Quality Monitoring of BOC Signals through Codeless Techniques

Daniele Borio, Marco Rao, Cillian O'Driscoll

Abstract

Codeless and semi-codeless techniques are recently finding new and unexpected applications. For example, they can be used as an effective means for signal authentication and spoofing detection.
In this paper, codeless tracking is adopted for processing Binary Offset Carrier (BOC) modulated signals where a Subcarrier Lock Loop (SLL) is used to remove the subcarrier component. The developed system is then used for signal quality monitoring of encrypted Global Navigation Satellite System (GNSS) signals. In this respect, a multi-correlator codeless architecture and a codeless Carrier-to-Noise density power ratio (C/N_0) estimator are developed and tested under different operating conditions. The effectiveness of the proposed codeless framework is tested using real data collected from the Galileo IOV satellites. The analysis supports the validity of the proposed architecture which enables quality monitoring of encrypted GNSS signals.

Index Terms

Codeless Tracking, Global Navigation Satellite Systems, GNSS, Signal Monitoring, Subcarrier Lock Loop, SLL

I. Introduction

Coexistence between Global Navigation Satellite System (GNSS) and communications services is becoming a more and more significant issue that is gathering the attention of the scientific community. This is due, on one side, to the spectrum scarcity that is pushing communications providers to ask for frequency bands previously reserved for other services. On the other side, new GNSS signals with larger frequency occupations and different centre frequencies are being

Institute for the Protection and Security of Citizen (IPSC), Joint Research Centre, Ispra (VA), Italy. Email: daniele.borio@ieee.org, {marco.rao, cillian.odriscoll}@jrc.ec.europa.eu,

deployed. GNSS services are thus more exposed to interference from communication services operating in the nearby frequencies (Landry and Renard; 1997). An example is the LightSquared case (Burgett and Hokuff; 2011; O'Driscoll et al.; 2012), which generated concern among the GNSS community and pushed several research groups to investigate the impact of such signals. The assessment of the impact of interfering sources is however often limited to Open Service (OS) signals and the analysis of encrypted modulations motivates the development of codeless techniques (Borio; 2011; Woo; 1999) that enable quality monitoring of signals with unknown Pseudo Random Noise (PRN) codes.

Codeless and semi-codeless techniques (Van Dierendonck; 1994) have long been used to obtain measurements from the Global Positioning System (GPS) L2 frequency when only the encrypted P(Y) code was present. In the codeless framework, no a priori information is assumed on the PRN that is used to spread the spectrum of encrypted signals. The unknown code is then removed through non-linear operations such as squaring or cross-correlation with an identical signal from another source (Borio; 2011; Van Dierendonck; 1994). Semi-codeless techniques exploit partial knowledge of the transmitted PRN to reduce the received noise and improve tracking performance. The P(Y) code is, for instance, given by the product of two terms: the Precision (P) code and the W modulation. The P code is known (ARINC Incorporated; 2006) and has a higher rate than the W code. Semi-codeless techniques use the knowledge of the P code to reduce the input noise and improve tracking performance.

Although the availability of new GNSS OS signals makes the use of codeless and semi-codeless techniques no longer required for obtaining measurements from different frequencies, codeless and semi-codeless algorithms are finding new and unexpected applications (O'Hanlon et al.; 2010; Psiaki et al.; 2011). For example, they can be used as an effective means against spoofing attacks even in narrowband receivers not designed for processing the P(Y) signal (O'Hanlon et al.; 2010). In addition to this, new GNSS signals are characterized by the presence of a subcarrier (Betz; 1999) that requires additional processing to avoid potential biases in the delay measurements. The subcarrier presence opens new prospectives for codeless/semi-codeless techniques that can be used to monitor the subcarrier correlation function.

In this paper, codeless techniques are adapted to the Binary Offset Carrier (BOC) modulation. In particular, a Subcarrier Lock Loop (SLL) (Hodgart and Blunt; 2007) is implemented to wipe-off the BOC sub-carrier and to provide a first filtering stage that reduces the input noise. The

remaining unknown PRN and data are removed through squaring. Simplifications based on the availability of OS signals broadcast jointly with the encrypted components are then examined. The main application of the proposed technique aims at monitoring the quality of encrypted GNSS signals. In this respect, a Carrier-to-Noise density power ratio (C/N_0) estimator is implemented and used to assess the impact of interfering signals. The C/N_0 estimator operates on the correlators obtained after squaring and uses a noise floor estimator designed to operate correctly even in the presence of colored interference. More specifically, the C/N_0 estimator is design to provide the effective C/N_0 as defined by Betz (2000, 2001). In this way, the impact of Radio-Frequency (RF) interference can be assessed even if the signal PRN is not available. The proposed codeless framework has been thoroughly characterized and its effectiveness has been supported through Monte Carlo simulations and real data analysis. More specifically, a test setup similar to that adopted by O'Driscoll et al. (2012) has been used to evaluate the effectiveness of the proposed codeless framework. A wideband interference has been added to GPS and Galileo encrypted signals. The Galileo signals were obtained from the GIOVE and In-Orbit Validation (IOV) satellites and subsequently regenerated using a high-fidelity record and playback system. The technique was also applied to signals with a known PRN, thus making possible the comparison between codeless and traditional techniques. The tests confirm the effectiveness of the developed codeless technique.

The remainder of this paper is organized as follows. Section II introduces the signal and system models used in the remainder of the paper whereas the developed codeless architecture is detailed in Section III. Simulation results are provided in Section IV whereas experimental results are analyzed in Section V. Some conclusions are finally drawn in Section VI.

II. Signal and System Model

The signal at the input of a GNSS receiver in a one-path additive Gaussian channel can be modeled as

$$r(t) = \sum_{l=0}^{N_s-1} y_l(t) + \eta(t) \tag{1}$$

which is the sum of N_s useful signals transmitted by N_s different satellites and a noise term, $\eta(t)$.

Each useful signal, $y_l(t)$ can be made of several elements:

$$y_l(t) = \sum_{h=0}^{N_h-1} e_{l,h}(t) \tag{2}$$

where N_h is the number of transmitted components. An example of composite GNSS is the Galileo E1 interplex (Rebeyrol et al.; 2007) which is made of three components: the OS E1b/E1c signals and the Public Regulated Service (PRS) E1a component.

Since all the components in (2) are broadcast by the same satellite, on the same communications channel and at the same time, it is possible to develop processing techniques that exploit phase, frequency and delay relationships between the different signal components.

Each term in (2) can be expressed as

$$e_{l,h}(t) = \sqrt{2C_{l,h}} d_{l,h}\left(t - \tau_{0,l}\right) c_{l,h}\left(t - \tau_{0,l}\right) \cos\left(2\pi(f_{RF} + f_{0,l})t + \varphi_{l,h}\right) \tag{3}$$

where

- $C_{l,h}$ is the power of the hth components of the lth useful signal;
- $d_{l,h}(\cdot)$ is the navigation message;
- $c_{l,h}(\cdot)$ is the pseudo-random sequence extracted from a family of quasi-orthogonal codes and used for spreading the signal spectrum;
- $\varphi_{l,h}$ is phase of the hth components of the lth useful signal;
- $\tau_{0,l}$ and $f_{0,l}$ are the delay and Doppler frequency introduced by the communications channel; these parameters are common to all the signal components in (2);
- f_{RF} is the centre frequency of the GNSS signal.

It is noted that the phase $\varphi_{l,h}$ can be different for each signal component. However, depending on the multiplexing scheme adopted by the transmitter, constant phase relationships can be assumed. In the Galileo E1 interplex, the E1b and E1c components are transmitted in-phase with a 180 degrees phase difference whereas the E1a signal is broadcast in quadrature with a 90 degrees phase offset.

The pseudo-random sequence, $c_{l,h}(t)$, is formed by several terms including a primary spreading sequence and a subcarrier:

$$c_{l,h}(t) = \sum_{i=-\infty}^{+\infty} c_{l,h}\left[i \bmod N_c\right] s_{b,h}(t - iT_h). \tag{4}$$

$s_{b,h}(t-iT_h)$ is the subcarrier of duration T_h which determines the spectral characteristics of the transmitted GNSS signal. The Galileo E1b/E1c signals adopt Composite Binary-Offset Carrier (CBOC) whereas Binary Phase Shift Keying (BPSK) is used for the GPS L1 Coarse/Acquisition (C/A) component. The sequence, $c_{l,h}[i]$, of length N_c defines the primary spreading code of the hth component of the lth GNSS signal. It is noted that, in some case, the sequence $c_{l,h}[i]$ is not known by the receiver and codeless processing has to be employed to recover the useful signal components.

Due to the quasi-orthogonality of the spreading codes, a GNSS receiver is able to process the L useful signals independently. Thus, (1) can be simplified as

$$r(t) = y(t) + \eta(t) = \sum_{h=0}^{N_h-1} e_h(t) + \eta(t) \tag{5}$$

where the index, l has been dropped for ease of notation.

After down-conversion and filtering, the input signal is sampled and quantized. In the following, the impact of quantization and sampling is neglected and, after these operations, (5) becomes:

$$r_{BB}[n] = y_{BB}(nT_s) + \eta_{BB}(nT_s) = y_{BB}[n] + \eta_{BB}[n] = \sum_{h=0}^{N_h-1} e_{BB,h}[n] + \eta_{BB}[n] \tag{6}$$

where the notation $x[n]$ is used to denote a discrete time sequence sampled at the frequency $f_s = \frac{1}{T_s}$. The index "BB" is used to denote a filtered signal down-converted to baseband. It is noted that the front-end filter can introduce small delay/phase variations on the different components, $e_h[n]$. These variations can be become significant when the components, $e_{BB,h}[n]$, have significantly different spectral characteristics and the front-end has a non-linear phase response. These variations will be considered in Section III.

In (6),

$$e_{BB,h}[n] = \sqrt{C_h} d_h\left(nT_s - \tau_0\right) c_h\left(nT_s - \tau_0\right) \exp\left\{j2\pi\left(f_{IF} + f_0\right) nT_s + j\varphi_h\right\}. \tag{7}$$

It is noted that also the different components of $y_{BB}[n]$ are characterized by quasi-orthogonal codes and orthogonal subcarriers. Thus, a GNSS receiver can, in general, process the different components of $y_{BB}[n]$ independently. In the case of interference between different components, the Multiple Access Interference (MAI) cancellation approach suggested by Borio (2011) can be adopted. In the following, the lack of mutual interference among signal components is assumed. More specifically, a single component with unknown primary spreading sequence will

be considered for the derivation of the codeless architecture described in Section III. The presence of additional components with known codes will be exploited for aiding codeless processing. Under this hypothesis, (6) can be further simplified as

$$r_{BB}[n] = \sqrt{C} d\left(nT_s - \tau_0\right) c\left(nT_s - \tau_0\right) \exp\left\{j2\pi\left(f_{IF} + f_0\right) nT_s + j\varphi\right\} + \eta_{BB}[n] \tag{8}$$

where the index h has been removed for ease of notation. Using the multiplicative representation suggested by Anantharamu et al. (2011), (8) can be restated as

$$r_{BB}[n] = \sqrt{C} x_{BPSK}(nT_s - \tau_0) \sum_{i=-\infty}^{+\infty} s_b(nT_s - iT - \tau_0) \exp\left\{j2\pi\left(f_{IF} + f_0\right) nT_s + j\varphi\right\} + \eta_{BB}[n] \tag{9}$$

where $x_{BPSK}[n]$ is a BPSK signal assuming values in $\{-1, 1\}$ with equal probability and modeling the effects of the unknown code and navigation message. In the following, the periodic repetition of the subcarrier will be denoted as

$$\tilde{s}_b(nT_s - \tau_0) = \sum_{i=-\infty}^{+\infty} s_b(nT_s - iT - \tau_0). \tag{10}$$

III. BOC Signal Codeless Tracking

Using an approach similar to that adopted by Borio (2011), it is possible to show that the Maximum Likelihood (ML) estimator for the signal parameters in (9) is given by

$$\left\{\hat{\tau}, \hat{f}_d, \hat{\phi}\right\} = \arg\max_{\tau, f_d, \phi} \Re\left\{\frac{1}{K}\sum_{k=0}^{K-1}\left[\frac{1}{L}\sum_{n=kL}^{(k+1)L-1} r_{BB}[n]\tilde{s}_b(nT_s - \tau)e^{-j[2\pi(f_{IF}+f_d)nT_s+\phi]}\right]^2\right\} \tag{11}$$

where L is the duration of the subcarrier in samples and $K \cdot L$ defines the total number of samples available for parameter estimation. In this case, the delay, τ_0 can be estimated only modulo T, the subcarrier duration. Eq. (11) defines the ML parameter estimator when the noise term in (9), $\eta_{BB}[n]$, is modeled as Gaussian with independent and identically distributed (i.i.d.) samples. It is important to note that the squaring operation in (11) is a complex squaring and *not* the square magnitude.

Maximization in (11) can be performed iteratively using two separate tracking loops that are a form of gradient descent/ascent algorithm (Borio; 2011). In this paper, the architecture depicted in Fig. 1 is suggested. An SLL is used to estimate the subcarrier delay whereas a codeless Phase Lock Loop (PLL) is adopted to determine the residual frequency and phase errors.

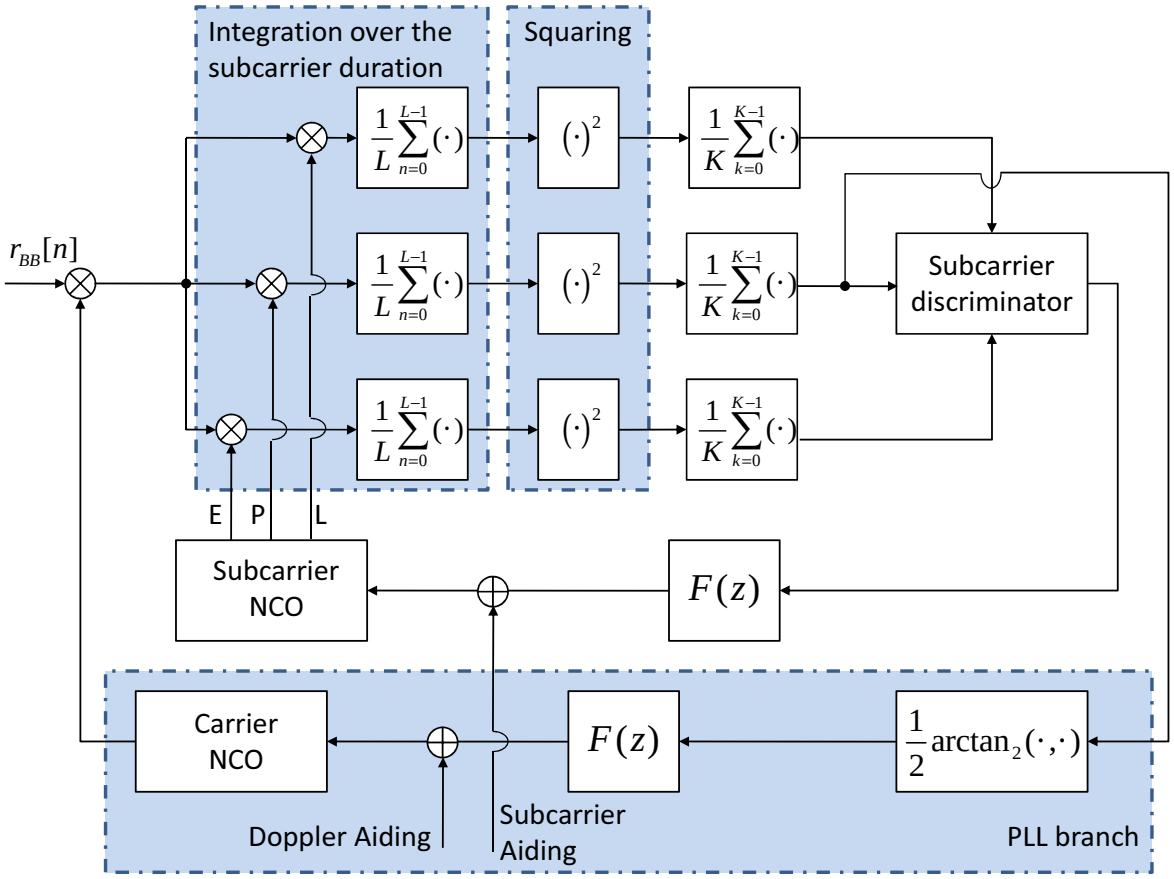

Fig. 1. Codeless tracking of encrypted GNSS signals adopting a BOC modulation. An SLL is used to estimate the subcarrier delay.

The classical SLL proposed by Hodgart and Blunt (2007) has been modified to operate on the correlators obtained through squaring:

$$P_s(\tau) = \frac{1}{K}\sum_{k=0}^{K-1}\left[\frac{1}{L}\sum_{n=kL}^{(k+1)L-1} r_{BB}[n]\tilde{s}_b(nT_s-\tau)e^{-j[2\pi(f_{IF}+f_d)nT_s+\phi]}\right]^2. \tag{12}$$

More specifically, three squaring correlators are computed in correspondence of the delays:

$$\tau = \begin{cases} \hat{\tau}_m - d_s/2 & \text{Early} \\ \hat{\tau}_m & \text{Prompt} \\ \hat{\tau}_m + d_s/2 & \text{Late} \end{cases} \tag{13}$$

where d_s is the Early-minus-Late spacing and $\hat{\tau}_m$ is the best subcarrier delay estimate at the mth processing epoch. The three aforementioned squaring correlators play the same role that

standard Early, Prompt and Late correlators play in standard Delay Lock Loops (DLLs). The correlators are computed using the best signal frequency and phase estimates. In the following the symbols E_s, P_s and L_s are used to denote the Early, Prompt and Late squaring correlators. Squaring correlators are used to compute the delay error that drives the SLL and the generation of the local subcarrier, $\tilde{s}_b(nT_s - \hat{\tau}_m)$. The SLL discriminator and loop filter are standard elements from conventional tracking loops.

The codeless PLL is from the literature (Borio; 2011) and is used to estimated the residual frequency and phase error. It is noted that if frequency/phase estimates from OS signal components are available, they can be used for aiding codeless processing as indicated in Fig. 1. A codeless squaring PLL can be however required to estimate the residual phase offsets mentioned in Section I.

A. Passive Processing and Subcarrier Correlation Monitoring

It is noted that the architecture detailed above has been developed assuming that the signal parameters in (9) are not available to the receiver. However, if other OS components are available, it is possible to estimate τ_0 and f_0 from signals with a known PRN code. In this way, the processing detailed in Fig. 1 can be significantly simplified. For example, the codeless SLL can be removed and the generation of the local subcarrier can be slaved to the delay estimated from OS signals.

If the phase relationship between encrypted and OS components is also known or the phase of the encrypted signal is not required, then codeless processing can be performed in a completely passive way. In this case, also the codeless PLL can be removed and local code and carrier are generated using the parameters of the OS signals. The correlators, $P_s(\tau)$, are computed in a passive way and used for signal quality monitoring rather than as a source of independent measurements as for the GPS L2 P(Y) signal.

A potential application of passive processing is shown in Fig. 2 where a bank of correlators is used to reconstruct the subcarrier squared correlation function for different delays. Monitoring the subcarrier correlation function allows one to detected anomalies in the received signals such as multipath and other signal distortions. The subcarrier correlation function is usually narrower than the correlation of OS signals and allows the resolution of closer multipath rays.

Although the same multi-correlator configuration can be used when the parameters of the

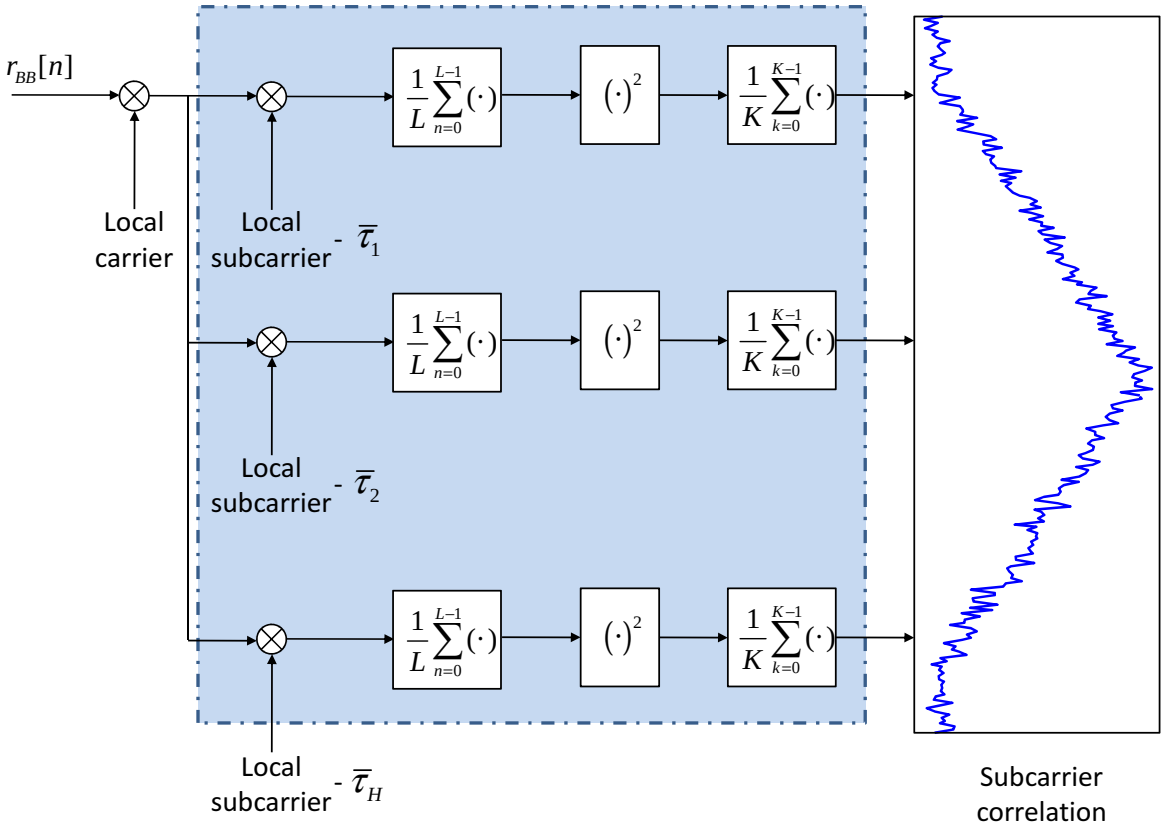

Fig. 2. Multi-correlator configuration for monitoring the subcarrier correlation function.

encrypted signal are actively estimated, passive processing significantly reduces the implementation and computational complexity of the system. An example of the potentialities of this type of approach is shown in Section V where real data, collected from one the first Galileo IOV satellites, are used to demonstrate the utility of the proposed technique.

B. Tracking Jitter

In this section, approximate expressions for the phase and subcarrier tracking jitter are provided. The tracking jitter quantifies the amount of noise transfered from the input signal to the final phase/delay estimate and can be computed as (Van Dierendonck; 1996)

$$\sigma_\phi = \frac{\sigma_d}{G_d}\sqrt{2B_{eq}T_c} = \frac{\sigma_d}{G_d}\sqrt{2B_{eq}KLT_s} \tag{14}$$

where σ_d is the standard deviation of the discriminator output, B_{eq} is the loop equivalent bandwidth and $T_c = KLT_s$ is the loop update interval. G_d is the discriminator gain defined

as

$$G_d = \left. \frac{\partial \mathrm{E}\left[S(\phi)\right]}{\partial \phi} \right|_{\phi=0} \tag{15}$$

where $S(\cdot)$ is the loop discriminator input-output function.

In the following, the same approach adopted by (Borio; 2011) for determining the tracking jitter of squaring and codeless PLLs is used for characterizing the performance of the SLL and PLL described above. The PLL case is considered first.

For the derivation, the input noise in (9), $\eta_{BB}[n]$, is assumed to be a zero mean complex white Gaussian sequence with independent real and imaginary parts. The variance of the real and imaginary parts of $\eta_{BB}[n]$ is given by

$$\sigma^2 = \frac{1}{2} N_0 B_{RX} \tag{16}$$

where N_0 is the Power Spectral Density (PSD) of the input noise and B_{RX} is the two-sided receiver equivalent bandwidth. In the ideal case, $B_{RX} = f_s$.

In order to compute the tracking jitter for the codeless PLL, the results provided in (Borio; 2011) can be exploited. More specifically, it is shown that, for a four-quadrant arctangent PLL, the normalized standard deviation of the discriminator output is given by:

$$\frac{\sigma_d}{G_d} = \frac{1}{2} \sqrt{\frac{R_s + 1}{R_s^2}} \tag{17}$$

where $R_s$is the post-coherent Signal-to-Noise Ratio (SNR) of the signal at the input of the arctangent discriminator defined as

$$R_s = \frac{\left|\mathrm{E}\left[P_s\right]\right|^2}{\frac{1}{2}\mathrm{Var}\left\{P_s\right\}}. \tag{18}$$

The factor $1/2$ in (17) is due to the phase normalization applied at the output of the PLL as shown in Fig. 1. A schematic representation of the different stages of the adopted codeless processing is shown in Fig. 3. Different SNRs can be defined at the different processing stages: R_s is computed after squaring and correlation. Using an approach similar to that adopted by Borio (2011), it is possible to show:

$$\begin{aligned} \left|\mathrm{E}\left[P_s\right]\right|^2 &= C^2 \\ \mathrm{Var}\left\{P_s\right\} &= \frac{8\sigma^2}{KL}\left[C + \frac{\sigma^2}{L}\right] \approx \frac{8\sigma_2^4}{KL^2} \\ R_s &= \frac{C^2}{\frac{4\sigma^2}{KL}\left[C + \frac{1}{L}\sigma^2\right]} \approx \frac{1}{4}\frac{KL^2C^2}{\sigma^4}. \end{aligned} \tag{19}$$

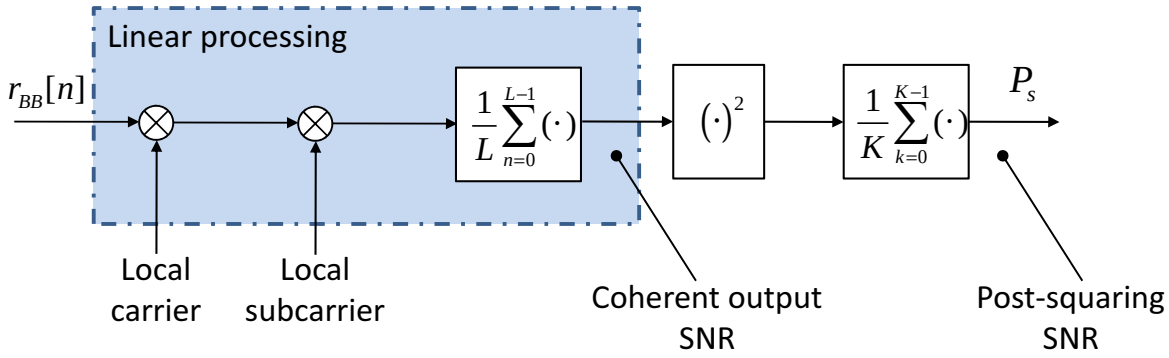

Fig. 3. Schematic representation of the different stages of codeless processing. Different SNRs can be defined at the different processing stages.

Finally, the codeless PLL tracking jitter is given by:

$$\sigma_\phi = \sqrt{\frac{2B_{eq}T_s}{LC^2/\sigma_2^4}\left(1+\frac{4}{KL^2C^2/\sigma^4}\right)}. \tag{20}$$

Assuming an ideal front-end filter and $\sigma^2 = N_0 f_s/2$, (20) further simplifies to

$$\sigma_\phi = \sqrt{\frac{B_{eq}}{2\left(\frac{C}{N_0}\right)^2 T}\left[1+\frac{1}{\left(\frac{C}{N_0}\right)^2 TT_c}\right]}. \tag{21}$$

Expression (21) is similar to the results provided in (Borio; 2011) for the standard squaring PLL. In this case, however, the sampling interval, T_s is replaced by the subcarrier duration, T. The integration over the subcarrier duration reduces the input noise and helps improve the performance of the loop.

The tracking jitter of the SLL strongly depends on the type of discriminator adopted by the loop. Approximate expressions for the tracking jitter for the coherent, quasi-coherent and non-coherent Early-minus-Late power discriminators (Kaplan and Hegarty; 2005) are provided in Table I without proof. The effect of front-end filtering has been neglected and

$$\begin{aligned} R_{sb}(\tau) &= \frac{1}{L}\sum_{n=0}^{L-1}\tilde{s}_b(nT_s)\tilde{s}_b(nT_s-\tau) \\ \dot{R}_{sb}(\tau) &= \frac{\partial R_{sb}(\tau)}{\partial \tau} \end{aligned} \tag{22}$$

TABLE I

APPROXIMATE EXPRESSIONS FOR THE SLL TRACKING JITTER FOR DIFFERENT DISCRIMINATOR TYPES.

Discriminator	**Tracking Jitter**
Coherent $\Re\{E_s - L_s\}$	$\sqrt{\frac{\sigma_s^2 B_{eq} T_c \left[1 - R_{sb}^2(d_s)\right]}{8\left[\dot{R}_{sb}(d_s/2) R_{sb}(d_s/2)\right]^2}}$
Quasi-Coherent Dot Product $\Re\{(E_s - L_s) P_s^*\}$	$\sqrt{\frac{\sigma_s^2 B_{eq} T_c \left[1 - R_{sb}^2(d_s)\right]}{8\left[\dot{R}_{sb}(d_s/2) R_{sb}(d_s/2)\right]^2}(1+\sigma_s^2)}$
Non-coherent Early-minus-Late Power $\lvert E_s\rvert^2 - \lvert L_s\rvert^2$	$\sqrt{\frac{\sigma_s^2 B_{eq} T_c \left[1 - R_{sb}^2(d_s)\right]}{8\left[\dot{R}_{sb}(d_s/2) R_{sb}(d_s/2)\right]^2}\left[1 + \sigma_s^2 \frac{1 + R_{sb}^2(d_s)}{2R_{sb}^4(d_s/2)}\right]}$

denote the periodic subcarrier autocorrelation function and its derivative. σ_s^2 is the normalized variance of the squaring correlators defined as

$$\sigma_s^2 = 8\frac{N_0 B_{RX}}{C \cdot K \cdot L}\left[1 + \frac{N_0 B_{RX}}{C \cdot L}\right] \tag{23}$$

In Section IV, Monte Carlo simulations will be used to support the validity of theoretical results provided above.

C. C/N_0 Estimation

Perhaps the simplest form of signal quality monitoring is the estimation of C/N_0, which is the ratio of the received carrier power, C, to the noise power spectral density, N_0. Note that C is primarily an attribute of the signal in space, while N_0 is an attribute of the receiver. In practice, C is too low to be accurately measured by the receiver without some pre-processing, hence, in GNSS receivers, the C/N_0 is typically estimated at the output of the correlators. The C/N_0 can be obtained by first computing the coherent post-correlation SNR then normalising as follows:

$$\text{SNR} = 2C/N_0 T$$

where T is the coherent integration time. The noise power at the output of the correlators is a function of both the thermal Additive White Gaussian Noise (AWGN) and any coloured noise due, for example, to interference sources. The resulting C/N_0 estimate is a function of the carrier power and the *effective* noise PSD, accounting for both white and coloured noise sources. It is

important to note that the impact of coloured noise on the correlator output is a function of both the noise spectrum and the spectrum of the locally generated replica with which it is correlated.

For signal quality monitoring purposes, it is desired to report the C/N_0 as would be measured by a receiver processing the signals in a traditional, fully code-aware fashion. Note therefore that it is not possible to simply scale the post-squaring SNR. Herein it is proposed to estimate the C/N_0 by estimating C and N_0 independently. The carrier power can readily be estimated from the post-squaring correlator output (19), whereas the estimation of the noise PSD is performed using a separate correlator utilizing a local replica which matches the subcarrier of the desired signal and overlays it with a random spreading code with the same chip rate as the desired signal. Letting $Y[k]$ denote the k^{th} output of this noise-power estimating correlator, then:

$$Y[k] = \frac{1}{N} \sum_{i=kN}^{(k+1)N-1} r_{BB}[i] \tilde{c}\left[i \bmod N\right] \tilde{s}_b(iT_s), \tag{24}$$

where $\tilde{c}[i] \in \{-1, 1\}$ is a random sequence of length N. Note that this correlator operates on the *baseband* signal $r_{BB}[n]$. The effective input noise variance can then be estimated as:

$$\widehat{\sigma^2} = \frac{N \text{Var}\left\{Y[k]\right\}}{2}, \tag{25}$$

assuming that the subcarrier has been normalised to unit power. The normalisation by $N/2$ above accounts for the fact that the variance of the sum of N Gaussian random variables grows linearly with N and that the variance of $Y[k]$ contains contributions from both real and imaginary components. Since $Y[k]$ is a Gaussian random variable, its variance can be estimated in the usual way. The noise PSD can finally be obtained from (16) as:

$$\widehat{N_0} = \frac{2}{f_s} \widehat{\sigma^2} = \text{Var}\left\{Y[k]\right\} T. \tag{26}$$

Finally, following (19), the carrier power can be estimated as:

$$\widehat{C} = \left|\text{E}\left[P_s\right]\right|. \tag{27}$$

Note that the estimation of both C and N_0 require statistical averaging of measurements. The choice of the averaging time is an important one, particularly for the case of carrier power estimation from codeless processing. In this case it is important to average over a sufficiently long period to overcome the losses due to squaring, while at the same time keeping the integration time sufficiently short that changes in carrier power can be observed. In the following an averaging interval of one second is considered, unless otherwise stated.

From a signal monitoring perspective, the estimation of both C and N_0 independently has some advantages. In general there are two sources of degradation to the measured C/N_0: 1) loss of carrier power; 2) increase in effective noise power, due to, for example, thermal effects or RF interference. Estimating the parameters independently allows to determine which type of degradation is being observed.

IV. Simulation Results

In this section, sample simulation results obtained for supporting the theoretical results developed in Section III-B are provided. A system tracking a cosine BOC(15, 2.5) modulation and with the parameters listed in Table II has been considered. The cosine BOC modulation was selected in order to mimic the properties of PRS E1 signals that adopt this modulation.

The PLL and SLL were considered separately. Perfect subcarrier and carrier synchronization was assumed for the PLL and SLL, respectively. The PLL case is considered in Fig. 4 where different equivalent loop bandwidths have been selected. As for the standard PLL case, low B_{eq} values better shield the loop against the input noise at the expense of a reduced reactivity to phase dynamics. As expected and predicted by (20), the PLL performance improves as the loop bandwidth is decreased. In the simulations, relatively low values of B_{eq} have been selected. This choice was dictated by the fact that stable tracking loops can be obtained only for $B_{eq}T_c$ values lower than unity. Squaring causes a significant noise increase and long integrations (T_c of the order of hundreds of ms) have to be adopted to enable loop operations. For this reason, the largest equivalent bandwidth selected for the simulations was equal to 4 Hz. On the other side, Doppler aiding from other OS signal components allows one to significantly reduce the PLL bandwidth. When Doppler aiding is provided only small phase variations between OS and

TABLE II

Parameters adopted for the evaluation of the tracking jitter through simulations.

Parameter	**Value**
Sampling frequency	$f_s = 50$ MHz
Sampling type	Complex I/Q
Total integration time	200 ms
Signal type	BOCc(15, 2.5)

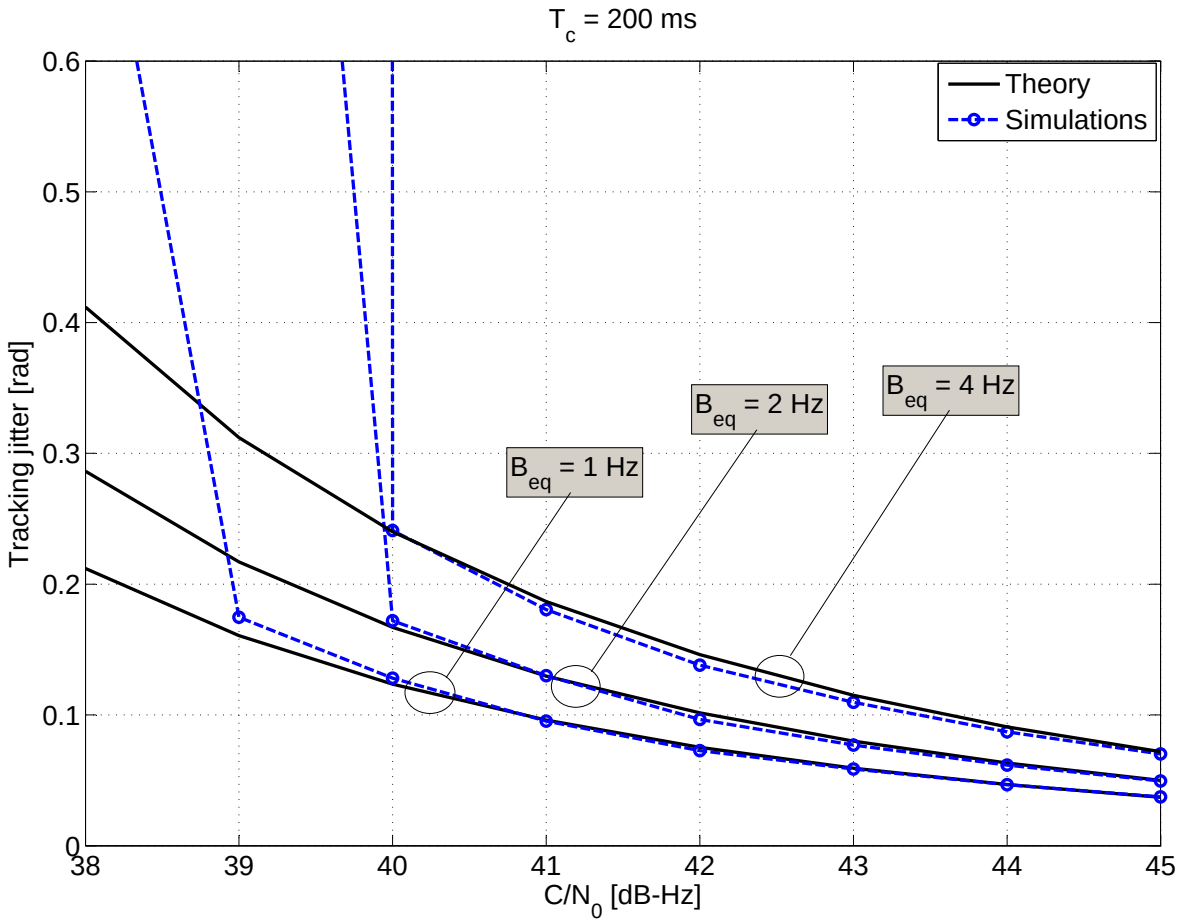

Fig. 4. Tracking jitter obtained for a second order codeless PLL. The vertical jumps in the curves obtained by simulations indicate that the loop loses lock. The simulation parameters are reported in Table II.

encrypted components have to be tracked and thus the input signal dynamics is significantly reduced.

A good agreement between theoretical and simulation results is noted in Fig. 4 for high C/N_0 values. For relatively low C/N_0 values, the curves obtained by simulations diverge. This is due to the fact that the PLL loses lock. Loss of lock is not modeled by (20), which is based on the linear loop theory. With a total integration time, T_c, of 200 ms, the PLL loses lock at C/N_0 values around 40 dB-Hz.

The SLL performance is considered in Fig. 5. In this case, three different loop discriminators (coherent, quasi-coherent and non-coherent Early-minus-Late power) have been considered. As expected the loop performance improves when moving from the non-coherent to the coherent

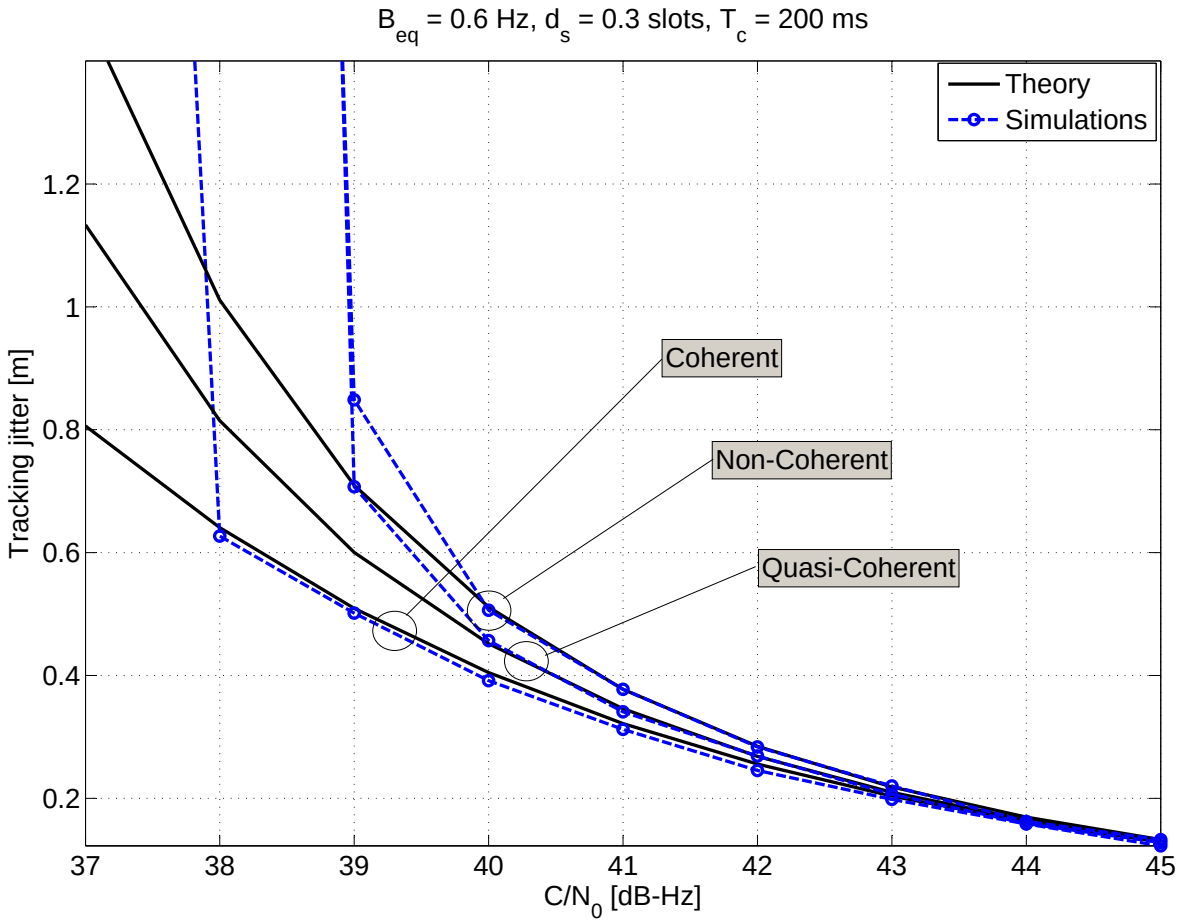

Fig. 5. Tracking jitter for a first order codeless SLL. Different discriminator types have been considered. The vertical jumps in the curves obtained by simulations indicate that the loop loses lock. The simulation parameters are reported in Table II.

discriminator. Also in this case, a good agreement between theoretical and simulation results is found, supporting the validity of the findings provided in Section III-B. From Fig. 5, it emerges that, with the parameters adopted for the simulations, the SLL loses lock for C/N_0 values around 39 dB-Hz. Also in this case, loss of lock is not accounted for by the theoretical formulas provided in Table I.

V. Experimental Results

In order to support the feasibility and show the potentiality of the techniques detailed above, real Galileo data broadcast for the first IOV elements have been collected and processed with a software receiver developed in MATLAB. For the data collection, a National Instruments

TABLE III

PARAMETERS USED FOR THE COLLECTION OF GALILEO E1A DATA.

Parameter	Value
Sampling frequency	$f_s = 40$ MHz
Signals	Galileo E1
Signal centre frequency	1575.42 MHz
Intermediate frequency	0 Hz
Sample type	Complex I/Q
Bits per sample	16

(NI) PXIe-5663 vector signal analyzer was used. The NI data acquisition board was configured according to the parameters listed in Table III where a sampling frequency large enough to capture the full E1 interplex modulation (Rebeyrol et al.; 2007) was selected. The code of the E1a component of the interplex modulation is not public and codeless processing was tested on this signal. The E1b and E1c components are OS and were used either for aiding codeless processing, as indicated in Fig. 1, or for implementing the passive architecture depicted in Fig. 2. Data from the GIOVE-B satellite were also collected and used for comparison purposes. Since the code of the GIOVE-B E1a component is available, it is possible to use both codeless and standard processing on this signal. The same parameters used for the collection of IOV data were used for GIOVE-B signals. Sample results obtained processing GIOVE and IOV signals are provided in the following.

The effectiveness of the codeless approach described in Section III has been at first tested using data from the GIOVE-B satellite. The E1a signal has been processed using the squaring SLL/PLL depicted in Fig. 1. The squaring correlators and the output of the noise estimator described in Section III-C have then been used to compute the C/N_0 of the E1a signal. A total integration time equal to 1 second was used. The same dataset was processed using standard code-aware tracking loops. The C/N_0 was estimated using the algorithm described by Badke (2009). Also in this case, a total integration time equal to 1 second was used.

The C/N_0 estimates obtained using these two approaches are depicted in Fig. 6 which shows the ability of codeless techniques to provide results similar to those obtained using standard processing. As expected, codeless C/N_0 estimates are noisier than their code-aware counterparts.

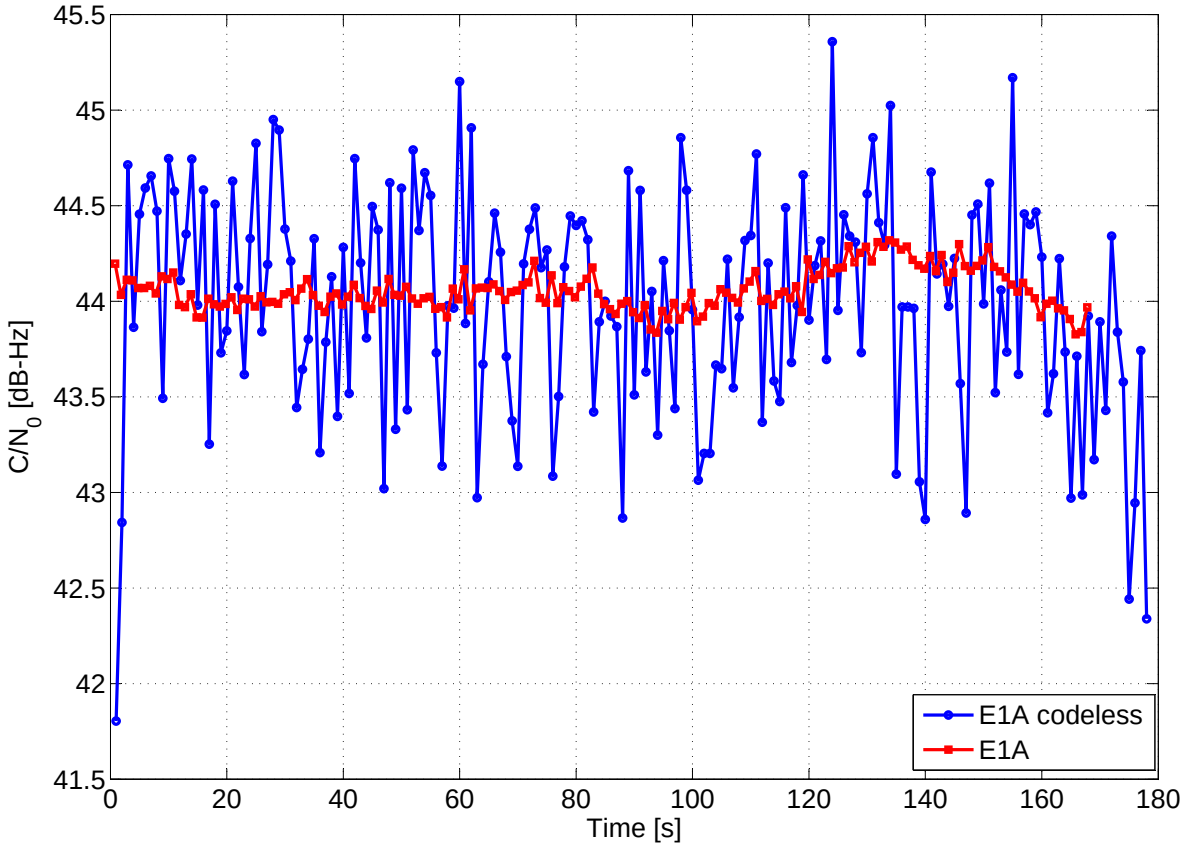

Fig. 6. Comparison between the C/N_0 values estimated using codeless and standard approaches for the E1a signal broadcast by the GIOVE-B satellite.

This is due to the noise amplification caused by the squaring operation. When used as lock indicators, the codeless C/N_0 estimates shown in Fig. 6 confirm the ability of codeless techniques to track signals with a moderate to high C/N_0.

Additional tests have been conducted using signals from the IOV element PRN 11. Samples results are shown in Fig. 7 where the multi-correlator architecture described in Section III-A is considered. More specifically, a bank of 21 passive squaring correlators has been used to estimate the subcarrier correlation as a function of the local subcarrier delay. The estimated correlation is compared with its theoretical counterpart that has been obtained as the squared correlation between a filtered periodic subcarrier with an ideal subcarrier. Filtering was implemented using a 10th order Butterworth filter with a 20 MHz cut-off frequency and was adopted to mimic the effect of the front-end filter. The good agreement between theoretical and empirical results

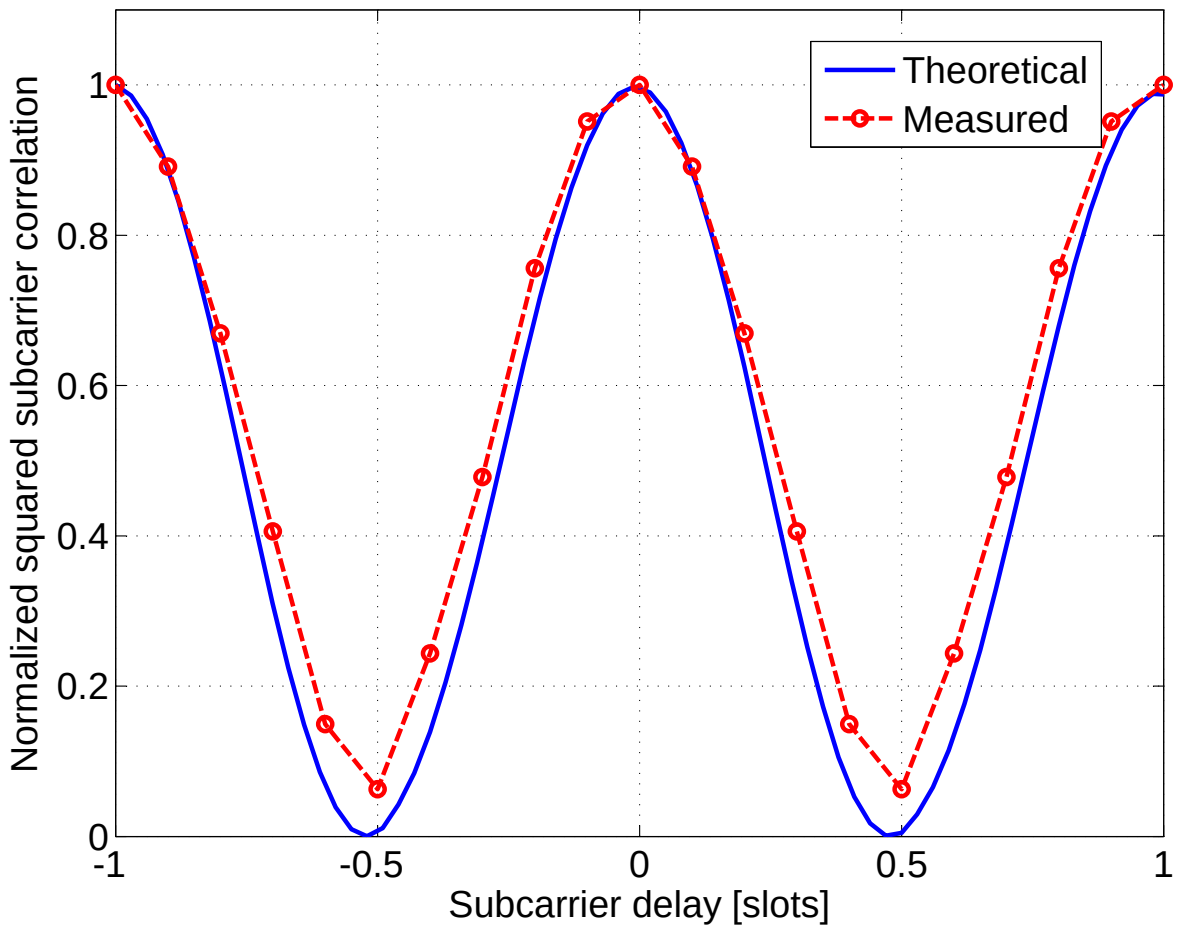

Fig. 7. Comparison between the subcarrier squared correlation estimated using the multi-correlator architecture depicted in Fig. 2 and its theoretical counterpart. The unit 'slot' is defined as one half period of the periodic subcarrier $\tilde{s}_b(t)$.

shows the effectiveness of the proposed multi-correlator approach for monitoring the quality of the subcarrier of the input signal.

To demonstrate the ability to perform signal quality monitoring using the proposed codeless approach an experiment was performed whereby the Galileo IOV was tracked in the presence of wideband interference. In this case the data used in the previous experiments was up-converted to L1, added to the wideband interferer then down-converted and re-digitised (see O'Driscoll et al. (2012) for more details). This permits the comparison of the carrier power and noise power spectral densities in the presence and absence of interference. The resulting losses for the E1a signal using codeless processing are shown in Fig. 8. Note in this case the C/N_0 was of the

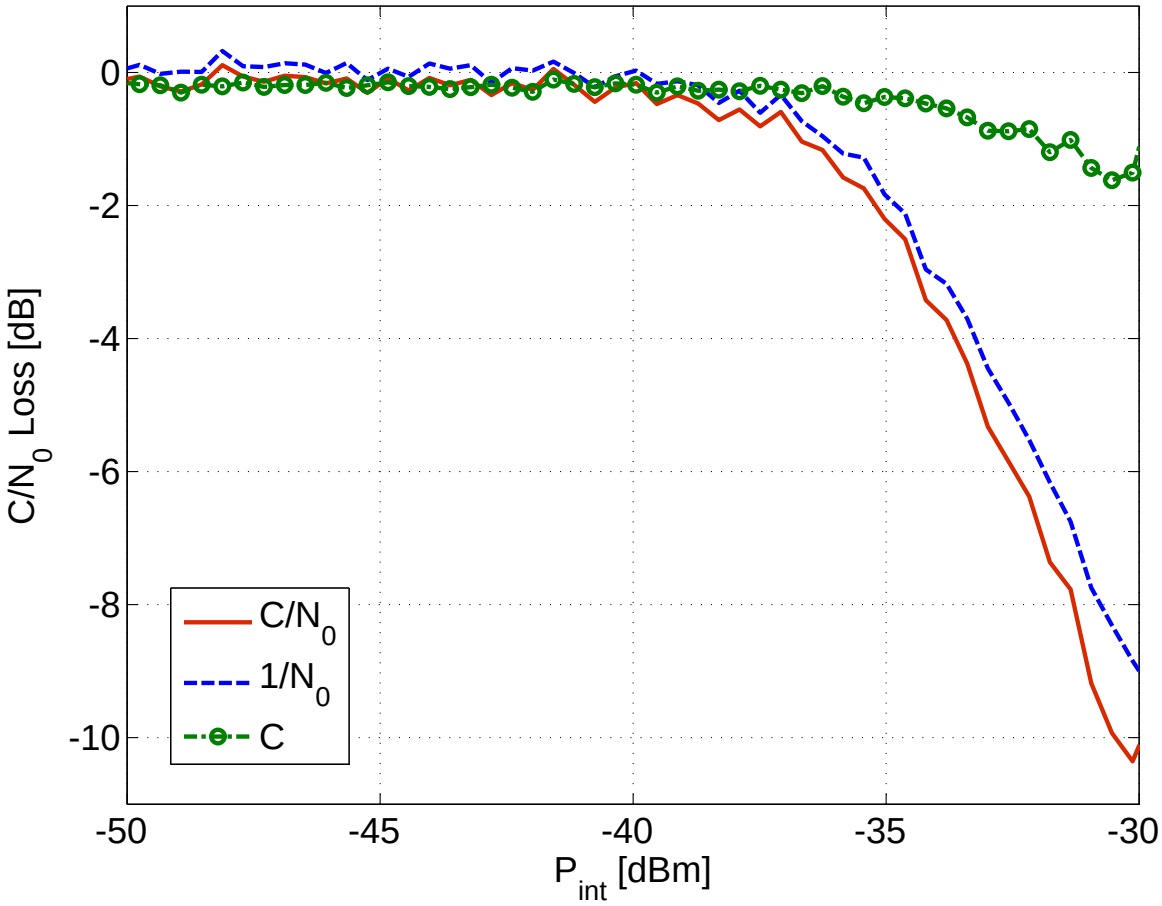

Fig. 8. Variation in estimates of C, N_0 and C/N_0 in the presence of a wideband interferer. The loss is a measure of the difference between the baseline value (no interference) and the value measured with interference. The N_0 loss is inverted so all curves follow the same trend.

order of 50 dBHz, so the PRS C/N_0 measurements are much smoother than in the GIOVE-B case. Clearly, the proposed approach can be used to measure the impact of interference on the PRS signal, even without knowledge of the PRS codes.

VI. Conclusions

In this paper, codeless techniques for the processing of BOC modulated GNSS signals have been considered. The use of a codeless SLL has been suggested to recover the BOC subcarrier and perform coherent integration over the duration of the subcarrier. This process reduces the impact of the input noise and improves the loop performance with respect to a pure squaring

approach. The proposed architecture was then simplified to exploit the information extracted from OS signals broadcast along with the encrypted component. In this way, codeless correlators can be passively computed and used for analysing the quality of encrypted signals. In this respect, a multi-correlator architecture was also proposed and used to monitor the squared correlation of the signal subcarrier. Monitoring the subcarrier correlation function allows one to detected anomalies in the received signals such as multipath and other signal distortions. Finally, a codeless C/N_0 estimator was developed and used to assess the impact of coloured wideband interference. Tests performed using live Galileo signals confirmed the validity of the proposed codeless framework and demonstrated that it is an effective tool for the analysis and monitoring of encrypted BOC modulated signals.

REFERENCES

Anantharamu, P., Borio, D. and Lachapelle, G. (2011). Sub-carrier shaping for BOC modulated GNSS signals, *EURASIP Journal on Advances in Signal Processing* **2011**(1): 133. **URL:** *http://asp.eurasipjournals.com/content/2011/1/133*

ARINC Incorporated (2006). Navstar GPS space segment/navigation user interfaces, *Tech. rep.*, IS-GPS-200 (IRN-200D-001).

Badke, B. (2009). What is C/N_0 and how is it calculated in a GNSS receiver?, *GNSS Solutions, Inside GNSS* **4**(5): 20–23.

Betz, J. W. (1999). The offset carrier modulation for GPS modernization, *Proc. of the 1999 National Technical Meeting of The Institute of Navigation*, San Diego, CA, pp. 639–648.

Betz, J. W. (2000). Effect of narrowband interference on GPS code tracking accuracy, *Proc. of ION National Technical Meeting*, Anaheim, CA, pp. 16–27.

Betz, J. W. (2001). Effect of partial-band interference on receiver estimation of C/N_0, *Proc. of the 2001 National Technical Meeting of The Institute of Navigation*, Long Beach, CA, pp. 817 – 828.

Borio, D. (2011). Squaring and cross-correlation codeless tracking: analysis and generalisation, *IET Radar, Sonar & Navigation* **5**(9): 958 –969.

Burgett, S. and Hokuff, B. (2011). Experimental evidence of a wide area GPS jamming that will result from Lightsquared's proposal to convert portions of L band 1 to high power terrestrial broadband, *Technical report*, Garmin International.

Hodgart, M. S. and Blunt, P. D. (2007). A dual estimate receiver of binary offset carrier (BOC) modulated signals global navigation satellite systems, *Electronics Letters* **43**(16): 877–878.

Kaplan, E. D. and Hegarty, C. J. (eds) (2005). *Understanding GPS: Principles and Applications*, 2 edn, Artech House Publishers, Norwood, MA, US.

Landry, R. J. and Renard, A. (1997). Analysis of potential interference sources and assessment of present solutions for GPS/GNSS receivers, *Proc. of the 4th International Conference on Integrated Navigation Systems (INS)*, Saint Petersburg, pp. 1–13.

O'Driscoll, C., Rao, M., Borio, D., Cano, E., Fortuny, J., Bastide, F. and Hayes, D. (2012). Compatibility analysis between LightSquared and L1/E1 GNSS signals, *Proc. of the IEEE/ION Position Location And Navigation Symposium (PLANS)*, Myrtle Beach, SC, pp. 1–8.

O'Hanlon, B., Psiaki, M., Humphreys, T. and Bhatti, J. (2010). Real-time spoofing detection in a narrow-band civil GPS receiver, *Proc. ION/GNSS*, Portland, OR, pp. 2211–2220.

Psiaki, M., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P. and Humphreys, T. E. (2011). Civilian GPS spoofing detection based on dual-receiver correlation of military signals, *Proc. of the ION/GNSS*, Portland, OR, pp. 2619–2645.

Rebeyrol, E., Julien, O., Macabiau, C., Ries, L., Delatour, A. and Lestarquit, L. (2007). Galileo civil signal modulations, *GPS Solutions* **11**: 159–171.
URL: *http://dx.doi.org/10.1007/s10291-006-0047-3*

Van Dierendonck, A. (1996). Ch. 5, GPS receivers, *in* B. W. Parkinson and J. J. Spilker Jr. (eds), *Global Positioning System Theory and Applications*, Vol. 1, American Institute of Aeronautics & Astronautics, pp. 329–407.

Van Dierendonck, A. J. (1994). Understanding GPS receiver technology: A tutorial on what those words mean, *Proc. of the International Symposium on Kinematic Systems in Geodesy, Geomatics and Navigation KIS94*, Banff, AB, Canada, pp. 15–24.

Woo, K. T. (1999). Optimum semi-codeless carrier phase tracking of L2, *Proc. of the ION/GPS*, Nashville TN, US, pp. 289–306.