






Joint Communication and Positioning Receiver Architecture for DSSS-overlaid OFDM Waveform

Alejandro Gonzalez-Garrido ¹ , Graduate student IEEE, Idir Edjekouane ¹ , Member IEEE, Jorge Querol ¹ , Member IEEE, Henk Wymeersch ² , Fellow IEEE, Symeon Chatzinotas ¹ , Fellow IEEE

¹¹ Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, 1359 Luxembourg City, Luxembourg

²² Department of Electrical Engineering, Chalmers University of Technology

CORRESPONDING AUTHOR: A. Gonzalez-Garrido (e-mail: alejandro.gonzalez@uni.lu).

This work was supported by the Framework of Fonds National de la Recherche: SMS2 Project, funded by FNR under Contract C-C24/IS/18957132/SMS2.

ABSTRACT The integration of satellite systems within the 5G new radio (NR) framework, designated as non-terrestrial networks (NTNs), relies on global navigation satellite systems (GNSS) to achieve precise synchronization. However, dependence on GNSS presents significant vulnerabilities in scenarios involving signal degradation, jamming, or spoofing, alongside increased cost and power consumption issues, particularly in extensive internet of things (IoT) deployments. To address these challenges, this paper proposes an innovative joint communication and positioning (JCAP) receiver architecture, which integrates direct sequence spread spectrum (DSSS) signals into the 5G orthogonal frequency division multiplexing (OFDM) waveform, enabling GNSS-free synchronization and positioning capabilities without embedded pilot overhead. The proposed hybrid architecture jointly exploits DSSS for robust channel parameter estimation and OFDM for high-throughput communication, thereby reducing the pilots signals traditionally required for synchronization and channel estimation. Comprehensive evaluations demonstrate that the proposed JCAP receiver achieves reliable detection and accurate estimation of delay and Doppler parameters, maintaining low bit error rates (BER) under realistic signal-to-interference ratios (SIR). The findings underscore the feasibility and effectiveness of the proposed hybrid scheme, paving the way for resilient GNSS-free operations in 5G NTN environments.

INDEX TERMS Joint communication and positioning, 5G NTN, Extended Kalman Filter.

I. INTRODUCTION

The integration of satellite communication systems into the fifth generation (5G) new radio (NR) architecture, termed non-terrestrial networks (NTNs), enables satellites to function as next generation base stations (gNBs). This architecture inherently requires user equipment (UE) to incorporate a global navigation satellite system (GNSS) receiver to maintain precise synchronization with satellite gNB and ensure a coherent system-wide timing reference [1]. While this integration facilitates synchronization, it introduces a critical vulnerability: service continuity becomes dependent on an external, third-party

system (the GNSS), whose operational integrity lies beyond the satellite network operator's control.

Consequently, scenarios characterized by degraded or intentionally denied GNSS signals, such as through jamming or spoofing [2], result in compromised network reliability, despite potentially direct line of sight (LOS) connectivity to satellites. Furthermore, for extensive internet of things (IoT) deployments, embedding GNSS receivers into each device presents significant economic and energy-efficiency barriers due to increased hardware costs and substantial power consumption of GNSS chips.

Addressing these constraints necessitates alternative synchronization approaches independent of GNSS, as

recognized by the 3rd generation partnership project (3GPP) through the conceptualization of GNSS-free operations [3]. Achieving effective GNSS-free synchronization at the physical layer poses substantial waveform design challenges [4]. Our approach maintain back compatibility with 5G.

The joint communication and positioning (JCAP) approach has been increasingly proposed as a viable strategy for providing integrated navigation services without exclusive reliance on GNSS, simultaneously supporting communication functionality [5]–[9]. However, within actual 5G terrestrial systems, localization typically relies on embedding dedicated pilot signals, such as positioning reference signal (PRS), into the communication waveform to facilitate observables estimation and subsequent user localization [10], [11]. Such approaches introduce significant overhead to the communication system as the resources dedicated to positioning, navigation, and timing (PNT) are not dedicated to communications and the business model for the network operators came from the communication service, not the navigation service. Also, the terrestrial approach does not scale well as the use of the PRS requires the UE to be connected to the network, and in NTN scenarios the UE position is required prior the network connection. Therefore, including the PRS for PNT services in NTN does not solve the problem for the UE initial access.

There is also a recent work in [12] where they show a JCAP system from low earth orbit (LEO) satellites, this work present a similar waveform used here called time coded (TC)-orthogonal frequency-division multiplexing (OFDM). A similar waveform has been also presented and evaluated in a previous work [13]. This hybrid waveform can be seen as an extension to the 5G downlink waveform, as it is transparent to the 5G system, if the UE has capabilities to exploit this hybrid waveform, it can benefit from it, and those UE who do not have these capabilities can work with only the 5G signal being completely transparent to the UE.

Novel advancements in this domain include approaches such as augmenting the 5G downlink waveform with direct-sequence spread spectrum (DSSS) signals, enabling simultaneous navigation functionality [13]. This hybridization not only allows to serve a JCAP services, it can also benefit the communication services as an authentication method for the communication signal as presented in [14]. The work [14] employs an overlap DSSS as a physical-layer watermark for authentication/security. Its DSSS component serves a verification role and is not used to derive navigation observables.

In the recent work [15] the author analysed the communication performance of a JCAP receiver comprising distinct navigation and communication modules interconnected primarily through data exchange for satellite ephemeris used in the navigation block. However, the architecture proposed in [15] segregates navigation and communication functions, operated in parallel without

architectural feedback from the navigation chain into the communication demodulator, limiting mutual enhancements at the physical layer.

To bridge this research gap, the current work proposes an innovative hybrid JCAP receiver architecture that fully integrates navigation and communication processes. This integration is done by using the channel parameters estimations using the DSSS component to enhance the signal used for the communication service. The key contributions of this paper are:

- The introduction of a hybrid JCAP receiver architecture that employs the DSSS component for accurate estimation of channel parameters, subsequently utilizing these estimates for signal compensation and OFDM demodulation, thereby eliminating the need for dedicated pilot signals.
- A thorough evaluation of navigation receiver tracking loops performance in terms of estimation accuracy, explicitly considering the coexisting OFDM waveform as interference. Performance assessment of the proposed communication system by analyzing the uncoded bit error rate (BER) under different DSSS interference conditions.

The remainder of the paper is organized as follows. Section II describes the mathematical models underpinning the proposed system. Section III elaborates on the proposed hybrid receiver architecture. In Section IV, we present a detailed performance evaluation, discussing simulation outcomes. Finally, Section V summarizes our findings and outlines future research directions.

Throughout this paper, vectors are denoted by boldface lowercase letters (**a**), matrices by boldface uppercase letters (**A**), the complex conjugate by $(\cdot)^*$, the Kronecker product by \otimes , complex Gaussian random variables with zero mean and variance σ^2 as $\mathcal{CN}(0, \sigma^2)$, a uniform random variable in the range $[a, b]$ is defined as $\mathcal{U}(a, b)$, expectation as $\mathbb{E}\{\cdot\}$, transpose by $(\cdot)^T$, Hermitian (conjugate transpose) by $(\cdot)^H$ and phase wrapping as $\text{wrap}\{\cdot\}$ confines the argument (angle) to $(-\pi, \pi]$.

II. SYSTEM MODEL

In this section, we introduce the mathematical models utilized in this work. First, we present the antenna beamforming model implemented by the LEO satellite payload. Subsequently, we describe the channel model and justify the adopted parameters based on realistic assumptions for satellite scenarios. Next, we derive the received signal model, followed by the definition of the hybrid transmitted waveform. Finally, we provide the analytical expressions for the signal-to-interference plus noise ratio (SINR) of the communication and navigation services.

A. ANTENNA AND BEAMFORMING

We consider a satellite payload equipped with a square uniform planar array (UPA) consisting of $N_t = N_x N_y$ antenna elements arranged with half-wavelength spacing. The normalized steering vectors along the x and y axes are expressed respectively as:

$$\mathbf{a}_x = [a_{x,0}(\theta, \phi), \dots, a_{x,p_x}(\theta, \phi), \dots, a_{x,N_x-1}(\theta, \phi)]^T, \quad (1)$$

$$\mathbf{a}_y = [a_{y,0}(\theta, \phi), \dots, a_{y,p_y}(\theta, \phi), \dots, a_{y,N_y-1}(\theta, \phi)]^T, \quad (2)$$

where each element of these vectors is defined as:

$$a_{x,p_x}(\theta, \phi) = \frac{1}{\sqrt{N_x}} e^{j\pi p_x u_x}, \quad u_x = \sin \theta \cos \phi, \quad (3)$$

$$a_{y,p_y}(\theta, \phi) = \frac{1}{\sqrt{N_y}} e^{j\pi p_y u_y}, \quad u_y = \sin \theta \sin \phi, \quad (4)$$

with indices $p_x \in \{0, \dots, N_x - 1\}$, $p_y \in \{0, \dots, N_y - 1\}$, and angles (θ, ϕ) representing the elevation and azimuth angles from the satellite antenna array towards the UE. The complete two-dimensional array response vector is obtained as:

$$\mathbf{a}(\theta, \phi) = \mathbf{a}_x \otimes \mathbf{a}_y \in \mathbb{C}^{N_t \times 1}. \quad (5)$$

The payload from satellite q implements a fixed digital beamforming (DBF) defined by $\mathbf{W}_q = [\mathbf{w}_{q,1}, \dots, \mathbf{w}_{q,K}]$, where each column vector $\mathbf{w}_{q,k} = \mathbf{a}^*(\theta_k, \phi_k)$ defines the beamforming weights corresponding to the wide area beam k pointing to a predefined direction (θ_k, ϕ_k) . This configuration corresponds to the *moving-cells* scenario standardized by 3GPP in [16]. In this scenario, each beam cover an area to serve several users, where due to the satellite movement, the area of coverage moves with it.

B. CHANNEL MODEL

Assuming a narrowband signal that $B/f_c \ll 1$ with B being the signal bandwidth, and f_c the carrier frequency, we adopt in (6) a discrete M -tap delay line model for the channel response of path m from satellite q of beam k sampled at T_s samples per second. Where $\alpha_{q,k,m} = |\alpha_{q,k,m}| \exp(j\varphi_{q,k,m}) \in \mathbb{C}$ denotes the complex channel gain, $\nu_{q,k,m}$ is the Doppler frequency from path m for satellite q and beam k , $d_{q,k,m}$ represents the delay, and $(\theta_{q,k,m}^{(rx)}, \phi_{q,k,m}^{(rx)})$ are the angles of departure for path m from beam k towards the UE.

Considering a LOS-dominated propagation scenario, typical for satellite-to-ground communications with elevation angles exceeding 30° , and a UE with an antenna with a radiation pattern similar to those found in GNSS antennas [17], the channel can be simplified substantially. The UE antenna is primarily a spatial filter to elevate the signal-to-noise ratio (SNR) of LOS signals from satellites, by suppressing multipath from ground. Due to the high reduction of multipath components by using these type of antenna in the UE [17], [18], and limited angular spread of the ground reflections [19], the LOS component

overwhelmingly dominates, leading to:

$$|\mathbf{h}_{q,k,0}^H \mathbf{w}_{q,k}| \gg |\mathbf{h}_{q,k,m}^H \mathbf{w}_{q,k}|, \quad m > 0, \quad (7)$$

where the subindex m is to denote the different multipaths of the same signal. Therefore, this work reasonably adopts the simplified assumption of a single-tap LOS channel model ($M = 1$), which remains valid given the primary focus on JCAP performance analysis under LOS conditions. To reduce notation, we remove the subindex m from the channel model.

C. RECEIVED SIGNAL MODEL

The discrete-time received baseband signal, sampled at T_s samples per second, can be expressed as the contributions from the Q satellites in LOS and the K beams from each satellite as

$$r[n] = \sum_{q=1}^Q \sum_{k=1}^K r_{q,k}[n] + w[n], \quad (8)$$

where $r_{q,k}[n] = \mathbf{h}_{q,k}^T[n] \mathbf{w}_{q,k} s_{q,k}[n - d_{q,k}]$ represent the signal received from satellite q and beam k , $\mathbf{w}_{q,k}$ is the steering vector for beam k at satellite q , $s_{q,k}$ is the downlink stream from satellite q and beam k , and $w[n] \sim \mathcal{CN}(0, \sigma_n^2)$ is additive Gaussian noise at the receiver.

D. HYBRID DOWNLINK WAVEFORM

The hybrid transmitter consists of the input bitstream from the upper layers, which are then subsequently mapped into the physical downlink shared channel (PDSCH) and modulated using OFDM according to the 3GPP specifications. Concurrently, a DSSS signal is generated and combined with the OFDM waveform, ensuring a predefined signal-to-interference ratio (SIR) $\text{SIR}_{\text{DSSS}} = \rho$ (where the signal is the communication service and the interference is the DSSS). Here we assume the value of ρ is the same for all satellites. The aggregation is performed by aligning the beginning of the DSSS waveform with the start of the 5G subframe, resulting in identical durations (1 ms) and sampling frequencies f_s for both waveforms. Finally, the aggregated waveform is processed through the DBF matrix.

The channel model described by (6) is then applied to the transmitted waveform to emulate the channel impairments and generate the received signal $r[n]$. The overall transmitter architecture, including the channel response \mathbf{h} for each beam, is depicted in Fig. 1. Where each beam k in Fig. 1 simultaneously transmits the hybrid waveform at a sampling frequency $f_s = 1/T_s$, defined as

$$s_{q,k}[n] = \sqrt{1 - \rho} z_{q,k}[n] + \sqrt{\rho} \tilde{z}_q[n], \quad 0 \leq \rho \leq 1, \quad (9)$$

where $z_{q,k}[n]$ is the time-domain 5G OFDM signal from beam k and satellite q with $\mathbb{E}\{|z_{q,k}[n]|^2\} = 1$, and $\tilde{z}_q[n]$ represents a DSSS sequence from satellite q of length L_c with $\mathbb{E}\{|\tilde{z}_q|^2\} = 1$.

The time-domain OFDM signal $z_{q,k}[n]$ has a length (in samples) that depends on the resource block (RB) used. The

$$\mathbf{h}_{q,k,m}[n] = \alpha_{q,k,m} e^{j\nu_{q,k,m} n T_s} \mathbf{a}(\theta_{q,k,m}^{(rx)}, \phi_{q,k,m}^{(rx)}) \delta[n - d_{q,k,m}] \quad (6)$$

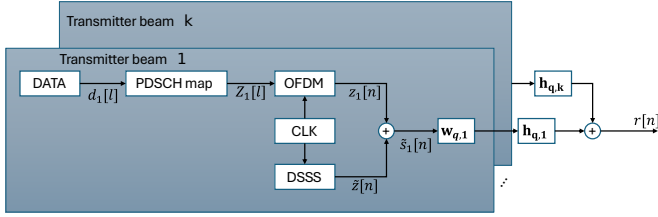


Fig. 1. Transmitter architecture for satellite q integrating DSSS and OFDM waveforms for JCAP services.

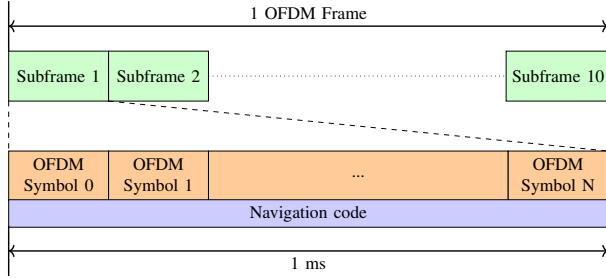


Fig. 2. OFDM+DSSS combining data transfer and a navigation signal using the 5G Frame structure.

number of RB defined as N_{RB} , are blocks of 12 subcarriers and define the bandwidth of the signal. This also defined the length of the DSSS as they are synchronized to have the same length in samples. Both signals share a common sampling clock at f_s rate, thus ensuring coherent alignment at sample-level as illustrated in Fig. 2.

This hybrid waveform corresponds to the *shared beam* model under the frequency re-use factor 3 (FRF3) scenario discussed in [13]. The choice of this waveform structure is motivated by its minimal impact on the satellite payload architecture, specifically avoiding modifications to the established DBF configuration, and its backward compatibility with non-JCAP receivers, enabling straightforward deployment in existing software-defined payloads via firmware updates [20], [21].

E. SIGNAL TO INTERFERENCE PLUS NOISE RATIO ANALYSIS

We can split (8) in terms of the signal of interest $r_{g,i}[n]$ from satellite g and beam i , and treat the rest of satellites and beams as interference plus the receiver noise. This model is as follows

$$r[n] = r_{g,i}[n] + \sum_{k \neq i}^K r_{g,k}[n] + \sum_{q=1}^Q \sum_{k=1}^K r_{q,k}[n] + w[n]. \quad (10)$$

We define the effective scalar channel gain for beam k from satellite q assuming a stationary channel over the time of observation, and considering only the LOS path (as seen

in the channel model subsection), we define the following

$$\begin{aligned} h_{q,k} &\triangleq \mathbb{E}\{|\mathbf{h}_{q,k}^T[n] \mathbf{w}_{q,k}|^2\} \\ &= \mathbb{E}\{|\alpha_{q,k}|^2\} |\mathbf{a}^T(\theta_{q,k}^{(rx)}, \phi_{q,k}^{(rx)}) \mathbf{w}_{q,k}|^2 \\ &= |\mu_q|^2 |\mathbf{a}^T(\theta_{q,k}^{(rx)}, \phi_{q,k}^{(rx)}) \mathbf{w}_{q,k}|^2, \end{aligned} \quad (11)$$

where μ_q represent the path loss due to the distance between the UE and the different satellites q .

By using the definition of $h_{q,k}$ as a scalar that represent the power loss due to the channel at the UE for the different elements in the system, we define the following quantities to analyze the SINR

$$\mathbb{E}\{|\mathbf{h}_{g,i}^T[n] \mathbf{w}_{g,i} \sqrt{1 - \rho} \tilde{z}[n - d_{g,i}]|^2\} = (1 - \rho) h_{g,i}, \quad (12)$$

$$\mathbb{E}\{|\mathbf{h}_{g,i}^T[n] \mathbf{w}_{g,i} \sqrt{\rho} \tilde{z}[n - d_{g,i}]|^2\} = \rho h_{g,i}, \quad (13)$$

$$\mathbb{E}\left\{\left|\sum_{k \neq i}^K \mathbf{h}_{g,k}^T[n] \mathbf{w}_{g,k} s_{g,k}[n - d_{g,k}]\right|^2\right\} = R_K, \quad (14)$$

$$\mathbb{E}\left\{\left|\sum_{q \neq g}^Q \sum_{k=1}^K \mathbf{h}_{q,k}^T[n] \mathbf{w}_{q,k} s_{q,k}[n - d_{q,k}]\right|^2\right\} = R_Q. \quad (15)$$

The resulting SINR for the 5G waveform component from satellite g and beam i can thus be expressed as

$$\gamma_{z,g,i} = \frac{(1 - \rho) h_{g,i}}{\rho h_{g,i} + R_K + R_Q + \sigma_n^2}, \quad (16)$$

and similarly, the SINR for the DSSS waveform component from the same satellite and beam is given by

$$\gamma_{\tilde{z},g,i} = \frac{\rho h_{g,i}}{(1 - \rho) h_{g,i} + R_K + R_Q + \sigma_n^2}. \quad (17)$$

These expressions form the analytical basis for the evaluation of communication performance within the proposed JCAP system. It can be seen that the impact the other beams R_K or satellites R_Q is the same for both services.

III. RECEIVER ARCHITECTURE

In this section, we detail the proposed hybrid receiver architecture. This receiver is designed to jointly integrate navigation and communication functionalities within a single receiver structure. Leveraging mutual interactions between both services, the proposed architecture aims to enhance overall performance by exploiting the complementary information provided by each subsystem.

A. NAVIGATION RECEIVER

It is required at least 4 parallel channels as a minimum of 4 satellites are needed for an estimation of the UE state

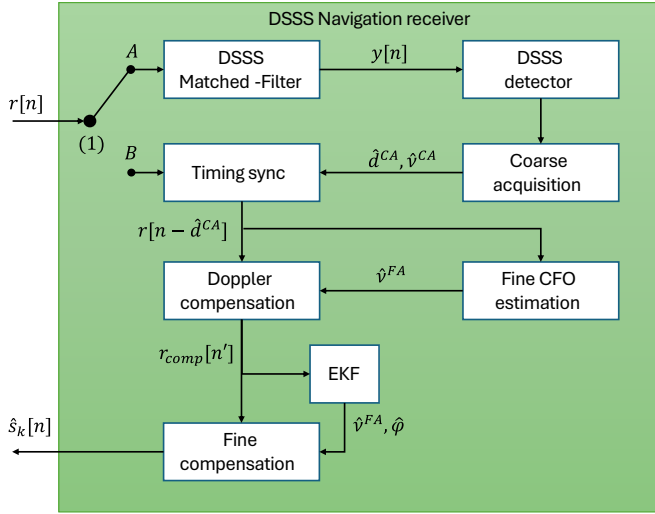


Fig. 3. Single channel navigation receiver architecture. The complete navigation receiver is composed by several channels running in parallel, each for a different DSSS.

$[x, y, z, t_{\text{sat}}]$. In this section we show the details of one of these channels, as the only difference between each channel is the local copy of the DSSS. Each channel consists of several processing stages as detailed below and presented in Fig. 3.

The navigation receiver architecture is inspired by the work in [22]. Fig. 3 shows a single channel for a navigation receiver, and as part of a navigation receiver, the observables to feed the PNT engine estimated in this block are:

- Noise estimation $P_{in,g,i}$.
- Delay estimation $\hat{d}_{g,i}$.
- Doppler estimation $\hat{\nu}_{g,i} = \hat{\nu}^{(CA)} + \hat{\nu}_p$.
- Phase estimation $\hat{\phi}_{g,i}$.

There are several PNT engines in the literature such as the ones found in [23]. Depending how the PNT engine is implemented, it will make use of some of the observables or all of them. However, this PNT engine implementation is outside the scope of this paper and we will leave for future work.

Furthermore, the output of this navigation block is the received signal after compensating for the channel impairments ready for its demodulation as $\hat{s}_k[n]$.

1) Signal switch

This initial switch is used to route the received signal between different steps in a similar to the architecture designed in [22] for the 5G signals. The main rationale to use this switch is that the initial coarse acquisition is required only once, at the beginning of the reception. Then, the tracking loops enter into action for the small adjustments of the estimations. However, if the tracking loops lost the track of the signal, the switch is then changed back to its initial position.

The input signal switch (1) is managed by the action of the DSSS detector. Initially, when the DSSS is undetected, the input is routed through (1)-A, enabling coarse estimation of delay and Doppler parameters ($\hat{\tau}_q, \hat{\nu}_q$). Upon detection of the DSSS waveform, the connection switches to (1)-B and stay in this state while the tracking loops keep the signal track.

2) DSSS matched filter

The DSSS matched filter performs coherent correlations over N_ν Doppler bins defined in the interval $[-\nu_{D_{\text{MAX}}}, \dots, \nu_{D_{\text{MAX}}}]$, where $\nu_{D_{\text{MAX}}}$ is the maximum Doppler shift expected and it will depends on the orbit altitude and f_c . Besides, the correlation is done for integer delay lags $d = 0, \dots, L_c - 1$, with L_c the length of the DSSS. Therefore, the matching filter is defined as

$$R_{r,z}[d, \nu] = \frac{1}{\sqrt{1-\rho}} \sum_{n=0}^{L_c-1} r[n+d] \tilde{z}^*[n] e^{j2\pi\nu n T_s}. \quad (18)$$

Expanding (18) using (10) can be approximated to (19), where to reduce notation we have defined the following terms:

$$X_z[d, \nu] = \frac{\sqrt{\rho}}{\sqrt{1-\rho}} \sum_{n=0}^{L_c-1} \mathbf{h}_{g,i}^\top [n+d] \mathbf{w}_{g,i} \times z_{g,i}[n+d-d_{g,i}] \tilde{z}^*[n] e^{j2\pi\nu n T_s}, \quad (20)$$

$$X_K[d, \nu] = \frac{1}{\sqrt{1-\rho}} \sum_{n=0}^{L_c-1} \sum_{k \neq i}^K r_{g,k}[n+d] \tilde{z}^*[n] e^{j2\pi\nu n T_s}, \quad (21)$$

$$X_Q[d, \nu] = \frac{1}{\sqrt{1-\rho}} \sum_{n=0}^{L_c-1} \sum_{q \neq g}^Q \sum_{k=1}^K r_{q,k}[n+d] \tilde{z}^*[n] e^{j2\pi\nu n T_s}, \quad (22)$$

$$X_{w'}[d, \nu] = \frac{1}{\sqrt{1-\rho}} \sum_{n=0}^{L_c-1} w_{q,k}[n+d] \tilde{z}^*[n] e^{j2\pi\nu n T_s}. \quad (23)$$

These residual terms can be approximated as a random Gaussian variable $\{X_z, X_K, X_Q, X_{w'}\} \sim \mathcal{CN}(0, \sigma^2)$, the value of σ^2 will be different for each residual term. The residuals represent the interference after the matched filter from the data service in: the same beam and satellite (as X_z); the interference from other beams in the same satellite (as X_K); the interference from other beams from satellites (as X_Q); and the receiver noise contribution (as $X_{w'}$). All of them are independent of the delay d and the Doppler ν , and the σ^2 for each contribution is

$$R_{r,\bar{z}}[d, \nu] \approx L_c \mathbf{h}_{g,i}^T [d_{g,i}] \mathbf{w}_{g,i} \delta[d - d_{g,i}] \delta[\nu - \nu_{g,i}] + X_z[d, \nu] + X_K[d, \nu] + X_Q[d, \nu] + X_{w'}[d, \nu]. \quad (19)$$

$$\sigma_z^2 = \frac{1 - \rho}{\rho} h_{g,i}, \quad (24)$$

$$\sigma_K^2 = \frac{R_K}{\rho}, \quad (25)$$

$$\sigma_Q^2 = \frac{R_Q}{\rho}, \quad (26)$$

$$\sigma_{w'}^2 = \frac{\sigma_w^2 L_c}{\rho}. \quad (27)$$

These values of σ show that the closer ρ is to 0, the higher the contribution of the OFDM and the other signals to the DSSS of interest.

3) DSSS detector

The detection stage employs a cell average (CA)-constant false alarm rate (CFAR) algorithm, as described in [24], to ascertain the presence of the DSSS signal. The detector evaluates the correlation peak $\max(|R_{r,\bar{z}}[d, \nu]|)$ against a dynamically computed threshold $\eta = \beta P_{in}$. The β is obtained from the probability of false alarm P_{fa} parameter as

$$\beta = M_d M_\nu (P_{fa}^{\frac{-1}{M_d M_\nu}} - 1). \quad (28)$$

where M_d is the number of training samples for the noise estimation in the time axis and M_ν the number of training samples in the Doppler bins axis.

The noise estimation P_{in} used in the threshold calculation is computed as the power of the signal within the subset of the acquisition samples centered in the position of $< d_0, \nu_0 > = \arg\max_{d,\nu} (|R_{r,\bar{z}}[d, \nu]|)$ defined by

$$\mathcal{I}_{M_d}[d_0] = \{d_0 - \frac{M_d}{2}, \dots, d_0, \dots, d_0 + \frac{M_d}{2}\}, \quad (29)$$

$$\mathcal{I}_{M_\nu}[\nu_0] = \{\nu_0 - \frac{M_\nu}{2}, \dots, \nu_0, \dots, \nu_0 + \frac{M_\nu}{2}\}. \quad (30)$$

Another set is defined for the guard area as

$$\mathcal{I}_{G_d}[d_0] = \{d_0 - \frac{G_d}{2}, \dots, d_0, \dots, d_0 + \frac{G_d}{2}\}, \quad (31)$$

$$\mathcal{I}_{G_\nu}[\nu_0] = \{\nu_0 - \frac{G_\nu}{2}, \dots, \nu_0, \dots, \nu_0 + \frac{G_\nu}{2}\}. \quad (32)$$

With these 4 sets defined, the noise estimation is the average power within the training set excluding the guard set as

$$P_{in} = \frac{1}{M_d M_\nu} \sum_{\substack{d \in \mathcal{I}_{M_d} \\ m \notin \mathcal{I}_{G_d}}} \sum_{\substack{\nu \in \mathcal{I}_{M_\nu} \\ \nu \notin \mathcal{I}_{G_\nu}}} |R_{r,\bar{z}}[d, \nu]|^2. \quad (33)$$

Finally, for the detection test, first it is needed to compare the peak of the matched filter output $< d_0, \nu_0 > = \arg\max_{d,\nu} |R_{x,y}[d, \nu]|$ with the threshold η as

$$O = \begin{cases} 1, & |R_{r,\bar{z}}[\hat{d}^{(CA)}, \hat{\nu}^{(CA)}]|^2 > \eta \\ 0, & |R_{r,\bar{z}}[\hat{d}^{(CA)}, \hat{\nu}^{(CA)}]|^2 \leq \eta \end{cases} \quad (34)$$

If detection succeeds $O = 1$, the switch configuration transitions from (1)-A to (1)-B; otherwise, the receiver continues in this step until a detection happens.

4) Coarse acquisition

Upon successful detection $O = 1$, the coarse estimates for delay and Doppler are extracted directly from the peak correlation value as used in the detection test $\hat{d}^{(CA)} = d_0$ and $\hat{\nu}^{(CA)} = \nu_0$.

5) Timing synchronization

The estimated coarse delay $\hat{d}^{(CA)}$ is used to compensate timing via $r[n'] = r[n - \hat{d}^{(CA)}]$. This delay has a resolution of a sample. Later, an extended kalman filter (EKF) tracking loop is used to refine this coarse estimation by adjusting the phase φ of the signal.

6) Fine Doppler estimation

The fine Doppler frequency offset refinement is performed using the phase difference across successive DSSS sequences. We assume the Doppler does not change significantly for the duration of 2 subframes. Therefore, the phase change between these two subframes follows a linear model $\phi[n] = (2\pi\nu T_s)n + w$ with $w \sim \mathcal{N}(0, \sigma^2)$ and correspond to the phase rotation generated by the Doppler in N_c samples as

$$\hat{\nu}^{(FA)} = \frac{\angle \left(R_{r,\bar{z}}[\hat{d}^{(CA)}, \hat{\nu}^{(CA)}] R_{r,\bar{z}}^*[\hat{d}^{(CA)} + L_c, \hat{\nu}^{(CA)}] \right)}{2\pi L_c T_s}. \quad (35)$$

7) Doppler compensation

Combining coarse and fine Doppler estimates, the signal is compensated as:

$$r_{\text{comp}}[n'] = r[n'] e^{-j2\pi(\hat{\nu}^{(CA)} + \hat{\nu}^{(FA)})n' T_s}. \quad (36)$$

8) Extended Kalman filter

The previous steps does not remove all the impairments from the channel, therefore it includes an EKF to estimate

the $\hat{\varphi}$ phase of the signal and the residual of the Doppler $\hat{\nu}^{(FA)}$. The inclusion of an EKF rationale is because the performance is higher compared with other tracking loops such as phase-locked loop (PLL) [25].

The state of the system at instant p is defined by the phase φ_p of the signal and the Doppler ν_p , where the subindex p represent the DSSS index block of one subframe duration. We assume that the Doppler is constant over the measurement period, as the change in Doppler for such small period can be assumed negligible [25]. This measurement period correspond to the length of a DSSS sequence $L_c \times T_s$. Therefore, the update model $\mathbf{x}_p = [\varphi_p, \nu_p]^T$ is defined as

$$\mathbf{x}_{p+1} = \mathbf{D}\mathbf{x}_p + \mathbf{v}_p, \quad (37)$$

$$\mathbf{D} = \begin{bmatrix} 1 & 2\pi L_c T_s \\ 0 & 1 \end{bmatrix}, \quad (38)$$

$$\mathbf{v}_p \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}), \quad (39)$$

where the process-noise covariance is $\mathbf{Q} = \text{diag}(\sigma_\varphi^2, \sigma_\nu^2)$, representing unavoidable perturbations on phase and frequency.

For every DSSS sequence called p , the base-band samples $r_{comp}[n']$ are correlated with a local replica of the PRN code $\tilde{z}[n]$. This correlation includes an a-priori estimation of the Doppler based on the previous estimation ($\nu_{p|p-1}$),

$$c_p = \sum_{n=0}^{L_c-1} r_{comp}[n' + p] \tilde{z}^*[n] e^{-j 2\pi \nu_{p|p-1} n T_s}. \quad (40)$$

Then, the phase of c_p is a noisy observation of φ_p :

$$u_p = \text{wrap}[\angle(c_p) - \pi] = g(\mathbf{x}) + v_p, \quad (41)$$

where $g(\mathbf{x}) = \varphi_p$, and $v_p \sim \mathcal{N}(0, \sigma_u^2)$ is the measurement noise.

The Jacobian required by the EKF is

$$\mathbf{G}_p = \left. \frac{\partial g}{\partial \mathbf{x}} \right|_{\mathbf{x}_{p|p-1}} = \begin{bmatrix} 1 & 0 \end{bmatrix}. \quad (42)$$

a: Step-by-Step EKF Algorithm

The following are the steps used by the EKF to estimate the phase and Doppler of the signal.

1) State prediction

$$\hat{\mathbf{x}}_{p|p-1} = \mathbf{D}\hat{\mathbf{x}}_{p-1|p-1}, \quad (43)$$

$$\mathbf{P}_{p|p-1} = \mathbf{D}\mathbf{P}_{p-1|p-1}\mathbf{F}^T + \mathbf{Q}. \quad (44)$$

2) Measurement innovation

$$\tilde{u}_p = \text{wrap}[u_p - \hat{\varphi}_{p|p-1}], \quad (45)$$

$$\mathbf{S}_p = \mathbf{G}_p \mathbf{P}_{p|p-1} \mathbf{G}_p^T + \sigma_u^2. \quad (46)$$

3) Kalman gain update

$$\mathbf{K}_p = \mathbf{P}_{p|p-1} \mathbf{G}_p^T \mathbf{S}_p^{-1}. \quad (47)$$

4) State estimation update

$$\hat{\mathbf{x}}_{p|p} = \hat{\mathbf{x}}_{p|p-1} + \mathbf{K}_p \tilde{u}_p, \quad (48)$$

$$\mathbf{P}_{p|p} = (\mathbf{I} - \mathbf{K}_p \mathbf{G}_p) \mathbf{P}_{p|p-1}. \quad (49)$$

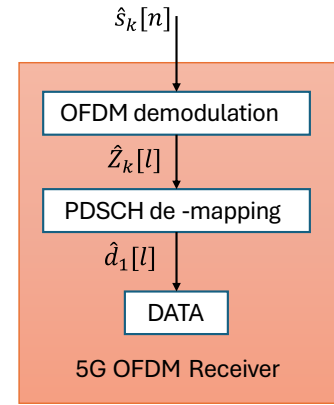


Fig. 4. 5G OFDM receiver architecture.

Once the EKF has finished its update estimation, its output is the new state of the system, $\hat{\mathbf{x}}_{p|p}$, with the new value of the phase and Doppler. These values of phase and Doppler are considered constant for the duration of the DSSS, and they are used to compensate the received signal as

$$\hat{s}_k[n] = r_{comp}[n'] e^{-j(2\pi \hat{\nu}^{(FA)} n T_s + \hat{\varphi})}, \quad (50)$$

where $\hat{s}_k[n]$ is the input to the communications block.

B. 5G COMMUNICATIONS RECEIVER

For this hybrid receiver, the communication part follows an approach similar to the architecture used in 5G. Fig. 4 shows the block of the receiver dedicated to the communication part, that has as input the signal compensated from the navigation part.

1) OFDM demodulation

In the OFDM demodulation, the receiver remove the cyclix prefix (CP) as $\hat{z}_k[n] = \hat{z}_k[n + s(N_{\text{FFT}} + N_{\text{CP}}) + N_{\text{CP}}]$, where N_{FFT} are the fast Fourier transform (FFT) points and N_{CP} is the CP length.

Then, the OFDM demodulation as the FFT of $\hat{Z}_k[l] = \text{FFT}\{\hat{z}_k[n]\}$, and extract the bits transmitted.

2) PDSCH de-mapping

Finally, the PDSCH de-mapping extract the bits from the resource elements (REs) within the resource grid (RG) dedicated to the PDSCH.

$$\mathbf{Z}_{\text{PDSCH}} = \{\hat{Z}[l, k] | (l, k) \in \mathcal{R}_{\text{subcarrier}} \times \mathcal{T}_{\text{symbol}}\} \quad (51)$$

where $\mathcal{R}_{\text{subcarrier}}$, $\mathcal{T}_{\text{symbol}}$ are the indices for the subcarriers and symbols within the RG dedicated to the PDSCH.

Once extracted the PDSCH elements, the receiver demodulate the symbols and generate the bitstream. In this work we did not include any channel coding as it is outside the scope of the work, therefore the final key performance indicator (KPI) for the communication block is the uncoded BER.

IV. PERFORMANCE EVALUATION

In order to evaluate the performance of the proposed JCAP receiver, we use the following metrics:

- 1) The error vector magnitude (EVM): This metric quantifies the degradation of the OFDM signal caused by the aggregation of the DSSS for different values of SIR between the OFDM and DSSS signal. We use the SIR between the DSSS (as signal of interest) and the OFDM (as interference for the navigation service). This metric provides insight into the effect of the aggregation of the DSSS waveform in the OFDM, prior to the channel and receiver effects.
- 2) The receiver operating characteristic (ROC) curve for the receiver. We compare the probability of false alarm P_{fa} detection with the probability of detection P_d for discrete values of SIR. Also, we show the probability of detection P_D of the DSSS signal for continuous values of DSSS SIR.
- 3) The accuracy of the observables estimators in the different steps in the receiver.
- 4) Finally we evaluate the uncoded BER of the system for different values of OFDM SIR. We include as benchmark the best scenario, the uncoded BER when there is no DSSS and only additive white Gaussian noise (AWGN) as channel.

Table I summarizes the simulation parameters and their corresponding values used along with a reference where it was used, they are based on typical values found in the literature for GNSS and 5G communication systems.

A. OFDM DEGRADATION AFTER INCLUDING THE DSSS

The first metric used is the EVM for different values of $SIR_{DSSS}[\text{dB}]$ of the JCAP waveform. The EVM is defined as

$$EVM_{\text{RMS}} = \sqrt{\frac{\sum_n |s[n] - z_k[n]|^2}{\sum_n |z_k[n]|^2}}, \quad (52)$$

where $z_k[n]$ is the signal without DSSS and $s[n]$ is the signal that includes the DSSS.

This metric is evaluated in Fig. 5 and provides insights on how the receiver perform ideally (without channel effects) when including the DSSS. Fig. 5 includes also the EVM reference thresholds defined by 3GPP for 5G systems, serving as a benchmark for acceptable signal quality.

Fig. 5 shows that a value of SIR for the limits to reach the maximum level of EVM for QPSK up to 256QAM. We use different values of RB to evaluate the EVM. We use the: minimum allowable number of RB as 1; the RB needed for the synchronization signal block (SSB) as 20; and the maximum number of RB allowed for frequency region 1 (FR1) as 273.

The observed non-linear decrease of EVM with the number of RBs is expected from the way the DSSS component is distributed in time/frequency as the occupied bandwidth grows. In our model, OFDM and DSSS share the

TABLE I. Simulations parameters

Parameter	Symbol	Value
Antenna elements x axis	N_x	16
Antenna elements y axis	N_y	16
Number of beams	K	7
Beam directions	(θ_k, ϕ_k)	$\theta_k = 0.1334$, $\phi = \{0, \pi/3, 2\pi/3, \pi, 4\pi/3, 5\pi/3\}$
Satellites in LOS	Q	1
Channel gain phase	φ	$\mathcal{U}(0, 2\pi)$
Channel gain magnitude	$ \alpha_{q,k} $	1
Carrier frequency	f_c	2.2 GHz
5G frames simulated	N_f	100
SIR range dB	ρ_0, \dots, ρ_z	$[-40, \dots, -5]$
DSSS sequence length	L_c	$1 \text{ ms} \times f_s$
OFDM subcarrier spacing		15 kHz
OFDM Resource Blocks	N_{RB}	$[1, 20, 273]$
Doppler bins	N_ν	61
Max Doppler	$\nu_{D_{\text{MAX}}}$	$\pm 15 \text{ kHz}$
Detector training delay	M_d	20
Detector training Doppler	M_ν	20
Detector guard band delay	G_d	2
Detector guard band Doppler	G_ν	2
Probability of false alarm	P_{fa}	$[10^{-10}, \dots, 10^0]$
Process phase update noise	σ_φ^2	10^{-2}
Process Doppler update noise	σ_ν^2	10^{-3} Hz^2
Measurement phase noise	σ_u^2	6^{-2} rad^2

same sampling clock and 1-ms subframe; hence the DSSS length in samples is $L_c = f_s \times 1 \text{ ms}$, which increases with N_{RB} because N_{RB} defines the occupied bandwidth and thus the sampling rate f_s . As N_{RB} increases, the same DSSS/OFDM SIR ρ is spread over more time-domain samples and FFT bins, lowering the in-band interference power spectral density (PSD) per resource element and therefore the EVM. This dilution is strongest from $1 \rightarrow 20$ RBs (bandwidth increase $\times 20$) and smaller from $20 \rightarrow 273$ RBs (bandwidth increase $\times 13.65$), hence the smaller incremental EVM improvement in the latter step.

B. RECEIVER OPERATING CURVE

The ROC curves in Fig. 6 are plots of the probability of detection (P_d) versus the probability of false alarm (P_{fa}) for a given DSSS SIR [26]. This Fig. 6 shows how the detector perform in different configurations, useful for the designer when evaluating the link budget analysis (LBA) and the expected P_{fa} .

The Fig. 7 shows what are the SINR limits to properly detect the DSSS when it has interference from the OFDM signal and AWGN noise for a given P_{fa} . We compare in Fig. 7 the effect of the 5G RG size by evaluating the probability of detection. The values used for the RG are the minimum value possible and the same RG used for the SSB.

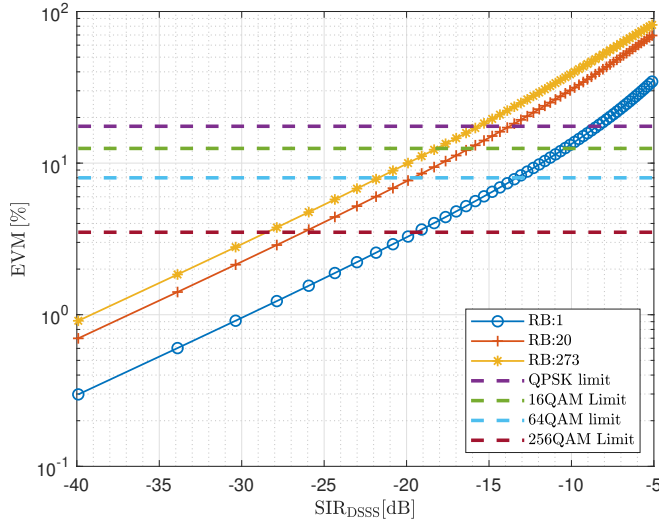


Fig. 5. EVM for different 5G signals. From the minimum RB of 1, the number of RB for the SSB as 20 and the maximum RB in FR1 as 273. It includes the EVM limits for different modulations as required by 3GPP.

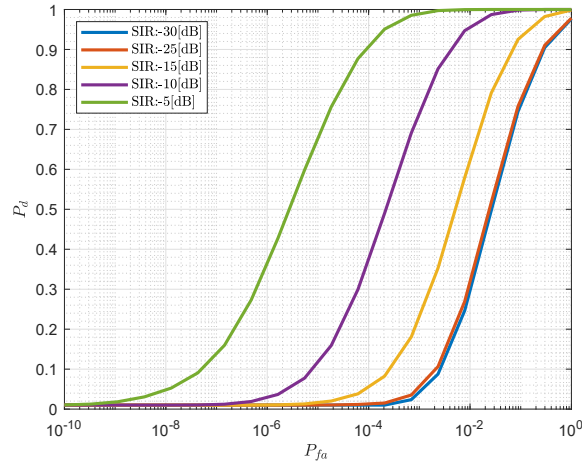


Fig. 6. Receiver operating curve for different values of DSSS SIR for a signal with RB=1.

In CA-CFAR, the threshold $\eta = \beta(P_{fa}, M_d M_\nu) P_{in}$ links P_{fa} and P_d through a common control parameter, hence, for fixed SIR, increasing P_{fa} (i.e., lowering η) monotonically increases P_d , producing the standard rising ROC curves in Fig. 7.

From Fig. 7 it is clear that the RBs affect the SINR level to reach 100% detection. Therefore, a system designer could set a limit in the SINR to detect the DSSS signal within the LBA. Besides, linking this result with the previous result, a SIR for the DSSS around -20 dB will be always detected and the EVM small enough to reach up to 64QAM modulation.

It should be mentioned that the acquisition/detection steps are based on a single DSSS. Here, we evaluate the worst case of a single DSSS, while a coherent integration of more DSSS will increase its energy and the detection SINR threshold

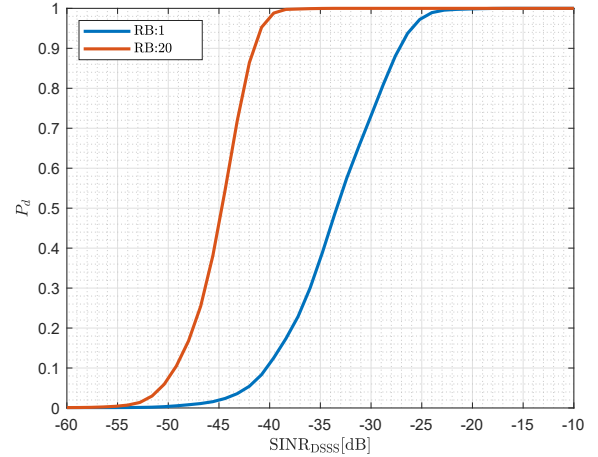


Fig. 7. Comparison of the RB to detect the DSSS for different values of interference from OFDM and receiver noise.

can go lower. In the following evaluations we assume the minimum SIR for the DSSS is enough for being always detectable, therefore, from Fig. 7 we set this minimum to -20 dB.

C. OBSERVABLE ESTIMATION

Once the signal is detected, we continue with the evaluation of the accuracy of the observable estimation by evaluating the variance of the estimator. We evaluate each estimator used in Fig. 3 separately in the following subsections.

1) Coarse delay estimation

We start by evaluating the variance of the delay estimation defined in (4). This estimator has a resolution of one sample or $[-T_s/2, +T_s/2]$, therefore, the error can be modeled as a uniform random variable within these limits $\chi_{d(CA)} \sim \mathcal{U}(-T_s/2, T_s/2)$. Therefore, the variance of this estimator can be obtained analytically as $\sigma^2(\hat{d}^{(CA)}) = 1/(12f_s^2)$.

2) Coarse Doppler estimation

From the coarse acquisition the accuracy on the Doppler estimation is directly related with the number of bins used and the maximum range of expected Doppler. There is a trade-off between processing time and accuracy, as a larger number of bins increase the resolution but at the same time the processing time. In our simulation we use a similar value used in GNSS application to reach 500 Hz of resolution per beam [23] give the maximum Doppler expected.

3) Fine Doppler estimation

Then, for the fine Doppler estimation, the phase change of two consecutive DSSS is due to the Doppler shift, modeled as $\Delta\varphi = 2\pi\nu L_c T_s + \epsilon$, where $\epsilon \sim \mathcal{N}(0, \sigma_\epsilon^2)$ represent the phase noise due to the interference and receiver noise.

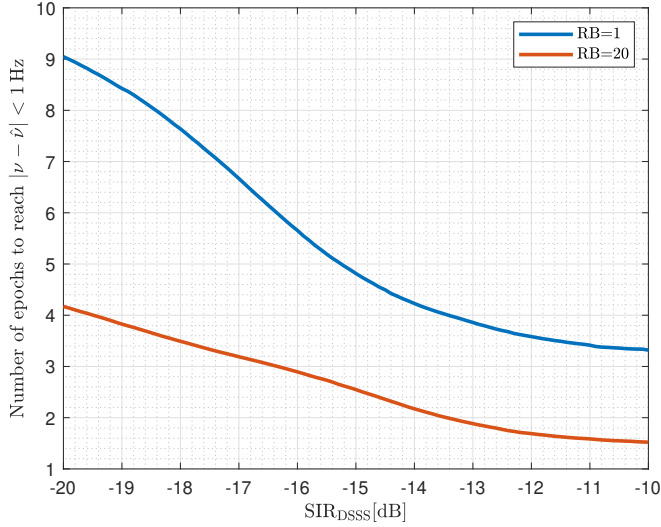


Fig. 8. Number of epochs to reach an error in the Doppler estimation below 1 Hz for different values of SINR of the DSSS.

In this work we do not have included the phase noise of the oscillators at the transmitter and receiver as the only impairment of interest is the external interference and the receiver noise. Therefore, we assume a $\sigma_\epsilon = 0.1$ rad as a typical value found in the literature [27], [28]. The estimator in (35) achieve an accuracy on the fine Doppler estimation as $\sigma_{\hat{\nu}(FA)} = \sigma_\epsilon / (2\pi L_c T_s) = 15.92$ Hz.

4) Extended Kalman filter

Up to now the performance of the previous estimators was done analytically as a block processing. However, to further improve the estimation, we have included an EKF. To evaluate its performance we use a simulation of the receiver in Fig. 3. In this simulation we evaluate the following parameters for the EKF block: the time to reach an error in the estimation below a certain threshold, and once it reaches a steady state, the accuracy achieved as the absolute error between the Doppler estimation and the real value of the Doppler.

The first parameter to evaluate is the time, in epochs or DSSS sequences, that the EKF takes to reach an error in the estimation below 1 Hz. Depending on the value of SIR, the algorithm will require more or less time to reach the threshold. In Fig. 8 we show the number of epochs required to reach and maintain the 1 Hz threshold for different values of SIR of the DSSS.

Now, we show some examples of the convergency of the EKF to reach as close as possible 0 Hz of error. In Fig. 9 and 10 the EKF algorithm reach an error very close to 0 Hz.

Finally, in Fig. 11 is evaluated the accuracy of the steady state of the tracking loop, after the initial epochs where there are some bouncing on the estimation, as seen in Fig. 9 or Fig. 10. This steady state is defined as the last epoch the error in the Doppler estimation passes the 1 Hz threshold, and we

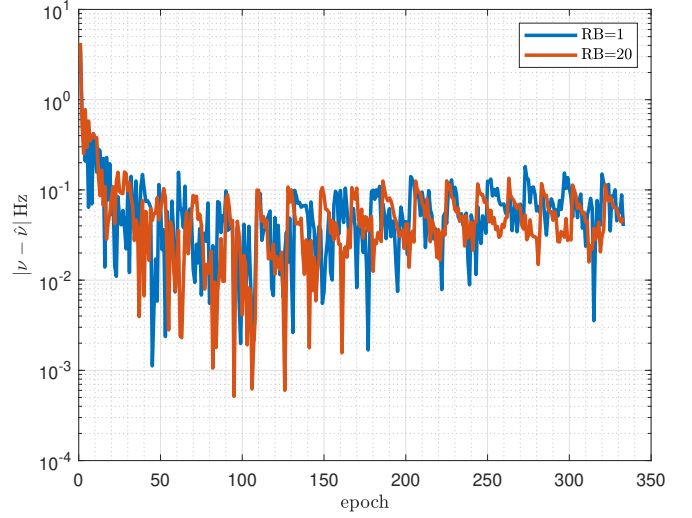


Fig. 9. DSSS Doppler tracking using EKF. With a SIR of -10 dB.

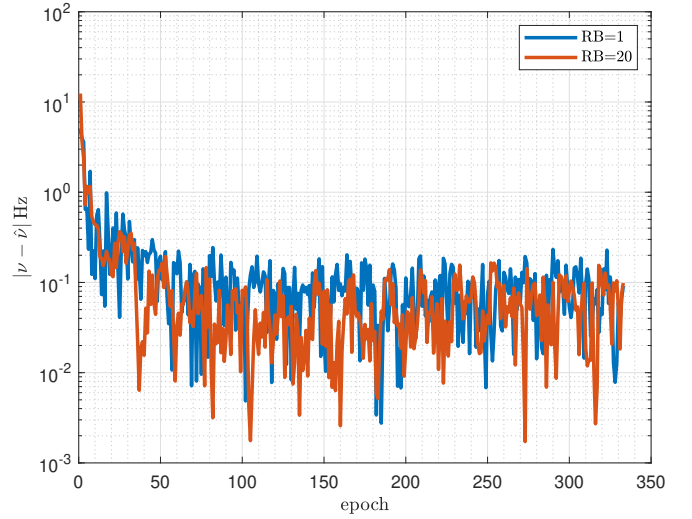


Fig. 10. DSSS Doppler tracking using EKF. With a SIR of -20 dB.

compute the mean value of this error within the steady state. This evaluation is done for several values of SIR.

This time, the error in the estimation is greatly reduced for SIR levels compared to the detection in Fig. 7. This allows to reach errors below 0.1 Hz on the estimation.

D. COMMUNICATION RECEIVER ASSISTED BY DSSS

The final evaluation of the system is the uncoded BER. Fig. 12 shows the uncoded BER for different values of DSSS SIR. It includes as a benchmark the case where there is no DSSS and the channel is just AWGN. This benchmark represent the best scenario possible. Therefore, one can see that reducing the SIR, the BER improves as we remove energy from the DSSS interference. However, this DSSS SIR is bounded by the detection and tracking limits shown in the previous results. If the DSSS cannot be detected, and the delay and Doppler cannot be properly estimated, the signal cannot be compensated for these impairments and the

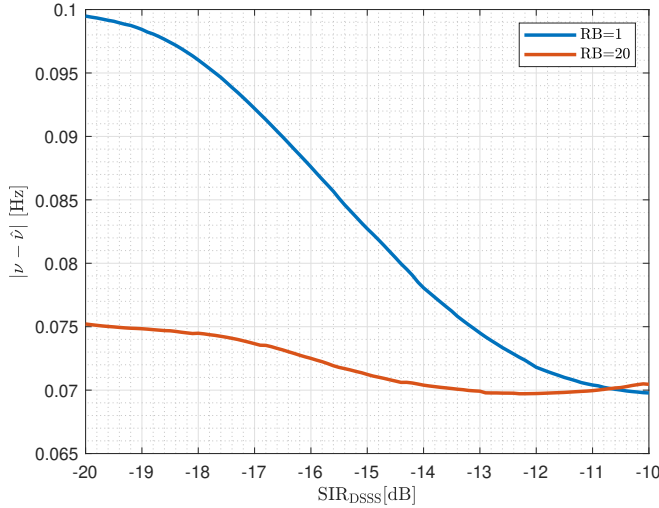


Fig. 11. Absolute error for Doppler estimation from EKF using the DSSS as reference for different values of SIR.

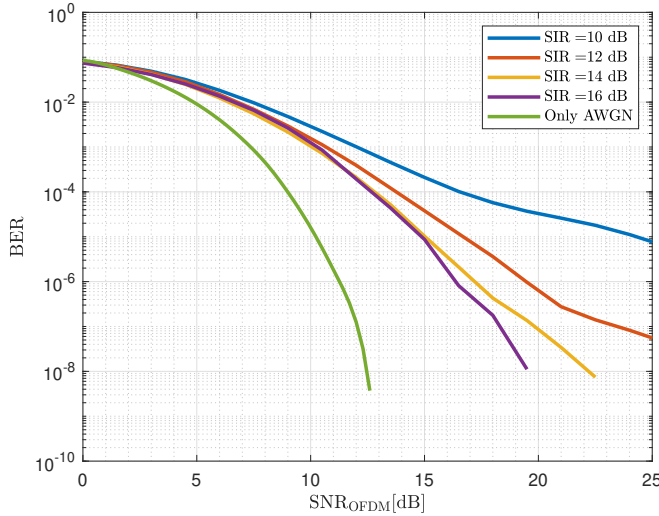


Fig. 12. Uncoded BER for the PDSCH in 5G for different values of SIR between the 5G OFDM signal and the DSSS pilots. The uncoded BER "Only AWGN" is our benchmark where no DSSS is include, and the channel is only AWGN.

demodulation is not possible. There is no plot with lower SIR of 16 dB as the navigation system perform poorly and no demodulation is possible.

Something to take into account in this result is that there is no channel estimation within the OFDM grid, in the sense that there are no pilots embedded. The main rationale for this is to reduce the overhead at the communication block and reuse the estimation done at the navigation block hybridization both receivers blocks.

All curves in Fig. 12 are single-satellite. Results from multi-satellite JCAP configurations (e.g., [15]) are not overlaid due to differing operating assumptions, which would render the comparison non-commensurate.

E. RESULT DISCUSSION

In summary, the use of DSSS combined with OFDM for navigation and channel estimation is a realizable system that benefits from both waveforms.

The results indicate that with a DSSS duration of one subframe a $SIR_{DSSS} \approx -20$ dB is recommended to maintain a stable detection and an acceptable accuracy estimation for the Doppler and a low impact of DSSS on the uncoded BER.

V. CONCLUSIONS

The proposed hybrid OFDM–DSSS scheme demonstrate that the number of pilots for channel estimation can be reduced for a data service using OFDM. By reducing the pilots more resource element can carry useful data. By substituting these pilots by the DSSS it is easier to integrate a navigation block that does not depend on the prior demodulation of the OFDM signal. Across the entire SIR range studied, the hybrid waveform delivers low BER with navigation capabilities, showing the hybrid system's advantage.

As future work, we plan to implement an over-the-air (OTA) testbed in a controlled laboratory environment using software defined radio (SDR) platforms to validate our simulation findings, and we are under discussion for using a transparent payload hosted in an actual satellite of the O3B mPower constellation [29]. These OTA experiments aim to evaluate the observables estimation for the navigation service and BER under real-world propagation conditions. This will provide direct confirmation of the performance of the hybrid OFDM+DSSS scheme. By incorporating hardware impairments and synchronization challenges into the test scenarios, we will bridge the gap between simulation and practical deployment, providing critical insights for integrating this approach into future NTN JCAP systems.

Future research in this topic include the evaluation of a DSSS duration of larger duration, for example at least 20 ms. This way it is possible to remove the ambiguity for the estimation of the time of arrival (ToA) as the duration of the code is larger than the maximum delay at 0 degrees of elevation angle for a LEO satellite. The complexity to acquire such large code, and the tradeoffs of using large codes needs to be evaluated in this future work.

APPENDIX. ACRONYMS

This paper uses an extensive number of acronyms, and to assist the reader, the following list presents all of them:

5G	fifth generation
3GPP	3rd generation partnership project
AWGN	additive white Gaussian noise
BER	bit error rate
CA	cell average
CFAR	constant false alarm rate
CP	cyclic prefix
DBF	digital beamforming
DSSS	direct-sequence spread spectrum
EKF	extended kalman filter

EVM	error vector magnitude
FFT	fast Fourier transform
FR1	frequency region 1
FRF3	frequency re-use factor 3
gNB	next generation base station
GNSS	global navigation satellite system
IoT	internet of things
JCAP	joint communication and positioning
KPI	key performance indicator
LBA	link budget analysis
LEO	low earth orbit
LOS	line of sight
NR	new radio
NTN	non-terrestrial network
OFDM	orthogonal frequency-division multiplexing
OTA	over-the-air
PDSCH	physical downlink shared channel
PLL	phase-locked loop
PNT	positioning, navigation, and timing
PRS	positioning reference signal
PSD	power spectral density
RB	resource block
RE	resource element
RG	resource grid
ROC	receiver operating characteristic
SDR	software defined radio
SIR	signal-to-interference ratio
SINR	signal-to-interference plus noise ratio
SNR	signal-to-noise ratio
SSB	synchronization signal block
TC	time coded
ToA	time of arrival
UE	user equipment
UPA	uniform planar array

ACKNOWLEDGEMENT

The simulations presented in this paper were carried out using the HPC facilities of the University of Luxembourg [30] (see `hpc.uni.lu`).

REFERENCES

- [1] 3rd Generation Partnership Project, "Solutions for NR to support non-terrestrial networks (NTN)," *3GPP TR 38.821 V16.0.0*, Jan. 2020.
- [2] C4ADS, "Above Us Only Stars. Exposing GPS Spoofing in Russia and Syria," C4ADS, Tech. Rep., 2019.
- [3] 3GPP, "Study on satellite access Phase 3," Dec. 2023. [Online]. Available: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4089>
- [4] Z. Zhou, N. Accettura, and P. Berthou, "A Wake-up Strategy Enabling GNSS-Free NB-IoT Links to Sparse LEO Satellite Constellations," *IEEE Internet of Things Journal*, pp. 1–1, 2025. [Online]. Available: <https://ieeexplore.ieee.org/document/10929718>
- [5] L. You, X. Qiang, Y. Zhu, F. Jiang, C. G. Tsinos, W. Wang, H. Wymeersch, X. Gao, and B. Ottersten, "Integrated Communications and Localization for Massive MIMO LEO Satellite Systems," *IEEE Transactions on Wireless Communications*, vol. 23, no. 9, pp. 11 061–11 075, Sep. 2024, conference Name: IEEE Transactions on Wireless Communications. [Online]. Available: <https://ieeexplore.ieee.org/document/10478820/authors#authors>
- [6] K. Ntontin, E. Lagunas, J. Querol, J. u. Rehman, J. Grotz, S. Chatzinotas, and B. Ottersten, "A Vision, Survey, and Roadmap Toward Space Communications in the 6G and Beyond Era," *Proceedings of the IEEE*, pp. 1–37, 2025, conference Name: Proceedings of the IEEE. [Online]. Available: <https://ieeexplore.ieee.org/document/10820534>
- [7] A. Shahmansoori, R. Montalban, J. A. Lopez-Salcedo, and G. Seco-Granados, "Design of OFDM sequences for joint communications and positioning based on the asymptotic expected CRB," in *International Conference on Localization and GNSS 2014 (ICL-GNSS 2014)*. Helsinki: IEEE, Jun. 2014, pp. 1–6. [Online]. Available: <https://ieeexplore.ieee.org/document/6934168/>
- [8] R. C. Adam and P. A. Hoeher, "Simultaneous Model and Parameter Estimation for Joint Communication and Positioning," *IEEE Access*, vol. 9, pp. 2934–2949, 2021, conference Name: IEEE Access.
- [9] W. Wang, T. Jost, C. Gentner, S. Zhang, and A. Dammann, "A Semiblind Tracking Algorithm for Joint Communication and Ranging With OFDM Signals," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 7, pp. 5237–5250, Jul. 2016. [Online]. Available: <http://ieeexplore.ieee.org/document/7194841/>
- [10] Y. Wang, S. Huang, Y. Yu, C. Li, P. A. Hoeher, and A. C. K. Soong, "Recent Progress on 3GPP 5G Positioning," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, Jun. 2023, pp. 1–6, iSSN: 2577-2465. [Online]. Available: <https://ieeexplore.ieee.org/document/10199811>
- [11] S. Dwivedi, R. Shreevastav, F. Munier, J. Nygren, I. Siomina, Y. Lyazidi, D. Shrestha, G. Lindmark, P. Ernstrom, E. Stare, S. M. Razavi, S. Muruganathan, G. Masini, A. Busin, and F. Gunnarsson, "Positioning in 5G Networks," *IEEE Communications Magazine*, vol. 59, no. 11, pp. 38–44, Nov. 2021, conference Name: IEEE Communications Magazine. [Online]. Available: <https://ieeexplore.ieee.org/document/9665436>
- [12] B. Liu, M. Peng, J. Li, X. Yang, and Y. Liu, "Integrated Communication and Navigation Enabled Low Earth Orbit Satellite Systems," *IEEE Network*, pp. 1–1, 2025. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10854561>
- [13] A. Gonzalez-Garrido, J. Querol, H. Wymeersch, and S. Chatzinotas, "Joint Communication and Navigation From LEO Multi-Beam Satellite," *IEEE Open Journal of the Communications Society*, pp. 1–1, 2025. [Online]. Available: <https://ieeexplore.ieee.org/document/10993443>
- [14] Y. Li, H. Hou, J. Lu, and W. Wang, "Digital spread-spectrum watermarking identity authentication technology based on OFDM in satellite-ground communication system," in *Proceedings of the 2023 International Conference on Communication Network and Machine Learning*, ser. CNML '23. New York, NY, USA: Association for Computing Machinery, Feb. 2024, pp. 140–144. [Online]. Available: <https://doi.org/10.1145/3640912.3640940>
- [15] R. De Gaudenzi, "An Integrated LEO Communication and PNT System for Beyond 5G NTN," *Wiley International Journal of Satellite Communications and Networking*, 2024.
- [16] X. Lin, S. Rommer, S. Euler, E. A. Yavuz, and R. S. Karlsson, "5G from Space: An Overview of 3GPP Non-Terrestrial Networks," *IEEE Communications Standards Magazine*, vol. 5, no. 4, pp. 147–153, Dec. 2021. [Online]. Available: <https://ieeexplore.ieee.org/document/9579443/>
- [17] J. J. H. Wang, "Antennas for Global Navigation Satellite System (GNSS)," *Proceedings of the IEEE*, vol. 100, no. 7, pp. 2349–2355, Jul. 2012. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/6130567>
- [18] J. Ning, J. Deng, Y. Li, C. Zhao, J. Liu, S. Yang, Y. Wang, J. Huang, and C.-X. Wang, "Ray-Tracing Channel Modeling for LEO Satellite-to-Ground Communication Systems," in *2024 IEEE/CIC International Conference on Communications in China (ICCC)*, Aug. 2024, pp. 1169–1174, iSSN: 2377-8644. [Online]. Available: <https://ieeexplore.ieee.org/document/10681740>
- [19] V. M. Baeza, E. Lagunas, H. Al-Hraishawi, and S. Chatzinotas, "An Overview of Channel Models for NGSO Satellites," in *2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)*, Sep. 2022, pp. 1–6, iSSN: 2577-2465. [Online]. Available: <https://ieeexplore.ieee.org/document/10012693>
- [20] A. W. Mast, "Reconfigurable Software Defined Payload architecture that reduces cost and risk for various missions," in *2011 Aerospace*

- Conference, Mar. 2011, pp. 1–5, iSSN: 1095-323X. [Online]. Available: <https://ieeexplore.ieee.org/document/5747366>
- [21] R. Birkeland, G. Quintana-Diaz, E. Honoré-Livermore, T. Ekman, F. A. Agelet, and T. A. Johansen, “Development of a multi-purpose SDR payload for the HYPPO-2 satellite,” in *2022 IEEE Aerospace Conference (AERO)*, Mar. 2022, pp. 1–11, iSSN: 1095-323X. [Online]. Available: <https://ieeexplore.ieee.org/document/9843447>
- [22] I. Lapin, G. S. Granados, J. Samson, O. Renaudin, F. Zanier, and L. Ries, “STARE: Real-Time Software Receiver for LTE and 5G NR Positioning and Signal Monitoring,” in *2022 10th Workshop on Satellite Navigation Technology (NAVITEC)*. Noordwijk, Netherlands: IEEE, Apr. 2022, pp. 1–11. [Online]. Available: <https://ieeexplore.ieee.org/document/9847544/>
- [23] E. Kaplan and C. Hegarty, *Understanding GPS: Principles and applications*, ser. Artech house mobile communications. Artech House, 2006, tex.lccn: 2005056270.
- [24] A. Gonzalez-Garrido, J. Querol, H. Wymeersch, and S. Chatzinotas, “Interference Analysis and Modeling of Positioning Reference Signals in 5G NTN,” *IEEE Open Journal of the Communications Society*, vol. 5, pp. 7567–7581, 2024, conference Name: IEEE Open Journal of the Communications Society. [Online]. Available: <https://ieeexplore.ieee.org/document/10759698>
- [25] J. Vila-Valls, P. Closas, M. Navarro, and C. Fernandez-Prades, “Are PLLs dead? A tutorial on kalman filter-based techniques for digital carrier synchronization,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 7, pp. 28–45, Jul. 2017. [Online]. Available: <http://ieeexplore.ieee.org/document/8039260/>
- [26] S. H. Dokhanchi, A. N. Barreto, and G. P. Fettweis, “Performance Analysis of Zero-Padded Sequences for Joint Communications and Sensing,” *IEEE Transactions on Signal Processing*, vol. 71, pp. 1725–1741, 2023. [Online]. Available: <https://ieeexplore.ieee.org/document/10121669>
- [27] X. Liu, H. Lu, Y. He, F. Wu, C. Zhang, and X. Wang, “Analysis on the Effect of Phase Noise on the Performance of Satellite Communication and Measurement System,” *Symmetry*, vol. 15, no. 11, p. 2053, Nov. 2023, number: 11 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: <https://www.mdpi.com/2073-8994/15/11/2053>
- [28] D. Petrovic, W. Rave, and G. Fettweis, “Common phase error due to phase noise in OFDM-estimation and suppression,” in *2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications*, vol. 3, Sep. 2004, pp. 1901–1905 Vol.3. [Online]. Available: <https://ieeexplore.ieee.org/document/1368329>
- [29] “O3b mPOWER | SES,” Sep. 2017. [Online]. Available: <https://www.ses.com/o3b-mpower>
- [30] S. Varrette, H. Cartiaux, S. Peter, E. Kieffer, T. Valette, and A. Olloh, “Management of an academic HPC & research computing facility: The ULHPC experience 2.0,” in *Proc. of the 6th ACM high performance computing and cluster technologies conf. (HPCCT 2022)*. Fuzhou, China: Association for Computing Machinery (ACM), Jul. 2022.



Alejandro Gonzalez-Garrido PhD student at the SIGCOM group of SnT (University of Luxembourg), specializing in hybrid GNSS and 5G PNT systems using Non-Terrestrial Networks. Holds an integrated degree and an M.Sc. in Telecommunication Engineering, obtained in 2015. Has professional experience in the timing and synchronization industry, satellite design, and network operations.



IDIR EDJEKOUANE is currently a Research Associate with the SIGCOM Research Group at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg. He received an engineering degree in electronics from the École Nationale Polytechnique, Algiers, in 2011, a master's degree in signal processing from Université Paul Sabatier, Toulouse, in 2012, and a Ph.D. in acoustics and signal processing from Aix-Marseille Université in 2016, with research conducted at Orange Labs, Lannion, France. He subsequently worked as a signal processing engineer in the NAVIR²eS group at ISAE-SUPAERO and later as a GNSS engineer at Airbus Defence and Space, Toulouse. Before joining SIGCOM, he served as Principal Signal Processing Engineer at Kleos Space, where he led the geolocation algorithm team for nearly four years.



Jorge Querol received his Ph.D. degree in Telecommunication Engineering from the Polytechnic University of Catalonia (UPC-BarcelonaTech), Barcelona, Spain, in 2018. His research interests include Software-Defined Radios (SDR), real-time signal processing, satellite communications, satellite navigation, and remote sensing. Jorge joined the Signal Processing and Satellite Communications group (SIGCOM), headed by Prof. Björn Ottersten, and he will be working with Dr. Symeon Chatzinotas.



Henk Wymeersch (S'01, M'05, SM'19, F'24) obtained the Ph.D. degree in Electrical Engineering/Applied Sciences in 2005 from Ghent University, Belgium. He is currently a Professor of Communication Systems with the Department of Electrical Engineering at Chalmers University of Technology, Sweden. He is Senior Member of the IEEE Signal Processing Magazine Editorial Board. During 2019-2021, he was an IEEE Distinguished Lecturer with the Vehicular Technology Society. His current research interests

include the convergence of communication and sensing, in a 5G and Beyond 5G context.



Symeon Chatzinotas (MEng, MSc, PhD, FIEEE) is currently Full Professor / Chief Scientist I and Head of the research group SIGCOM in the Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg.

In the past, he has lectured as Visiting Professor at the University of Parma, Italy and contributed in numerous R&D projects for the Institute of Informatics & Telecommunications, National Center for Scientific Research “Demokritos” the Institute of Telematics and Informatics, Center of

Research and Technology Hellas and Mobile Communications Research Group, Center of Communication Systems Research, University of Surrey. He has received the M.Eng. in Telecommunications from Aristotle University of Thessaloniki, Greece and the M.Sc. and Ph.D. in Electronic Engineering from University of Surrey, UK in 2003, 2006 and 2009 respectively. He has authored more than 700 technical papers in refereed international journals, conferences and scientific books and has received numerous awards and recognitions, including the IEEE Fellowship and an IEEE Distinguished Contributions Award. He is currently in the editorial board of the IEEE Transactions on Communications, IEEE Open Journal of Vehicular Technology and the International Journal of Satellite Communications and Networking.