

Robust Ranging in the Presence of Repeater Signals

Andreas Iliopoulos*, Christoph Enneking * °, Thomas Jost*, Omar García Crespillo* , Manuel Appel * ⊕ and Felix Antreich * °,
* *Institute of Communications and Navigation, German Aerospace Center (DLR)*
° *Department of Teleinformatics Engineering, Federal University of Ceara (UFC)*
⊕ *RWTH Aachen University*

BIOGRAPHY

Andreas Iliopoulos received his M.Sc. in electrical engineering from the Munich University of Technology (TUM), Germany, in 2012. From 2012 to 2013 he was working as researcher in the Institute for Integrated Systems at the Munich University of Technology (TUM). Since 2013 he has been with the Institute of Communications and Navigation at the German Aerospace Center (DLR). His research interests include statistical signal processing, interference mitigation, wireless communications, antenna array processing, estimation theory and optimization.

Christoph Enneking received his MSc. in electrical engineering from the Munich University of Technology (TUM), Germany, in 2014. In September 2014, he joined the Institute of Communications and Navigation of the German Aerospace Center (DLR). His research interests include GNSS signal design, estimation theory, and GNSS intra- and intersystem interference.

Dr. Thomas Jost received the Diploma degree (FH) in electrical engineering from University of Applied Science Wiesbaden, Germany, in 2001, the Diploma degree in Electrical engineering and information technology from Technical University of Darmstadt, Germany, in 2003 and the Doctoral degree from University of Vigo, Spain, in 2013. From 2003 to 2006, he held a research assistant position in the Signal Processing Group at TU Darmstadt. Since 2006, he is a member of the scientific staff of the Institute of Communications and Navigation at the German Aerospace Center.

Omar García Crespillo received his M.Sc. in Telecommunication Engineering from the University of Malaga in Spain in 2013. In the same year, he joined the Integrity group of the Navigation department of the German Aerospace Center (DLR). His current field of research includes GNSS, integrated inertial navigation, Bayesian estimation and integrity. Since 2015, he is also a PhD student at the Swiss Federal Institute of Technology (EPFL) in Lausanne.

Manuel Appel received his diploma degree in electrical engineering from the university of applied science Ingolstadt, Germany in 2008. Additionally he received a M.Sc. degree from Technical University Munich in 2013 after working at Fraunhofer Institute for Integrated Circuits in Erlangen. He joined the Institute for Communication and Navigation of DLR in January 2014. His main research interest is in development of signal processing algorithms for robust GNSS receivers with the main focus on spoofing detection and mitigation.

Dr. Felix Antreich received the Diploma degree in electrical engineering from the Munich University of Technology (TUM), Munich, Germany, in 2003. In 2011 he also received the Doktor-Ingenieur (Ph.D.) degree from the TUM. From 2003 to 2016, he was an Associate Researcher with the Department of Navigation, Institute of Communications and Navigation of the German Aerospace Center (DLR), Wessling- Oberpfaffenhofen. Since September 2016 he is a visiting professor in the Department of Teleinformatics Engineering (DETI) at the Federal University of Ceara (UFC) in Fortaleza, Brazil. His research interests include sensor array signal processing for GNSS and wireless communications, estimation theory, wireless sensor networks, and signal design for synchronization.

ABSTRACT

This paper tackles the problem of robust Global Navigation Satellite System (GNSS) ranging in the presence of GNSS repeater signals. In such cases repeater signals act as an interference to live GNSS satellite signals and need to be mitigated. The first contribution of this paper is the impact analysis of repeater signals on Delay-Locked-Loops (DLL), which are traditionally utilized for the time of arrival estimation in GNSS receivers. In the analysis, we determine different threat regions based on satellite signal and repeater signal parameters. Secondly, it introduces a novel algorithm that performs simultaneous channel estimation and equalization for GNSS signals. The proposed algorithm proves to be resilient in the presence of GNSS repeater signals in comparison to regular DLL structures. Finally, based on the inherent channel estimation the algorithm provides, it is possible to characterize the parameters of GNSS repeaters.

I INTRODUCTION

Global Navigation Satellite System (GNSS) repeaters are devices designed to receive GNSS signals, amplify them and retransmit them in enclosed areas. Those devices find various uses in civil applications. For instance, civil aircraft undergoing maintenance in hangars are using repeater signals that are being captured on the roof of a hangar and retransmitted into the hall in order to test their avionic systems without leaving the enclosure of the hangar [1]. Recent research has also found usage in repeaters for indoor positioning and navigation by arranging them in a certain geometry in large buildings and treating them as "repeater-lites" [2].

Aside from their aforementioned benefits, GNSS repeaters can introduce a significant hazard. That usually occurs in the case of simultaneous existence of GNSS satellite signals and repeated signals. Then, repeated signals are viewed as interference instead of beneficial signals. Repeated signals have inherently a larger travel distance than the direct Line-of-Sight (LOS) signals and act as interference to the Delay-Locked-Loop (DLL). Additionally, repeater signals are amplified before transmission which poses an additional challenge. The amplified repeated signals have usually a much higher power than regular live GNSS signals and thus usually dominate them. Furthermore, by amplifying the live signals, repeater devices simultaneously amplify environmental noise as well as thermal noise from the reception antenna and the amplifiers. The latter has a profound effect on regular GNSS repeater signals, since the noise amplification acts as an Additive White Gaussian-Noise (AWGN) jammer.

The combined effect of GNSS signal shadowing and jamming can lead to disastrous results. Depending on the repeater set up parameters, regular GNSS receivers can produce a large variance in their positioning solution, provide no positioning solution at all and more importantly produce a falsified position. In the last case, the repeated signals have such a low power to go undetected yet large enough to dominate the live signals. As a result, the GNSS receiver will estimate a range that approximately corresponds to the site of the repeater reception antenna and hereby estimate the position of the reception antenna as its own. Usually, such phenomena go undetected in civil applications. However, there are instances, where repeaters have posed a significant risk for safety critical applications, most importantly for avionic applications. In 2010, at Hannover airport, a GNSS repeater installed in a hangar caused problems to aircraft that were taxiing and taking off [3]. The interference was reported to have caused alerts and alarms with aircraft systems at ranges up to several hundred meters from the hangar.

The structure of this paper is as follows. In Section II, we conduct a study on the current repeater mitigation options and we conduct a literature review on Extended Kalman Filter (EKF) based satellite signal code delay algorithms. In Section III, we perform a threat analysis of the repeater interference on the widely utilized Delay-Locked-Loops (DLLs) in the GNSS community. Section IV introduces the developed signal model, which is used in Section V to describe the proposed mitigation algorithm. Finally, in Section VI, we show the mitigation performance of the proposed algorithm by simulations.

II STATE OF THE ART

Currently the usage of GNSS repeaters is strongly regulated. International Civil Aviation Organization (ICAO) member states have to ensure that the interference is controlled and in line with the requirements of [4]. Thus, repeater manufacturers and operators have to be aware and follow certain regulations. The aforementioned examples however indicate that regulation cannot completely protect against interference-like repeated signals.

Other countermeasures against repeaters serve solely as detectors that identify the existence of repeaters in the intermediate area. This can be achieved through different techniques. The first and easiest includes interference monitoring through investigation of the power spectral density of the designated GNSS bands. A different category includes the determination of different interference metrics in a customized GNSS receiver. Those can include the Delta Metric [5], Ratio Metric [5], Early-Late Phase Metric [6], Magnitude-Difference Metric [7].

An additional methodology for repeater detection and characterization includes the implementation of Receiver Autonomous Integrity Monitor (RAIM) algorithms [8]. Those algorithms can either estimate inconsistencies in GNSS signals by generating subsets of the measured satellite signals and by processing different GNSS signal frequencies and comparing them [9].

Kalman filters utilization in the GNSS context has found many applications. The most wide spread usage of them in the GNSS community is the coupling different satellite tracking modules, which in turn increases overall tracking robustness [10]. A different usage is coupling Delay/Phase Locked Loops (DLL/PLL) structures with inertial sensors in order to provide navigation information under harsh conditions and even in the absence of GNSS signals [11].

The use of Extended Kalman Filter (EKF) for code delay/channel estimation in signal tracking was first introduced in communications by [12, 13]. In both cases the introduced structure is in the pre-correlation domain, assuming short Code Division Multiple Access (CDMA) code lengths and Signal-to-Noise Ratio (SNR) many orders of magnitude higher than in GNSS. The placement of post-correlation EKF has been studied in the GNSS community. In [14], the authors utilize prompt and discriminator outputs as EKF measurements for carrier phase, code phase and carrier amplitude determination. Similar work was presented in [15], where interleaved but separate EKFs are used that include regular early, late and prompt correlators as input as well as Doppler, acceleration and phase information for stable delay code tracking under harsh SNR conditions. Finally, [16] presents a method to jointly estimate code delays and channel coefficients using EKF coupled with an interference cancellation scheme and test statistics for the case of a multicell CDMA transmission scheme.

A systematic approach of a correlator bank usage for parameter estimation was suggested by Selva [17] and is suited for parameter estimation in multipath environments. The use of a correlator bank reduces sample sizes considerably, so that estimation of a potentially large number of parameters in digital signal processing becomes computationally affordable as long as the data depends linearly on most of the parameters. This methodology has since been adopted in many works on GNSS parameter estimation for multipath scenarios. These works include estimation or tracking of multiple signal arrivals, optimality criteria being ML [18], Bayesian mean squared error [19] or mixtures of the two [20, 21].

In [22], we presented a novel algorithm based on the EKF, which substitutes traditional DLLs and is able to robustly track the satellite signal code delay and simultaneously estimate the GNSS signal channel, with the help of a multicorrelator bank structure. In this paper, we optimize the aforementioned algorithm and further develop it to also handle and estimate complex amplitudes of the signals contained in the channel seen by a GNSS receiver.

III GNSS LINK BUDGET IN THE PRESENCE OF REPEATER SIGNALS

There are two major repeater types on the market [23]. The first type is the so-called Decode-and-Forward repeater (DF). This type receives GNSS signals, performs decoding and retransmits a composite signal based on the decoded parameters. The second repeater type is Amplify-and-Forward (AF) repeaters. That type filters and amplifies the captured signals before retransmission. In this paper, we focus on AF repeaters, since this type is predominant in the GNSS community and the elaborate operation of DF repeaters falls within the realm of spoofing.

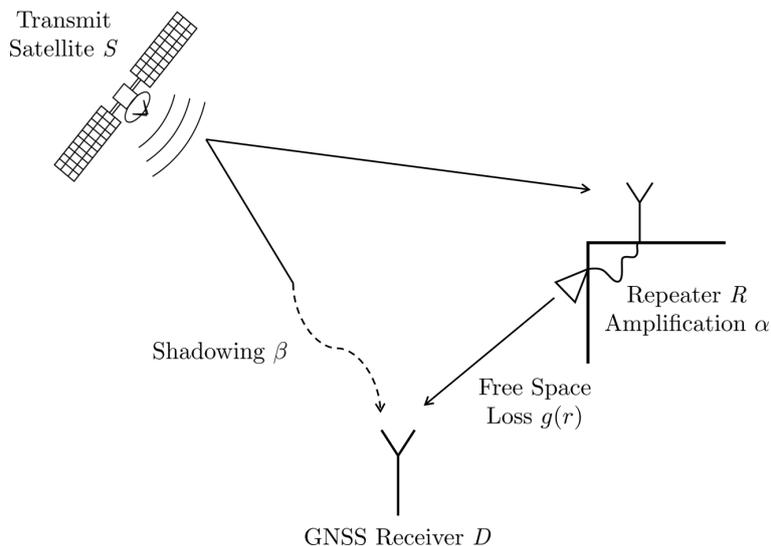


Figure 1: Illustration of a typical repeater interference scenario.

In the following segment, we study the impact of AF repeaters on the parameter estimation using regular DLLs. We define parameter regions, where different repeater effects are dominant on the estimation quality of DLLs.

Figure 1 illustrates a typical setup, where a repeater could potentially influence a GNSS receiver. As displayed, the receive antenna of the repeater is placed in open sky conditions and captures a GNSS signal with a carrier-to-noise density ratio of

C/N_0 . The captured signal is then filtered and amplified with an amplification factor α before being re-transmitted to a local area, such as a hangar, a mall or similar. After transmission, the repeater signal is attenuated by Free-Space-Loss (FSL) according to

$$g(r) = \left(\frac{c}{4\pi r f_{Li}} \right)^2, \quad (1)$$

where r stands for the repeater-destination distance, f_{Li} the signal carrier frequency and c the speed of light. As seen in Equation (1), FSL decreases with distance r as well as with the signal frequency f_{Li} .

A GNSS receiver located outside of the building with the installed repeater will see the Line-of-Sight (LOS) signal with a carrier-to-noise ratio of $\beta C/N_0$ due to shadowing effects. The attenuation factor $\beta \leq 1$ represents shadowing and varies between β_{min} and 1. $\beta = 1$ indicates that the GNSS receiver has open sky conditions and sees the same C/N_0 as the repeater. $\beta = \beta_{min}$ illustrates the case where shadowing is so severe that the GNSS receiver sees the minimum guaranteed signal power [24].

In case the repeater signal escapes the building enclosure, it experiences a net amplification of $\alpha g(r)$ and acts as interference to the nominal operation of the GNSS receiver.

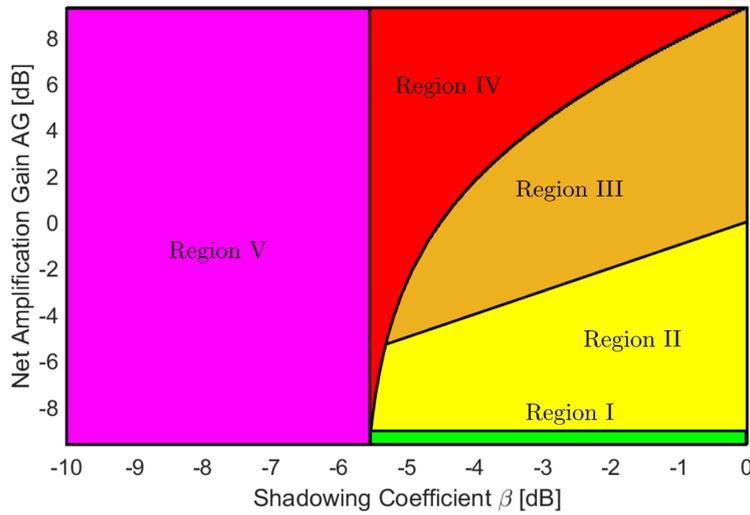


Figure 2: Illustration of dominant repeater effect regions.

If the free space loss overpowers the repeater amplification and the net power of the repeated signal $\alpha g(r)$ is less than 0.01, then the receiver DLL is assumed to be operating in nominal conditions (Region I in Figure 2).

If the amplification of the repeater is stronger or is the receiver is closer to the transmit antenna of the repeater, the net amplification of the repeated signal get stronger. We assume that if the net amplification varies between 0.01 and the shadowing value of β , then the repeated signal affects the receiver DLL and behaves similar to multipath (Region II in Figure 2).

When the net amplification reaches β , any gain from the LNA amplification is negated by the FSL. That means that the repeated signal has the same power as the LOS signal and thus a DLL cannot differentiate between the actual LOS and the "counterfeit" signal.

The differentiation becomes even more difficult, if the net amplification of the repeated signal seen at the GNSS receiver exceeds β . At that point (Region III in Figure 2), the repeated signal dominates the actual LOS and the DLL of the GNSS receiver eventually locks to the stronger repeated signal.

If the repeater signal power further increases, an interesting effect takes place. The repeater does not only amplify GNSS signals but also its thermal white Gaussian noise. Therefore, the repeater signal leads to an increase of the noise floor due to the noise figure of the repeater electronics. Thus, if the net amplification seen at the GNSS receiver exceeds a certain value, the GNSS receiver cannot work satisfactorily, even if it completely mitigates the effect of the repeater signal. The reason is that over a certain threshold, the noise amplification caused by the repeater acts as an Additive-White-Gaussian-Noise (AWGN) jammer and thus anti-jamming signal processing algorithms are required before dealing with the repeated GNSS signal. But what net amplification leads to such a jamming effect on the GNSS receiver?

Before dealing with that question, we have to define what constitutes a jammer in the GNSS framework and what are the minimum ranging degradation a DLL can endure before being characterized as being jammed.

In [25, Appendix-H] an indication is given on what constitutes jamming by defining power masks within the L-band based on the bandwidth of the jamming signal. This way however, we cannot associate the jammer's influence on the DLL operation. [26, S.2.1.4.1.4] defines a more concrete metric for aeronautical applications and specifies a ranging error $RMS_{air,GPS} \leq 0.36$

meters. Equation [27, 6.31] gives the tracking error standard deviation due to interference for an optimal and coherent DLL with an E-L discriminator

$$\sigma_{\text{DLL},m} = \frac{c\sqrt{B_L}}{2\pi \int_{-B}^B f S_S(f) \sin(\pi f D T_c) df} \times \left(\left(\frac{\beta C_s}{N_0} \right)^{-1} \int_{-B}^B S_S(f) \sin^2(\pi f D T_c) df + \frac{C_I}{\beta C_s} \int_{-B}^B S_I(f) S_S(f) \sin^2(\pi f D T_c) df \right)^{\frac{1}{2}}, \quad (2)$$

where c the speed of light, B_L the DLL loop bandwidth, B the one-sided signal bandwidth, D the correlator spacing, $\frac{\beta C}{N_0}$ the receiver C/N_0 due to shadowing, $S_S(f)$ the normalized power spectral density of the LOS signal, $\frac{C_I}{\beta C}$ the interference to carrier ratio and finally $S_I(f)$ the interference power spectral density.

By utilizing Equation (2) and sweeping over $\beta \in [\beta_{\min}, 1]$ and $\alpha g(r) \in [-\infty, 100]$, we can define two more regions. Region IV gives the area, where the DLL under study is jammed due to the net amplification gain $\alpha g(r)$. The second region (Region V in Figure 2) indicates the area where the DLL cannot reach the $RM S_{\text{prair},GPS} \leq 0.36$ meters requirement due to the combined effect of the shadowing factor β and the repeater net amplification gain $\alpha g(r)$.

The composite areas described above are drawn together in Figure 2 for a DLL with an E-L discriminator, a correlator spacing $d = 0.1$, a loop bandwidth of $B_L = 0.8\text{Hz}$, one-sided signal bandwidth $B = 5.115\text{MHz}$ and an integration time of $T_{\text{int}} = 5\text{ms}$.

IV SIGNAL MODEL

A GNSS satellite S transmits a real valued and periodic pseudorandom (PN) signal

$$s(t) \equiv s(t - mT) \quad \in \mathbb{R}, \quad \forall m \in \mathbb{Z} \quad (3)$$

with autocorrelation function (ACF)

$$\Phi_{ss}(\tau) = \int_T s(t)s(t+\tau)dt, \quad (4)$$

where we denote the signal period by T and use $\Phi_{ss}(0) = \sigma_s^2$. The signal has a chipping rate of $1/T_c$ and is bandlimited to a one-sided bandwidth $B = \lambda/T_c$, where $\lambda \in \mathbb{N}$. If radio propagation is distortionless, the baseband signal observed by a receiver experiences a range-dependent propagation delay, free space attenuation, phase shift and additive white Gaussian noise (AWGN), making the signal at the receiver D

$$x(t) = h^{(0)}(t)s(t - \tau^{(0)}(t)) + \eta^D(t) \quad \in \mathbb{C}, \quad (5)$$

with $\tau^{(0)}(t) \in \mathbb{R}$ being the code delay, $h^{(0)}(t) = \sqrt{\beta(t)g(r)}e^{j\theta^{(0)}(t)} \in \mathbb{C}$ the LOS complex amplitude due to free space loss, shadowing $\beta(t)$ and phase shift $\theta^{(0)}(t)$. Finally, $\eta^D(t) = \sqrt{\frac{1}{2}}\eta_R^D(t) + j\sqrt{\frac{1}{2}}\eta_I^D(t) \in \mathcal{CN}(0,1)$ is complex AWGN with zero mean and unit variance.

A repeater R situated under open sky conditions and at a distance r from the stationary receiver D (Figure 1) will receive the LOS signal without shadowing (e.g., $\beta(t) = 1$) and a delay

$$\tau_{\text{rec}}^R(t) = \tau^{(0)}(t) + \Delta\tau_G, \quad (6)$$

where $\Delta\tau_G$ the geometry dependent relative delay between receiver and repeater. The AF repeater subsequently filters, amplifies the captured signal with an unknown amplification factor α and retransmits it. Thus, the total code delay of the repeated signal seen at the GNSS receiver becomes

$$\tau^R(t) = \tau_{\text{rec}}^R(t) + \frac{r}{c} = \tau^{(0)}(t) + \Delta\tau_G + \Delta\tau_C. \quad (7)$$

Assuming that the relative delay of the repeater transmitted signal to the LOS is smaller than the chip width T_c , that is $\Delta\tau = \tau^{(0)}(t) - \tau^R(t) \leq T_c$, the repeater signal will distort the cross-correlation function of the receiver.

The amplified repeater signal is attenuated by $g(r)$ according to Equation (1) and a combined phase shift $\theta^R(t)$ by the repeater electronics and the propagation. The repeater transmitted signal received at the GNSS receiver can be thus written as

$$i(t) = \sqrt{\alpha g(r)}e^{j\theta^R(t)}(s(t - \tau^R(t)) + \eta^R(t)) = h^R(t)s(t - \tau^R(t)) + h^R(t)\eta^R(t), \quad (8)$$

where $h^R(t) = \sqrt{\alpha g(r)}e^{j\theta^R(t)}$ the complex amplitude for the repeater due to amplification α , Free Space Loss $g(r)$ and phase shift $\theta^R(t)$. Similarly $h^R(t)\eta^R(t)\mathcal{CN}(0, (|h^R(t)|^2))$ is the amplified and transmitted AWGN, assuming normal noise at the repeater input.

The received signal containing the LOS to the satellite, the repeater signal and the AWGN can be thus expressed as

$$\begin{aligned}
y(t) &= x(t) + i(t) \\
&= h^{(0)}(t)s(t - \tau^{(0)}(t)) + h^R(t)s(t - \tau^R(t)) + \eta^D(t) + h^R(t)\eta^R(t) \\
&= h^{(0)}(t)s(t - \tau^{(0)}(t)) + h^R(t)s(t - \tau^R(t)) + \eta(t),
\end{aligned} \tag{9}$$

since the sum of the two complex AWGN sources, $(\eta^D \in \mathcal{CN}(0, 1)$ and $\eta^R \in \mathcal{CN}(0, (|h^R(t)|^2))$) will also produce an AWGN $\eta \in \mathcal{CN}(0, (|h^R(t)|^2 + 1))$.

We approximate the complex amplitudes of the signals and their respective delays by a tap delay line channel coefficients with Dirac distributions that are equidistantly arranged in time

$$h(t, \tau) \approx \sum_{\ell=0}^L h^{(\ell)}(t)\delta(\tau - \ell T_s) \tag{10}$$

with time-variant weights $h^{(\ell)}(t)$. That is a valid assumption when the sampling period T_s is significantly smaller than the chip duration T_c , that is $T_s \ll T_c$ and L satisfying $LT_s = T_c$. Inserting (10) into (9), we get

$$y(t) \approx \sum_{\ell=0}^L h_k^{(\ell)} s(t - \tau_k^{(0)} - \ell T_s) + \eta(t). \tag{11}$$

Since the channel coherence time (i.e. the time where the channel parameters remains quasi-constant) is typically larger than the coherent integration time TN_c over N_c PN periods T , the last approximation in the equation above is that the LOS delay and the channel weights are block-wise constant, $\tau_k^{(0)} \triangleq \tau^{(0)}(kTN_c)$ and $h_k^{(\ell)} \triangleq h^{(\ell)}(kTN_c)$ and $\ell = 0, \dots, L$ for

$$k = \lfloor \frac{t}{TN_c} \rfloor = \lfloor \frac{t}{T_s N N_c} \rfloor = \lfloor \frac{t}{T_s M} \rfloor \tag{12}$$

with $M = NN_c$ the number of samples in one coherent integration period.

As a next processing step, the received signal is lowpass filtered with one-sided bandwidth B and sampled at the Nyquist rate $\frac{1}{T_s} = 2B$. The design parameter λ , representing the oversampling factor, can be chosen sufficiently high to satisfy $T_s \ll T_c$. The number of observable channel coefficients is then $L = \frac{T_c}{T_s} = 2\lambda$. Sampling the signal in (11) for the n -th sample of the k -th coherent integration period leads to

$$\begin{aligned}
y_k[n] &\triangleq y((kM + n)T_s) \\
&= \sum_{\ell=0}^L h_k^{(\ell)} s((kM + n)T_s - \tau_k^{(0)} - \ell T_s) + \eta((kM + n)T_s) \\
&= \sum_{\ell=0}^L h_k^{(\ell)} s((n - \ell)T_s - \tau_k^{(0)}) + \eta((kM + n)T_s),
\end{aligned} \tag{13}$$

where the periodicity of the PN sequence $s(t)$ is exploited (Equation (3)). Collecting periods $k = 0, 1, \dots$ and stacking M samples per period in one column vector leads to

$$\mathbf{y}_k = [y_k[1], \dots, y_k[M]]^H \in \mathbb{C}^{M \times 1}, \quad k = 0, 1, \dots \tag{14}$$

Thus, our discrete signal can be written in matrix-vector notation as

$$\mathbf{y}_k = \mathbf{H}_k \mathbf{s}(\tau_k^{(0)}) + \boldsymbol{\eta}_k, \tag{15}$$

with the ideal transmit PN signal

$$\mathbf{s}(\tau_k^{(0)}) = \begin{pmatrix} s(T_s - \tau_k^{(0)}) \\ s(2T_s - \tau_k^{(0)}) \\ \vdots \\ s(MT_s - \tau_k^{(0)}) \end{pmatrix} \in \mathbb{C}^{M \times 1}$$

and the white circular symmetric normal distributed noise term

$$\boldsymbol{\eta}_k = [\eta(T_s + kT), \dots, \eta(MT_s + kT)]^H \in \mathbb{C}^{M \times 1}. \quad (16)$$

The channel in Equation (15) is expressed by a convolution matrix with circulant Toeplitz structure

$$\mathbf{H}_k = \sum_{\ell=0}^L h_k^{(\ell)} \mathbf{Z}^\ell \in \mathbb{C}^{M \times M}, \quad (17)$$

with \mathbf{Z} being the polynomial basis of the $[M \times M]$ circulant matrix

$$\mathbf{Z} = \begin{pmatrix} \mathbf{0}^H & 1 \\ \mathbf{I} & \mathbf{0} \end{pmatrix} \in \mathbb{R}^{M \times M}, \quad (18)$$

where $\mathbf{I} \in \mathbb{R}^{(M-1) \times (M-1)}$ stands for an identity matrix, and $\mathbf{0} \in \mathbb{R}^{(M-1) \times 1}$ a vector containing only zeros.

The unknown time-varying signal and channel parameters are summarized by the state vector

$$\mathbf{x}_k = [\tau_k^{(0)}, h_k^{(0)}, h_k^{(1)}, \dots, h_k^{(L)}]^H \in \mathbb{C}^{(L+2) \times 1}, \quad (19)$$

containing the real valued LOS delay and the complex valued channel coefficients.

V PROPOSED ALGORITHM

Measurement Model - Multicorrelator Bank

The number of data M collected per coherent integration period k proves to be computationally challenging. Thus, we need an efficient representation of the incoming signal without loss of information. In order to do so, we employ a projection of the observed signal to a much smaller space, thus reducing the subsequent processing requirements. A variant of these projections is employing a bank of signal-matched correlators and building the temporal cross-correlation function of the incoming signal with a local set of time shifted replicas [17]

$$\mathbf{1} \otimes \begin{pmatrix} \mathbf{s}^H(\hat{\tau}_k^{(-q)}) \\ \mathbf{s}^H(\hat{\tau}_k^{(-q+1)}) \\ \vdots \\ \mathbf{s}^H(\hat{\tau}_k^{(0)}) \\ \vdots \\ \mathbf{s}^H(\hat{\tau}_k^{(q-1)}) \\ \mathbf{s}^H(\hat{\tau}_k^{(q)}) \end{pmatrix} \mathbf{y}_k \in \mathbb{C}^{P \times 1}, \quad (20)$$

where $\mathbf{1} \in \mathbb{R}^{1 \times N_c}$ represents a vector containing ones and is responsible for the coherent integration, \otimes the Kronecker product operator, $\mathbf{s}(\cdot) \in \mathbb{C}^{N \times 1}$ represents the sampled PN signal $s(t)$, $\hat{\tau}_k^{(q)} \in \mathbb{R}$ represents the temporal delay of the q -th local PN replica and $P = 2q + 1$ is the total number of local replicas. Through this operation, we project the signal from a $\mathbb{C}^{M \times 1}$ space to a much smaller $\mathbb{C}^{P \times 1}$ space. In order to minimize the loss of information due to reduced dimensionality, we assume that the correlator bank's middle/prompt replica is roughly synchronized with the code delay of the LOS signal, i.e., $|\hat{\tau}_k^{(0)} - \tau_k^{(0)}| \leq T_c/2$. Additionally, we place the remaining $2q$ correlators symmetrically and equidistantly around the prompt correlator within $\pm T_c$ using a spacing of $\Delta = \frac{T_c}{q}$. Thus we have

$$\hat{\tau}_k^{(\pm i)} - \hat{\tau}_k^{(0)} = \pm i\Delta, \quad i = 1, \dots, q. \quad (21)$$

This simplifies the parameters that describe the correlator bank

$$\mathbf{Q}^H(\hat{\tau}_k^{(0)}) \triangleq \mathbf{1} \otimes \begin{pmatrix} \mathbf{s}^H(\hat{\tau}_k^{(0)} - q\Delta) \\ \mathbf{s}^H(\hat{\tau}_k^{(0)} - (q-1)\Delta) \\ \vdots \\ \mathbf{s}^H(\hat{\tau}_k^{(0)}) \\ \vdots \\ \mathbf{s}^H(\hat{\tau}_k^{(0)} + (q-1)\Delta) \\ \mathbf{s}^H(\hat{\tau}_k^{(0)} + q\Delta) \end{pmatrix} \in \mathbb{C}^{P \times M}, \quad (22)$$

which is now determined only by Δ , that is the temporal spacing of adjacent correlators, and $\hat{\tau}_k^{(0)} \in \mathbb{R}$ the estimated real valued delay of the LOS signal. The result of the cross-correlation yields the post-correlation signal

$$\mathbf{z}_k = \mathbf{Q}^H(\hat{\tau}_k^{(0)}) \mathbf{y}_k = \mathbf{Q}^H(\hat{\tau}_k^{(0)}) \mathbf{H}_k \mathbf{s}(\tau_k^{(0)}) + \mathbf{Q}^H(\hat{\tau}_k^{(0)}) \boldsymbol{\eta}_k \quad (23)$$

for $k = 0, 1, \dots$

Extended Kalman Filter Description

The received signal \mathbf{y}_k in the absence of noise can be fully described given the state $\mathbf{x}_k \in \mathbb{C}^{L+2}$ from (19). Thus, given a multicorrelator bank, we set the correlator spacing $\Delta = T_s$, which results in a number $P = 2L + 1$ of correlators. This way, we are able to align the $L + 1$ correlators, that is the "prompt" and the "late" part of the bank, with the channel \mathbf{H}_k experienced by the satellite signal $\mathbf{s}(\tau_k^{(0)})$. In the following, we propose a post-correlation EKF which for each $k = 0, 1, \dots$ estimates the state vector \mathbf{x}_k based on minimizing the mean square error using the measurements $\mathbf{z}_0, \dots, \mathbf{z}_k$.

The channel coefficients $h_k^{(\ell)}$ and LOS delay $\tau_k^{(0)}$ are assumed to be independent and the state transition of the EKF algorithm follows a random walk dynamic model

$$\tau_k^{(0)-} = \alpha_\tau \tau_{k-1}^{(0)+} + u_{\tau,k} \quad (24)$$

$$h_k^{(\ell)-} = \alpha_h^{(\ell)} h_{k-1}^{(\ell)+} + u_{h,k}^{(\ell)} \quad \forall \ell = 0, 1, \dots, L, \quad (25)$$

where $\tau_k^{(0)-}, h_k^{(\ell)-}$ is the filter prediction of the code delay and complex amplitude for the coherent integration k , $\tau_{k-1}^{(0)+}, h_{k-1}^{(\ell)+}$ the filter update of the code delay and complex amplitude for the coherent integration $k - 1$. $u_{\tau,k}$ and $u_{h,k}^{(\ell)}$ are mutually independent additive white Gaussian noise processes with variances β_τ and $\beta_h^{(\ell)}$. State transition model and measurement model can be written more compactly using the state prediction \mathbf{x}_k^- of the coherent period k and the state update \mathbf{x}_{k-1}^+ of the coherent integration period $k - 1$ as

$$\mathbf{x}_k^- = \mathbf{A} \mathbf{x}_{k-1}^+ + \mathbf{u}_k \quad (26)$$

$$\tau_{\text{ref},k}^- = \Re(\tau_k^{(0)-}) \quad (27)$$

$$\mathbf{z}_k = \mathbf{f}(\mathbf{x}_k, \tau_{\text{ref},k}^-, \boldsymbol{\eta}_k) \quad (28)$$

with the state transition matrix \mathbf{A} containing the forgetting factors for delay α_τ and for the channel taps $\alpha_{h^{(i)}}$

$$\mathbf{A} = \begin{pmatrix} \alpha_\tau & 0 & 0 & \dots & 0 \\ 0 & \alpha_{h^{(0)}} & 0 & \dots & 0 \\ 0 & 0 & \alpha_{h^{(1)}} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \alpha_{h^{(L)}} \end{pmatrix} \quad (29)$$

and the process noise vector

$$\mathbf{u}_k = [u_{\tau,k}, u_{h,k}^{(0)}, u_{h,k}^{(1)}, \dots, u_{h,k}^{(L)}]^H. \quad (30)$$

The process noise covariance matrix is defined as

$$\mathbf{B} \triangleq \mathbb{E}[\mathbf{u}_k \mathbf{u}_k^H] = \begin{pmatrix} \beta_\tau & 0 & 0 & \dots & 0 \\ 0 & \beta_{h^{(0)}} & 0 & \dots & 0 \\ 0 & 0 & \beta_{h^{(1)}} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \beta_{h^{(L)}} \end{pmatrix}. \quad (31)$$

The nonlinear measurement function is given by

$$\mathbf{z}_k = \mathbf{f}(\mathbf{x}_k, \tau_{\text{ref},k}^-, \boldsymbol{\eta}_k) = \mathbf{Q}^H(\tau_{\text{ref},k}^-) \left[\mathbf{H}_k \mathbf{s}_k(\tau_k^{(0)}) + \boldsymbol{\eta}_k \right], \quad (32)$$

where $\tau_{\text{ref},k}^-$ denotes the real part of the LOS delay prediction $\tau_k^{(0)}$ (Equation 27). The estimates for $\tau_k^{(0)}$ are in general complex due to the complex valued measurements \mathbf{z}_k . However, the physical true delay is real valued. In order to overcome a similar problem, [13] introduces a correction term in the innovation derivation of his EKF depending on the predicted imaginary part of his LOS delay estimate. This way, the LOS delay update estimate is forced to become real. In this paper however, we pursue a different but equivalent method. We can let the LOS delay estimation become complex but constrain the predicted delay estimation, which drives the correlator bank, to be real valued. Allowing the imaginary part to run free and driving the bank with the real valued part of the delay estimation achieves the same result while at the same time omitting the computation of a cumbersome correction term. It is important to notice that at time k , the measurement \mathbf{z}_k depends not only on noise and the true state \mathbf{x}_k , but also on the current prompt delay of the correlator bank. For instance, if the prompt delay deviates from the true LOS delay by more than T_c , the measurement will be independent of the state vector. We assume that the correlator bank's prompt delay to calculate \mathbf{z}_k is driven by the best current estimate, which is the prediction $\tau_k^{(0)-}$.

A. Prediction Stage

In the joint delay and channel estimation and tracking problem, the system model is linear as shown above. Thus, the EKF equations for the state prediction and associated covariance are

$$\mathbf{x}_k^- = \mathbf{A} \mathbf{x}_{k-1}^+ \quad (33)$$

$$\mathbf{P}_k^- = \mathbf{A} \mathbf{P}_{k-1}^+ \mathbf{A}^H + \mathbf{B}, \quad (34)$$

where \mathbf{P}_{k-1}^+ is the covariance associated with the EKF's state estimate at the end of the previous iteration (update). Further, the predicted measurement is defined as

$$\mathbf{z}_k^- = \mathbb{E} \{ \mathbf{z}_k | \mathbf{z}_{k-1}, \dots, \mathbf{z}_0 \} = \mathbb{E} \{ \mathbf{z}_k | \mathbf{x}_k^- \} = \mathbf{f}(\mathbf{x}_k^-, \mathbf{x}_k^-, \mathbf{0}) \quad (35)$$

which is equivalent to the measurement function evaluated at the predicted state vector \mathbf{x}_k^- .

B. Update Stage

The residual between measurement and predicted measurement is defined as

$$\boldsymbol{\epsilon}_k = \mathbf{z}_k - \mathbf{z}_k^-. \quad (36)$$

The computed predicted measurement \mathbf{z}_k^- can be computed using the measurement function in (32)

$$\mathbf{z}_k^- = \mathbf{f}(\mathbf{x}_k, \tau_{\text{ref},k}^-, \mathbf{0}) = \mathbf{Q}^H(\tau_{\text{ref},k}^-) \left[\mathbf{H}_k \mathbf{s}_k(\tau_k^{(0)}) \right]. \quad (37)$$

Assuming that the code delay model is well matched and that the satellite signal code delay does not change significantly within one coherent integration period, we have

$$\tau_{\text{ref},k}^- \approx \tau_k^{(0)}. \quad (38)$$

By exploiting Equation (38) and the relationship $\mathbf{s}^H(\tau)\mathbf{s}(\tau + n\Delta) = \Phi_{ss}(n\Delta)$ for any $n \in \mathbb{Z}$, $\tau \in \mathbb{R}$, we can simplify the expression for the predicted measurement as

$$\begin{aligned}
\mathbf{z}_k^- &= \mathbf{Q}^H(\tau_{\text{ref},k}^-) \mathbf{H}_k \mathbf{s}_k(\tau_k^{(0)}) \\
&= \sum_{\ell=0}^L h_k^{(\ell)-} \mathbf{Q}^H(\tau_{\text{ref},k}^-) \mathbf{Z}_k^\ell \mathbf{s}_k(\tau_k^{(0)}) \\
&= \sum_{\ell=0}^L h_k^{(\ell)-} \mathbf{Q}^H(0) \mathbf{Z}_k^\ell \mathbf{s}_k(0) \\
&= \sum_{\ell=0}^L h_k^{(\ell)-} \begin{pmatrix} \Phi_{ss}((\ell+q)\Delta) \\ \vdots \\ \Phi_{ss}((\ell-q)\Delta) \end{pmatrix}
\end{aligned} \tag{39}$$

That means that the inner term of Equation (39) needs to be calculated once and subsequently only updated accordingly with the predicted complex amplitudes.

From the residual, the updated state estimate and associated covariance are obtained as

$$\mathbf{x}_k^+ = \mathbf{x}_k^- + \mathbf{K}_k \boldsymbol{\epsilon}_k \tag{40}$$

$$\mathbf{P}_k^+ = (\mathbf{I} - \mathbf{K}_k \mathbf{F}_k) \mathbf{P}_k^- \tag{41}$$

with the Kalman gain

$$\mathbf{K}_k = \mathbf{P}_k^- \mathbf{F}_k^H \mathbf{S}_k^{-1} \in \mathbb{C}^{(L+2) \times P}, \tag{42}$$

the residual covariance matrix

$$\mathbf{S}_k = \mathbf{F}_k \mathbf{P}_k^- \mathbf{F}_k^H + \mathbf{V}_k \mathbf{R}_k \mathbf{V}_k^H. \tag{43}$$

The linearization of (32) with respect to the state, evaluated at the predicted state vector, provides matrix \mathbf{F}_k i.e.,

$$\mathbf{F}_k \triangleq \left. \frac{\partial \mathbf{f}(\mathbf{x}_k, \tau_{\text{ref},k}^-, \mathbf{0})}{\partial \mathbf{x}_k^*} \right|_{\mathbf{x}_k = \mathbf{x}_k^-} = \left(\begin{array}{c} \left. \frac{\partial \mathbf{f}^H(\mathbf{x}_k, \tau_{\text{ref},k}^-, \mathbf{0})}{\partial \tau_k^{*(0)}} \right|_{\mathbf{x}_k = \mathbf{x}_k^-} \\ \left. \frac{\partial \mathbf{f}^H(\mathbf{x}_k, \tau_{\text{ref},k}^-, \mathbf{0})}{\partial h_k^{*(0)}} \right|_{\mathbf{x}_k = \mathbf{x}_k^-} \\ \vdots \\ \left. \frac{\partial \mathbf{f}^H(\mathbf{x}_k, \tau_{\text{ref},k}^-, \mathbf{0})}{\partial h_k^{*(L)}} \right|_{\mathbf{x}_k = \mathbf{x}_k^-} \end{array} \right)^H \in \mathbb{C}^{P \times (L+2)}.$$

The partial derivative in (44) with respect to $\tau_k^{(0)}$ can be calculated as

$$\left. \frac{\partial \mathbf{f}(\mathbf{x}_k, \tau_{\text{ref},k}^-, \mathbf{0})}{\partial \tau_k^{*(0)}} \right|_{\mathbf{x}_k = \mathbf{x}_k^-} = \mathbf{Q}^H(\tau_{\text{ref},k}^-) \mathbf{H}_k \left. \frac{\partial \mathbf{s}(\tau_k^{(0)})}{\partial \tau_k^{(0)}} \right|_{\tau_k^{(0)} = \tau_{\text{ref},k}^-} \tag{44}$$

Similar to Equation 39, we exploit the relationship $\mathbf{s}^H(\tau)\mathbf{s}(\tau + n\Delta) = \Phi_{ss}(n\Delta)$ for any $n \in \mathbb{Z}$, $\tau \in \mathbb{R}$ and use (4) and (17), (44) to further simplify the measurement function derivative with respect to code delay. Thus, equation (44) becomes

$$\left. \frac{\partial \mathbf{f}(\mathbf{x}_k, \tau_{\text{ref},k}^-, \mathbf{0})}{\partial \tau_k^{*(0)}} \right|_{\mathbf{x}_k = \mathbf{x}_k^-} = \sum_{\ell=0}^L h_k^{(\ell)-} \begin{pmatrix} \Phi'_{ss}((\ell+q)\Delta) \\ \vdots \\ \Phi'_{ss}((\ell-q)\Delta) \end{pmatrix}, \tag{45}$$

where $\Phi'_{ss}(\tau) = \frac{d}{d\tau} \Phi_{ss}(\tau)$.

Likewise, we calculate the partial derivative in (44) with respect to $h_k^{*(\ell)}$ for $\ell = 0, \dots, L$

$$\begin{aligned} \left. \frac{\partial \mathbf{f}(\mathbf{x}_k, \tau_{\text{ref},k}^-, \mathbf{0})}{\partial h_k^{*(\ell)}} \right|_{\mathbf{x}_k = \mathbf{x}_k^-} &= \mathbf{Q}^H(\tau_{\text{ref},k}^-) \mathbf{Z}^\ell \mathbf{s}(\tau_{\text{ref},k}^-) \\ &= \mathbf{Q}^H(0) \mathbf{Z}^\ell \mathbf{s}(0) \\ &= \begin{pmatrix} \Phi_{ss}((\ell + q)\Delta) \\ \vdots \\ \Phi_{ss}((\ell - q)\Delta) \end{pmatrix}. \end{aligned} \quad (46)$$

It is worth noting that (46) does not depend on the prompt delay, hence is time-invariant. Thus, the $L + 1$ last columns of \mathbf{F}_k need to be calculated only once. On the other hand (45) can be expressed as a weighted sum of vectors with fixed vectors and time-variant weights, thus it needs to be updated at every measurement epoch with the predicted channel coefficient estimates. Since the pre-correlation noise $\boldsymbol{\eta}_k$ has i.i.d. standard normally distributed entries, the measurement noise covariance matrix is given as

$$\begin{aligned} \mathbf{R}_k &= \mathbf{Q}^H(\mathfrak{R}(\tau_k^{(0)-})) \mathbb{E}[\boldsymbol{\eta}_k^H \boldsymbol{\eta}_k] \mathbf{Q}(\mathfrak{R}(\tau_k^{(0)-})) \\ &= \mathbf{Q}^H(\mathfrak{R}(\tau_k^{(0)-})) \mathbb{E}[\boldsymbol{\eta}_k^H \boldsymbol{\eta}_k] \mathbf{Q}(\mathfrak{R}(\tau_k^{(0)-})) \\ &= \mathbf{Q}^H(0) \mathbb{E}[\boldsymbol{\eta}_k^H \boldsymbol{\eta}_k] \mathbf{Q}(0) \\ &= (1 + |h_k^{R-}|^2) \begin{pmatrix} \Phi_{ss}(0) & \dots & \Phi_{ss}(2q\Delta) \\ \vdots & \ddots & \vdots \\ \Phi_{ss}(2q\Delta) & \dots & \Phi_{ss}(0) \end{pmatrix}, \end{aligned} \quad (47)$$

where $|h_k^{R-}|^2$ corresponds to the interpolated and absolute squared predicted channel coefficient of the repeater in the channel. If the repeater is off or located outside the correlator bank, then $|h_k^{R-}|^2 \rightarrow 0$ and we have nominal operation for the proposed scheme. Also it is important to notice that the post-correlation measurement noise vector $\mathbf{Q}^H(\tau_{\text{ref},k}^-) \boldsymbol{\eta}_k$ has correlated entries despite $\boldsymbol{\eta}_k$ having i.i.d. entries. Due to multiplication with the correlator bank, the measurement noise of the EKF is colored with covariance \mathbf{R}_k .

C. Algorithm Discussion - Implementation Analysis

In the following, we discuss the requirements for a possible implementation of the proposed algorithm.

Traditional DLLs would feed the incoming signal \mathbf{y}_k to a "Correlator Bank" block containing a number of time shifted replicas of the PN sequence. The results of the cross-correlation operation is coherently integrated in the "Integrate & Dump", which produces a measurement every N_c integration periods. Its integrated correlator outputs are combined to calculate the delay correction for the current measurement epoch with the usage of a discriminator function. DLLs subsequently filter their discriminator output with a low-pass filter and may also utilize carrier-aiding to further smooth the delay correction. Next, they translate the calculated correction to a NCO rate update by which they control the PRN generator of the GNSS receiver. The updated PRN replica is finally used to close the DLL loop and perform the cross-correlation operation with the incoming signal at the next integration period.

Figure 3 illustrates the adaptations that need to be carried out in order to implement the proposed algorithm in the place of a "traditional" DLL.

The proposed algorithm requires a bank with P correlators according to Equation (22), whose number depends on the front-end bandwidth. This requires more computational resources than the regular three "early-prompt-late" correlators in a DLL but it is comparable for small front-end bandwidths the computational effort required for other discriminators such as the double delta discriminators. As seen in Figure 3, the proposed algorithm substitutes the discriminator function and the low-pass filter with an EKF filter. It tracks the form of the cross-correlation function by comparing the estimated cross-correlation function with the measurement z_k . Contrary to other extended Kalman filter implementations, the proposed scheme does not need to recalculate the predicted measurement or the measurement function partial derivative with respect to the complex amplitudes. Those remain constant and thus can be calculated at start-up and then stored in a Look-Up-Table (LUT). Similarly, the partial derivative with respect to delay and the measurement noise covariance matrix, only need to be updated with the current complex amplitude predictions. Thus, they also can be saved in a LUT and refreshed at every update iteration of the propose scheme. Overall, the

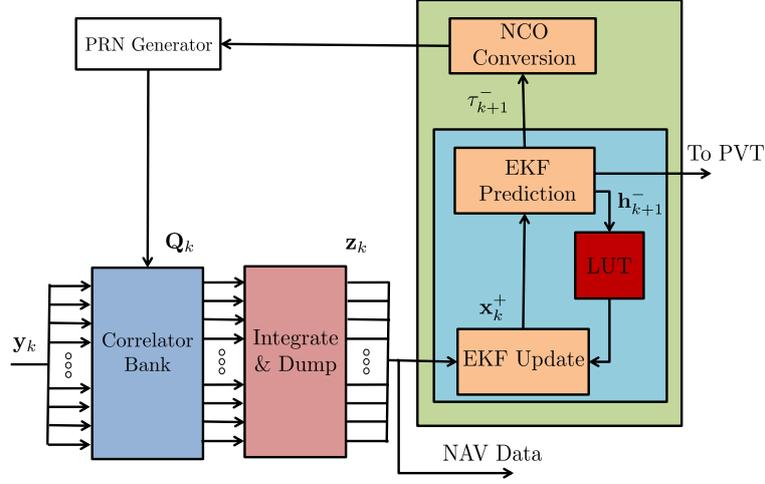


Figure 3: Block-wise visualization of the proposed EKF scheme.

internal EKF computations involve small matrix multiplications, additions and one inversion at a low rate, which depends on the integration time chosen, which can be handled with a small overhead in comparison to regular DLLs. As already mentioned, the main bottleneck of the algorithm remains the high number of correlators required in the bank for large front-end bandwidths.

VI SIMULATIVE RESULTS

In order to test the capabilities of the algorithm proposed, we carried out computer simulations to demonstrate its LOS delay and channel coefficients estimation capabilities. For the following simulation scenario, we choose $\lambda = 5$. Therefore, the nominal signal has single-sided bandwidth $B = \lambda/T_c = 5.115\text{MHz}$, is sampled with the Nyquist frequency frequency $f_s = \frac{2\lambda}{T_c} = 10.23\text{MHz}$ and subsequently cross-correlated with a correlator bank containing a total of $P = 2L + 1 = 21$ equispaced correlators with a spacing of $\Delta = \frac{2T_c}{L} = 0.1 T_c$. The nominal carrier-to-noise density (i.e. $\frac{C_0}{N_0}$) is set to 42dB-Hz, the LOS phase $\theta_k^0 = 0$ and therefore its LOS channel coefficient starts at $h_0^{(0)} = \sqrt{\frac{C_0}{N_0 B}} = 0.0557$. The received signal is subsequently cross-correlated and coherently integrated over $N_c = 5$ epochs. Thus, the effective $C/N_0' = C/N_0 + 10\log_{10}(N_c) = 49\text{dB-Hz}$. The initial delay estimation error is $\tau_0^{(0)} - \tau_0^{(0)+} = 0.0 T_c$, modeling stable tracking behavior, and the initial amplitude error is $h_0^{(0)} - h_0^{(0)+} = 0.0$, thus assuming accurate initial guess. The associated standard deviation of the initial guess is $0.5 T_c$ for the LOS delay and 0.1 for all amplitudes. Hereafter, the ground truth delay and amplitude of the LOS signal perform a random walk as defined in Equations (24-31) with $\mathbf{A} = \mathbf{I}$, $\sqrt{\beta_\tau} = 0.001 T_c$ and $\sqrt{\beta_h^{(\ell)}} = 0.01$ for $\ell = 0, \dots, L$. The EKF utilizes $N_c \beta_\tau$ for the delay process noise and respectively $N_c \beta_h^{(\ell)}$ for the coefficient process noise to account for the accumulated noise over the coherent integration time. For comparison, a second order DLL with an early-late spacing of $0.2 T_c$, a loop bandwidth of 0.8Hz and a normalized early-minus-late discriminator has been implemented and tested for the same scenario.

Sudden Repeater Interference

In the following, we investigate a scenario with a sudden start of AF repeater interference corresponding to the example in Figure 1. For the first 500ms the GNSS receiver only receives LOS satellite signals. After that, the signal of an AF repeater located at a distance of $r = 80\text{m}$ and with an $\alpha = 77.5\text{dB}$ amplification is received and interferes with nominal GNSS reception. Based on (1), the repeated signal undergoes a free space loss $g(r) = 74.5\text{dB}$ and thus the net amplification gain becomes $\alpha g(r) = 3\text{dB}$. Additionally, the repeater signal arrives with a relative phase difference $\Delta\theta = \theta_k^0 - \theta_k^R = \frac{\pi}{4}$ respective to the LOS, meaning that the repeated signal power is split equally between the in-phase and the quadrature channel seen at the receiver. It is interesting to note that since the resulting C/N_0 at the receiver is 49dB-Hz and the net amplification gain of the repeater $\alpha g(r) = 3\text{dB}$, a GNSS receiver with a "traditional" DLL estimator would experience effects corresponding to Region III in Figure (2). Thus, we expect that the DLL would track the repeated signal instead of the satellite signal.

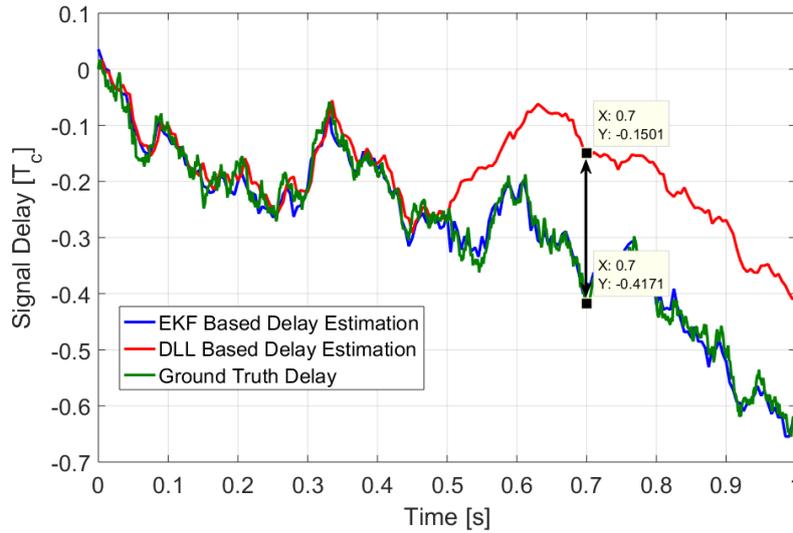


Figure 4: Comparison of the real LOS delay with the DLL and EKF based estimate.

Figure (4) illustrates the influence of the repeated signal on the delay estimation. In the first 500ms both the traditional DLL and the proposed algorithm are able to perfectly follow the random walk that the ground truth delay is undergoing. However, as soon as the repeater signal is introduced, the traditional DLL experiences a delay bias due to its effect. That is since the repeated signal replica is 3dB stronger than the LOS and arrives with a relative delay equal to $\Delta\tau = \frac{r}{cT_c} = 0.273$ chips. As a matter of fact, the bias to the ground truth for the regular DLL is approximately 0.27 chips as it can be seen in Figure (4). The proposed algorithm however appears to be immune to the repeater effect and is able to accurately track the ground truth delay.

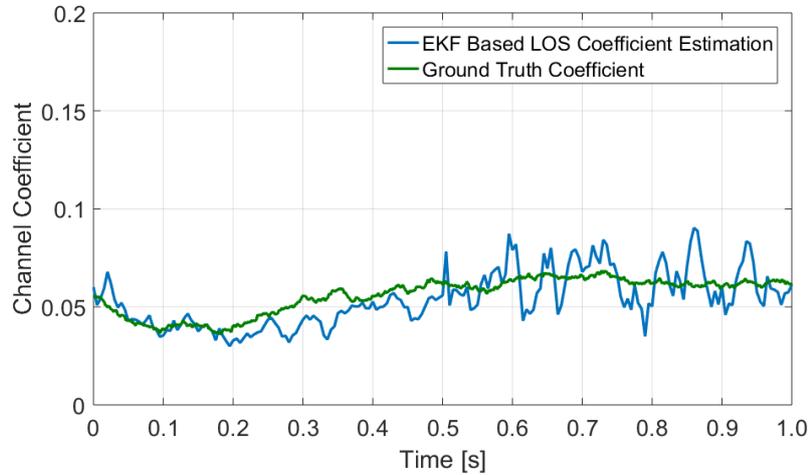


Figure 5: Comparison of the real and estimated LOS amplitude.

Figure (5) shows the estimation and ground truth for the LOS channel coefficient. It can be seen that proposed algorithm is able to estimate and track the behavior of LOS with a small variance in the first 500ms. As soon as the repeater signal is turned on, the proposed algorithm is still able to track the LOS amplitude but the variance of the estimation is increased due to the increased noise introduced by the repeater.

As it can be seen from Figure (6), the proposed algorithm converges and keeps the relative error for both the LOS delay and amplitude estimation small and well bounded. This can be inferred by the $3\sigma_\tau$ and $3\sigma_{h^0}$ standard deviations for LOS delay and amplitude, which can be extracted by the respective elements of the state covariance matrix \mathbf{P}_k . Both of them quickly converge to a steady value and confidently over-bound the respective calculated absolute errors for delay and amplitude estimation.

Figure (7-8) show the respective estimates of the inphase and quadrature Channel Impulse Responses (CIR) over time and delay. As it can be seen from Figure (7), at the start of the simulation, the LOS is dominant and centered around $0T_c$ delay. All the subsequent channel coefficient estimates have a noise-like behaviour. Since the LOS phase θ_k^0 is set to zero, the LOS is purely

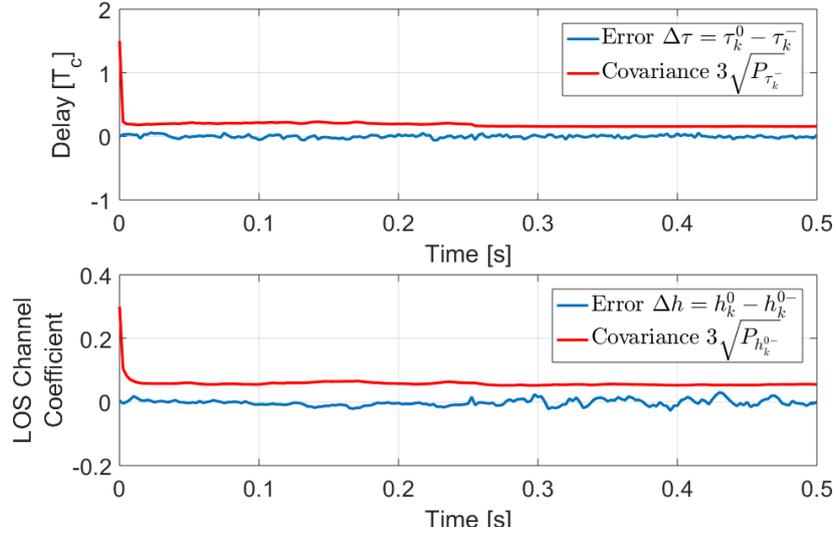


Figure 6: LOS delay and amplitude estimation error over their respective 3σ variances.

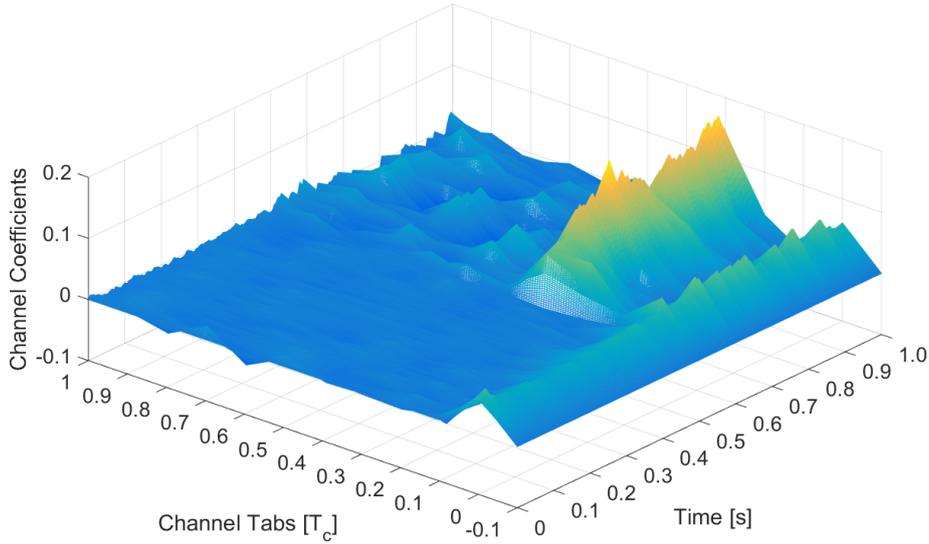


Figure 7: Visualization of the interpolated inphase CIR.

real. Thus, it appears in the inphase part of the channel (Figure 7) and only noise can be observed in the quadrature (Figure 8). After 500ms, the repeater is turned on and the proposed algorithm adapts to the joint LOS and repeater signal presence. It is able to estimate the repeater presence between the channel tabs $h_k^{(2)}$ and $h_k^{(3)}$, which correspond to a 0.2 and 0.3 relative chip delay with respect to the LOS. Due to the repeaters relative phase $\Delta\theta = \frac{\pi}{4}$, the repeated signal appears in both the inphase and quadrature channel impulse response. Furthermore, as Figure 7-Figure 8 indicate, the repeater channel coefficients have approximately the same weighting, which is to be expected to the relative phase of the repeated signal. At this point it is also interesting to mention that the inactive channel taps now have a larger noise variance in comparison to the nominal operation during the first 500ms. This can be traced to the thermal noise amplification of the repeater.

Figure (9) shows the averaged and interpolated estimated channel impulse response during the repeater presence. The interpolated inphase channel coefficients show the LOS at $0T_c$ with an estimated $h_0 \approx 0.053$. That corresponds well with the LOS channel coefficient during the last 500ms of the simulation under the repeater presence (Figure 5). At the same time the LOS does not appear in the quadrature channel since its channel coefficient is real valued ($\theta_k^0 = 0$). The repeated signal appears in both inphase and quadrature components of the channel. The interpolation of both components yields a maximum at a channel delay $0.2727\text{chips} \approx 79.9011$ meters, which fits nicely to the receiver-repeater distance which is 80 meters or 0.2723 chips. That

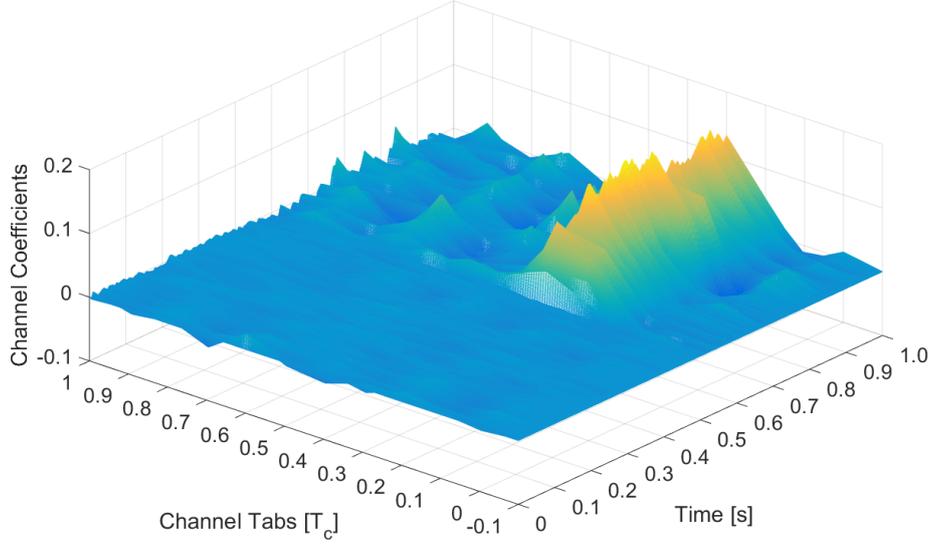


Figure 8: Visualization of the interpolated quadrature CIR.

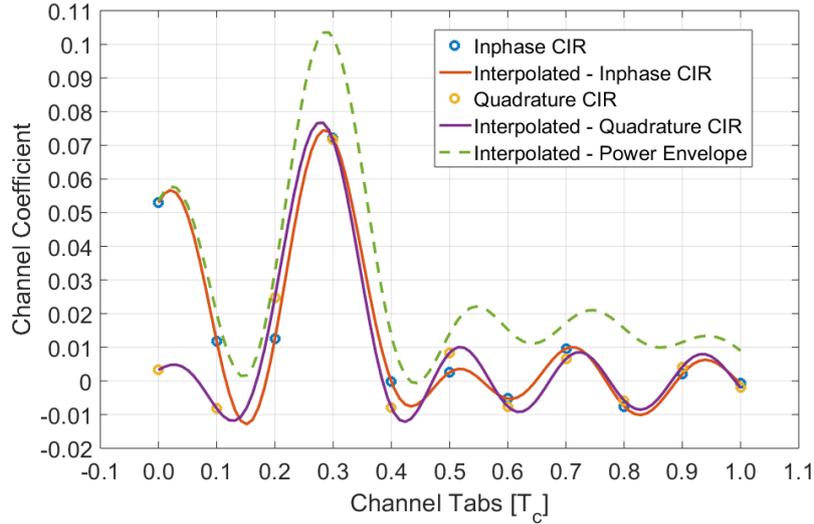


Figure 9: Averaged and interpolated Channel Impulse Response (CIR).

means that the proposed algorithm can estimate the repeater-receiver range. At the same time taking the tangent inverse of the quadrature to inphase maximum ratio, we can also estimate the repeater phase relative to that of the LOS

$$\begin{aligned} \theta^R &= \arctan\left(\frac{Q_{max}}{I_{max}}\right) \\ &= \arctan\left(\frac{0.074}{0.077}\right) \approx \frac{\pi}{4}. \end{aligned} \quad (48)$$

Finally, based on the channel impulse response we can also infer the transmit power of the repeater. In order to estimate the repeater net amplification gain seen at the receiver, we need to compute the mean power envelope of the channel impulse response seen in Figure (9). Specifically, we take the repeater power envelope contributions in both components and normalize with the respective LOS power. That is

$$AG_{dB} = 10 \log_{10}\left(\frac{0.1035}{0.05302}\right) = 2.9dB. \quad (49)$$

By utilizing Equation (1) and the estimated distance to the repeater $r \approx 79.9011$, we have

$$\begin{aligned}\alpha &= AG_{dB} - g(r) \\ &= 2.9dB - (-74.45dB) = 77.35dB,\end{aligned}\tag{50}$$

which fits well with the simulated amplification of $\alpha = 77.4575dB$. That means that with the help with the proposed scheme, we are not only immune to repeater effects and able to track satellite signals with high accuracy under repeater presence but also able to characterize and localize in real time repeaters with respect to their distance to the receiver, their relative phase and their transmitted power.

VII CONCLUSION

In this paper, we have studied the problem of Global Navigation Satellite System (GNSS) code delay tracking under the presence of GNSS repeater signals. First, we completed a satellite signal code delay threat analysis, since repeater signals act as interference to Delay-Locked-Loops (DLLs) estimators used in GNSS. Next, we proposed an Extended Kalman Filter (EKF) based algorithm that utilized a correlator bank structure, which is able to mitigate the interference effects of GNSS repeaters. Finally, based on simulation results, we have shown that the proposed algorithm is able to characterize the interfering repeater in its parameters.

ACKNOWLEDGMENTS

The research leading to these results has been carried out under the framework of the project "R&D for the maritime safety and security and corresponding real time services". The project started in January 2013 and is led by the Program Coordination Defense and Security Research within the German Aerospace Center (DLR).

REFERENCES

- [1] GPSS Operations Enabled, "Defense GPS Hangar Repeater Kit," <https://www.gpssource.com/products/gli-hangar>.
- [2] A. Vervisch-Picois and N. Samama, "Interference Mitigation in a Repeater and Pseudolite Indoor Positioning System," *IEEE Journal of Selected Topics in Signal Processing*, vol. 3, no. 5, pp. 810–820, Oct 2009.
- [3] Aeronautical Communications Panel (ACP), "EUR Frequency Management Group Meeting – Summary of Discussions," 23rd Meeting of Working Group F, Cairo Egypt, September 2010.
- [4] E. E. . 645, "Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices; Global Navigation Satellite Systems (GNSS) Repeaters," March 2010.
- [5] R. E. Phelts, "Multicorrelator Techniques for Robust Mitigation of Threats to GPS Signal Quality," Stanford University, March 2001.
- [6] O. M. Mubarak and A. G. Dempster, "Analysis of early late phase in single-and dual-frequency GPS receivers for multipath detection," 2010.
- [7] K. Wesson, D. Shepard, J. Bhatti, and T. Humphreys, "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation*, 2011.
- [8] J. Blanch, T. Walker, P. Enge, Y. Lee, B. Pervan, M. Rippl, A. Spletter, and V. Kropp, "Baseline advanced RAIM user algorithm and possible improvements," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 51, no. 1, pp. 713–732, January 2015.
- [9] I. Martini, M. Rippl, and M. Meurer, "Advanced RAIM Architecture Design and User Algorithm Performance in a Real GPS, GLONASS and Galileo Scenario," *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, 2013.
- [10] K. Giger, *Multi-Signal Tracking in GNSS*. Dr. Hut, 2014.
- [11] A. Angrisano, "GNSS/INS Integration Methods," Ph.D. dissertation, Università degli Studi di Napoli "Parthenope", 2010.
- [12] R. A. Iltis, "Joint estimation of PN code delay and multipath using the extended Kalman filter," *IEEE Transactions on Communications*, vol. 38, no. 10, pp. 1677–1685, Oct 1990.

- [13] R. A. Iltis and A. W. Fuxjaeger, "A digital DS spread-spectrum receiver with joint channel and Doppler shift estimation," *IEEE Transactions on Communications*, vol. 39, no. 8, pp. 1255–1267, Aug 1991.
- [14] M. L. Psiaki and H. Jung, "Extended Kalman Filter Methods for Tracking Weak GPS Signals," *Proceedings of the 15th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*, September 2002.
- [15] Z. N. and J. Garrison., "Extended Kalman Filter-Based Tracking of Weak GPS Signals under High Dynamic Conditions," *Proceedings of the 17th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*, September 2004.
- [16] A. Lakhzouri, E. S. Lohan, R. Hamila, and M. Renfors, "Extended Kalman Filter Channel Estimation for Line-of-Sight Detection in WCDMA Mobile Positioning," *EURASIP J. Adv. Sig. Proc.*, vol. 2003, pp. 1268–1278, 2003.
- [17] J. S. Vera, "Efficient Multipath Mitigation in Navigation Systems," Ph.D. dissertation, Universitat Politècnica de Catalunya, Feb. 2004.
- [18] N. Blanco-Delgado and F. D. Nunes, "Multipath Estimation in Multicorrelator GNSS Receivers using the Maximum Likelihood Principle," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 48, no. 4, pp. 3222–3233, October 2012.
- [19] M. Lentmaier and B. K. P. Robertson, "Bayesian Time Delay Estimation of GNSS Signals in Dynamic Multipath Environments," *International Journal of Navigation and Observation*, 2008.
- [20] C. Cheng, Q. Pan, V. Calmettes, and J. Y. Tourneret, "A maximum likelihood-based unscented Kalman filter for multipath mitigation in a multi-correlator based GNSS receiver," in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, March 2016, pp. 6560–6564.
- [21] S. Negin, A. Broumandan, J. Curran, and G. Lachapelle, "Accurate GNSS Range Estimation in Multipath Environments Using Stochastic-Gradient-Based Adaptive Filtering," *Navigation*, vol. 63, no. 1, pp. 39–52, 2016, nAVI-2014-034.R1.
- [22] A. Iliopoulos, C. Enneking, O. G. Crespillo, T. Jost, S. Thoenert, and F. Antreich, "Multicorrelator Signal Tracking and Signal Quality Monitoring for GNSS with Extended Kalman Filter," *IEEE Aerospace Conference*, March 2017.
- [23] C. Hoymann, W. Chen, J. Montojo, A. Golitschek, C. Koutsimanis, and X. Shen, "Relaying operation in 3GPP LTE: challenges and solutions," *IEEE Communications Magazine*, vol. 50, no. 2, pp. 156–162, February 2012.
- [24] Global Positioning Systems Directorate Systems Engineering & Integration, "Interface Specification IS-GPS-200H, NAVSTAR GPS Space Segment/ Navigation User Segment Interfaces," Tech. Rep., December 2015.
- [25] SC-159, "Minimum Aviation System Performance Standards for Local Area Augmentation System, RTCA DO-245A," Radio Technical Commission for Aeronautics, 1150 18th Street, NW, Suite 910 Washington, DC, Tech. Rep., September 2004.
- [26] —, "Minimum Operational Performance Standards for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment, RTCA DO-229E," Radio Technical Commission for Aeronautics, 1150 18th Street, NW, Suite 910 Washington, DC, Tech. Rep., December 2016.
- [27] E. Kaplan and C. Hegarty, *Understanding GPS: Principles and Applications*, ser. Artech House mobile communications series. Artech House, 2006.