# Signal Quality Monitoring Aspects in GNSS Signals Affected by Evil Waveforms

Fernando Sousa
*Instituto de Telecomunicações*
*and Instituto Superior de Engenharia de Lisboa*
Lisboa, Portugal
fsousa@isel.pt

Fernando Nunes
*Instituto de Telecomunicações*
*and Instituto Superior Técnico*
Lisboa, Portugal
nunes@lx.it.pt

António Negrinho, Pedro Fernandes, Pedro Boto
*GMV*
Lisboa, Portugal
{anegrinho, pedro.fernandes, pedro.boto}@gmv.com

2022 10th Workshop on Satellite Navigation Technology (NAVITEC) | 978-1-6654-1616-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/NAVITEC53682.2022.9847553

***Abstract*—Evil waveforms (EWF) are anomalies in the GNSS transmitted signals that can degrade significantly the accuracy of the PVT solution. The cross-correlation function of the incoming signal disturbed by EWF distortion and the locally-generated code signal is obtained analytically for threat models TM-A, TM-B and TM-C. These results are useful to evaluate efficiently the performance of EWF detectors, namely the detectability and hazard regions.**

***Index Terms*—evil waveform, threat model, threat space**

## I. Introduction

Evil waveform (EWF) detection comprises algorithms to detect the presence of different types of distortion in the transmitted signals provoked by electric anomalies that occur in the signal generators aboard the GNSS space vehicles [1]-[4]. The processing of EWF distorted signals by the GNSS receiver may lead to a significant loss of accuracy in the PVT solution, thus preventing its utilization in most applications. Three different types of EWFs are usually considered in the literature [1], [3]: threat models TM-A, TM-B and TM-C, which are associated with digital, analog and digital plus analog distortion, respectively. Performance of the EWF detector is measured in terms of probability of missing detection of the signal anomaly after the false alarm probability is pre-defined.

Following [3], [6], the main EWF detection algorithms are based on three tests: $T_1$ (simple ratio), $T_2$ (difference ratio) and $T_3$ (sum ratio), which use a bank of early and late correlators. These tests measure the distortion of the code autocorrelation shape, such as the flatness of the main peak and the correlation asymmetry. Based on the determination of the distorted function, the threat space (TS) EWF detectability and corresponding hazard regions can be calculated resorting to Monte Carlo simulation [13].

The work included in this paper has been supported by the European Space Agency Navigation Innovation and Support Programme (NAVISP), which aims to generate innovative concepts, technologies and system solutions in the wide-field of Positioning, Navigation and Time.



In this work we derive mathematical expressions for the signal cross-correlation functions that are applicable to different threat models and modulations. The result is a significant reduction of the computational effort spent by the semi-analytic Monte Carlo simulations in the different EWF scenarios. A bank of E-L (symmetric) correlators plus a prompt correlator are used together with an algorithm that encompasses the tests based on the simple, difference, and sum ratio metrics.

## II. Threat model A

Threat Model A (TM-A) was originally defined for C/A GPS signals where the positive chips have a falling edge that leads or lags relative to the correct end-time for that chip [7]. This threat model is associated with a failure in the navigation data unit (NDU), the digital partition of the satellite.

### A. Threat model TM-A1

This threat model corresponds to the digital distortion 1 described in [5]: a lead/lag on every falling transitions after modulation by the code signal. For this model of distortion only the lead/lag parameter $d$ is required as the distortion affects the falling transitions of the signal modulated by the code sequence. Typical waveforms for TM-A1 with BOCs$(m,m)$ signals are represented in Fig. 1.

The distorted signal is $\widetilde{s}(t) = s(t) + \epsilon(t)$ where the error signal is

$$\epsilon(t) = \frac{1}{2}[s(t-d) - s(t)][1 + \text{sign}\{s(t-d) - s(t)\}] \quad (1)$$

with $\text{sign}(x)$ equal to $-1$, $0$ and $+1$, if $x < 0$, $x = 0$ and $x > 0$, respectively. Note that, for $|d| > T_c$, the error model (1) may not be realistic. We have

$$\epsilon(t)s(t-\tau) = \frac{1}{2}\Big([s(t-d)-s(t)] + |s(t-d)-s(t)|\Big)s(t-\tau). \quad (2)$$

Define now the cross-correlation operator as

$$R_{xy}(\tau) = \langle x(t)y(t-\tau)\rangle = \frac{1}{T}\int_0^T x(t)y(t-\tau)\,dt \quad (3)$$

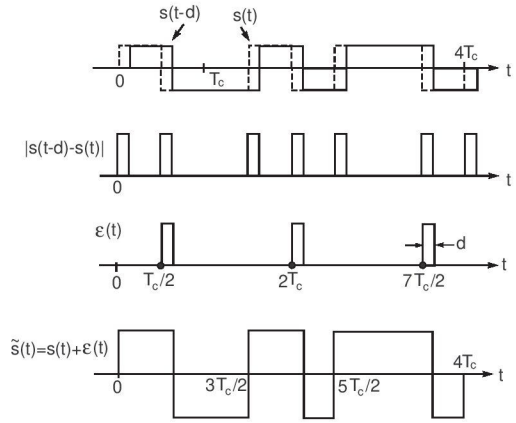



Fig. 1: Typical waveforms for TM-A1 with BOCs$(m,m)$ signals and $|\Delta| \leq T_c$

with $T$ denoting the correlation interval. We obtain by time averaging (2)

$$R_{\epsilon s}(\tau) = \frac{1}{2}R_s(\tau - d) - \frac{1}{2}R_s(\tau) + \frac{1}{2}\langle |s(t-d) - s(t)| s(t-\tau)\rangle \tag{4}$$

where the time autocorrelation of $s(t)$ is

$$R_s(\tau) = \frac{1}{T}\int_0^T s(t)s(t-\tau)\,dt \tag{5}$$

and

$$\begin{aligned}&\langle |s(t-d) - s(t)| s(t-\tau)\rangle = \\ &\langle [s(t-d) - s(t)]s(t-\tau) \times \text{Prob}\{s(t-d) > s(t)\} \\ &- [s(t-d)s(t)]s(t-\tau) \times \text{Prob}\{s(t-d) < s(t)\}\rangle.\end{aligned} \tag{6}$$

But, for practical codes we have $\text{Prob}\{s(t-d) > s(t)\} \approx \text{Prob}\{s(t-d) < s(t)\}$ and

$$\langle |s(t-d) - s(t)| s(t-\tau)\rangle = 0. \tag{7}$$

Thus, $R_{\epsilon s}(\tau) = [R_s(\tau - d) - R_s(\tau)]/2$ and the cross-correlation of $\widetilde{s}(t)$ and $s(t)$ is

$$\begin{aligned}R_{\widetilde{ss}}(\tau) &\equiv \langle \widetilde{s}(t)s(t-\tau)\rangle = \langle [s(t) + \epsilon(t)]s(t-\tau)\rangle \\ &= R_s(\tau) + R_{\epsilon s}(\tau) = \frac{1}{2}\left[R_s(\tau) + R_s(\tau - d)\right].\end{aligned} \tag{8}$$

The cross-spectrum corresponding to $R_{\widetilde{ss}}(\tau)$ is

$$G_{\widetilde{ss}}(f) = \frac{1}{2}G_s(f)[1 + \exp(-j2\pi f d)] \tag{9}$$

where $G_s(f) = \mathcal{F}\{R_s(\tau)\}$ is the power spectrum of $s(t)$, with $\mathcal{F}$ denoting the Fourier transform.

Consider now the effect of lowpass filtering the distorted incoming signal $\widetilde{s}(t)$, as shown in Fig. 2 with $H(f)$ indicating the filter transfer function. The correlator output is given by

$$R_A(\tau) = \frac{1}{T}\int_0^T E\{y(t)g(t-\tau)\}\,dt \tag{10}$$

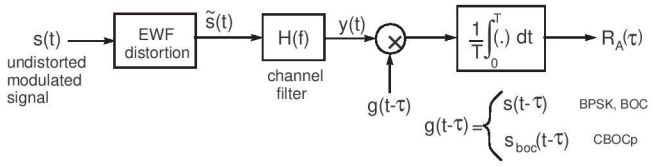



Fig. 2: Cross-correlation of the incoming filtered and distorted signal $y(t)$ with the local non-distorted replica $g(t-\tau)$.

where the average $E\{\cdot\}$ is performed over all the code sequences. The filter output is

$$y(t) = \widetilde{s}(t) * h(t) = \int_{-\infty}^{\infty} \widetilde{s}(\lambda)h(t-\lambda)\,d\lambda \tag{11}$$

where $h(t)$ is the filter impulse response.

The receiver's locally generated signal is

$$g(t-\tau) = \begin{cases} s(t-\tau), & \text{BPSK} \\ s_{BOC}(t-\tau), & \text{BOC, CBOCp.}\end{cases} \tag{12}$$

That is, the correlation is carried out between the distorted and filtered signal and the corresponding locally-generated non-distorted and unfiltered version of the signal but, in the case of transmission of the CBOCpilot signal, we perform instead the correlation with the BOCs(1,1) carrier. Thus

$$\begin{aligned}R_A(\tau) &= \frac{1}{T}\int_0^T \int_{-\infty}^{\infty} h(t-\lambda)E\{\widetilde{s}(\lambda)g(t-\lambda)\}d\lambda dt \\ &= \frac{1}{T}\int_0^T \int_{-\infty}^{\infty} h(\alpha)R_{\widetilde{sg}}(\tau - \alpha)d\alpha\,dt \\ &= R_{\widetilde{sg}}(\tau) * h(\tau)\end{aligned} \tag{13}$$

or in the frequency domain

$$G_A(f) = G_{\widetilde{sg}}(f)H(f). \tag{14}$$

*1) BPSK(m) signals:* Define the triangular pulse $\Lambda_L(x - x_0)$ as

$$\Lambda_L(x - x_0) = \begin{cases} 1 - \frac{|x-x_0|}{L}, & |x - x_0| < L \\ 0, & \text{otherwise}\end{cases} \tag{15}$$

with $L$ denoting the pulse half-duration and $x_0$ its center.

Thus $R_s(\tau) = \Lambda_{T_c}(\tau)$ and

$$R_{\widetilde{ss}}(\tau) = \frac{1}{2}[\Lambda_{T_c}(\tau) + \Lambda_{T_c}(\tau - d)] \tag{16}$$

where $T_c = T_{c0}/m$, $m = 1, 2, \ldots$, is the chip duration of the generic BPSK$(m)$ signal, with $T_{c0} = 10^{-3}/1023$ s denoting the chip duration of the GPS C/A code.

Consider the cross-spectrum (14) with $g(t) = s(t)$. Taking the inverse Fourier transform and using (8) yields

$$\begin{aligned}R_A(\tau) &= \int_{-\infty}^{\infty} G_{\widetilde{ss}}(f)H(f)\exp(j2\pi f\tau)\,df \\ &= \frac{1}{2}\int_{-\infty}^{\infty} G_s(f)[1 + \exp(-j2\pi f d)]H(f)\exp(j2\pi f\tau)\,df.\end{aligned} \tag{17}$$

Henceforth, we will assume that the lowpass filter in the scheme of Fig. 2 is ideal with bandwidth $B$ and zero group delay such that $H(f) = 1$, for $|f| < B$ and 0, otherwise.

Consider that

$$G_s(f) = T_c \,\mathrm{sinc}^2(fT_c) \tag{18}$$

and let $fT_c = x$ (normalized frequency) and $d/T_c = D$ (normalized delay). We obtain

$$\begin{aligned} R_A(\tau) = &\frac{1}{2}\int_{-BT_c}^{BT_c} \mathrm{sinc}^2(x)\cos\left[2\pi\left(\frac{\tau}{T_c}\right)x\right]\,dx \\ &+\frac{1}{2}\int_{-BT_c}^{BT_c} \mathrm{sinc}^2(x)\cos\left[2\pi\left(\frac{\tau}{T_c}-D\right)x\right]\,dx. \end{aligned} \tag{19}$$

The cross-correlation $R_{A,BPSK}(\tau)$ is displayed in Fig. 3 for $BT_c = 1.17$ and different values of $D$. The selected normalized bandwidth $BT_c$ corresponds to a BPSK(10) modulation with a pre-correlation filter of bandwidth $2B = 24$ MHz.

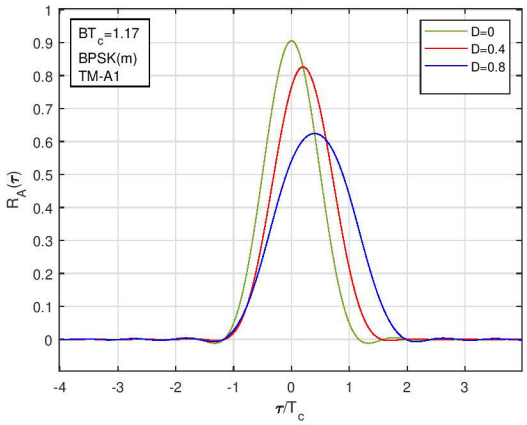



Fig. 3: Cross-correlations $R_A(\tau)$ for $BT_c = 1.17$. Modulation: BPSK($m$).

*2) BOCs($m,m$) signals:* The autocorrelation function for BOCs signals can be expressed in terms of triangular pulses as [11]

$$R_s(\tau) = \Lambda_{T_c/2}(\tau) - \frac{1}{2}\Lambda_{T_c/2}\left(|\tau| - \frac{T_c}{2}\right) \tag{20}$$

with $\Lambda_L(|x| - x_0) = \Lambda_L(x + x_0) + \Lambda_L(x - x_0)$ denoting two triangles centered at positions $\pm x_0$.

The cross-correlation of $\widetilde{s}(t)$ and $s(t)$ may be derived by replacing (20) in (8). That is

$$\begin{aligned} R_{\widetilde{s}s}(\tau) = &\frac{1}{2}\Lambda_{T_c/2}(\tau) - \frac{1}{4}\Lambda_{T_c/2}\left(|\tau| - \frac{T_c}{2}\right) \\ &+\frac{1}{2}\Lambda_{T_c/2}(\tau - d) - \frac{1}{4}\Lambda_{T_c/2}\left(|\tau - d| - \frac{T_c}{2}\right). \end{aligned} \tag{21}$$

From [11] we have for the power spectrum of the BOCs($m,m$) modulation

$$G_s(f) = \frac{T_c}{2}\mathrm{sinc}^2\left(\frac{fT_c}{2}\right)[1 - \cos(\pi f T_c)]. \tag{22}$$

Using now (17) and doing $fT_c = x$ and $d/T_c = D$ leads to

$$\begin{aligned} R_A(\tau) = &\frac{1}{4}\int_{-BT_c}^{BT_c} \mathrm{sinc}^2\left(\frac{x}{2}\right)\cos\left[2\pi\left(\frac{\tau}{T_c}\right)x\right]\,dx \\ &-\frac{1}{8}\int_{-BT_c}^{BT_c} \mathrm{sinc}^2\left(\frac{x}{2}\right)\cos\left[\pi\left(1+\frac{2\tau}{T_c}\right)x\right]\,dx \\ &-\frac{1}{8}\int_{-BT_c}^{BT_c} \mathrm{sinc}^2\left(\frac{x}{2}\right)\cos\left[\pi\left(1-\frac{2\tau}{T_c}\right)x\right]\,dx \\ &+\frac{1}{4}\int_{-BT_c}^{BT_c} \mathrm{sinc}^2\left(\frac{x}{2}\right)\cos\left[2\pi\left(\frac{\tau}{T_c}-D\right)x\right]\,dx \\ &-\frac{1}{8}\int_{-BT_c}^{BT_c} \mathrm{sinc}^2\left(\frac{x}{2}\right)\cos\left[\pi\left(1+\frac{2\tau}{T_c}-2D\right)x\right]\,dx \\ &-\frac{1}{8}\int_{-BT_c}^{BT_c} \mathrm{sinc}^2\left(\frac{x}{2}\right)\cos\left[\pi\left(1-\frac{2\tau}{T_c}+2D\right)x\right]\,dx. \end{aligned} \tag{23}$$

The integrals in (19) and (23) are of the form

$$I(a,b;L) = \int_{-L}^{L} \mathrm{sinc}^2(ax)\cos(bx)\,dx. \tag{24}$$

Expressions are given in [17] that permit to calculate $I(a,b;L)$ using sine integral functions $\mathrm{Si}(\cdot)$. It is shown therein that

$$I(a,b;L) \approx \frac{1}{a}\Lambda_{2\pi a}(b), \quad a > 0. \tag{25}$$

The approximation is good provided that $L \geq 4$ (for $a = 1/2$) or $L \geq 2$ (for $a = 1$).

Fig. 4 shows cross-correlation curves obtained from (23) for different lags $D$ and $BT_c = 10$. Fig. 5 presents the cross-correlation curves for symmetric values of $D$ and $BT_c = 15$.

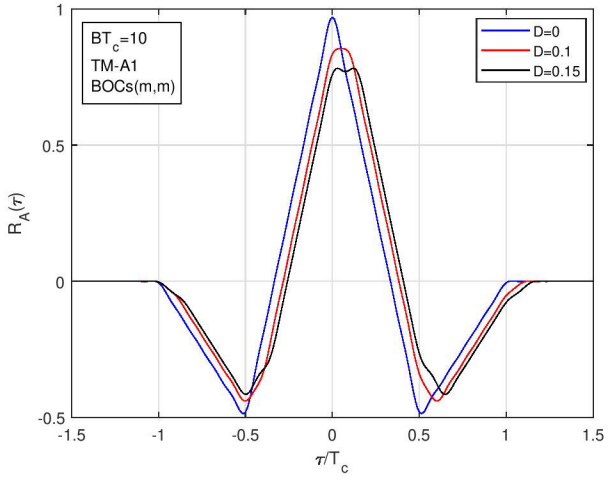



Fig. 4: Cross-correlations $R_A(\tau)$ for different distortion lags $D$ with $BT_c = 10$. Modulation: BOCs($m,m$).

*3) CBOCpilot signal:* The distorted signal is $\widetilde{s}(t) = s_{cboc,p}(t) + \epsilon(t)$ with the CBOC(6,1,1/11) pilot signal being defined by [12]

$$s_{cboc,p}(t) = [\alpha p_{11}(t) - \beta p_{61}(t)]c(t) = \alpha s_{11}(t) - \beta s_{61}(t) \tag{26}$$

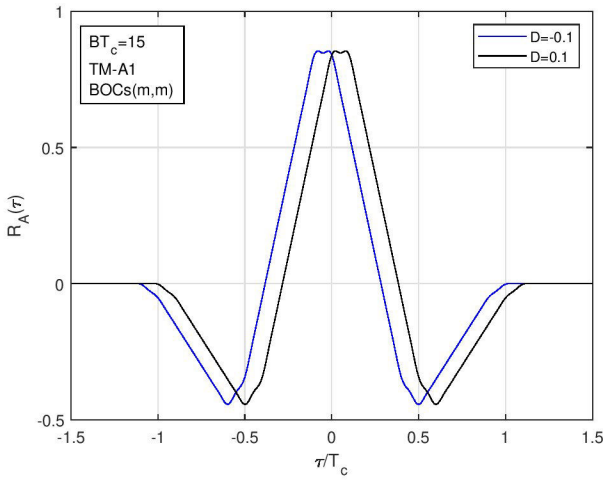



Fig. 5: Cross-correlations $R_A(\tau)$ for $D = \pm 0.10$ with $BT_c = 15$. Modulation: BOCs$(m, m)$.

where $\alpha = \sqrt{10/11}$ and $\beta = \sqrt{1/11}$, $p_{11}(t)$ is the BOCs(1,1) sub-carrier, $p_{61}(t)$ is the BOCs(6,1) sub-carrier, $c(t)$ is the code signal and $s_{11}(t) = c(t)p_{11}(t)$ is the BOCs(1,1) signal. The receiver correlation scheme is the one sketched in Fig. 2 with the local generator given by $s(t-\tau) = s_{11}(t-\tau)$. Notice that this correlation scheme is different from those of the BPSK and BOCs modulations, as the signal of the local oscillator is not a replica of the nominal transmitted signal. The purpose is to simplify the receiver architecture.

It can be shown that

$$\begin{aligned} R_{\widetilde{ss}11}(\tau) &\equiv \langle \widetilde{s}(t) s_{11}(t-\tau) \rangle \\ &= \langle [\alpha s_{11}(t) - \beta s_{61}(t)] s_{11}(t-\tau) \rangle + R_{\epsilon,s11}(\tau) \\ &= \frac{1}{2}\big[\alpha R_{11}(\tau) - \beta R_{61,11}(\tau) \\ &+ \alpha R_{11}(\tau - d) - \beta R_{61,11}(\tau - d)\big]. \end{aligned} \tag{27}$$

The correlations $R_{11}(\tau)$ and $R_{61,11}(\tau)$ can be expressed by the sum of triangle functions. Namely [11]

$$R_{11}(\tau) = \Lambda_{T_c/2}(\tau) - \frac{1}{2}\Lambda_{T_c/2}\left(|\tau| - \frac{T_c}{2}\right) \tag{28}$$

and

$$\begin{aligned} R_{61,11}(\tau) = \frac{1}{12}\Bigg[ &\Lambda_{T_c/12}\left(|\tau| - \frac{T_c}{12}\right) + \Lambda_{T_c/12}\left(|\tau| - \frac{3T_c}{12}\right) \\ &+ \Lambda_{T_c/12}\left(|\tau| - \frac{5T_c}{12}\right) - \Lambda_{T_c/12}\left(|\tau| - \frac{7T_c}{12}\right) \\ &- \Lambda_{T_c/12}\left(|\tau| - \frac{9T_c}{12}\right) - \Lambda_{T_c/12}\left(|\tau| - \frac{11T_c}{12}\right)\Bigg]. \end{aligned} \tag{29}$$

The cross-spectral density corresponding to $R_{\widetilde{ss}11}(\tau)$ is

$$G_{\widetilde{ss}11}(f) = \frac{1}{2}[\alpha G_{11}(f) - \beta G_{61,11}(f)][1 + \exp(-j2\pi f d)]. \tag{30}$$

The cross-correlation at the receiver is

$$\begin{aligned} R_A(\tau) &= \int_{-B}^{B} G_{\widetilde{ss}11}(f) \exp(j2\pi f\tau)\, df \\ &= \frac{\alpha}{2}\int_{-B}^{B} G_{11}(f)\cos(j2\pi f\tau)\, df \\ &+ \frac{\alpha}{2}\int_{-B}^{B} G_{11}(f)\cos(j2\pi f(\tau - d))\, df \\ &- \frac{\beta}{2}\int_{-B}^{B} G_{61,11}(f)\cos(j2\pi f\tau)\, df \\ &- \frac{\beta}{2}\int_{-B}^{B} G_{61,11}(f)\cos(j2\pi f(\tau - d))\, df. \end{aligned} \tag{31}$$

The power spectrum $G_{11}(f)$ is given by [11]

$$G_{11}(f) = T_c\,\mathrm{sinc}^2(fT_c)\tan^2\left(\frac{\pi f T_c}{2}\right). \tag{32}$$

Using (29), the cross power spectrum $G_{61,11}(f)$ results in [11]

$$G_{61,11}(f) = \frac{T_c}{36}\,\mathrm{sinc}^2\left(\frac{fT_c}{12}\right)\frac{\sin^2\left(\frac{\pi f T_c}{2}\right)\sin(\pi f T_c)}{\sin\left(\frac{\pi f T_c}{6}\right)}. \tag{33}$$

Comparing (17) and (31) we can write

$$R_{A,CBOCp}(\tau) = \alpha R_{A,BOC}(\tau) - \beta C(\tau) \tag{34}$$

with $R_{A,BOC}(\tau)$ determined by (23) and

$$\begin{aligned} C(\tau) = &\frac{1}{144}\sum_{i=1}^{3}\int_{-BT_c}^{BT_c} S(x)\cos\left(\frac{\pi(2i-1)x}{6}\right)\Gamma(x)\, dx \\ &- \frac{1}{144}\sum_{i=1}^{3}\int_{-BT_c}^{BT_c} S(x)\cos\left(\frac{\pi(2i+5)x}{6}\right)\Gamma(x)\, dx \end{aligned} \tag{35}$$

where we did $fT_c = x$, $d/T_c = D$, $S(x) = \mathrm{sinc}^2(x/12)$ and $\Gamma(x) = \cos[2\pi x(\tau/T_c)] + \cos[2\pi x(\tau/T_c - D)]$. Fig. 6 exhibits the receiver cross-correlations for CBOC pilot with $BT_c = 15$ and different values of $D$.

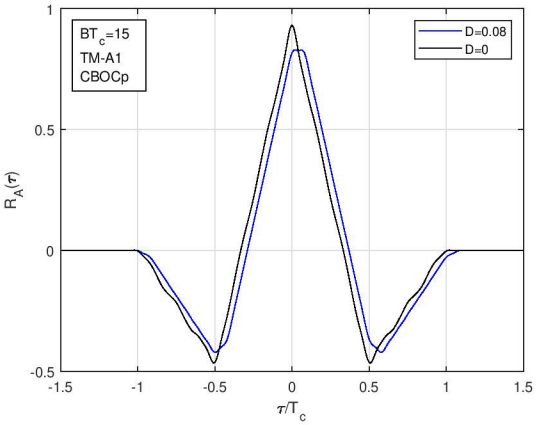



Fig. 6: Cross-correlations $R_A(\tau)$ for $D = 0.08$ and $D = 0$ with $BT_c = 15$. Modulation: CBOCpilot.

*B. Threat model TM-A2*

In this threat model the distortion in the sub-carriers occurs before the modulation by the code signal. It corresponds to the digital distortion 2 described in [5], being applicable to signallings where there is one or more sub-carriers separated from the code signal, namely BOCs$(m,m)$ and CBOCp.

*1) BOCs$(m,m)$ signals:* Let parameter $d_{11}$ express the sub-carrier lead/lag. The distorted sub-carrier is $\widetilde{p}_{11}(t) = p_{11}(t) + \epsilon_{11}(t)$ and the error signal is

$$\epsilon_{11}(t) = \frac{1}{2}[p_{11}(t-d_{11}) - p_{11}(t)][1+\text{sign}\{p_{11}(t-d_{11}) - p_{11}(t)\}]. \tag{36}$$

Note that, for $|d_{11}| > T_c/2$, the error model (36) may not be realistic. The distorted modulated signal is $\widetilde{s}(t) = \widetilde{p}_{11}(t)c(t)$ where $c(t)$ is the code signal. The receiver cross-correlation with the local BOCs signal is $R_{\widetilde{ss}}(\tau) = \langle \widetilde{s}(t)s_{11}(t-\tau)\rangle$ which can be written as

$$R_{\widetilde{ss}}(\tau) = R_{11}(\tau) + \langle \epsilon_{11}(t)c(t)s_{11}(t-\tau)\rangle. \tag{37}$$

It can be shown that $R_{\epsilon,11}(\tau) \equiv \langle \epsilon_{11}(t)c(t)s_{11}(t-\tau)\rangle$ can be expressed as the difference between triangles

$$R_{\epsilon,11}(\tau) = \Lambda_{T_c/2}(\tau - d_{11}) - \Lambda_{T_c/2}(\tau). \tag{38}$$

In the frequency domain (37) can be written as

$$G_{\widetilde{ss}}(f) = G_{11}(f) + G_{\epsilon,11}(f) \tag{39}$$

with $G_{11}(f)$ given by (32). The cross-spectrum $G_{\epsilon,11}(f)$ can be determined from (38), leading to

$$G_{\epsilon,11}(f) = \frac{T_c}{2}\,\text{sinc}^2\left(\frac{fT_c}{2}\right)[\exp(-j2\pi f d_{11}) - 1]. \tag{40}$$

We have, using (39)

$$\begin{aligned} R_A(\tau) \;=\; & 2\int_0^{BT_c} P_1(x)\cos\left(2\pi\frac{\tau}{T_c}x\right)\,dx \\ & + \int_0^{BT_c} P_3(x)\cos\left[2\pi\left(\frac{\tau}{T_c} - \frac{d_{11}}{T_c}\right)x\right]\,dx \\ & - \int_0^{BT_c} P_3(x)\cos\left(2\pi\frac{\tau}{T_c}x\right)\,dx \end{aligned} \tag{41}$$

with

$$P_1(x) \equiv \text{sinc}^2(x)\tan^2\left(\frac{\pi}{2}x\right) \tag{42}$$

and

$$P_3(x) \equiv \text{sinc}^2\left(\frac{x}{2}\right). \tag{43}$$

*2) CBOCpilot signal:* Two parameters are required to express the lead/lag of each sub-carrier: $d_{11}$ and $d_{61}$. These delays are assumed to be independent.

For BOCs(1,1) the distorted sub-carrier is $\widetilde{p}_{11}(t)$ and for BOCs(6,1) the distorted sub-carrier is $\widetilde{p}_{61}(t) = p_{61}(t) + \epsilon_{61}(t)$. The error signals are $\epsilon_{11}(t)$, given by (36), and

$$\epsilon_{61}(t) = \frac{1}{2}[p_{61}(t-d_{61}) - p_{61}(t)][1+\text{sign}\{p_{61}(t-d_{61}) - p_{61}(t)\}]. \tag{44}$$

Note that, for $|d_{61}| > T_c/12$, the error model (44) may not be realistic. The distorted modulated signal is $\widetilde{s}(t) = [\alpha\widetilde{p}_{11}(t) - \beta\widetilde{p}_{61}(t)]c(t)$. The receiver cross-correlation with the local BOCs signal is $R_{\widetilde{sg}}(\tau) = \langle \widetilde{s}(t)s_{11}(t-\tau)\rangle$ which can be written as

$$\begin{aligned} R_{\widetilde{sg}}(\tau) = & \alpha R_{11}(\tau) - \beta R_{61,11}(\tau) + \alpha\langle \epsilon_{11}(t)c(t)s_{11}(t-\tau)\rangle \\ & - \beta\langle \epsilon_{61}(t)c(t)s_{11}(t-\tau)\rangle. \end{aligned} \tag{45}$$

In the frequency domain (45) can be written as

$$G_{\widetilde{sg}}(f) = \alpha G_{11}(f) - \beta G_{61,11}(f) + \alpha G_{\epsilon,11}(f) - \beta G_{\epsilon,61}(f) \tag{46}$$

with $G_{11}(f)$ and $G_{61}(f)$ given, respectively, by (32) and (33). It can be shown that

$$\begin{aligned} R_{\epsilon,61}(\tau) \;=\; & \sum_{i=0}^{5}\Lambda_{T_c/2}(\tau - d_{61} + 5T_c/12 - iT_c/6) \\ & - \Lambda_{T_c/2}(\tau + 5T_c/12 - iT_c/6) \end{aligned} \tag{47}$$

leading to

$$\begin{aligned} G_{\epsilon,61}(f) = & \frac{T_c}{2}\text{sinc}^2\left(\frac{fT_c}{2}\right) \\ & \times \sum_{i=0}^{5}\exp\left[-j2\pi f\left(d_{61} - \frac{5T_c}{12} + i\frac{T_c}{6}\right)\right] \\ & - \exp\left[-j2\pi f\left(-\frac{5T_c}{12} + i\frac{T_c}{6}\right)\right]. \end{aligned} \tag{48}$$

But

$$\sum_{k=0}^{n}\exp(-jkx) = \frac{\sin((n+1)x/2)}{\sin(x/2)}\exp\left(-j\frac{nx}{2}\right) \tag{49}$$

thus

$$G_{\epsilon,61}(f) = \frac{T_c}{2}\,\text{sinc}^2\left(\frac{fT_c}{2}\right)\frac{\sin(\pi fT_c)}{\sin(\pi fT_c/6)}[\exp(-j2\pi f d_{61}) - 1]. \tag{50}$$

Using (46) and doing $fT_c = x$, we have

$$\begin{aligned} R_A(\tau) \;=\; & 2\alpha\int_0^{BT_c} P_1(x)\cos\left(2\pi\frac{\tau}{T_c}x\right)\,dx \\ & - \frac{\beta}{18}\int_0^{BT_c} P_2(x)\cos\left(2\pi\frac{\tau}{T_c}x\right)\,dx \\ & + \alpha\int_0^{BT_c} P_3(x)\cos\left[2\pi\left(\frac{\tau}{T_c} - \frac{d_{11}}{T_c}\right)x\right]\,dx \\ & - \alpha\int_0^{BT_c} P_3(x)\cos\left(2\pi\frac{\tau}{T_c}x\right)\,dx \\ & - \beta\int_0^{BT_c} P_4(x)\cos\left[2\pi\left(\frac{\tau}{T_c} - \frac{d_{61}}{T_c}\right)x\right]\,dx \\ & + \beta\int_0^{BT_c} P_4(x)\cos\left(2\pi\frac{\tau}{T_c}x\right)\,dx \end{aligned} \tag{51}$$

with

$$P_2(x) \equiv \text{sinc}^2\left(\frac{x}{12}\right)\frac{\sin^2(\pi x/2)\sin(\pi x)}{\sin(\pi x/6)} \tag{52}$$

and

$$P_4(x) \equiv \text{sinc}^2\left(\frac{x}{2}\right)\frac{\sin(\pi x)}{\sin(\pi x/6)}. \tag{53}$$

Fig. 7 displays the cross-correlation $R_A(\tau)$ for $d_{11} = 0.15T_c$ and $d_{61} = 0.05T_c$. The cross-correlation for $d_{11} = d_{61} = 0$ is also shown (nominal signal).

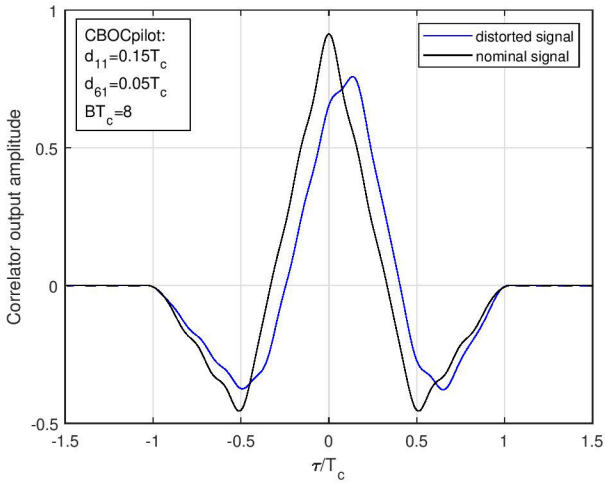



Fig. 7: TM-A2 CBOC(6,1,1/11) pilot with BOCs(1,1) receiver and ideal filtering with $BT_c = 8$.

## III. Threat Model B

Threat Model B (TM-B) introduces amplitude modulation and models degradations in the analog section of a satellite. More specifically, it consists of the output from a second order system when the code modulated baseband signal is the input [7]. The TM-B assumes that the degraded satellite subsystem can be described as a linear system dominated by a pair of conjugate poles. The poles are located at $\sigma \pm j2\pi f_d$, where $\sigma$ is the damping factor in Mnepers/second and $f_d$ is the resonant frequency in MHz.

Consider the transfer function of the second order low-pass filter defined as

$$\widetilde{H}(\omega) = \frac{1}{1-\Omega^2+j2\xi\Omega} = \frac{\exp\left(-j\arctan\frac{2\xi\Omega}{1-\Omega^2}\right)}{\sqrt{(1-\Omega^2)^2+4\xi^2\Omega^2}} \quad (54)$$

with $\Omega \equiv \omega/\omega_n$ and $\omega = 2\pi f$. The impulse response is [15]

$$\widetilde{h}(t) = \begin{cases} \frac{\omega_n}{\sqrt{1-\xi^2}}\exp(-\xi\omega_n t)\sin(\omega_n\sqrt{1-\xi^2}t), & t>0 \\ 0, & \text{otherwise} \end{cases} \quad (55)$$

and the filter response to the step function with discontinuity at $t = 0$, for $t \geq 0$, is

$$\begin{aligned} y(t) &= \int_{-\infty}^{t} \widetilde{h}(\lambda)\, d\lambda \\ &= 1-\exp(-\sigma t)\left[\cos(\omega_d t)+\frac{\sigma}{\omega_d}\sin(\omega_d t)\right] \end{aligned} \quad (56)$$

where the damping factor and the resonant frequency in rad/s are, respectively, $\sigma = \xi\omega_n$ and $\omega_d = \omega_n\sqrt{1-\xi^2}$.

The response $y(t)$ for $t \geq 0$ is shown in Fig. 8 for $f_d = 10.5$ MHz and different values of $\sigma$.

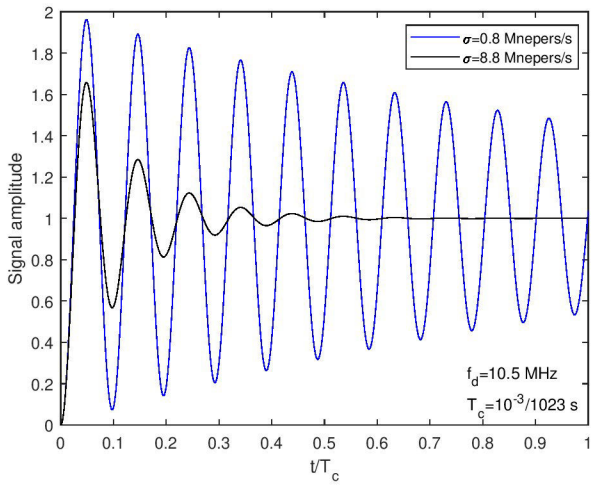



Fig. 8: Filter response to the step function for $f_d = 10.5$ MHz.

The natural frequency and the (normalized) damping factor are, respectively,

$$\omega_n = \sqrt{\sigma^2+\omega_d^2}, \quad \xi = \frac{\sigma}{\omega_n} = \frac{\sigma}{\sqrt{\sigma^2+\omega_d^2}}. \quad (57)$$

Next we present the expressions for the cross-correlation $R_A(\tau)$ obtained in the scenario corresponding to TM-B, i.e.

$$R_A(\tau) = \int_{-B}^{B} G_s(f)\exp(j2\pi f\tau)\widetilde{H}(f)\, df \quad (58)$$

yielding

$$\begin{aligned} R_A(\tau) = &\int_{-B}^{B}\frac{(1-\Omega^2)G_s(f)}{(1-\Omega^2)^2+4\xi^2\Omega^2}\cos(2\pi f\tau)\, df \\ &+2\xi\int_{-B}^{B}\frac{\Omega G_s(f)}{(1-\Omega^2)^2+4\xi^2\Omega^2}\sin(2\pi f\tau)\, df. \end{aligned} \quad (59)$$

### A. BPSK(m) signals

The power spectrum of BPSK signals is given by (18). Replacing that result in (59) and doing

$$\mu \equiv \frac{\omega_n T_c}{2\pi}, \quad \rho \equiv \frac{2\pi B}{\omega_n} \quad (60)$$

we obtain

$$\begin{aligned} R_A(\tau) &= 2\mu\int_0^{\rho}(1-x^2)Q_1(\mu,\xi;x)\cos\left(2\pi\mu\frac{\tau}{T_c}x\right)dx \\ &+ 4\mu\xi\int_0^{\rho}xQ_1(\mu,\xi;x)\sin\left(2\pi\mu\frac{\tau}{T_c}x\right)dx \end{aligned} \quad (61)$$

with

$$Q_1(\mu,\xi;x) \equiv \frac{\mathrm{sinc}^2(\mu x)}{(1-x^2)^2+4\xi^2x^2}. \quad (62)$$

Fig. 9 illustrates the correlation deformation induced by a TM-B distortion. The nominal signal in the figure refers to the cross-correlation in the absence of TM-B distortion which is obtained from (19) with $D = 0$, leading to

$$R_A(\tau) = 2\int_0^{BT_c}\mathrm{sinc}^2(x)\cos\left(2\pi\frac{\tau}{T_c}x\right)dx. \quad (63)$$

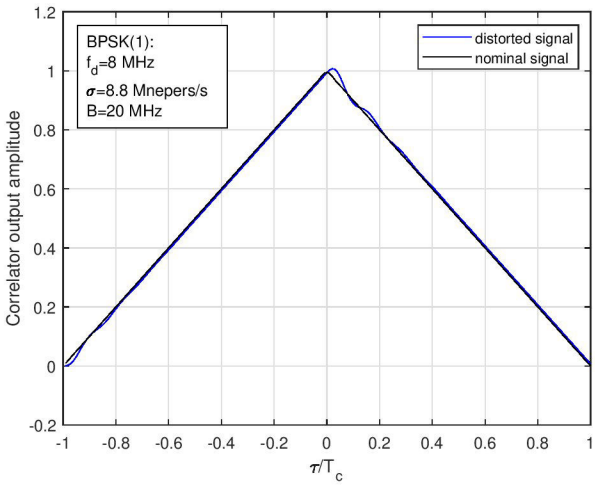



Fig. 9: TM-B distortion for BPSK(1) signals with $f_d = 8$ MHz and $\sigma = 8.8$ Mnepers/s.

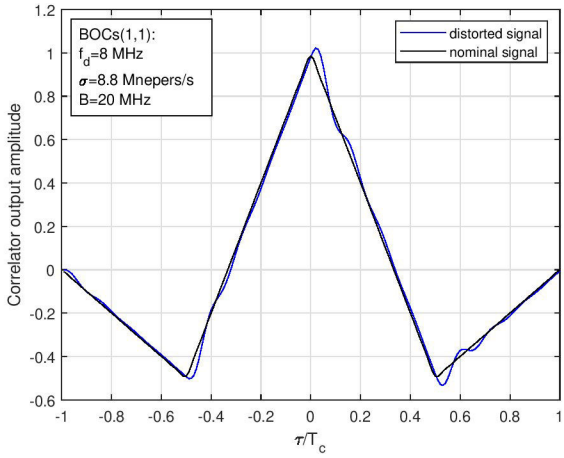



Fig. 10: TM-B distortion for BOCs(1,1) signals with $f_d = 8$ MHz and $\sigma = 8.8$ Mnepers/s.

### *B. BOCs(m,m) signals*

From (22) we have

$$G_s(f) = T_c \,\mathrm{sinc}^2(fT_c)\tan^2\left(\frac{\pi f T_c}{2}\right). \tag{64}$$

Replacing this result in (59) and using (60) leads to

$$\begin{aligned} R_A(\tau) &= 2\mu\int_0^\rho (1-x^2)Q_2(\mu,\xi;x)\cos\left(2\pi\mu\frac{\tau}{T_c}x\right)\,dx \\ &+ 4\mu\xi\int_0^\rho xQ_2(\mu,\xi;x)\sin\left(2\pi\mu\frac{\tau}{T_c}x\right)\,dx \end{aligned} \tag{65}$$

where

$$Q_2(\mu,\xi;x) \equiv \frac{\mathrm{sinc}^2(\mu x)\tan^2\left(\frac{\pi}{2}\mu x\right)}{(1-x^2)^2+4\xi^2x^2}. \tag{66}$$

Fig. 10 illustrates the correlation deformation induced by a TM-B distortion. The nominal signal in the figure refers to the cross-correlation in the absence of TM-B distortion which is obtained from

$$\begin{aligned} R_A(\tau) &= \int_{-B}^{B} G_s(f)\cos(2\pi f\tau)\,df \\ &= 2\int_0^{BT_c}\mathrm{sinc}^2(x)\tan^2\left(\frac{\pi}{2}x\right)\cos\left(2\pi\frac{\tau}{T_c}x\right)\,dx. \end{aligned} \tag{67}$$

### *C. CBOCpilot signal*

For the nominal CBOCpilot signal affected by TM-B distortion we have, using (31) with $d = 0$

$$\begin{aligned} R_A(\tau) &= \alpha\int_{-B}^{B} G_{11}(f)\widetilde{H}(f)\exp(j2\pi f\tau)\,df \\ &- \beta\int_{-B}^{B} G_{61,11}(f)\widetilde{H}(f)\exp(j2\pi f\tau)\,df. \end{aligned} \tag{68}$$

Replacing now (32) and (33) in (68) and defining

$$Q_3(\mu,\xi;x) \equiv \frac{\mathrm{sinc}^2(\mu x/12)\sin^2(\pi\mu x/2)\sin(\pi\mu x)}{\sin(\pi\mu x/6)[(1-x^2)^2+4\xi^2x^2]} \tag{69}$$

leads to

$$\begin{aligned} R_A(\tau) &= 2\alpha\mu\int_0^\rho (1-x^2)Q_2(\mu,\xi;x)\cos\left(2\pi\mu\frac{\tau}{T_c}x\right)\,dx \\ &+ 4\alpha\xi\mu\int_0^\rho xQ_2(\mu,\xi;x)\sin\left(2\pi\mu\frac{\tau}{T_c}x\right)\,dx \\ &- \frac{\beta\mu}{18}\int_0^\rho (1-x^2)Q_3(\mu,\xi;x)\cos\left(2\pi\mu\frac{\tau}{T_c}x\right)\,dx \\ &- \frac{\beta\xi\mu}{9}\int_0^\rho xQ_3(\mu,\xi;x)\sin\left(2\pi\mu\frac{\tau}{T_c}x\right)\,dx. \end{aligned} \tag{70}$$

Fig. 11 illustrates the correlation deformation induced by a TM-B distortion. The nominal signal in the figure refers to the cross-correlation in the absence of TM-B distortion which is obtained from

$$\begin{aligned} R_A(\tau) &= 2\alpha\int_0^B G_{11}(f)\cos(2\pi f\tau)\,df \\ &- 2\beta\int_0^B G_{61,11}(f)\cos(2\pi f\tau)\,df \end{aligned} \tag{71}$$

yielding

$$\begin{aligned} R_A(\tau) &= 2\alpha\int_0^{BT_c}\mathrm{sinc}^2(x)\tan^2\left(\frac{\pi}{2}x\right)\widetilde{\Gamma}(x)\,dx \\ &- \frac{\beta}{18}\int_0^{BT_c}\frac{\mathrm{sinc}^2(x/12)\sin^2(\pi x/2)\sin(\pi x)}{\sin(\pi x/6)}\widetilde{\Gamma}(x)\,dx \end{aligned} \tag{72}$$

with $\widetilde{\Gamma}(x) = \cos(2\pi\tau x/T_c)$.

## IV. Threat Model C

Threat Model C introduces both lead/lag and amplitude modulation. Specifically, it consists of outputs from a second order system when modulated baseband signal suffers from lead or lag. This waveform is a combination of TM-A and TM-B effects [7]. Thus, the main difference between the

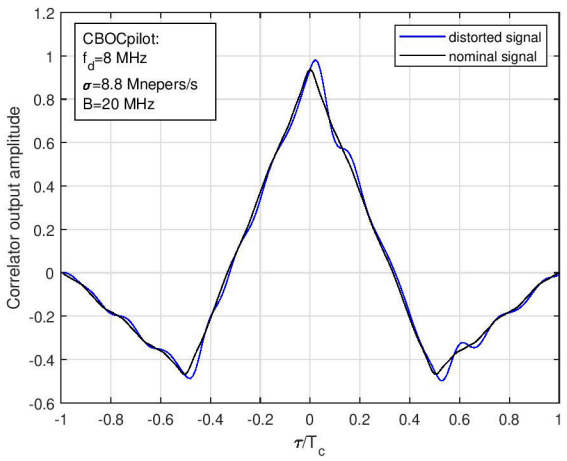



Fig. 11: TM-B distortion for CBOCpilot signal with $f_d = 8$ MHz and $\sigma = 8.8$ Mnepers/s.

expressions obtained in the case of TM-A and those to be derived for TM-C is that, (14) is now replaced by

$$G_A(f) = G_{\widetilde{ss}}(f)H(f)\widetilde{H}(f) \tag{73}$$

where $H(f)$ stands for the channel filter (due essentially to the receiver's front-end filtering effect) and $\widetilde{H}(f)$, given by (54), is due to the degradation introduced in the analog section of the satellite.

## V. Metrics and tests

Consider the scheme of Fig. 12 for the reception of distorted GNSS signals, constituted by early (E), prompt (P), and late (L) correlators. In the figure $r(t)$ is the received signal which includes the GNSS signal of power $P$ and additive white Gaussian noise of power spectral density $N_0/2$. The corresponding carrier-to-noise ratio is $(C/N_0) = P/N_0$. The correlators early-late spacing is $\Delta_{EL}$ and $\epsilon$ denotes the code synchronization error. The baseband signal is

$$y(t) = \sqrt{2P}\widetilde{s}(t) * h(t) + n(t) \tag{74}$$

where $\widetilde{s}(t)$ is the baseband GNSS distorted signal, $h(t)$ is the impulse response of the receiver filter and $n(t)$ is Gaussian lowpass noise with power spectral density

$$G_n(f) = N_0|H(f)|^2 \approx \begin{cases} N_0, & |f| \le B \\ 0, & \text{otherwise} \end{cases} \tag{75}$$

where $2B$ is the front-end filter bandwidth.

The early, prompt and late correlator outputs are the Gaussian random variables (r.v.)

$$Z_E = \overline{Z}_E + n_E, \quad Z_P = \overline{Z}_P + n_P, \quad Z_L = \overline{Z}_L + n_L \tag{76}$$

with expected values

$$\begin{aligned} \overline{Z}_E &= \sqrt{2P}R_A(\epsilon - \Delta_{EL}/2), \\ \overline{Z}_P &= \sqrt{2P}R_A(\epsilon), \\ \overline{Z}_L &= \sqrt{2P}R_A(\epsilon + \Delta_{EL}/2). \end{aligned} \tag{77}$$

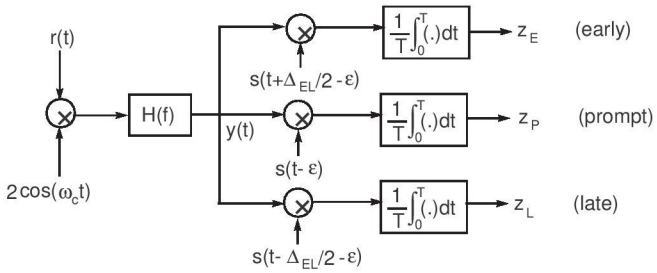



Fig. 12: Receiver with E, P and L correlators.

The cross-correlation $R_A(\cdot)$ takes into account the autocorrelation function of the (baseband) GNSS signal, the distortion due to the EWF and the lowpass filtering effect in the receiver front-end. The additive noises in (76) are defined by

$$\begin{aligned} n_E &= \frac{1}{T}\int_0^T n(t)s(t + \Delta_{EL}/2 - \epsilon)\,dt \\ n_P &= \frac{1}{T}\int_0^T n(t)s(t - \epsilon)\,dt \\ n_L &= \frac{1}{T}\int_0^T n(t)s(t - \Delta_{EL}/2 - \epsilon)\,dt \end{aligned} \tag{78}$$

being correlated, zero-mean, Gaussian r.v., with common variance

$$E\{n_E^2\} = E\{n_P^2\} = E\{n_L^2\} = \sigma_N^2. \tag{79}$$

Since, in general, $2BT \gg 1$, then $E\{n(t)n(\lambda)\} \approx N_0\delta(t-\lambda)$ and

$$\sigma_N^2 \approx \frac{N_0}{T}R_s(0). \tag{80}$$

If the power of the received signal is normalized, i.e., $R_s(0) = 1$ watt, then

$$\sigma_N^2 = \frac{N_0}{T} = \frac{1}{(C/N_0)T} \tag{81}$$

where $(C/N_0)$ is the carrier-to-noise ratio.

Signal Quality Monitoring (SQM) consists of a test to determine if the signal is affected by distortion or not. Consider the hypotheses $H_0$ (signal is not distorted) and $H_1$ (signal is distorted). Let $\mathcal{T}$ denote the test variable. The result of the test is binary: $\mathcal{T} < 1$ (assumes that the signal is not distorted) and $\mathcal{T} \ge 1$ (assumes that the signal is distorted). For a given test we define the following probabilities:

$$\begin{aligned} P_{fa} &= \text{Prob}\{\mathcal{T} \ge 1|H_0\} \text{ (probability of false alarm)} \\ P_{md} &= \text{Prob}\{\mathcal{T} < 1|H_1\} \text{ (probability of missing detection).} \end{aligned}$$

It is not possible to minimize simultaneously $P_{fa}$ and $P_{md}$. An workable solution to this issue is the Neyman-Pearson criterion which consists of fixing $P_{fa}$ at a preselected value and then computing $P_{md}$ [14].

For a given metric $\mu$ the corresponding test variable is defined by

$$\mathcal{T} = \frac{\mu_{\text{mea}} - \mu_{\text{nom}}}{\lambda} \tag{82}$$

where $\mu_{\text{mea}}$ is the measured value of the metric, which is disturbed by thermal noise and may or not be affected by signal distortion (anomaly), $\mu_{\text{nom}}$ is the nominal value of the metric (without additive noise or distortion) and $\lambda$ is a parameter that depends on the desired $P_{fa}$. In practice, $\mu_{\text{nom}}$ may be difficult to determine, being often estimated from the average value of that metric for a given PRN [5], which allows to minimize the effect of thermal noise.

The probabilities of false alarm and missing detection are represented in Fig. 13. The parameter $\lambda$ is adjusted to achieve a certain value of $P_{fa}$. Then, $P_{md}$ is determined from the observations. This probability depends on the amount of distortion of the autocorrelation function, the carrier-to-noise ratio $(C/N_0)$, etc. ICAO [7] defines the Minimum Detectable Error (MDE) as the one that yields $P_{md} = 10^{-3}$ when $P_{fa} = 1.5 \times 10^{-7}$ (see also [1]).

In [5], three tests based on ratio metrics were proposed. The metrics considered are: simple ratio, difference ratio and sum ratio. These metrics will be analyzed next. The ratio tests (or tests based on ratio metrics) attempt specifically to detect the presence of deadzones (flat correlation peaks) and abnormally sharp or elevated correlation peaks [1].

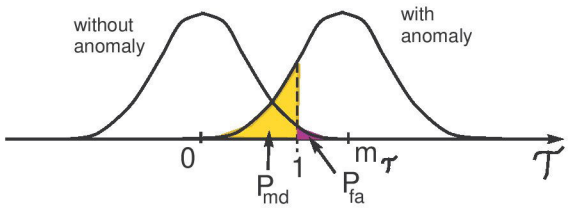



Fig. 13: Probability density functions of the test variable $T_1$ with and without signal anomaly.

To improve the reliability of the SQM tests multiple combinations of pais of correlators will be used with simple ratio, difference ratio and sum ratio metrics, provided the receiver is constituted by a bank of $2N+1$ correlators, with $N > 1$, as sketched in Fig. 14. Pagot [5] has shown that the delay interval of the bank of correlators need not be equal to twice the chip duration ($T_c$). In fact, it is in general enough that $N\Delta \approx 0.25\,T_c$. The reasons for that are:

1) ICAO TM like distortions are more visible around the prompt of the correlation function
2) Correlator outputs situated at a too significant distance from the prompt are more subject to multipath.

The separation $\Delta$ between correlators is typically lower-bounded by $\Delta \approx 10$ ns because:

1) The correlators outputs with very small values of $\Delta$ are strongly correlated (and, thus, redundant) due to the effect of the front-end filter.
2) A time delay of 10 ns between correlators is nowadays reachable but lower values of time delay are more difficult to achieve by ADC converters.

The correlator outputs in the scheme of Fig. 14 are

$$Z_i = \sqrt{2P} R_A(\epsilon - i\Delta) + n_i, \quad i = 0, \pm \ldots, \pm N. \tag{83}$$

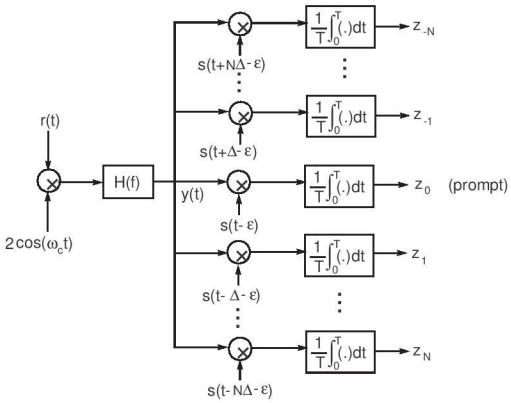



Fig. 14: Receiver with bank of correlators.

The additive noises are

$$n_i = \frac{1}{T}\int_0^T n(t)s(t - i\Delta - \epsilon)\,dt \tag{84}$$

being correlated, zero-mean, Gaussian r.v., with common variance given by (79)

$$E\{n_i^2\} = \sigma_N^2 = \frac{N_0}{T} R_s(0). \tag{85}$$

The covariance matrix of the noise vector $[n_{-N}, \ldots, n_0, \ldots, n_N]^T$ of size $(2N+1) \times (2N+1)$ is

$$\mathbf{C} = \frac{N_0}{T}\begin{bmatrix} 1 & \frac{R_s(\Delta)}{R_s(0)} & \cdots & \frac{R_s(2N\Delta)}{R_s(0)} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{R_s(2N\Delta)}{R_s(0)} & \frac{R_s((2N-1)\Delta)}{R_s(0)} & \cdots & 1 \end{bmatrix}. \tag{86}$$

### A. Simple ratio metric

Assuming that there are $2N+1$ correlators it is possible to form $2N$ simple ratio metrics

$$\mu_1^{(i)} = \frac{Z_i}{Z_0}, \quad i = \pm 1, \ldots, \pm N. \tag{87}$$

In the absence of EWF distortion the tests are expressed by

$$T_1^{(i)} = \frac{\overline{Z}_0 n_i - \overline{Z}_i n_0}{\overline{Z}_0(\overline{Z}_0 + n_0)\lambda_1^{(i)}} \tag{88}$$

having zero means and variances

$$\sigma^2_{T_1^{(i)}} = \frac{(1+\rho_i^2)R_s(0) - 2\rho_i R_s(i\Delta)}{2(C/N_0)TR_A^2(0)[\lambda_1^{(i)}]^2} \tag{89}$$

with

$$\rho_i \equiv \frac{R_A(i\Delta)}{R_A(0)}, \quad i \neq 0. \tag{90}$$

The probability of false alarm of test $i$ is

$$P_{fa}^{(i)} = \text{Prob}\{T_1^{(i)} \geq 1 | H_0\} = Q\left(\frac{1}{\sigma_{T_1^{(i)}}}\right) \tag{91}$$

with $Q(\cdot)$ denoting the error function

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-y^2/2)\, dy. \tag{92}$$

Consider for the sake of simplicity that all the tests are characterized by a common probability of false alarm ($P_{fa}$), that is:

$$P_{fa}^{(i)} = P_{fa} \quad i = \pm 1, \ldots, \pm N. \tag{93}$$

The decision criterion consists of declaring an anomaly if, at least, one of the tests is positive ($T_1^{(i)} \geq 1$).

Taking into account (93) we obtain for each pair of correlators a different value of

$$\lambda_1^{(i)} = \frac{Q^{-1}(P_{FA}/(2N))}{R_A(0)} \sqrt{\frac{(1+\rho_i^2)R_s(0) - 2\rho_i R_s(i\Delta)}{2(C/N_0)T}} \tag{94}$$

where $P_{FA}$ is the overall probability of false alarm and we assume $P_{FA} \approx 2NP_{fa}$, with $2N$ being the number of pairs of Early-Prompt or Prompt-Late correlators; that is, $Q^{-1}(P_{fa}) = Q^{-1}(P_{FA}/(2N))$.

### B. Difference ratio metric

Considering $2N+1$ correlators, i.e., $N$ pairs of early-late correlators, we can form $N$ symmetric difference ratio metrics

$$\mu_2^{(i)} = \frac{Z_{-i} - Z_i}{Z_0}, \quad i = 1, \ldots, N. \tag{95}$$

In the absence of EWF distortion the tests are given by

$$T_2^{(i)} = \frac{n_{-i} - n_i}{(\overline{Z}_0 + n_0)\lambda_2^{(i)}} \tag{96}$$

having zero means and variances

$$\sigma^2_{T_2^{(i)}} = \frac{R_s(0) - R_s(2i\Delta)}{[\lambda_2^{(i)}]^2 (C/N_0) T R_A^2(0)}. \tag{97}$$

The probability of false alarm of test $i$ is

$$P_{fa}^{(i)} = \text{Prob}\{|T_2^{(i)}| \geq 1 | H_0\} = 2Q\left(\frac{1}{\sigma_{T_2^{(i)}}}\right). \tag{98}$$

As in the simple ratio metric we assume that all the tests should by characterized by a common probability of false alarm ($P_{fa}$), that is, $P_{fa}^{(i)} = P_{fa}$. We obtain for each pair of early-late correlators a different value of

$$\lambda_2^{(i)} = \frac{Q^{-1}(P_{FA}/(2N))}{R_A(0)} \sqrt{\frac{R_s(0) - R_s(2i\Delta)}{(C/N_0)T}} \tag{99}$$

where $P_{FA}$ is the overall probability of false alarm.

### C. Sum ratio metric

Considering $2N+1$ correlators, we can form $N$ symmetric sum ratio metrics

$$\mu_3^{(i)} = \frac{Z_{-i} + Z_i}{Z_0}, \quad i = 1, \ldots, N. \tag{100}$$

In the absence of EWF distortion the tests are given by

$$T_3^{(i)} = \frac{n_{-i} + n_i - 2\rho_i n_0}{(\overline{Z}_0 + n_0)\lambda_3^{(i)}} \tag{101}$$

with $\rho_i$ defined in (90). The tests have zero means and variances

$$\sigma^2_{T_3^{(i)}} = \frac{R_s(0) + R_s(2i\Delta) - 2R_s^2(i\Delta)/R_s(0)}{[\lambda_3^{(i)}]^2 (C/N_0) T R_A^2(0)}. \tag{102}$$

The probability of false alarm of test $i$ is

$$P_{fa}^{(i)} = \text{Prob}\{T_3^{(i)} \geq 1 | H_0\} = Q\left(\frac{1}{\sigma_{T_3^{(i)}}}\right). \tag{103}$$

We obtain for each pair of early-late correlators a different value of

$$\lambda_3^{(i)} = \frac{Q^{-1}(P_{FA}/N)}{R_A(0)} \sqrt{\frac{R_s(0) + R_s(2i\Delta) - 2R_s^2(i\Delta)/R_s(0)}{(C/N_0)T}}. \tag{104}$$

## VI. EWF DETECTION BASED ON MULTIPLE TESTS

In the previous section we carried out the analysis of the different tests (single, difference, and sum ratio tests) using a bank of $N$ pairs of correlators. Herein, we propose to apply those tests simultaneously to detect different types of EWF distortion, corresponding to threat models TM-A (digital distortion), TM-B (analog distortion) and TM-C (digital+analog distortion). The modulations considered are BPSK($m$), BOCs($m,m$) and CBOC(6,1,1/11) pilot. When processing the CBOCpilot signal the receiver correlates the received signal with locally-generated BOCs(1,1), as depicted in Fig. 2. Extensive Monte Carlo simulations implemented with parameters belonging to the TM space have shown that, in general, no single test provides a reliable method to detect an EWF anomaly. Consequently, the **global test** implemented (all tests) is a combination of three tests: simple ratio (T1 simple), difference ratio (T2 diff) and sum ratio (T3 sum). The tests, performed with a bank of $N$ pairs of early-late (symmetric) correlators, were adjusted to achieve an overall probability of false alarm $P_{FA} = 1.5 \times 10^{-7}$. The probability is defined as

$$\begin{aligned} P_{FA} = 1 - \text{Prob}\{&T_1^{(-i)} < 1,\, T_1^{(i)} < 1,\, |T_2^{(i)}| < 1,\, T_3^{(i)} < 1, \\ &i = 1, \ldots, N | H_0\} \end{aligned} \tag{105}$$

where $T_k^{(i)}$ denotes the output of test $k$ (with $k = 1, 2, 3$) obtained with the correlator pair of index $i$. For test 1, the index $-i$ refers to an early-prompt pair of correlators and the index $i$ indicates a prompt-late pair.

The thresholds $\lambda_1^{(i)}$, $\lambda_2^{(i)}$ and $\lambda_3^{(i)}$ are computed using, respectively, equations (94), (99) and (104), with $P_{FA}$ replaced with $P_{FA}/3$, as we are assuming that each of the three tests

contributes with one third to the overall probability of false alarm. That is, for test T1:

$$\lambda_1^{(i)} = \frac{Q^{-1}(P_{FA}/(6N))}{R_A(0)} \sqrt{\frac{(1+\rho_i^2)R_s(0) - 2\rho_i R_s(i\Delta)}{2(C/N_0)T}} \quad i = \pm 1, \ldots, \pm N. \tag{106}$$

For test T2:

$$\lambda_2^{(i)} = \frac{Q^{-1}(P_{FA}/(6N))}{R_A(0)} \sqrt{\frac{R_s(0) - R_s(2i\Delta)}{(C/N_0)T}} \quad i = 1, \ldots, N. \tag{107}$$

For test T3:

$$\lambda_3^{(i)} = \frac{Q^{-1}(P_{FA}/(3N))}{R_A(0)} \tag{108}$$

$$\times \sqrt{\frac{R_s(0) + R_s(2i\Delta) - 2R_s^2(i\Delta)/R_s(0)}{(C/N_0)T}}, \quad i = 1, \ldots, N.$$

The overall probability of missing detection is defined as

$$P_{MD} = \text{Prob}\{T_1^{(-i)} < 1,\, T_1^{(i)} < 1,\, |T_2^{(i)}| < 1,\, T_3^{(i)} < 1, \quad i = 1, \ldots, N | H_1\}. \tag{109}$$

In the Monte Carlo simulations next presented we assume ideal code delay synchronization for the DLL using a pair of correlators driven by the values of the EWF-distorted and filtered cross-correlation $R_A(\tau)$. However, we have not included channel (thermal) noise, aiming to simulate the best case of noise reduction introduced by the DLL loop filter. A more in-depth analysis of this topic is addressed, for instance, in [18].

The simulations are divided in three groups according to the type of EWF distortion: TM-A, TM-B and TM-C. We use a central correlator (prompt), aligned with the DLL code synchronization mechanism, and $N$ pairs of early-late correlators with uniform spacing $\Delta$. We assume for the front-end bandwidth and modulations BPSK(1), BOCs(1,1) and CBOCpilot a baseband equivalent bandwidth $B$ with $BT_c = 12$. Besides, we use a DLL early-late spacing equal to $0.1\,T_c$ and $\Delta = 0.02\,T_c$. This spacing between correlators provided the best performance for a wide scope of simulations. For BPSK(10) we use $BT_c = 1.2$, $\Delta = 0.15\,T_c$ and DLL early-late spacing equal to $T_c$.

All the simulations are performed with $C/N_0 = 50$ dB-Hz but different correlation intervals $T$ are used to highlight the regions of the TM space where the anomalies can be successfully detected (with $P_{MD} \leq 10^{-3}$). In general, we used larger correlation (integration) intervals in the cases where the global test is less sensitive to the EWF distortion. Although a single value for the $C/N_0$ is considered, the results can be easily extrapolated to different carrier-to-noise ratios by taking into account that the results should not change provided that the product $(C/N_0)T$ is kept constant. Note, however, that, in practice, this assumption may not be entirely correct as other mechanisms that have to do with code and carrier synchronization make the receiver performance more difficult to establish.

There are different possibilities of analyzing the results provided by the global test. The next subsections display the detectability regions of the EWF anomaly ($P_{MD} < 10^{-3}$) and the hazard regions for a given value of MERR (maximum-allowable error in range) [16]. The hazard region corresponds to the threat space (TS) parameters for which the range error exceeds the MERR value and the EWF anomaly is not detected by the global test. As such, the regions of non-detectability and hazard do not coincide in the diagram of Fig. 15, with the hazard region (dashed pattern) being contained in the region of non-detectability.

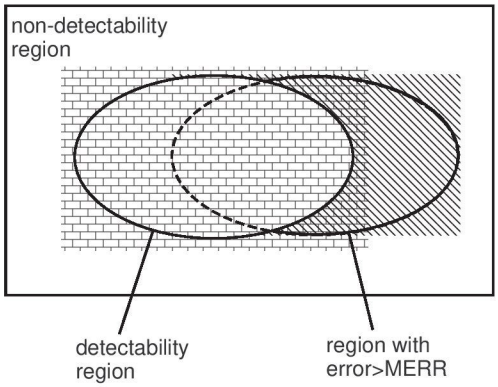



Fig. 15: Diagram showing the relation between detectability and hazard regions.

## VII. Simulation Results

Fig. 16 displays the detectability region (darker color) for TM-A with BPSK(1) versus parameters $D$ and $T$. It can be recognized that the anomaly is not detected for any integration interval (with $T \leq 3$ s) if $D$ is small, with the interval of non-detectability decreasing as the integration interval grows.

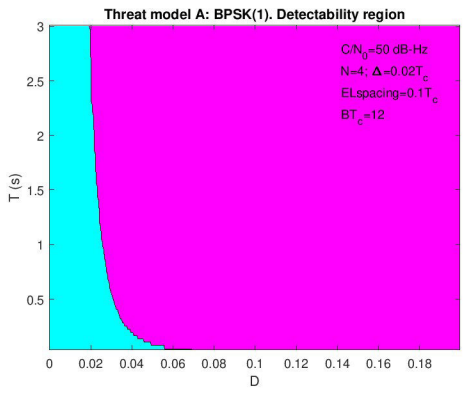
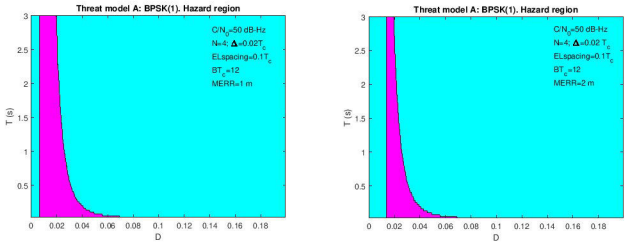



Fig. 16: Detectability region for threat model A with BPSK(1).

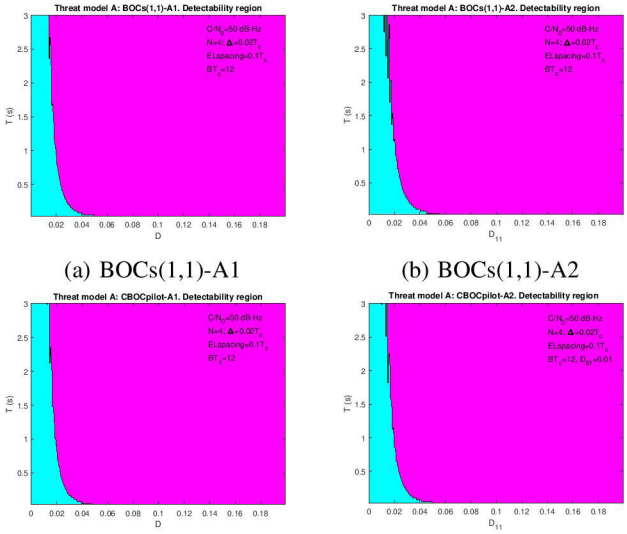
Fig. 17 shows the corresponding hazard regions for MERR values of 1 m and 2 m. As expected, when parameter MERR grows, the range error requirements become looser and the hazard region decreases (the light stripe for small values of $D$ is larger in the right plot).




(a) MERR = 1 m (b) MERR = 2 m

Fig. 17: Hazard regions for threat model A with BPSK(1).

Fig. 18 displays the detectability regions for TM-A1 and TM-A2 with BOCs(1,1) and CBOCpilot modulations. The plots are very similar and exhibit better results (larger detectability areas) than the BPSK(1) case. Fig. 19 presents the corresponding hazard regions for MERR = 1 m (darker color).



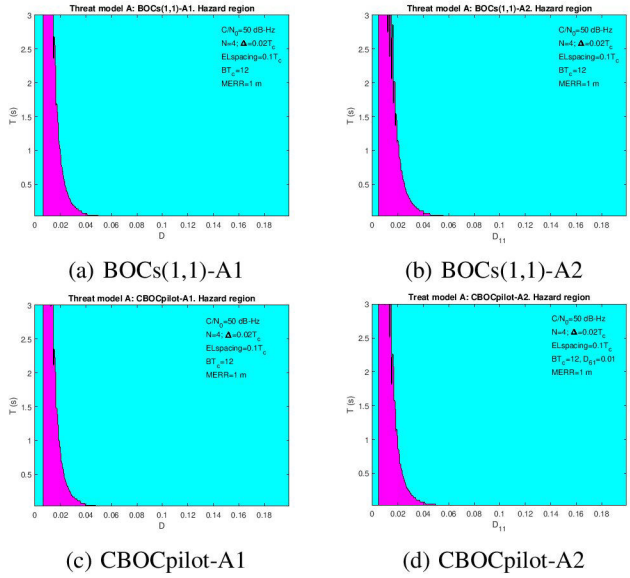

(a) BOCs(1,1)-A1 (b) BOCs(1,1)-A2

(c) CBOCpilot-A1 (d) CBOCpilot-A2

Fig. 18: Detectability regions for threat models A1 and A2 with BOCs(1,1) and CBOCpilot modulations.

Fig. 20 presents the detectability regions (darker color) for BPSK(1), BPSK(10), BOCs(1,1) and CBOCpilot modulations in the TS region $0 < f_d < 20$ MHz and $0 < \sigma < 200$ Mnepers/s with integration interval $T = 3$ s. In all modulations it was observed that the region of detectability increases significantly when the integration interval grows. Besides, the plots reveal that TM-B distortion is more easily detected using BOCs(1,1) or CBOCpilot than BPSK(1), with the performance obtained with BOCs(1,1) and CBOCpilot being approximately the same.

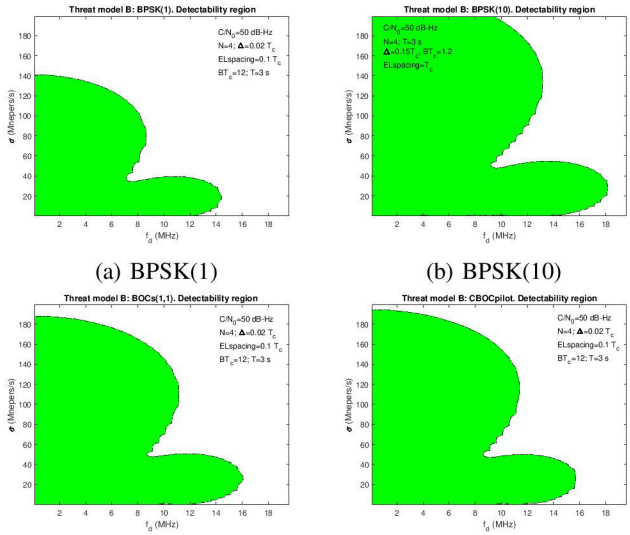
Fig. 21 displays the corresponding hazard regions for $T = 3$ s with MERR = 1 m. For BPSK(1) the code tracking errors in the hazard region may reach values above 5 m. The performance achieved with BPSK(1) is the worst of all the modulations.




(a) BOCs(1,1)-A1 (b) BOCs(1,1)-A2

(c) CBOCpilot-A1 (d) CBOCpilot-A2

Fig. 19: Comparison of hazard regions for threat models A1 and A2 with BOCs(1,1) and CBOCpilot modulations. MERR = 1 m.

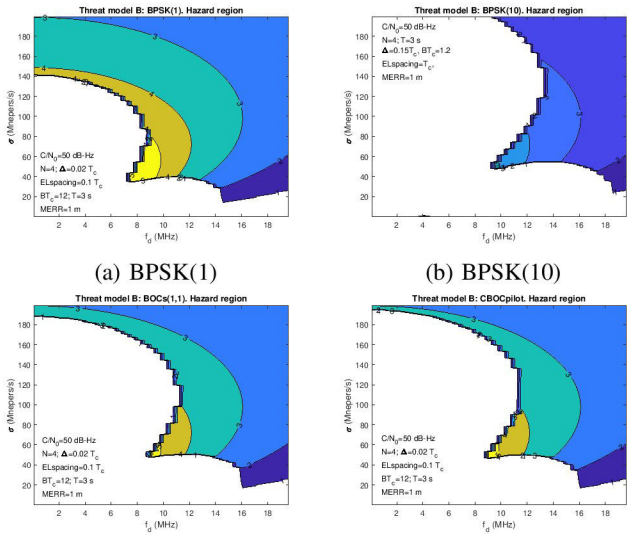



(a) BPSK(1) (b) BPSK(10)

(c) BOCs(1,1) (d) CBOCpilot

Fig. 20: Detectability regions for threat model B with BPSK(1), BPSK(10), BOCs(1,1) and CBOCpilot modulations.

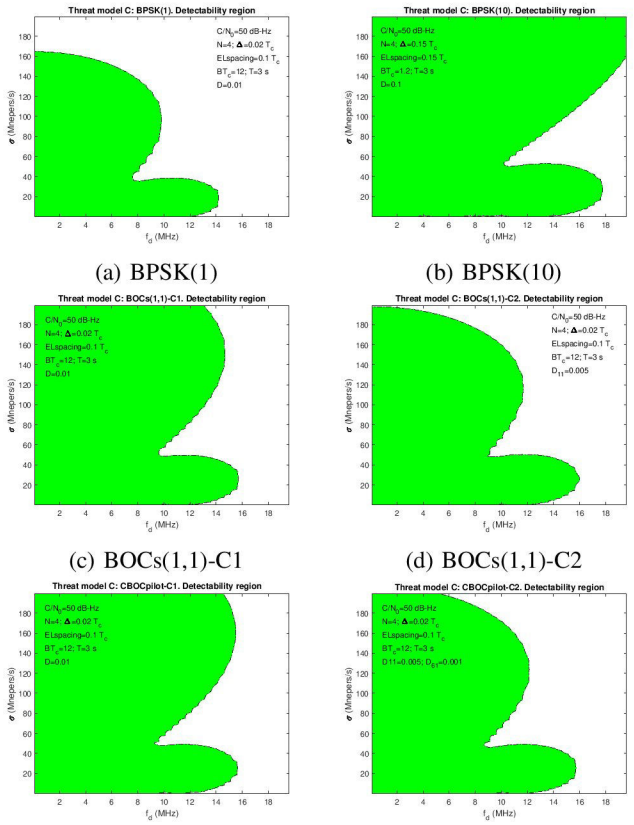
The TM-C encompasses the analog and digital EWF anomalies; so, it is expectable that the effects of the two types of distortions are added. This is corroborated by the simulation results presented next. Comparing Figs. 20 with 22, it can be concluded that the regions of detectability of TM-B are approximately equal or are contained in the regions of TM-C. This effect is more pronounced in the case of the integration interval $T = 3$ s. The expansion of the detectability region is carried out only in the $\sigma$-axis. This means that, whereas for TM-B the tests are insensitive to large values of $\sigma$,




(a) BPSK(1) (b) BPSK(10)

(c) BOCs(1,1) (d) CBOCpilot

Fig. 21: Hazard regions for threat model B with BPSK(1), BPSK(10), BOCs(1,1) and CBOCpilot modulations. $\mathrm{MERR} = 1$ m.




(a) BPSK(1) (b) BPSK(10)

(c) BOCs(1,1)-C1 (d) BOCs(1,1)-C2

(e) CBOCpilot-C1 (f) CBOCpilot-C2

Fig. 22: Detectability regions for threat model C with BPSK(1), BPSK(10), BOCs(1,1) and CBOCpilot modulations.

the detection of anomalies is due, essentially, to the digital distortion component introduced by the TM-A. Compare, for instance, Fig. 20(c) with 22(c)-(d) for BOCs(1,1), or 20(d) with 22(e)-(f) for CBOCpilot.

Observing Figs. 21 and 23 permits to conclude that there is a reduction of the hazard regions by passing from TM-B to TM-C, but for a given pair $(f_d, \sigma)$ in the common hazard region, the code tracking errors are larger in TM-C. The reason is that the addition of digital EWF distortion to the analog distortion causes the growth of the DLL tracking errors (although the capacity of the tests to detect any anomaly also increases).

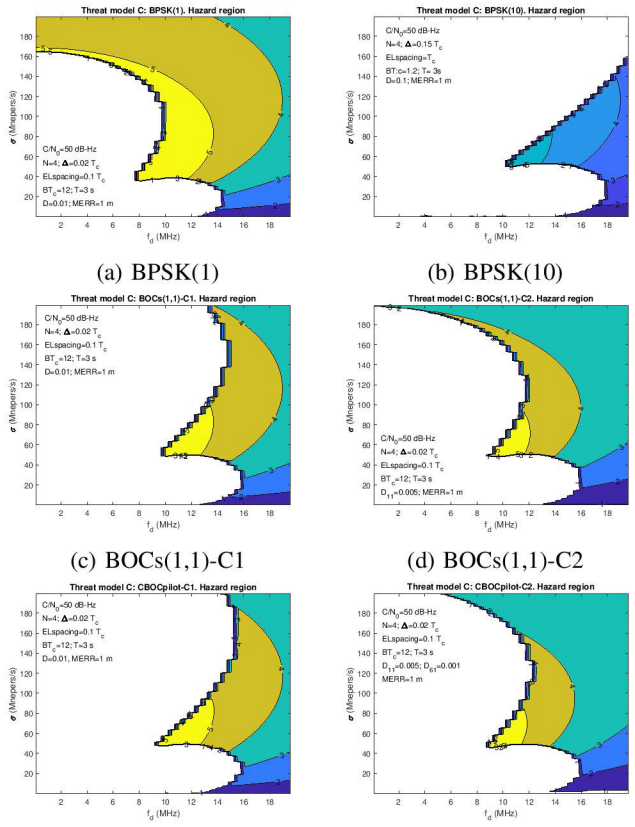
## VIII. Conclusion

The first part of this work consisted of deriving mathematical expressions for the signal cross-correlation functions that are applicable to different threat models and modulations. This aspect is important as it allows to reduce significantly the computational effort spent by the semi-analytic Monte Carlo simulations of the different EWF scenarios, with emphasis on the determination of the detectability and hazard regions of the threat space.

In the second part a bank of $N$ pairs of E-L (symmetric) correlators plus a prompt correlator were used together with an overall test that encompasses the tests based on the simple, difference, and sum ratio metrics. Although the simultaneous use of the three metrics may introduce some degree of redundancy, it avoids the problem of selecting the optimal metric for each type of EWF anomaly as, in general, the nature of the anomalies is not known.

The simulation results obtained permit to draw the following conclusions:

1) The EWF detection performance improves with the number of pairs of correlators $N$ but, for $N > 4$, there is no significant improvement. However, one must be cautious as this condition may not hold in other scenarios.
2) The regions of detectability tend to increase with the growth of the coherent integration interval $T$. In fact, the important parameter to be considered in the performance analysis is the product $(C/N_0)T$. This means that, for small values of $(C/N_0)$, large integration intervals are required. This condition raises multiple design difficulties. Closing the code tracking loops with large intervals is complicated, especially in scenarios with fast-varying Doppler frequency shifts, as happens typically with mobile receivers. Besides, even for large values of $T$ the anomaly detectability is not guaranteed in significant parts of the threat space. In addition, large values of $T$ imply large delays (latency) in the anomaly detection which may not be tolerable in quickly moving receivers. Simulation results were obtained for $T = 100$ ms and $T = 3$ s. Notice that, in general, fixed reference stations permit to use larger integration intervals than mobile receivers because they are not affected by random dynamic stress and the multipath effect is usually reduced.
3) The simulation results previously presented were obtained in relatively benign conditions. Namely, it was




(a) BPSK(1) (b) BPSK(10)

(c) BOCs(1,1)-C1 (d) BOCs(1,1)-C2

(e) CBOCpilot-C1 (f) CBOCpilot-C2

Fig. 23: Hazard regions for threat model C with BPSK(1), BPSK(10), BOCs(1,1) and CBOCpilot modulations. MERR = 1 m.

assumed that the $(C/N_0)$ was known, or at least it could be correctly estimated, and the DLL could determine the position of the prompt correlator without being disturbed by thermal noise and dynamic stress. As such, the results correspond to an upper bound of the expected performance of a real receiver.

4) The simulation results in this research were obtained using a MERR of 1 meter. It was assumed that this is the maximum pseudorange error provoked by an EWF anomaly that can be tolerated. However, changing the MERR value may have a significant impact in the determination of the hazard regions. Thus, for each scenario, a suitable value of MERR should be carefully evaluated taking into account the satellite-user geometry and the desired levels of protection required by the receiver.
5) The usefulness of the EWF detection algorithms may be jeopardized in the presence of multipath, as discussed in [17]. As a consequence, its applicability to mobile receivers in harsh environments is questionable. However, they may still be useful in fixed stations where the multipath may be eliminated or is, at least, well-defined.
6) Given the limitations of the EWF detectors, the aid of other techniques may be necessary, such as the RAIM (receiver autonomous monitoring) techniques that operate at the navigation solution level.
7) An alternative strategy to the direct GNSS signal processing by the mobile vehicle receiver for SQM purpose would be using fixed stations to detect EWF anomalies and broadcasting the SQM status of each satellite to the mobile receiver. The drawback of this solution is the latency of the station-to-receiver link. However, most of the problems that affect the processing of GNSS signals used in SQM could be avoided or minimized: multipath, shadowing and canyon (occultation) effects, besides the part of the random dynamic stress induced by the receiver motion.

## DISCLAIMER

The view expressed herein can in no way be taken to reflect the official opinion of the European Space Agency.

## REFERENCES


[1] R. Phelts, "Multicorrelator techniques for robust mitigation of threats to GPS signal quality," PhD Thesis, Stanford University, June 2001.
[2] P. Thevenon, O. Julien, Q. Tessier, D. Maillard, M. Cabantous, F. Amarillo-Fernández, and F. Oliveira-Salgueiro, "Detection performances of evil waveform monitors for the GPS L5 signal", ION GNSS+ 2014, pp. 3312–3322, Tampa, FL, September 2014.
[3] J. Pagot,"Modeling and monitoring of new GNSS signal distortions in the context of civil aviation", PhD Thesis, MITT, Toulouse, France, December 2016.
[4] I. Selmi, P. Thevenon, C. Macabiau, J. Olivier, and M. Mabilleau, "Signal quality monitoring algorithm applied to Galileo signals for large evil waveform threat space", ION ITM 2020, pp. 352-365, San Diego, CA, January 2020.
[5] J. Pagot, P. Thevenon, O. Julien, F. A. Fernandez, and D. Maillard, "Threat model design for new GNSS signals", ION ITM 2016, pp. 970-982, Monterey, CA, January 2016.
[6] J. Pagot, P. Thevenon, O. Julien, F. A. Fernandez, and D. Maillard, "Signal quality monitoring for new GNSS signals", ION GNSS+, pp. 1750-1763, Portland, OR, September 2016.
[7] ICAO (International Civil Aviation Organization), "Annex 10, Aeronautical Telecommunications, Volume 1 (Radio Navigation Aids)", 7th ed. Montreal: ICAO, July 2018.
[8] J. Proakis and M. Salehi, Digital Communications, 5th ed. Boston, MA: McGraw-Hill, 2008.
[9] M. Abramowitz and I. Stegun (edts), Handbook of Mathematical Functions. New York: Dover, 1970.
[10] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series, and Products. San Diego, CA: Academic Press, 1980.
[11] F. Sousa and F. Nunes, "New expressions for the autocorrelation function of BOC GNSS signals", Navigation, vol. 60(1), pp. 1-9, 2013.
[12] European GNSS (Galileo) Open Service, "Signal-in-Space interface control document", Issue 2.0. European Union, January 2021.
[13] A. Negrinho, P. Fernandes, P. Boto, F. Nunes, and F. Sousa, "Evil waveforms detection solutions for autonomous navigation integrity", ION GNSS+, pp. 4097-4115, September 2021.
[14] S. Kay, Fundamentals of Statistical Signal Processing. Detection Theory. Vol. II. New York: Prentice-Hall, Inc., 1998.
[15] J. D'Azzo, C. Houpis, and S. Sheldon, Linear Control System Analysis and Design with Matlab, 5th ed. New York: Marcel Dekker, 2003.
[16] J. Rife and E. Phelts, "Formulation of a time-varying maximum allowable error for ground-based augmentation systems", ION NTM, pp. 441-453, Monterey, CA, 2006.
[17] F. Nunes and F. Sousa, "Performance of GNSS evil waveform detectors in the presence of multipath", ESA Navitec, April 2022.
[18] M. Vergara, F. Antreich, C. Enneking, M. Sgammini, and G. Seco-Granados, "A model for assessing the impact of linear and nonlinear distortions on a GNSS receiver", GPS Solutions, vol. 24(5), pp. 1-18, 2020.