HOSTED BY
ELSEVIER
CrossMark
Available online at www.sciencedirect.com
ScienceDirect
ICT Express 2 (2016) 33–36
www.elsevier.com/locate/icte

Use of the Karhunen–Loève Transform for interference detection and mitigation in GNSS☆

Fabio Dovis, Luciano Musumeci*

Politecnico di Torino, Department of Electronics and Telecommunications, Navigation Signal Analysis and Simulation Group, Corso Duca degli Abruzzi, 24, 10129 Torino, Italy

Received 30 October 2015; received in revised form 8 January 2016; accepted 5 February 2016
Available online 11 February 2016

Abstract

Improving the Global Navigation Satellite System (GNSS) receiver robustness in a radio interfered environment has been always one of the main concerns for the GNSS community. Due to the weakness of the signal impinging the GNSS receiver antenna, GNSS receiver performance can be seriously threatened by the presence of stronger interfering signals. In these scenarios, classical interference countermeasures may fail due to the fact that interference detection and removal process causes also a non-negligible degradation of the received GNSS signal. This paper introduces an innovative interference detection and mitigation technique against the well-known jamming threat. This technique is based on the use of the Karhunen–Loève Transform (KLT) which allows for the representation of the received interfered signals in a transformed domain where interference components can be better identified, isolated and removed, avoiding significant degradation of the useful GNSS signal.

Keywords: Interference; Jamming; Karhunen–Loève Transform; Chirp signal; Adaptive notch filter

1. Introduction

The effect of an interfering signal on the GNSS receiver performance can vary from the increase of the noise on the pseudo-ranges measurements, leading to large errors in the positioning domain, up to the complete disruption of the GNSS receiver operation thus causing the complete denial of the positioning service. Intentional interference generated by the jammers, known also as Personal Privacy Devices (PPDs), to the GNSS based services has become recently the main concern for the GNSS community. Such jammers can be easily purchased on-line even for few dollars despite their use being illegal in the United States and in several European Countries [1]. These devices are capable of transmitting strong Radio Frequency (RF) power overlapping a large part of the targeted GNSS frequency band thus preventing the receivers from operating correctly within an area and causing hazardous outages of the GNSS based systems. Many documented incidents caused by PPDs have already occurred as for example, the infamous case at Newark Airport where one of the Local Area Augmentation System (LAAS) ground facility receiver was occasionally jammed by a Personal Privacy Device (PPD) installed in a vehicle passing along a nearby motorway [2].

Very detailed classification of existent civil GNSS jammers can be found in [3,4] and in [5]. The RF signal transmitted by most of the available in car jammers are chirp signals with unidirectional or bidirectional, linear and positive sweep functions.

Nowadays, professional GNSS receivers are equipped with interference detection and mitigation algorithms capable of dealing with a wide range of interfering signals. The adaptive notch filtering is the most known jamming mitigation algorithm [6]. This low-complexity technique is based on the use of a notch filter, characterized by a pass-band frequency response which rejects a very narrow portion of spectrum in correspondence of the interference frequency components, and an adaptive block tracking the instantaneous jamming frequency [7]. However, such a traditional countermeasure performs interference detection and excision in the frequency domain only, leading to a not negligible distortion on the useful received GNSS

* Corresponding author.
E-mail address: luciano.musumeci@polito.it (L. Musumeci).

Peer review under responsibility of The Korean Institute of Communications Information Sciences.

☆ This paper is part of a special issue entitled "Positioning Techniques and Applications" guest edited by Prof. Sunwoo Kim, Prof. Dong-Soo Han, Prof. Chansu Yu, Dr. Francesco Potorti, Prof. Seung-Hyun Kong and Prof. Shiho Kim.

http://dx.doi.org/10.1016/j.icte.2016.02.008

signals. This paper introduces an innovative interference detection and mitigation algorithm based on the use of an advanced signal processing technique: the Karhunen–Loève Transform (KLT). The KLT makes a projection of the digitized signal on the eigenfunctions domain where interference components can be better identified and isolated from the rest of the received signal.

The paper is organized as follows: after a brief description of the jamming signal characteristics and its signal model in Section 2, the KLT based detection and mitigation algorithm will be addressed in Section 3. A set of experimental test will be described in Section 4 showing the benefits in improving GNSS receiver robustness against jamming interference.

2. Jamming in GNSS: signal model

The composite digitized Intermediate Frequency (IF) signal at the input of the baseband processing block of a GNSS receiver under jamming interference can be modeled as

$$s[n] = \sum_{m=0}^{M-1} y_m[nT_s] + i[nT_s] + \eta[nT_s] \tag{1}$$

where $y_m[nT_s]$ identify the useful GNSS signal coming from the mth Line-of-Sight (LoS) satellite, $i[nT_s]$ is the digitized jamming signal component and $\eta[nT_s]$ is the Additive White Gaussian Noise (AWGN) term. Neglecting the satellite index subscript for sake of simplicity of the notation, each useful digital GNSS signal at IF can be expressed as

$$y[n] = \sqrt{2C} \cdot d[nT_s - n_0] \cdot c[nT_s - n_0] \cdot \cos\left(2\pi\left(f_{L1} + f_d\right) nT_s + \theta_0\right) \tag{2}$$

where C is the power at the antenna port, $d[nT_s]$ is the navigation data component, $c[nT_s]$ is the pseudo random sequence for spreading the signal spectrum, while n_0, f_d and θ_0 are the received code delay, the Doppler frequency and the phase introduced by the channel respectively. As mentioned in the Introduction, the RF signal generated by the majority of the available in-car PPDs is a chirp signal, which can be expressed, according to the model in [4], as

$$i(t) = a \cdot \sin\left[2\pi\left(f_0 + \frac{k}{2}t\right)t\right] \quad \forall t : 0 \le t \le T_{sw} \tag{3}$$

where f_0 is the starting frequency, k is the sweeping frequency rate, T_{sw} is the sweeping frequency period and a is the constant chirp signal amplitude. Fig. 1 shows the spectrogram of a chirp signal typically transmitted by an in-car jammer, characterized by a linear frequency sweep of 14 MHz and by a sweep period of 9 μs.

3. Advanced signal processing algorithms: the transformed domain techniques

The KLT based mitigation algorithm belongs to the family of the transformed domain techniques, which are based on the use of advanced signal processing techniques on the digitized GNSS signal. Such techniques offer the possibility to perform interference detection and excision in a domain where interference components can be better identified and removed without causing large distortion of the received useful GNSS signal.

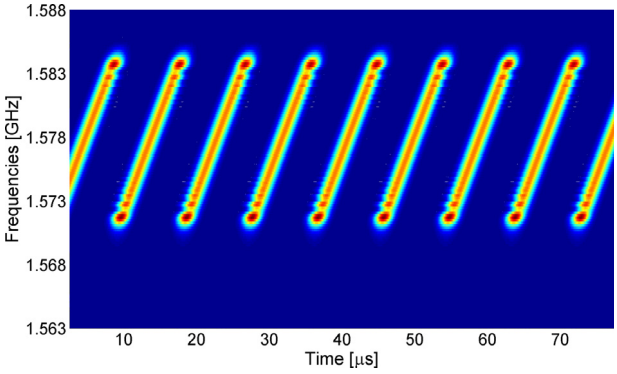

Fig. 1. Spectrogram of the RF jamming signal transmitted by a typical in-car cigarette lighter powered jammer.

Several examples of transformed domain techniques for interference detection and mitigation can be found in literature, such as those based on the use of the Short Time Fourier Transform (STFT) [8], or those exploiting the properties of the Wavelet Packet Decomposition (WPD) as in [9] and [10].

3.1. The Karhunen–Loève transform

The KLT provides a decomposition of the digitized signal in a vectorial space using orthonormal functions which can have in principle any shape. The KLT decomposition of a general time dependent function is given by

$$x(t) = \sum_{j=1}^{\infty} Z_j \Phi_j(t) \tag{4}$$

where Z_j are scalar random variables that are statistically independent and $\Phi_j(t)$ are the basis functions, derived from the covariance matrix of a digitized version of the stochastic process $x(t)$. The KLT offers the better separation between the deterministic components within the received signal and the stochastic ones. The random variables Z_j are obtained projecting the given stochastic process $x(t)$ over the corresponding eigenvector $\Phi_j(t)$, as

$$Z_j = \int_{-\infty}^{+\infty} x(t)\, \Phi_j(t)\, dt. \tag{5}$$

In [11] it is stated that the KLT is the only possible statistical expansion in which all the expansion terms are uncorrelated from each other.

3.2. KLT for interference detection and mitigation

First use of KLT for Continuous Wave Interference (CWI) detection is described in [12], while application of the KLT decomposition against pulsed interference has been proposed first in [13]. The KLT decomposition has been implemented according to the following steps: