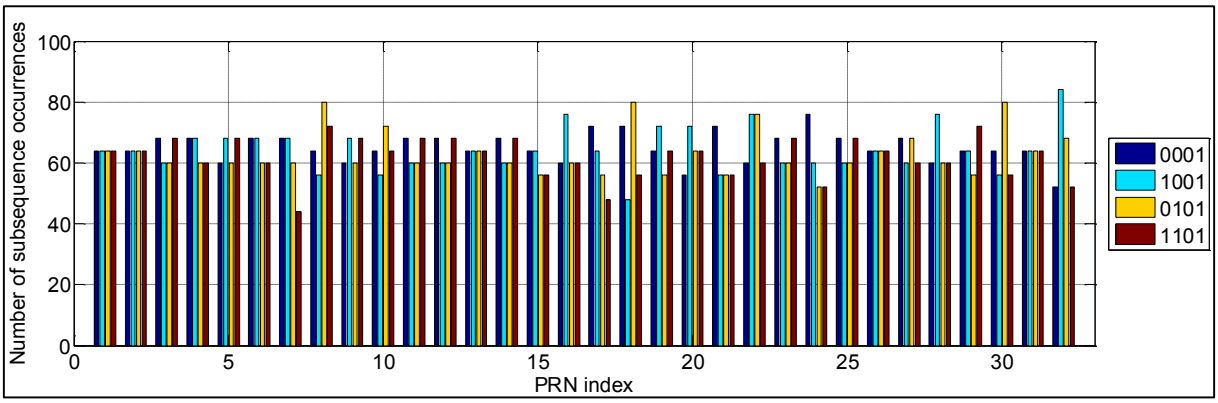

Figure 2 – number of 4-chip long subsequences ending by a rising transition in PRN 1 to 32. Each color corresponds to one subsequence.

An acceptable approximation is to consider an equal number of each subsequence. It has been verified that such hypothesis will not modify the CDO model by more than a few percent. This has the further advantage to remove the dependency of the TM-B expression in the Chip domain on the PRN. In this case, the CDO model becomes:

$$CDO_{TM-B}^{rising}(t) = \frac{n.s_1(t) + n.s_2(t) + n.s_3(t) + n.s_4(t)}{4n} = \frac{1}{4}\left(s_1(t) + s_2(t) + s_3(t) + s_4(t)\right) \quad \text{Eq. 13}$$

Replacing Eq. 11 in Eq. 13, all the terms depending on transitions farther than 2 chips from the considered transition are simplified, leading to Eq. 14

$$CDO_{TM-B}^{rising}(t) = -e(t + T_c) + 2e(t) \quad \text{Eq. 14}$$

The general formulation of the CDO affected by a TM-B is therefore:

$$\boxed{CDO_{TM-B}^{rising} = \begin{cases} -f(t + T_c) & \text{for} -T_c/2 \le t \le 0 \\ -f(t + T_c) + 2f(t) & \text{for } 0 \le t \le T_c/2 \end{cases}} \quad \text{Eq. 15}$$

With $f(t) = 1 - e^{-\sigma t}\left[\cos(2\pi f_d t) + \frac{\sigma}{2\pi f_d}\sin(2\pi f_d t)\right]$

Mixed Failure Model (Threat Model C)

The same approach as for TM-B can be followed for TM-C, except that since the falling edge is offset by Δ, there will not be any simplification of the ringing of the previous transitions when averaging over all possible subsequence.

$$\begin{array}{llllll} \text{for } C_1 = 0001, & s_1(t) = & -e(t + 3T_c - \Delta) & & & +2e(t) \\ \text{for } C_2 = 1001, & s_2(t) = & +e(t + 3T_c) & -2e(t + 2T_c - \Delta) & & +2e(t) \\ \text{for } C_3 = 0101, & s_3(t) = & -e(t + 3T_c - \Delta) & +2e(t + 2T_c) & -2e(t + T_c - \Delta) & +2e(t) \\ \text{for } C_4 = 1101, & s_4(t) = & +e(t + 3T_c) & & -2e(t + T_c - \Delta) & +2e(t) \end{array} \quad \text{Eq. 16}$$

We make the same assumption that there is an equal number of each subsequence in a PRN code.

$$CDO_{TM-C}^{rising} = \frac{1}{2}[e(t + 3T_c) - e(t + 3T_c - \Delta)] + \frac{1}{2}[e(t + 2T_c) - e(t + 2T_c - \Delta)] - e(t + T_c - \Delta) + 2e(t) \quad \text{Eq. 17}$$

In the end, the general formulation of the CDO affected by a TM-C is therefore:

$$\boxed{CDO_{TM-C}^{rising} = \begin{cases} \frac{1}{2}g(t + 3T_c, \Delta) + \frac{1}{2}g(t + 2T_c, \Delta) - f(t + T_c - \Delta) & \text{for} -T_c/2 \le t \le 0 \\ \frac{1}{2}g(t + 3T_c, \Delta) + \frac{1}{2}g(t + 2T_c, \Delta) - f(t + T_c - \Delta) + 2f(t) & \text{for } 0 \le t \le T_c/2 \end{cases}} \quad \text{Eq. 18}$$

With $f(t) = 1 - e^{-\sigma t}\left[\cos(2\pi f_d t) + \frac{\sigma}{2\pi f_d}\sin(2\pi f_d t)\right]$

$g(t, \Delta) = f(t) - f(t - \Delta)$

It is possible to see that the TM-C CDO model makes the use of transitions occurring before the studied transitions. The number of these earlier transitions to be taken into account has been set to 3, by considering a subsequence length of 4 chips. It has been verified that longer subsequence does not bring much difference to the model, even for some worst case ringings with low damping parameters σ.

ACCURACY OF THE CHIP DOMAIN OBSERVABLE

The thermal noise has two effects on the CDO computation:

1. It affects the amplitude of the signal sample.
2. It affects the estimation of the signal parameters that are used for the signal correction and time-stamping.

Both these effects result in an additive error on the actual values of the CDO. This section aims at characterizing the impact of both sources of errors on the CDO, by providing a model of the standard deviation of the CDO.

Impact of the noise present on the IQ samples

The received signal can be modelled as the sum of the GNSS signal and some noise. The noise can be considered as being an Average White Gaussian Noise, with a power that can be deduced from the C/N_0 at the input of the RF front-end:

$$P_n = \sigma_n^2 = \frac{1}{2}.P_s * \frac{f_s}{C/N_0} \quad \text{Eq. 19}$$

Where P_s is the GNSS signal power. In our simulation, $P_s = 1$ W, since the GNSS code chips is generated as a sequence of amplitude +/- 1;
f_s is the sample frequency in Hz;
C/N_0 is the carrier to noise density ratio expressed in Hz (natural scale)

The factor 1/2 comes from the fact that we are looking the noise affecting only one component of the signal (pilot or data, or in-phase or quadrature component).

The technique to obtain the CDO is to resynchronize the samples around a given chip transition type, and to take the average of the samples' values falling into a delay bin.

Therefore, the standard deviation of the noise affecting the CDO is equal to $\sigma_{CDO} = \frac{\sigma_n}{\sqrt{N}}$, where N is the number of samples averaged to obtain the CDO.

N depends on several parameters:

$$N = f_s \Delta_{bin} \frac{T_{int}}{T_{code}} N_{trans} \quad \text{Eq. 20}$$

With the sampling frequency f_s in Hz
the integration time T_{int} in seconds
the code period T_{code} in seconds
the number of transition N_{trans} of the wanted transition type per code period.
the size of the bin Δ_{bin} in seconds

Combining these different formulas, the relative standard deviation of the CDO can be expressed:

$$\frac{\sigma_{CDO}}{\sqrt{P_s}} = \frac{\sigma_n}{\sqrt{NP_s}} = \sqrt{\frac{\frac{1}{2} * f_s}{\frac{C}{N_0} f_s \Delta_{bin} \frac{T_{int}}{T_{code}} N_{trans}}} = \sqrt{\frac{1}{2 \frac{C}{N_0} \Delta_{bin} \frac{T_{int}}{T_{code}} N_{trans}}} \quad \text{Eq. 21}$$

In the case of a filtered signal by an RF front-end bandpass filter for example, the power of the noise is reduced compared to the infinite bandwidth case. The power reduction is equal to f_s/BW, where BW is the bandwidth of the RF filter in Hz. This formula assumes that the power loss on the useful signal is negligible, ie that $BW \gg R_c$.

The formula becomes:

$$\frac{\sigma_{CDO}}{\sqrt{P_s}} == \sqrt{\frac{1}{2 \frac{C}{N_0} \frac{BW}{f_s} \Delta_{bin} \frac{T_{int}}{T_{code}} N_{trans}}} \quad \text{Eq. 22}$$

Impact of tracking error on the CDO accuracy

A tracking error results in a wrong correction of the received samples and of their time stamping. For example, a delay tracking error will result in time stamping the received samples at a wrong instant, therefore offsetting every sample time stamp by the delay tracking error.

However for long integration duration, over 20 ms, different values of estimated signal parameters will be used for the correction and time stamping of each slice of 20 ms of signal. The impact of the tracking errors will therefore be averaged in the final CDO computation.

The tracking error is determined using the formulas found detailed in [6, Chapter 5.6].

The parameters chosen for the tracking loops in the GPS L1 C/A case are summarized in Table 2. The values chosen here have been chosen considering a monitoring receiver in a good environment. Therefore, it is possible to use the full permitted predetection integration time, and narrow loop noise bandwidth.

Table 2 – Tracking loop parameters for GPS L1 C/A

Parameter name		Parameter value
RF Front-end bandwidth	B_{fe}	24 MHz
Predetection integration time	T	20 ms
Discriminator spacing	D	0.1 chip
DLL loop order		1
DLL noise bandwidth	B_n^{DLL}	0.1 Hz
PLL loop order		3
PLL noise bandwidth	B_n^{PLL}	1 Hz
FLL loop order		2
FLL noise bandwidth	B_n^{FLL}	0.1 Hz

Table 3 – Tracking error for GPS L1 C/A

Parameter name		Parameter value	
Signal to noise density ratio	C/N_0	50 dBHz	
Integration time for the computation of the CDO	T_{int}	1s	
DLL error standard deviation	σ_{DLL}	$1.98.10^{-4}$ chip	5.81 cm
PLL error standard deviation	σ_{PLL}	$3.16.10^{-3}$ rad	95.79 µm
FLL error standard deviation	σ_{FLL}	$1.59.10^{-2}$ Hz	3.03 mm/s

The resulting tracking error is given in Table 3. With the parameters chosen for the tracking simulation, the tracking error has a very low amplitude.
Figure 3 shows the resulting normalized standard deviation of the CDO for different CDO computation parameters (T_{int} and C/N_0). For the simulations, the standard deviation was computed by checking the deviation of the CDO between the case with and without tracking loop error for 50 Monte-Carlo simulations. It can be seen that there are no visible differences between the standard deviation of the CDO with or without tracking error. This is due to the fact that the tracking error is very small and therefore has no visible impact on the CDO compared to the effect of noise on the samples.

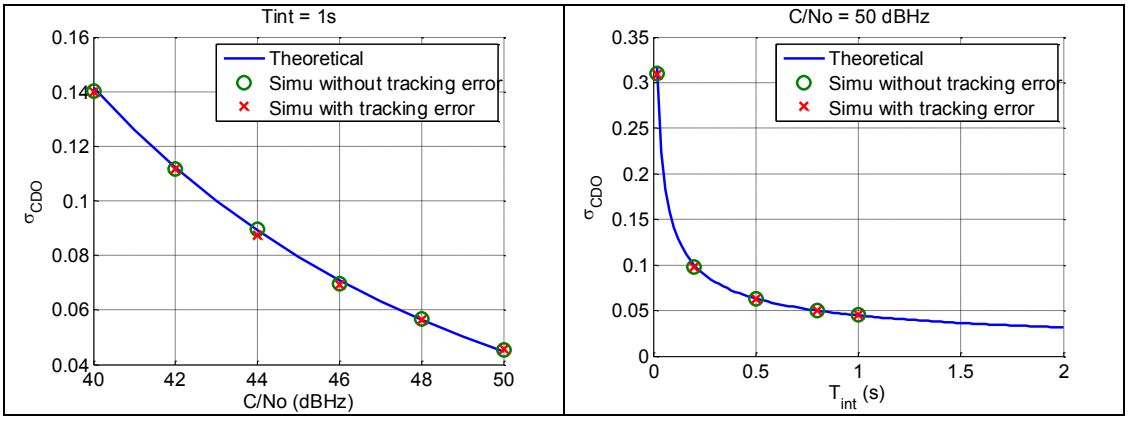

Figure 3 – Comparison of the normalized standard deviation of the CDO without and with a tracking error for different C/N_0 and T_{int}

ILLUSTRATIONS OF CHIP DOMAIN OBSERVABLE DISTRIBUTION

This section aims at illustrating the results obtained by the CDO computation for different scenario.
The scenario parameters are illustrated in Table 4. Figure 4 shows the obtained CDO.

- Scenario #1: no EWF observed with an omnidirectional antenna
- Scenario #2: TM-A observed with a parabolic dish
- Scenario #3: TM-B observed with a parabolic dish
- Scenario #4: TM-C observed with an omnidirectional antenna

The scenarios with a parabolic dish (#2 and #3) benefits from a high C/N_0, corresponding to values observable with a parabola having a diameter of ~1m. This permits to lower the integration time to 20 ms. The scenario with an omnidirectional antenna can provide a similar observation noise by increasing the integration time to 1 s. A front-end filtering was introduced in the scenario without EWF and with a TM-A, in order to make the chip transition smooth, and therefore observable.

Table 4 – Scenario of CDO computation

Parameter name		Scenario #1	Scenario #2	Scenario #3	Scenario #4
Evil Waveform Parameter	Δ σ f_d	- - -	0.12 chip - -	- 2 MNeper/s 8 MHz	0.12 chip 2 MNeper/s 8 MHz
Carrier to noise dentsity ratio	C/N_0	45 dBHz	70	70	45
Front-end bandwidth	BW	24 MHz	24 MHz	∞	∞
Number of delay bins	N_{bins}	100	100	100	100
Integration time	T_{int}	1 s	20 ms	20 ms	1 s

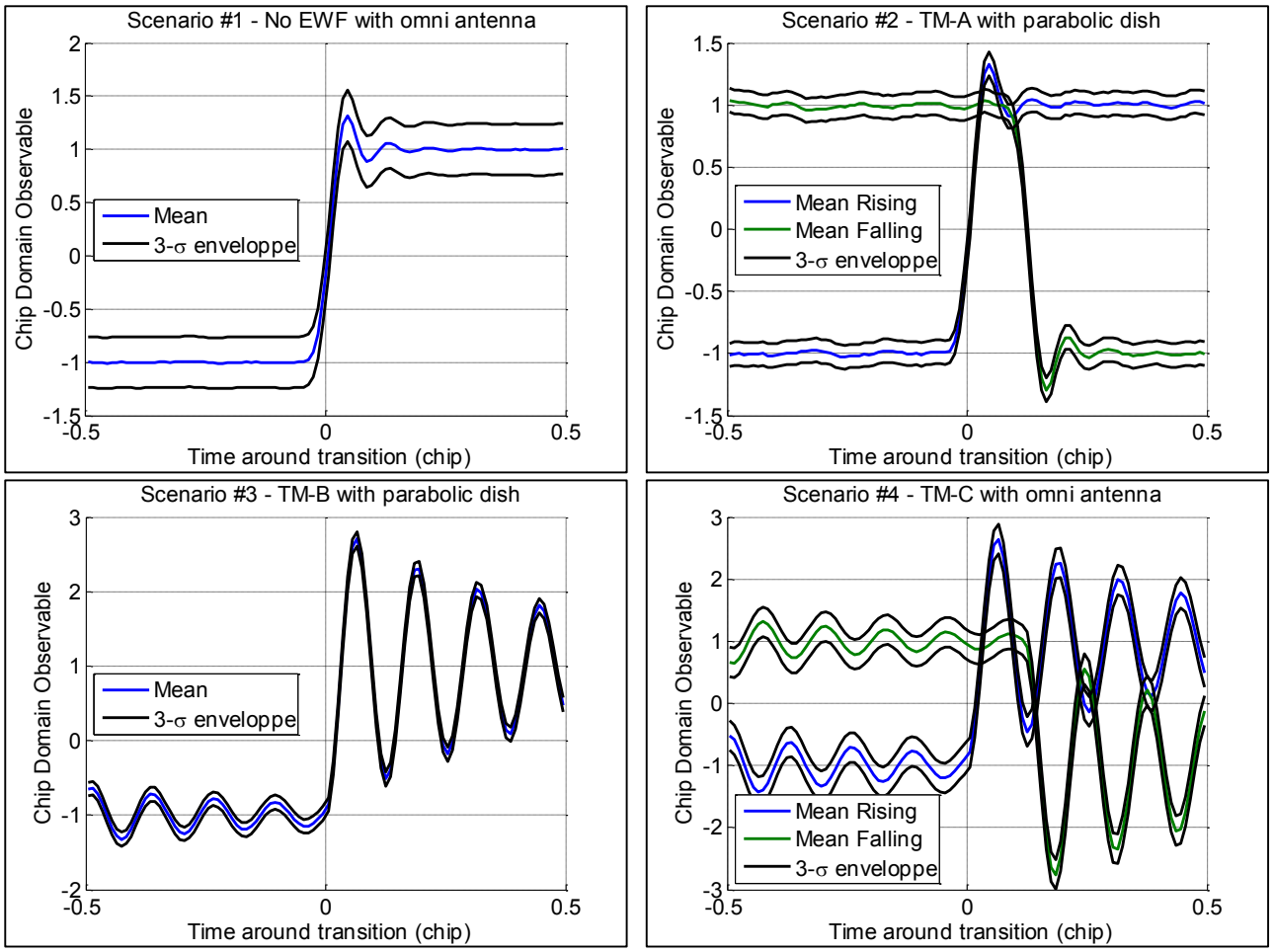

Figure 4 – Illustrations of the observation of Evil Waveforms Threat Models with the Chip Domain Observable

CONCLUSION AND PERSPECTIVES

This paper has presented in details how to process a digitized GNSS signal to obtain the Chip Domain Observable. This type of observable holds interesting promises for the analysis of signal distortions, and hence for the monitoring of Evil Waveforms. The impact of the ICAO Threat Model on the CDO have been established, as well as the distribution characteristics, mainly standard deviation, of the CDO values depending on the conditions of observation and on the parameters of the CDO computation.

While the proposed model has been validated through simulations, to would be interesting to test the CDO computation on recordings of real digitized signals, and to check that the proposed model is valid. Then, a wide array of techniques can be applied to the CDO, to monitor the presence of EWF or to study the nominal deformations of the GNSS signals. The model can serve as a foundation for the determination of the performances of such techniques.

REFERENCES

[1] Brocard P., Thevenon P., Julien O., Salos D., Mabilleau M., "Measurement Quality Assessment in Urban Environments Using Correlation Function Distortion Metrics," Proceedings of ION GNSS+ 2014, Tampa, FL, September 2014.

[2] Edgar C., Czopek F., Barker B., "A Co-operative Anomaly Resolution on PRN-19," Proceedings of the 12th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1999), Nashville, TN, September 1999, pp. 2269-2268.

[3] Fenton, P. C. and J. Jones (2005, September). The theory and performance of NovAtel Inc.'s Vision Correlator. In Proceedings of the ION GPS/GNSS 2005, Palm Springs, CA.

[4] International Standards and Recommended Practices. Annex 10 to. ICAO. 6th Edition. July 2006.

[5] Irsigler, M. and G. W. Hein (2005, September). Development of a Real-Time multipath monitor based on Multi-Correlator observations. In ION GNSS 2005, pp. 2626-2637.

[6] Kaplan E.D., Hegarty C.J., "Understanding GPS: Principle and Applications," 2nd Edition. 2006.

[7] Phelts, R. E. (2001). Multicorrelator techniques for robust mitigation of threats to GPS signal quality (Doctoral dissertation, Stanford University).

[8] P. Thevenon, O. Julien, Q. Tessier, D. Maillard, M. Cabantous, F. Amarillo-Fernández, F. De Oliveria Salgueiro. "Detection Performances of Evil Waveform Monitors for the GPS L5 Signal".Proceedings of ION GNSS+ 2014, Tampa, FL, September 2014.