STARE: Real-Time Software Receiver for LTE and 5G NR Positioning and Signal Monitoring

Ivan Lapin*, Gonzalo Seco Granados†, Jaron Samson*, Olivier Renaudin†, Francesca Zanier*, and Lionel Ries*
*Radio Frequency Systems Division, European Space Agency, Keplerlaan 1, 2201 AZ Noordwijk, The Netherlands
ORCID: 0000-0002-1847-5499
†Department of Telecommunications and Systems Engineering, Universitat Autònoma de Barcelona, 08193 Bellaterra, Spain

***Abstract*—STARE, a real-time SofTwAre REceiver for positioning with the long-term evolution (LTE) and fifth-generation (5G) new radio (NR) cellular downlink signals, is presented and demonstrated. The real-time operation is achieved by interfacing directly with the software-defined radio (SDR), therefore avoiding the requirement to store the captured signal on a drive and allowing to process signals continuously over arbitrarily long periods. STARE supports multi-channel SDRs and parallel execution of an arbitrary number of tracking channels, which independently acquire and track the desired signals. During the acquisition stage, the tracking channel applies a path selection criterion based on the signal-to-noise ratio (SNR) of the earliest path to prevent incorrect delay and phase estimation, which may occur when the channel order is overestimated. The design of the tracking stage follows a closed-loop architecture providing a continuous estimation of the delay, Doppler, phase, and SNR. The real-time operation of STARE is demonstrated by monitoring downlink signals of a commercially operated LTE base station for an uninterrupted period of one week. For this purpose, STARE is deployed on a static monitoring setup composed of a processing unit, an SDR, an omnidirectional antenna, and a high-precision Rubidium reference clock. The collected measurements are used to study the SNR and delay errors. The delay errors are estimated using the code-minus-carrier (CMC) technique and are observed to achieve a sub-meter standard deviation.**

***Index Terms*—5G NR, Code-minus-carrier, LTE, Positioning, Real-time, Software receiver, STARE**

I. Introduction

The fourth-generation (4G) long-term evolution (LTE) and fifth-generation (5G) new radio (NR) cellular systems have evolved to become relevant sources of positioning thanks to their favorable signal characteristics and good coverage in urban environments [1]. The cellular signals are of particular interest to the users of the Global Navigation Satellite System (GNSS) who may improve their availability, continuity, accuracy, and integrity positioning performance by integrating the cellular downlink delay and phase measurements in the navigation engine [2]–[5].

The GNSS receivers rely traditionally on a computationally inexpensive closed-loop receiver architecture implementing the delay-locked loop (DLL) and phase-locked loop (PLL) to obtain the delay and phase measurements [6]. Various LTE and 5G NR software positioning receivers based on the closed-loop architecture were presented [7]–[11]. These receivers were shown to operate in a post-processing mode, where the captured baseband signal is first stored on a drive before being processed. Since the source code of the receivers has not been shared publicly, their real-time capabilities remain unclear. A real-time receiver accesses directly the software-defined radio (SDR) baseband stream, allowing to process signals continuously over arbitrarily long periods. Real-time receivers have become popular in GNSS, enabling studies based on signal monitoring or long positioning field trials spanning hours or days. A publicly available real-time software receiver would support similar studies in cellular positioning.

LTE and 5G NR cellular downlink waveforms utilize the orthogonal frequency division multiplexing (OFDM) scheme and contain various signals that can be used to estimate the delay and phase measurements. A signal dedicated for positioning, called the positioning reference signal (PRS) [12], [13], may be used for this purpose. However, the PRS requires user subscription and specific network configuration, reducing its availability. Alternatively, signals intended for other purposes not requiring user subscription may be used to obtain the delay and phase measurements, allowing for greater signal availability. One such signal in LTE systems, called the cell-specific reference signal (CRS), has been shown to provide satisfactory performance for positioning purposes [14], [15].

In this paper, STARE, a real-time SofTwAre REceiver for positioning with LTE and 5G NR cellular downlink signals, is presented. To demonstrate the real-time operation, STARE is deployed on a static monitoring setup to track LTE downlink signals for a continuous period of one week. The collected measurements are used to study the signal-to-noise ratio (SNR) and delay errors of the signal.

The remainder of the paper is organized as follows. Section II introduces the LTE and 5G NR downlink waveforms. Section III presents the design of STARE. Section IV defines the code-minus-carrier (CMC) metric that allows estimating the delay errors. The results of the real-time monitoring realized by STARE are studied in Section V. Conclusions are given in Section VI.

Notation: Matrices are denoted as uppercase boldface letters, such as $\mathbf{X} \in \mathbb{C}^{M\times N}$. Column vectors are denoted as lowercase boldface letters, such as $\mathbf{x} \in \mathbb{C}^{M\times 1}$. $\mathbf{I}_{P\times P}$ is a $P \times P$ eye matrix, $\mathbf{0}_{P\times Q}$ is a $P \times Q$ zero matrix, and $\mathbf{0}_{P\times 1}$ is a zero column vector of length P. The operators $(\cdot)^T$, $(\cdot)^H$, $(\cdot)^{-1}$, and $(\cdot)^\dagger$ denote the transpose, the Hermitian

978-1-6654-1616-0/22/$31.00 ©2022 IEEE

transpose, the inverse, and the Moore–Penrose pseudoinverse of a matrix, respectively. $|\cdot|$, $\angle(\cdot)$, and $(\cdot)^*$ denote the absolute value, the argument, and the conjugate of a complex number, respectively. The operator $\min(\mathbf{x})$ denotes the minimum value of a vector $\mathbf{x}$. The operator $\mathrm{sort}(\mathbf{x})$ produces a vector whose values are sorted in ascending order. The operator $\lceil\cdot\rceil$ denotes a ceiling function.

II. LTE and 5G NR Downlink Waveforms

The LTE and 5G NR cellular downlink waveforms are based on the OFDM transmission scheme that is described by a time-frequency grid in which a symbol time index i and a frequency subcarrier index n uniquely identify a single transmitted complex data symbol. The digital baseband signal $x_i[l]$ of the i-th OFDM symbol is expressed as

$$x_i[l] = \frac{1}{N_{\mathrm{fft}}} \sum_{n=-\frac{N_{\mathrm{fft}}}{2}}^{\frac{N_{\mathrm{fft}}}{2}-1} X_i[n] \cdot e^{j\frac{2\pi}{N_{\mathrm{fft}}} n (l-N_{\mathrm{cp}})}, \qquad (1)$$

for $l = 0, 1, \ldots, N_{\mathrm{fft}} + N_{\mathrm{cp}} - 1$, where n is the OFDM subcarrier index, $X_i[n]$ is the complex data symbol transmitted on the n-th subcarrier, N_{fft} is the total number of subcarriers available for modulation that are symmetrically arranged around the central frequency with the index $n = 0$, and N_{cp} is the number of samples within the cyclic prefix (CP). The CP is a sequence of the last N_{cp} samples of the symbol prepended to its beginning to provide a guard interval preventing the inter-symbol interference from the previous symbol whilst transforming the effect of the channel into a linear convolution. The digital signal in (1) can be conveniently generated using the inverse fast Fourier transform (IFFT). The continuous signal is then generated using the digital-to-analog converter. The resulting subcarrier spacing is $\Delta f = \frac{1}{T_{\mathrm{s}}}$ [Hz], where T_{s} [s] is the duration of the OFDM symbol without the CP.

The 3GPP specification [12], [13] maps the $N_{\mathrm{sc}} \leq N_{\mathrm{fft}}$ transmitted resource elements to the N_{fft} available subcarriers. The OFDM subcarrier index n on which the k-th resource element is transmitted can be obtained using the mapping function $\kappa(k)$ defined in the frame of this paper as

$$n = \kappa(k) = \begin{cases} k - \frac{N_{\mathrm{sc}}}{2} & \text{when } k < \frac{N_{\mathrm{sc}}}{2}, \\ k - \frac{N_{\mathrm{sc}}}{2} + \xi & \text{otherwise,} \end{cases} \qquad (2)$$

for $k = 0, 1, \ldots, N_{\mathrm{sc}}-1$, where $\xi \in \{0, 1\}$ reflects whether the central frequency is used for transmission or not. The unused subcarriers are left empty.

The 5G NR OFDM transmission scheme is logically organized into 10 ms long radio frames. The radio frame is composed of $10 \cdot 2^{\mu}$ slots, where $\mu \in \{0, 1, 2, 3, 4\}$ is called the numerology parameter whose value is driven by the frequency band and the signal bandwidth [13]. In the normal CP mode, the slot is composed of $N_{\mathrm{symb}}^{\mathrm{DL}} = 14$ symbols. The smallest logical block of the OFDM grid is called the resource block (RB) and comprises $N_{\mathrm{RB}}^{\mathrm{DL}} = 12$ subcarriers and $N_{\mathrm{symb}}^{\mathrm{DL}}$ symbols. The subcarriers are spaced $\Delta f_{\mathrm{sc}} = 15 \cdot 2^{\mu}$ kHz apart. In the frequency range 1 (FR1), the maximum allowable transmission bandwidth is $B = 100$ MHz and the time division duplexing (TDD) scheme is used. The central frequency is used for data transmission, so $\xi = 0$ in (2).

The OFDM scheme of LTE systems can be interpreted as a subset of the 5G NR scheme configured with $\mu = 0$ [12], resulting in $\Delta f = 15$ kHz. Each LTE radio frame lasts 10 ms and is composed of 20 slots. Each slot is composed of $N_{\mathrm{symb}}^{\mathrm{DL}} = 7$ symbols. Notable differences of LTE, when compared to 5G NR, are the smaller maximum bandwidth of $B = 20$ MHz and frequency division duplexing (FDD) scheme that is used in the deployments on the European continent [16]. The central frequency is omitted from data transmission in LTE, so $\xi = 1$ in (2).

III. Receiver Design

The cellular software receivers used for positioning research purposes work traditionally in a post-processing mode, where the captured baseband signal is first stored on a drive before being processed. The main drawback of this approach is its demand for data storage for high signal bandwidths. For example, a 100 MHz 5G NR waveform requires a sampling rate of 122.88 Msps. Assuming 24 bits per complex sample, every minute of the baseband capture of this signal would require around 22 GB of storage space. Although such demand can be met for short demonstrations, this is no longer the case for the studies requiring days or weeks of continuous signal tracking. To allow for operation over arbitrarily long periods, STARE, a SofTwAre REceiver capable of real-time processing of LTE and 5G NR signals directly from the SDR baseband stream, is proposed.

A. Operational Modes

STARE supports two operational modes: real-time and post-processing. In the real-time mode, STARE is connected to the SDR unit and accesses the live baseband streams using the SoapySDR application programming interface [17]. SoapySDR makes the receiver compatible with a wide range of SDR brands. To fully utilize the hardware, STARE supports parallel processing of all radio channels of the SDR. The proposed channel hierarchy is shown in Fig. 1. Each radio channel represents a separate baseband stream provided by the hardware front-end and can be configured with a specific carrier frequency, input antenna, and front-end gain. All radio channels share a common sampling rate.

The stream of each radio channel can be processed by an arbitrary number of tracking channels as shown in Fig. 1. Each tracking channel then keeps applying independently the signal processing stages to its input stream to acquire and track the desired signal. During tracking, each tracking channel outputs the estimated time-tagged delay, Doppler, phase, and SNR measurements. These measurements can then be stored in a custom binary data format. Each tracking channel generates less than 1.3 GB of data storage for each collected hour when a 2 kHz measurement update rate is set. The tracking channels are software-based and executed in parallel using multi-threaded processing. The number of tracking channels

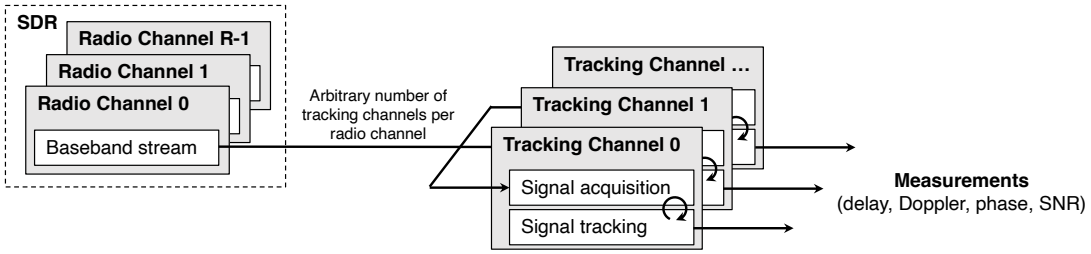

Fig. 1. Channel hierarchy of STARE allowing to configure various radio and tracking channels for the SDR. Each radio channel represents an individual baseband input stream. The maximum number of radio channels is determined by the SDR hardware. Each tracking channel executes independently the signal processing stages for the configured cell ID, antenna port, and algorithm parameters. The tracking channel may be configured arbitrarily and does not depend on the other channels. The number of tracking channels is limited only by the memory and computational power of the processing unit.

is limited only by the memory and computational power of the employed processing unit. The real-time mode is useful to process signals over arbitrarily long periods. Notable use cases include signal monitoring or long positioning field trials.

In the post-processing mode, STARE processes the baseband samples from a binary input file. In this mode, the SDR in Fig. 1 is replaced by the input file and only a single radio channel is allowed. The number of tracking channels remains arbitrary. To process multiple files at the same time, several instances of the receiver can be executed in parallel. The post-processing mode is useful to evaluate the signal processing algorithms or to process outputs of signal generators.

B. Supported Cellular Signals

The tracking channel supports various signals that can be transmitted on the LTE and 5G NR downlink waveforms. The coarse signal acquisition and synchronization are for both systems obtained using the primary synchronization signal (PSS) and secondary synchronization signal (SSS). PSS and SSS are code sequences that are always available in the downlink waveform to allow the user to find and identify the given cell and perform time and frequency synchronization.

In the case of 5G NR, the channel state information reference signal (CSI-RS) configured as the tracking reference signal (TRS) on antenna port 1000 can be tracked. The supported TRS is transmitted periodically every slot with the frequency density 3 pilots per the RB, full occupation of all the available RBs, and no code division multiplexing [13]. The supported signal bandwidth is $B = 100$ MHz and numerology $\mu = 1$. The CSI-RS is user-dependent and its tracking is supported mainly to evaluate the performance of 5G NR networks [18].

In the case of LTE, the CRS can be tracked. The tracking channel supports the full configuration of the CRS including the desired cell ID, CP mode, and antenna port. Since the CRS does not require the user subscription or specific protocol implementation, this signal is suitable for signal monitoring or opportunistic positioning.

Thanks to the modular design of STARE, the processing of other OFDM signals can be introduced easily, such as the PRS or the demodulation reference signal (DM-RS) of the 5G synchronization signal block (SSB) [11].

C. Signal Processing Stages of Tracking Channel

The tracking channel of STARE estimates continuously the carrier frequency offset (CFO) and sample timing offset (STO) of the desired signal and outputs the related delay ($\hat{\tau}$), Doppler ($\hat{\upsilon}$), and phase ($\hat{\phi}$) measurements. The tracking channel also outputs the estimated SNR. The measurements are stored in a dedicated hourly file for each tracking channel. The diagram of the signal processing blocks of a single tracking channel is shown in Fig. 2. The design is inspired by the previous works on LTE and 5G NR positioning receivers [7]–[11]. The tracking channel operates in three stages:

(A) *Coarse acquisition stage* initializes the CFO and STO estimates and establishes the timing synchronization to the downlink signal.
(B) *Fine acquisition stage* refines the initial estimates to allow the tracking loops to acquire the lock of the signal.
(C) *Tracking stage* keeps continuously updating the estimates and outputs the delay, Doppler, and phase measurements until the lock of the signal is lost and its re-acquisition is needed.

The stages are implemented using a combination of C++ and Python programming languages. For complex matrix operations, the coarse and fine acquisition stages are implemented in Python. To achieve the speed needed for the real-time mode, the tracking stage is implemented in C++. The interface between the languages is transparent and the user only interacts with the C++ code. Further details on the signal processing employed in each stage are provided in the next sections.

D. Coarse Acquisition Stage

The coarse acquisition stage estimates the initial CFO and STO of the signal and synchronizes the tracking channel to the beginning of the radio frame. The coarse acquisition is performed in the time domain and does not require demodulation. The node (1) in Fig. 2 is connected to the node (A) during the coarse acquisition.

1) Coarse Carrier Frequency Offset Acquisition: The initial CFO estimation is performed by the non-data-aided maximum likelihood estimator proposed by van de Beek et al. [19], with the energy term omitted. The algorithm exploits the

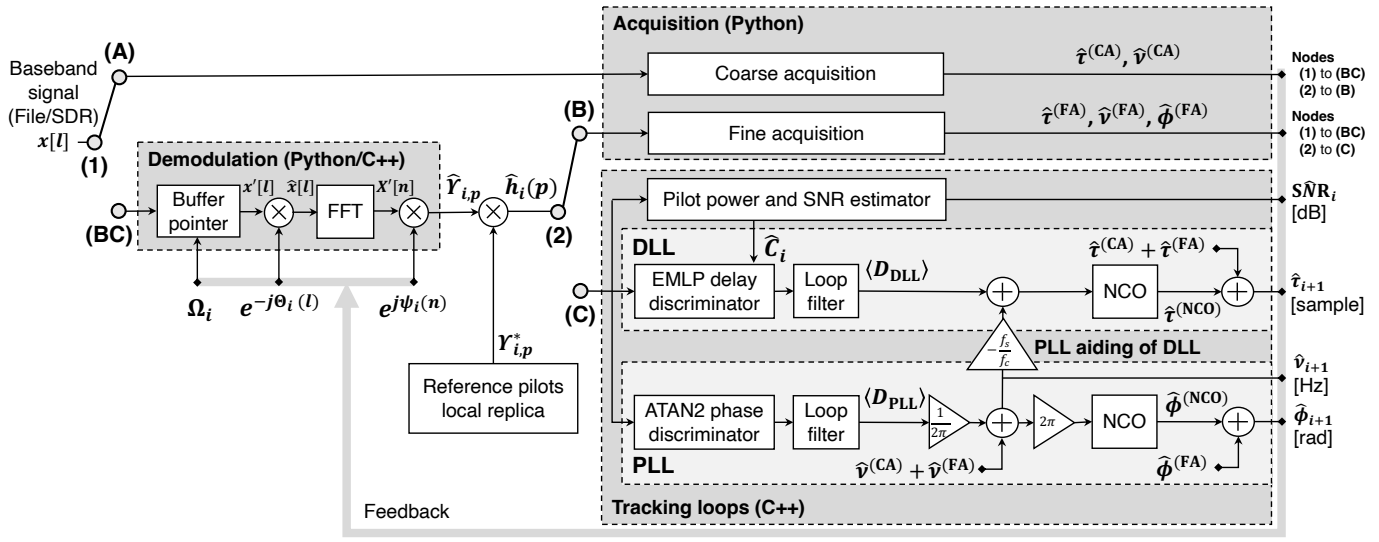

Fig. 2. Block diagram of a single tracking channel of STARE. Coarse acquisition (A) and fine acquisition (B) stages initiate the CFO and STO estimates. The design of the tracking stage (C) follows a closed-loop architecture, where the tracking loops keep updating the estimates, which are then fed back to the received signal in the next iteration to maintain the lock of the signal. The integer part of the delay estimate ($\lceil \hat{\tau} \rceil$) is used to shift the FFT window in the time domain and the fractional part ($\hat{\tau} - \lceil \hat{\tau} \rceil$) is applied as a phase rotation of the subcarriers in the frequency domain. The estimated SNR belongs to the current channel iteration and the delay, Doppler, and phase measurements belong to the next iteration. The NCO denotes the numerically controlled oscillator in the figure.

redundancy of the CP to estimate the CFO over the sliding window of N_{cp} samples. The CFO can be estimated as

$$\hat{v}^{(\mathrm{CA})} \approx -\frac{\Delta f}{2\pi} \angle \left(R_{\mathrm{x}} \left(\underset{l}{\operatorname{argmax}} \left\{ |R_{\mathrm{x}}(l)| \right\} \right) \right) \ [\mathrm{Hz}], \quad (3)$$

where $R_{\mathrm{x}}(l)$ is the autocorrelation function defined as

$$R_{\mathrm{x}}(l) = \sum_{j=l}^{l+N_{\mathrm{cp}}-1} x[j]\, x^*[j + N_{\mathrm{fft}}]. \quad (4)$$

2) Coarse Sample Timing Offset Acquisition: Although (3) also provides the initial estimate of the STO, this timing is aligned only to the start of the OFDM symbol. To obtain STO aligned to the start of the LTE frame, the previously estimated CFO is removed from the received signal and the result is correlated in time with the locally generated PSS and SSS replicas. The coarse STO $\hat{\tau}^{(\mathrm{CA})}$ has the resolution of the sample period.

E. Fine Acquisition Stage

After obtaining the initial STO and CFO estimates in the coarse acquisition stage, the estimates are refined in the fine acquisition stage by connecting the nodes (1) and (2) in Fig. 2 to nodes (BC) and (B), respectively. The fine acquisition is performed using the OFDM subcarriers in the frequency domain and requires demodulation. The received signal is related to the local replica through the channel frequency response (CFR) that can be estimated from the subcarrier pilots as

$$\hat{h}_i(p) = \hat{\Upsilon}_{i,p} \Upsilon^*_{i,p} \quad \text{for} \quad p = 0, 1, \ldots, P_i - 1, \quad (5)$$

where p is the pilot index, P_i is the total number of pilots, i is the symbol time index reflecting the loop iteration, $\hat{\Upsilon}_{i,p}$ is the received pilot symbol with the removed delay and phase estimates from the previous iteration of the tracking loops as shown in Fig. 2, and $\Upsilon_{i,p}$ is the pilot symbol replica at the receiver. Unless needed, the symbol time index i is for simplicity omitted for the remainder of this section.

1) Fine Carrier Frequency Offset Estimation: The fine CFO is estimated using the phase difference between two consecutive estimates of the CFR as

$$\hat{v}_i^{(\mathrm{FA})} = \frac{1}{2\,\pi\, T_\eta} \angle \left(\sum_{p=0}^{P-1} \hat{h}_i(p) \hat{h}^*_{i+\iota}(p) \right) \ [\mathrm{Hz}], \quad (6)$$

where ι and T_η [s] are the intervals between the CFR estimates expressed as the number of OFDM symbols and elapsed time, respectively.

2) Fine Sample Timing Offset Estimation: The ESPRIT algorithm is used to estimate the fine STO using the rotational invariance property of the CFR. The estimated CFR in (5) can be organized into snapshot vectors $\mathbf{x}(q)$ of length M as

$$\mathbf{x}(q) = [\hat{h}(q),\ \hat{h}(q+1), \ldots,\ \hat{h}(q+M-1)]^T \in \mathbb{C}^{M \times 1}, \quad (7)$$

where $M \leq P$. The parameter $m \in [0, 1]$ determines the length of snapshots as $M = \lfloor m \cdot P \rfloor$. Higher values of m increase the multipath resolution at the cost of reduced noise averaging. The configuration of this parameter should consider the number of expected paths in the channel, denoted as L, as it is necessary that $M \geq L$. The number of snapshots is determined as $N = P - M$. The data matrix $\mathbf{X}$ can be constructed as

$$\mathbf{X} = [\mathbf{x}(0),\ \mathbf{x}(1), \ldots,\ \mathbf{x}(N-1)]^T \in \mathbb{C}^{M \times N}. \quad (8)$$

The standard ESPRIT approach can be used to estimate the delays of L paths from the snapshot matrix $\mathbf{X}$ as

$$\begin{aligned}\hat{\boldsymbol{\tau}} &= \operatorname{sort}\left(-\frac{\boldsymbol{\psi}}{2\pi\Delta P\Delta f}\right)\\ &= [\hat{\tau}_0,\ \hat{\tau}_1, \ldots, \hat{\tau}_{L-1}]^T \in \mathbb{C}^{L\times 1}\ [s],\end{aligned} \tag{9}$$

where $\boldsymbol{\psi}$ are the eigenvalues of the estimated ESPRIT rotational matrix $\boldsymbol{\Psi}$ obtained from the unitary matrix $\mathbf{U}$ of the singular value decomposition $\mathbf{X} = \mathbf{U}\,\boldsymbol{\Sigma}\,\mathbf{V}^H$. The matrix $\boldsymbol{\Sigma} \in \mathbb{C}^{M\times N}$ is diagonal and contains the singular values

$$\operatorname{diag}\left(\hat{\boldsymbol{\Sigma}}\right) = [\sigma_0, \sigma_1, \ldots, \sigma_{\min([M,N])}]^T, \tag{10}$$

where the assumed order is $\sigma_j \geq \sigma_{j+1}$.

3) Phase Offset Estimation: The phase offsets can be determined from the complex amplitudes of paths $\boldsymbol{\Lambda} = [\Lambda_o, \Lambda_1\ \ldots, \Lambda_{L-1}]^T \in \mathbb{C}^{L\times 1}$ that can be estimated using the least-squares solution as

$$\hat{\boldsymbol{\Lambda}} = \left(\hat{\mathbf{G}}^H\hat{\mathbf{G}}\right)^{-1}\hat{\mathbf{G}}^H\hat{\mathbf{h}} \in \mathbb{C}^{L\times 1}, \tag{11}$$

where $\hat{\mathbf{G}}$ is the delay matrix defined as

$$\hat{\mathbf{G}} = \exp\left(-\frac{j2\pi f_{\mathrm{s}}}{N_{\mathrm{fft}}}\,\hat{\boldsymbol{\tau}}\ [n_0, \ldots, n_{P-1}]\right)^T \in \mathbb{C}^{P\times L}. \tag{12}$$

The phase of of the l-th path is

$$\hat{\phi}_l = \angle\left(\hat{\Lambda}_l\right)\ [\mathrm{rad}]. \tag{13}$$

4) Path Selection Criterion: To properly estimate the delay and phase offsets in multipath environments, the ESPRIT algorithm requires knowledge of the channel order L, which represents the number of paths in the radio channel. Channel order estimators usually rely on the information included in the eigenvalues $\lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_{M-1}$ of the autocorrelation matrix obtained from the data matrix $\mathbf{X}$. The eigenvalues can be conveniently determined from the singular values in (10) as $\lambda_j = \frac{\sigma_j^2}{N}$. The channel order is estimated using the minimum descriptive length (MDL) method as [20]

$$\begin{aligned}\mathrm{MDL}\,(l) = -N\,(M-l)\ln\left[\frac{\prod_{j=l}^{M-1}\lambda_j^{\frac{1}{M-l}}}{\frac{1}{M-l}\sum_{j=l}^{M-1}\lambda_j}\right]\\ +\frac{1}{2}l\,(2M-l)\log N,\end{aligned} \tag{14}$$

where $l \in \{0, 1, \ldots, M-1\}$. The MDL channel order estimate is

$$\hat{L} = \underset{l}{\operatorname{argmin}}\ \mathrm{MDL}\,(l)\,. \tag{15}$$

The MDL method tends to overestimate the channel order that can cause the ESPRIT algorithm to produce delay outliers in the form of the false paths arriving before the true earliest path, resulting in range biases [10], [21], [22]. To mitigate the channel order overestimation, the estimated paths are filtered by a path selection criterion proposed by Lapin et al. in [18]. The criterion selects the earliest path whose SNR exceeds a configurable threshold γ [dB]. The SNRs of the paths are estimated as

$$\hat{\mathrm{SNR}}_l = 10\log_{10}\left(\frac{P\,|\hat{\Lambda}_l|^2}{\hat{\mathbf{w}}^H\hat{\mathbf{w}}}\right)[\mathrm{dB}]. \tag{16}$$

where $\hat{\mathbf{w}}$ is the noise vector that is estimated from the complex amplitudes in (11) as $\hat{\mathbf{w}} = \hat{\mathbf{h}} - \hat{\mathbf{G}}\,\hat{\boldsymbol{\Lambda}}$. The index of the earliest path l_γ exceeding the threshold is determined as

$$l_\gamma = \underset{l}{\operatorname{argmin}}\{\hat{\mathrm{SNR}}_l > \gamma\}. \tag{17}$$

The fine acquisition algorithm uses the l_γ-th path to determine the STO as

$$\tau^{(\mathrm{FA})} = \frac{\hat{\tau}_{l_\gamma}}{T_{\mathrm{s}}}\ [\mathrm{sample}], \tag{18}$$

and the phase offset as

$$\phi^{(\mathrm{FA})} = \hat{\phi}_{l_\gamma}\ [\mathrm{rad}]. \tag{19}$$

The threshold γ can be derived empirically using the results of the outlier analysis of the ESPRIT algorithm outputs for a given configuration and various SNRs.

F. Tracking Stage

After the fine acquisition stage, the tracking stage commences. The continuous signal tracking is realized by a closed-loop architecture where the DLL and PLL estimate the respective residual delay and phase offsets between the received signal and the locally generated replica. During tracking, the nodes (1) and (2) in Fig. 2 are connected to nodes (BC) and (C), respectively. Each tracking loop is composed of three parts that are discussed in the next sections: discriminator, loop filter, and numerically controlled oscillator (NCO). The main role of the tracking loops is to drive the discriminator outputs to zero and thus maintain the lock of the signal. To achieve this, the outputs of the tracking loops are fed back to the received signal in the next loop iteration to remove the estimated offsets.

1) Early-Minus-Late Power Delay Discriminator: The EMLP delay discriminator used in the DLL estimates the delay offset by correlating the received signal with the local replica. The replica is delayed and advanced by $\pm\delta$ samples and the resulting two correlators are referred to as the early and late branches. A delay offset e_τ of the received signal causes phase rotations of the OFDM subcarriers in the frequency domain and can be expressed at a given time symbol as [23]

$$R\,(e_\tau, \mp\delta) = \frac{1}{P}\sum_{p=0}^{P-1}\hat{h}(p)\,e^{-j\frac{2\pi}{N_{\mathrm{fft}}}(e_\tau\pm\delta)\,n_p}, \tag{20}$$

where $R\,(e_\tau, -\delta)$ represents the output of the early branch and $R\,(e_\tau, +\delta)$ represents the output of the late branch. For equally spaced pilots with a constant transmission pattern, the OFDM index n_p in (20) can be expressed using the mapping function in (2) as $n_p = \kappa\,(p\,\Delta P + k_0)$, where ΔP is the constant pilot spacing, and k_0 is the subcarrier offset of the first pilot.

The power of the transmitted pilot is assumed to be equal on each subcarrier and is denoted as C. The power of each pilot replica at the receiver is assumed to be unitary, so $|\Upsilon_p|^2 = 1$. The normalized non-coherent EMLP delay discriminator of the DLL is then defined as

$$D_{\mathrm{DLL}}\left(e_\tau, \delta\right) = \frac{|R\left(e_\tau, -\delta\right)|^2 - |R\left(e_\tau, \delta\right)|^2}{C\, k_{\mathrm{EMLP}}\left(\delta\right)} \text{ [sample]}, \quad (21)$$

where $k_{\mathrm{EMLP}}\left(\delta\right)$ is the normalization factor to keep $D_{\mathrm{DLL}}\left(e_\tau, \delta\right) \approx e_\tau$ when $e_\tau \approx 0$. The normalization factor can be expressed for an arbitrary correlator half-spacing as [24]

$$k_{\mathrm{EMLP}}\left(\delta\right) = \frac{2\left[1 - \delta\pi\beta\sin\left(2\pi\beta\delta\right) - \cos\left(2\pi\beta\delta\right)\right]}{\left(\pi\beta\right)^2 \delta^3}, \quad (22)$$

where $\beta = \frac{P\,\Delta P}{N_{\mathrm{fft}}}$ is the OFDM waveform factor that corresponds to the ratio between the usable signal bandwidth spanned by the pilots and the IFFT/FFT length.

Every discriminator has a limited operational range that determines the tracking threshold of the loop. Delay offsets above the tracking threshold will likely cause the tracking loop to loose lock of the signal. In the case of the EMLP discriminator, the DLL tracking threshold ζ_{DLL} is determined as the delay offset after which the discriminator function deviates from the ideal linearity by more than α as

$$\zeta_{\mathrm{DLL}} = \underset{e_\tau}{\mathrm{argmax}}\{|D_{\mathrm{DLL}}\left(e_\tau, \delta\right) - e_\tau| \leq \alpha\}. \quad (23)$$

As a rule of thumb, ζ_{DLL} determines the maximum acceptable 3-sigma of the total jitter and dynamic stress error of the DLL ($3\,\sigma_{\mathrm{DLL}} \leq \zeta_{\mathrm{DLL}}$) [6]. To enable the analytical evaluation of the EMLP discriminator function, the non-coherent early and late branch outputs of the EMLP discriminator can be approximated for large FFT sizes N_{fft} in a noiseless multipath-free channel as [24]

$$|R\left(e_\tau, \pm\delta\right)|^2 \approx C\,\mathrm{sinc}^2\left(\pi\beta\left(e_\tau \pm \delta\right)\right), \quad (24)$$

where $\mathrm{sinc}\left(x\right) = \frac{\sin(x)}{x}$. The approximated EMLP discriminator function of the CRS of the LTE waveform with $N_{\mathrm{fft}} = 2048$ evaluated for various correlator half-spacings is shown in Fig. 3. The shape of the discriminator function gives a name to the so-called S-curve. Outside the linear region, the discriminator output no longer corresponds to the delay offset and the performance of the tracking loop degrades. Fig. 3 shows that δ has a negligible impact on the shape of the discriminator function around the linear region. To derive ζ_{DLL}, a linearity threshold $\alpha = 0.05$ is assumed. The tracking thresholds evaluated for various bandwidths of the LTE signal are shown in Table I.

2) Pilot Power and SNR Estimation: To estimate the pilot power $\hat{C}$ needed by the EMLP discriminator in (21), the CFR $\hat{h}(p)$ and the total power $\hat{P}_p = |\hat{h}(p)|^2$ are first averaged on each subcarrier separately using time-variant moving average filters with the window of length Q. Each averaging filter is reset when any of the tracking loops looses the lock of the signal. The time-averaged CFR and the time-averaged total power are further averaged across the subcarriers in frequency using a moving frequency window of maximum length 19 (e.g. the pilot $p = 0$ is not averaged, the pilot $p = 1$ is averaged with the pilots $p = 0$ and $p = 2$, and the tenth pilot $p = 9$ onwards is averaged using nine pilots on each side). The pilot power is estimated as

$$\hat{C} = \frac{1}{P}\sum_{p=0}^{P-1} |\langle\hat{h}(p)\rangle|^2, \quad (25)$$

where $\langle\hat{h}_i(p)\rangle$ is the resulting average CFR on a given pilot. The SNR is estimated as

$$\hat{\mathrm{SNR}} = 10\log_{10}\left(\frac{\hat{C}}{\frac{1}{P}\sum_{p=0}^{P-1}\langle\hat{P}_p\rangle - \hat{C}}\right), \quad (26)$$

where $\langle\hat{P}_{i,p}\rangle$ is the resulting average total power on a given pilot.

3) ATAN2 Phase Discriminator: The phase discriminator function D_{PLL} estimates the phase offset between the received signal and the local replica at the receiver by applying the ATAN2 operator to the estimated CFR, which is expressed as [7], [10]

$$D_{\mathrm{PLL}} = \angle\left(\sum_{p=0}^{P-1}\hat{h}(p)\right) \text{ [rad]}. \quad (27)$$

The PLL tracking threshold is limited by the 2π pull-in range of the ATAN2 argument operator used in (27). As

TABLE I
LTE DOWNLINK BANDWIDTHS (B) AND RELATED SIGNAL PARAMETERS, OFDM WAVEFORM FACTORS (β), AND TRACKING THRESHOLDS (ζ_{DLL})

B [MHz]	N_{fft}	N_{sc}	P	ΔP	β	ζ_{DLL}
20	2048	1200	200	6	0.586	0.388
15	1536	900	150	6	0.586	0.388
10	1024	600	100	6	0.586	0.388
5	512	300	50	6	0.586	0.388
3	256	180	30	6	0.703	0.344
1.4	128	72	12	6	0.563	0.398

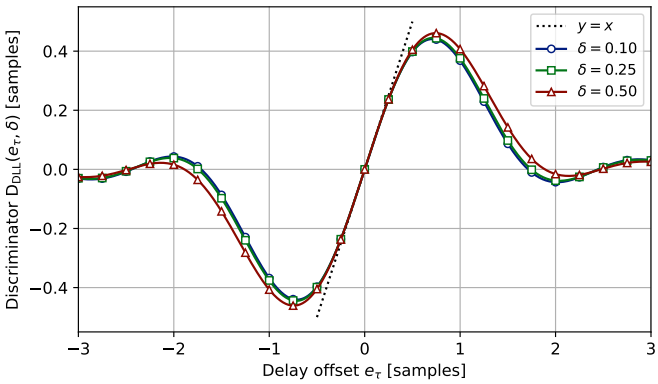

Fig. 3. Approximated EMLP discriminator function of the CRS of the LTE waveform with $N_{\mathrm{fft}} = 2048$ evaluated for various values of the correlator half-spacing δ. The linear region with the unit slope ($y = x$) is also shown.

a conservative rule of thumb, the tracking threshold ζ_{PLL} determines the maximum acceptable 3-sigma of the total jitter and dynamic stress error of the PLL ($3\,\sigma_{\mathrm{PLL}} \leq \zeta_{\mathrm{PLL}}$) [6]. The threshold is set to one-fourth of the pull-in range of the ATAN2 discriminator resulting in

$$\zeta_{\mathrm{PLL}} = \frac{\pi}{2}\ [\mathrm{rad}]. \tag{28}$$

4) Loop Filter: The outputs of the DLL (D_{DLL}) and PLL (D_{PLL}) discriminators are fed to the discrete loop filters to reduce the higher frequency noise components. The tracking loops are updated repeatedly with a period called the loop integration time denoted as η [sample] or $T_\eta = \eta\, T_{\mathrm{s}}$ [s].

The loop filter transfer function $F(z)$ of the second-order DLL can be expressed in the z-domain as

$$F(z) = \frac{\left(\frac{T_\eta \omega_0^2}{2} + 2\zeta\omega_0\right) + \left(\frac{T_\eta \omega_0^2}{2} - 2\zeta\omega_0\right) z^{-1}}{1 - z^{-1}}, \tag{29}$$

where ζ is the loop damping factor and ω_0 [Hz] is the loop natural frequency. To parameterize the loop, the loop bandwidth B_{n} [Hz] is frequently used and relates to ω_0 as

$$\omega_0 = \frac{8\zeta}{4\zeta^2 + 1} B_{\mathrm{n}}\ [\mathrm{Hz}]. \tag{30}$$

The loop filter transfer function of the third-order PLL can be expressed in the z-domain as

$$F(z) = \frac{\left(\frac{T_\eta^2 \omega_0^3}{4} + \frac{a T_\eta \omega_0^2}{2} + b\omega_0\right) + \left(\frac{T_\eta^2 \omega_0^3}{2} - 2b\omega_0\right) z^{-1}}{1 - 2z^{-1} + z^{-2}} + \frac{\left(\frac{T_\eta^2 \omega_0^3}{4} - \frac{a T_\eta \omega_0^2}{2} + b\omega_0\right)}{1 - 2z^{-1} + z^{-2}}, \tag{31}$$

where a and b are the filter coefficients and ω_0 is determined using B_{n} [Hz] as

$$\omega_0 = \frac{4\,(ab - 1)}{ab^2 + a^2 - b} B_{\mathrm{n}}\ [\mathrm{Hz}]. \tag{32}$$

The outputs of the delay and phase loop filters at i-th channel iteration are denoted as $\langle D_{\mathrm{DLL}} \rangle_i$ and $\langle D_{\mathrm{PLL}} \rangle_i$, respectively.

5) Numerically Controlled Oscillator: The Doppler of the next channel iteration $(i+1)$ is estimated using the output of the phase loop filter $\langle D_{\mathrm{PLL}} \rangle_i$ representing the rate of change of the phase as

$$\hat{v}_{i+1} = \hat{v}^{(\mathrm{CA})} + \hat{v}^{(\mathrm{FA})} + \frac{1}{2\pi} \langle D_{\mathrm{PLL}} \rangle_i\ [\mathrm{Hz}]. \tag{33}$$

The DLL and PLL NCOs are implemented as integrators obtained via boxcart z-transformation. The PLL NCO updates the phase estimate for the next channel iteration $(i+1)$ using the Doppler estimate in (33) as

$$\hat{\phi}_{i+1}^{(\mathrm{NCO})} = \hat{\phi}_i^{(\mathrm{NCO})} + 2\,\pi\, T_\eta\, \hat{v}_{i+1}\ [\mathrm{rad}]. \tag{34}$$

The phase estimate of the next channel iteration is obtained as

$$\hat{\phi}_{i+1} = \hat{\phi}^{(\mathrm{FA})} + \hat{\phi}_{i+1}^{(\mathrm{NCO})}\ [\mathrm{rad}]. \tag{35}$$

The DLL NCO updates the delay estimate for the next channel iteration $(i+1)$ with the delay loop filter output $\langle D_{\mathrm{DLL}} \rangle_i$ as

$$\hat{\tau}_{i+1}^{(\mathrm{NCO})} = \hat{\tau}_i^{(\mathrm{NCO})} + T_\eta \left(\langle D_{\mathrm{DLL}} \rangle_i - \frac{f_s}{f_c}\, \hat{v}_{i+1} \right)\ [\mathrm{sample}], \tag{36}$$

where the term $-\frac{f_s}{f_c}\, \hat{v}_{i+1}$ represents the PLL aiding of the DLL. The aiding allows reducing the bandwidth of the DLL as it compensates the sample timing drift caused by the Doppler. The aiding may be utilized when the same oscillator is used for sampling and down-conversion. The delay estimate of the next channel iteration is obtained as

$$\hat{\tau}_{i+1} = \hat{\tau}^{(\mathrm{CA})} + \hat{\tau}^{(\mathrm{FA})} + \hat{\tau}_{i+1}^{(\mathrm{NCO})}\ [\mathrm{sample}]. \tag{37}$$

6) Loop Feedback and Demodulation: The delay, Doppler, and phase estimates in (37), (33), and (35), respectively, are fed back to the received signal in the next channel iteration to remove the estimated offsets. The sample counter representing the start of the FFT window since beginning of the stream is determined using the integer part of the delay estimate $\lceil \hat{\tau}_i \rceil$ as

$$\Omega_i = \lceil \hat{\tau}_i \rceil + N_{\mathrm{d}}(i) + i \cdot \eta, \tag{38}$$

where $N_{\mathrm{d}}(i) \leq N_{\mathrm{cp}}(i)$ is the discarded part of the CP to allow the tracking channel to apply the FFT operation anywhere within the OFDM symbol. The sample counter is used to drive the pointer in the sample buffer to obtain the correct start of the input signal as $x'[l] = x[l + \Omega_i]$. In the time domain, the Doppler and phase estimates are removed from the shifted input signal $x'[l]$ before entering the FFT block as

$$\hat{x}[l] = x'[l]\, e^{-j\Theta(l)}, \quad \text{for} \quad l = 0, 1, \ldots, N_{\mathrm{fft}} - 1, \tag{39}$$

where

$$\Theta(l) = \frac{2\,\pi\, \hat{v}_i\, T_{\mathrm{s}}\, (l + N_{\mathrm{d}}(i) + \lceil \hat{\tau} \rceil) + \hat{\phi}_i}{N_{\mathrm{fft}}}. \tag{40}$$

After applying FFT block of length N_{fft} expressed as $X'[n] = \mathrm{FFT}\{\hat{x}[l]\}$, the fractional part of the delay estimate $\hat{\tau} - \lceil \hat{\tau}_i \rceil$ is removed from the subcarriers in the frequency domain as

$$\hat{X}[n] = X'[n]\, e^{j\Psi(n)}, \quad \text{for} \quad n = 0, 1, \ldots, N_{\mathrm{fft}} - 1, \tag{41}$$

where

$$\Psi(n) = \frac{2\,\pi\, n\, (N_{\mathrm{cp}}(i) - N_{\mathrm{d}}(i) + \hat{\tau} - \lceil \hat{\tau} \rceil)}{N_{\mathrm{fft}}}. \tag{42}$$

IV. Code-Minus-Carrier Technique

The code-minus-carrier (CMC) technique is used to estimate the delay errors by subtracting the phase measurements $\hat{\phi}$ from the delay measurements $\hat{\tau}$ to remove the geometry and clock effects. This is possible because the variance of the phase error $\sigma_{\varepsilon^{(\phi)}}$ is significantly smaller than the variance of the delay error $\sigma_{\varepsilon^{(\tau)}}$. The CMC can be expressed as

$$\mathrm{CMC} = \hat{\tau} - \left(-\hat{\phi}\right) = -B^{(\phi)} + \varepsilon^{(\tau)} - \varepsilon^{(\phi)}\ [\mathrm{m}], \tag{43}$$

where c is the speed of light assumed to be $299.792.458 \frac{m}{s}$, f_c [Hz] is the carrier frequency of the signal, $B^{(\phi)}$ is the

ambiguity due to unknown number of carrier cycles, and $\varepsilon^{(\tau)}$ and $\varepsilon^{(\phi)}$ are the delay and phase measurement errors, respectively, including the effects of the noise and multipath. The negative sign of the phase measurement $\left(-\hat{\phi}\right)$ in (43) is applied because the phase measurements have opposite signs than the delay measurements at the receiver output. On the contrary to GNSS, terrestrial positioning is not impacted by the ionosphere and multi-frequency measurements are not needed to compute the CMC. Considering the bias term $-B^{(\phi)}$ in (43) is constant within a continuous arc in which no cycle slips occurred, the mean $\langle \mathrm{CMC} \rangle$ is subtracted from each arc to determine the variance of the delay noise.

The identification of the continuous arcs of phase measurements requires detection of cycle slips. The cycle slip detection technique exploits the different polarizations between the antenna ports 0 and 1 transmitted by the station as proposed by Shamaei and Kassas in [5]. The difference between the q-th phase measurements on the two antenna ports on the same frequency within a given arc is defined as

$$\Delta\hat{\phi}_q^{(\mathrm{AP0,AP1})} = \hat{\phi}_q^{(\mathrm{AP0})} - \hat{\phi}_q^{(\mathrm{AP1})} \text{ [rad]}, \tag{44}$$

where $\hat{\phi}_q^{(\mathrm{AP0})}$ and $\hat{\phi}_q^{(\mathrm{AP1})}$ are the phase measurements of the first and second antenna ports, respectively. The cycle slip is detected by comparing the q-th phase measurement with the first measurement of the given arc ($q = 0$) to a cycle slip threshold α_{cs} as

$$\left|\Delta\hat{\phi}_q^{(\mathrm{AP0,AP1})} - \Delta\hat{\phi}_0^{(\mathrm{AP0,AP1})}\right| \geq \alpha_{\mathrm{cs}} \text{ [rad]}. \tag{45}$$

Above the threshold α_{cs}, a cycle slip is detected and a new phase measurement arc is started. The cycle slip threshold is set to one-half of the PLL discriminator range in the receiver, resulting in $\alpha_{\mathrm{cs}} = \pi$ [rad].

V. Monitoring of LTE Signals

The real-time operation of STARE is demonstrated by monitoring LTE downlink signals for an uninterrupted period of one week. A static monitoring setup running STARE is deployed in the European Space Research and Technology Centre (ESTEC) navigation laboratory of the European Space Agency (ESA) in Noordwijk, the Netherlands. The block diagram of the setup is shown in Fig. 4. The setup includes a single conventional Eightwood LTE magnetic mount antenna with vertical polarization and 3 dBi peak gain, Ettus Universal Software Radio Peripheral (USRP) N310 SDR driven by a high-precision Rubidium reference clock, and a processing unit running Intel Core i9 with 32 threads and 64 GB of memory. The antenna is mounted indoors on the metal window sill of the laboratory. The SDR is connected to the processing unit via the 10 Gigabit copper Ethernet connection, providing a reliable interface to stream the sampled signal.

A commercially operated LTE base station, located in the vicinity of the navigation laboratory and referred to as the eNodeB, is selected for monitoring. Approximate locations of the laboratory and the eNodeB are shown in Fig. 5. There is no line-of-sight between the laboratory and eNodeB

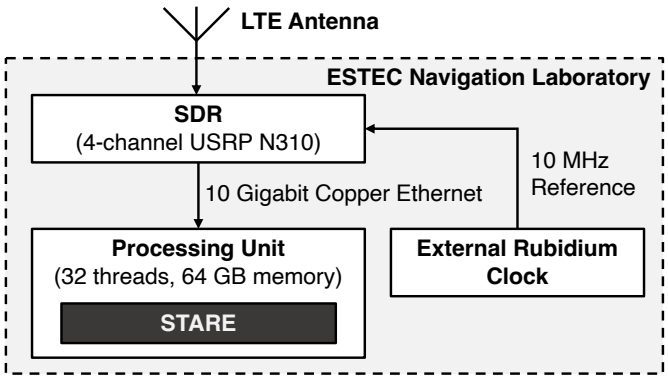

Fig. 4. Block diagram of the LTE signal monitoring setup.

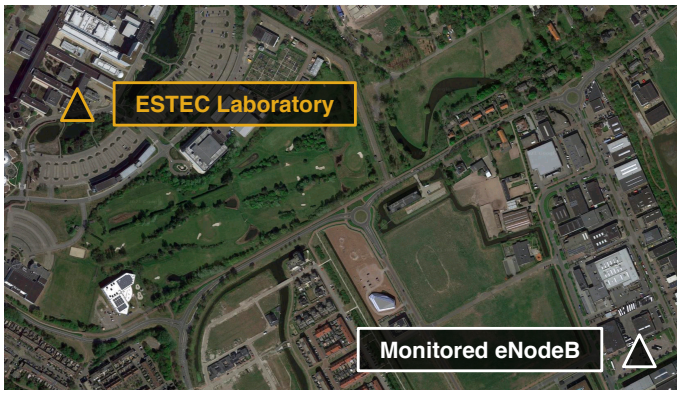

Fig. 5. Approximate locations of the ESTEC navigation laboratory and the monitored eNodeB in its vicinity. The location of the eNodeB is based on the public Dutch antenna register as of August 2021 [25].

antennas. The eNodeB transmits a 10 MHz downlink signal at a 796 MHz carrier frequency. The strongest cell is identified by cell ID 117 and utilizes normal CP mode and two antenna ports (AP0 and AP1) for transmission.

A. Receiver Configuration

STARE is configured to utilize a single radio channel fed by the antenna. The sampling rate of the baseband stream is set to 15.36 Msps. The radio channel is connected to two tracking channels, each configured to track the CRS of one of the two antenna ports of the cell. The algorithm parameters are common for both tracking channels. The configuration of STARE is summarized in Table II. The loop integration time is set to $T_\eta = 0.5$ ms for both DLL and PLL as the CRS pilots in the first symbol of every LTE slot are tracked. The loop bandwidth of the second-order DLL is set to $B_{\mathrm{n}} = 0.5$ Hz and the loop bandwidth of the third-order PLL is set to $B_{\mathrm{n}} = 18$ Hz, providing sufficient responsiveness to track the eNodeB clock dynamics. The tracking thresholds of the DLL and PLL are set to 0.39 sample and $\frac{\pi}{2}$ rad, respectively. The DLL tracking threshold is based on the values from Table I. If the estimated 3-sigma of the delay or phase tracking errors exceeds the given thresholds, the lock of the signal is considered lost and the impacted tracking

TABLE II
CONFIGURATION OF STARE FOR LTE SIGNAL MONITORING

Radio channel ID	**0**	
Carrier frequency f_c [MHz]	796	
Signal bandwidth B [MHz]	10	
FFT length N_{fft}	1024	
Sampling rate f_{s} [Msps]	15.36	
Tracking channel ID	**0**	**1**
Cell ID	117	117
CP mode	Normal	Normal
Antenna port (AP)	0	1
Algorithm configuration (common for both tracking channels)		
DLL / PLL integration time T_η [ms]	0.5^{a} / 0.5^{a}	
DLL / PLL order	2 / 3	
DLL / PLL bandwidth B_{n} [Hz]	0.5 / 18	
DLL filter damping factor ζ	$\frac{1}{\sqrt{2}}$	
PLL filter coefficients a / b	1.1 / 2.4	
DLL EMLP correlator half-spacing δ	0.1	
DLL / PLL tracking threshold	0.39 sample / $\frac{\pi}{2}$ rad	
SNR tracking threshold [dB]	-20	
SNR averaging window length Q	100	
Demodulation CP discard $N_{\text{d}}(i)$	$\lfloor 0.9 \cdot N_{\text{cp}}(i) \rfloor$	
ESPRIT design parameter m	0.48	
ESPRIT path selection threshold γ [dB]	-3	

[a] The CRS pilots in the first symbol of every LTE slot are tracked

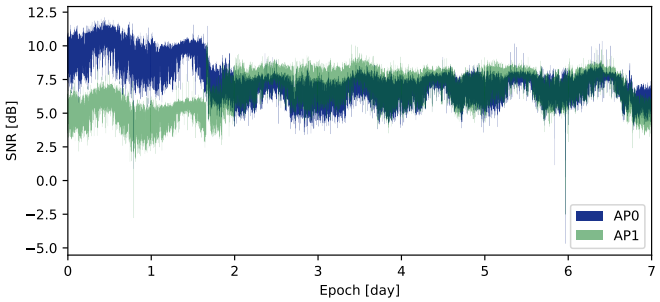

Fig. 6. SNR measurements observed on the two antenna ports of the monitored eNodeB.

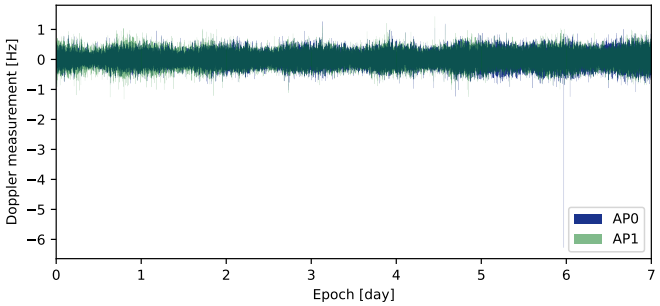

Fig. 7. Doppler measurements observed on the two antenna ports of the monitored eNodeB.

channel repeats the acquisition. Alternatively, the lock is lost when the SNR of the tracked signal drops below -20 dB for 100 consecutive LTE radio frames. During demodulation, 90 % of the CP is discarded before the FFT operation. The ESPRIT design parameter is set to $m = 0.48$ resulting in $M = \lfloor 200 \cdot 0.48 \rfloor = 96$ eigenvalues, providing a sufficient multipath resolution for the signal acquisition. The ESPRIT path selection threshold is determined to be $\gamma = -3$ dB. Although this threshold may also potentially discard a very weak LOS component, signals with such low SNRs are not considered relevant for monitoring.

B. SNR and Delay Errors

The two antenna ports of cell ID 117 are monitored continuously for one week starting on Wednesday, August 25, 2020, 17:40. The delay, phase, Doppler, and SNR measurements are collected for both antenna ports and stored on a dedicated drive. The SNR measurements are shown in Fig. 6. It can be seen that both antenna ports experience similar SNR levels, except for a higher SNR on AP0 during the first two days. The mean SNRs are estimated as $\mu_{\text{SNR}}^{(\text{AP0})} = 7.39$ dB and $\mu_{\text{SNR}}^{(\text{AP1})} = 6.48$ dB. The SNRs seem to follow a daily trend on both antenna ports, which could be caused by the power management of the eNodeB.

The collected Doppler, phase, and delay measurements are shown in Figs. 7, 8, and 9, respectively. Fig. 7 shows that the measured Doppler remains stable on both antenna ports with a zero mean and a standard deviation of $\sigma_v \approx 0.23$ Hz. This is attributed to the Rubidium clock standard used in the monitoring setup and sufficient stability of the clock of the monitored eNodeB. Stable clocks can also be observed from the phase and delay measurements shown in Figs. 8 and 9, respectively, as no significant drift is present.

The delay errors are estimated by applying the CMC technique from Section IV. The measurements of the first and the last 10 s of each arc are skipped to consider only the steady-state of the tracking loops. The probability of cycle slip is 2.92×10^{-6} s^{-1}. The delay errors observed on the two antenna ports are shown in Fig. 10. The standard deviations of the delay errors on the two antenna ports are $\sigma_{\varepsilon^{(\tau)}}^{(\text{AP0})} = 0.435$ m and $\sigma_{\varepsilon^{(\tau)}}^{(\text{AP1})} = 0.492$ m. This can be considered a good tracking performance achieved by the given base station and STARE. These results are not representative of other base stations.

a

VI. CONCLUSIONS

STARE, a real-time software receiver for positioning with LTE and 5G NR cellular downlink signals, was presented. The real-time operation was demonstrated by monitoring downlink signals of a commercially operated LTE base station for an uninterrupted period of one week. The observed delay errors achieve a sub-meter standard deviation. Besides monitoring, STARE may find its use in real-time navigation kernels or as a real-time source of measurement corrections for relative positioning techniques.

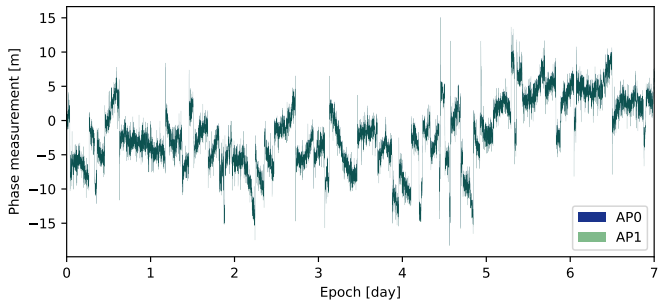

Fig. 8. Phase measurements observed on the two antenna ports of the monitored eNodeB.

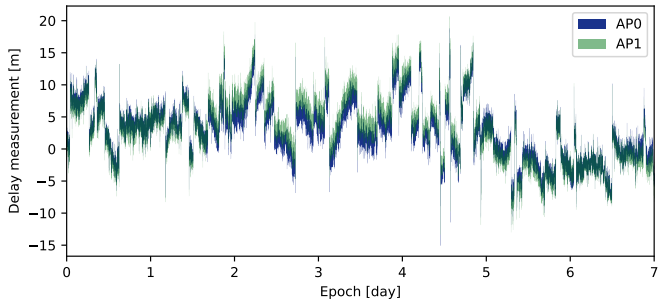

Fig. 9. Delay measurements observed on the two antenna ports of the monitored eNodeB. The first measurement is aligned to the zero y-axis.

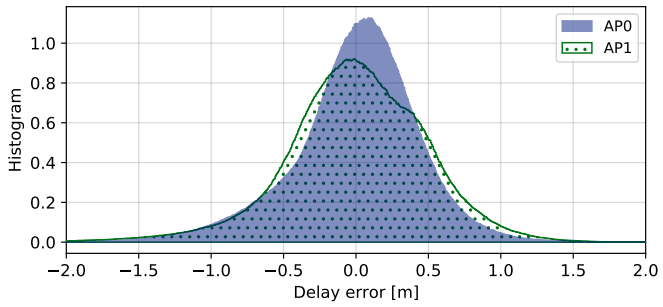

Fig. 10. Histograms of the delay errors observed on the two antenna ports of the monitored eNodeB estimated using the CMC technique.

Software Availability

The source code of STARE is available from the European Space Software Repository (ESSR) under the terms of European Space Agency Software Community License Permissive (Type 3) – v2.4 at https://essr.esa.int/project/stare.

Acknowledgment

This work was supported in part by the European Space Agency through the Networking Partnering Initiative (NPI) Program under Grant 4000123584/18/NL/MH, in part by the Secretariat of Universities and Research of the Enterprise and Knowledge Department of Generalitat of Catalonia through Beatriu de Pinós under Grant 2018 BP 0266, and in part by the H2020 Marie Skłodowska-Curie Co-funding of regional, national and international programmes (COFUND) under Contract 801370.

References

[1] 3rd Generation Partnership Project, "3GPP TR 38.855: Study on NR positioning support," Technical Report V16.0.0, Mar. 2019.

[2] C. Mensing, S. Sand, and A. Dammann, "Hybrid Data Fusion and Tracking for Positioning with GNSS and 3GPP-LTE," *International Journal of Navigation and Observation*, vol. 2010, 06 2010.

[3] G. De Angelis, G. Baruffa, and S. Cacopardi, "GNSS/Cellular Hybrid Positioning System for Mobile Users in Urban Scenarios," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 313–321, 2013.

[4] J. A. Del Peral-Rosado, R. E. I Castillo, J. A. López-Salcedo, G. Seco-Granados, Z. Chaloupka, L. Ries, and J. A. Garcıa-Molina, "Evaluation of Hybrid Positioning Scenarios for Autonomous Vehicle Applications," in *Proc. ION GNSS+ 2017*, Portland, Oregon, USA, Sep. 2017, pp. 2541–2553.

[5] K. Shamaei and Z. M. Kassas, "Sub-Meter Accurate UAV Navigation and Cycle Slip Detection with LTE Carrier Phase Measurements," in *Proc. ION GNSS+ 2019*, Miami, Florida, USA, Sep. 2019, pp. 2469–2479.

[6] E. Kaplan and C. Hegarty, *Understanding GPS/GNSS: Principles and Applications, Third Edition*. Artech House, 2017.

[7] J. A. Del Peral-Rosado, J. A. López-Salcedo, G. Seco-Granados, F. Zanier, P. Crosta, R. Ioannides, and M. Crisci, "Software-Defined Radio LTE Positioning Receiver Towards Future Hybrid Localization Systems," Florence, Italy, pp. 1–11, Oct 2013.

[8] J. A. D. Peral-Rosado, J. M. Parro-Jiménez, J. A. López-Salcedo, G. Seco-Granados, P. Crosta, F. Zanier, and M. Crisci, "Comparative results analysis on positioning with real LTE signals and low-cost hardware platforms," 2014.

[9] K. Shamaei, J. Khalife, and Z. M. Kassas, "Performance Characterization of Positioning in LTE System," in *Proc. ION GNSS+ 2016*, Portland, Oregon, USA, Sep. 2016, pp. 2262–2270.

[10] K. Shamaei and Z. M. Kassas, "LTE receiver design and multipath analysis for navigation in urban environments," *Navigation*, vol. 65, no. 4, pp. 655–675, 2018.

[11] ——, "Receiver Design and Time of Arrival Estimation for Opportunistic Localization With 5G Signals," *IEEE Transactions on Wireless Communications*, vol. 20, no. 7, pp. 4716–4731, 2021.

[12] 3rd Generation Partnership Project, "3GPP TS 36.211: Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation," Technical Specification V16.7.0, Sep. 2021.

[13] ——, "3GPP TS 38.211: NR; Physical channels and modulation," Technical Specification V16.7.0, Sep. 2021.

[14] W. Xu, M. Huang, C. Zhu, and A. Dammann, "Maximum likelihood TOA and OTDOA estimation with first arriving path detection for 3GPP LTE system," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 3, pp. 339–356, 2014.

[15] K. Shamaei, J. Khalife, and Z. M. Kassas, "Comparative Results for Positioning with Secondary Synchronization Signal versus Cell Specific Reference Signal in LTE Systems," in *Proc. ION ITM 2017*, Monterey, California, USA, Jan. 2017, pp. 1256–1268.

[16] 3rd Generation Partnership Project, "3GPP TS 36.104: Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception," Technical Specification V17.0.0, Dec. 2020.

[17] The SoapySDR Project. [Online]. Available: https://github.com/pothosware/SoapySDR/wiki

[18] I. Lapin, G. Seco-Granados, O. Renaudin, F. Zanier, and L. Ries, "Joint Delay and Phase Discriminator Based on ESPRIT for 5G NR Positioning," *IEEE Access*, pp. 1–1, 2021.

[19] J. van de Beek, M. Sandell, and P. Borjesson, "ML estimation of time and frequency offset in OFDM systems," *IEEE Transactions on Signal Processing*, vol. 45, no. 7, pp. 1800–1805, 1997.

[20] M. Wax and T. Kailath, "Detection of signals by information theoretic criteria," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 33, no. 2, pp. 387–392, 1985.

[21] M. Driusso, C. Marshall, M. Sabathy, F. Knutti, H. Mathis, and F. Babich, "Vehicular Position Tracking Using LTE Signals," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3376–3391, 2017.

[22] P. Wang and Y. Morton, "Performance comparison of time-of-arrival estimation techniques for LTE signals in realistic multipath propagation channels," *Navigation*, vol. 67, no. 4, pp. 691–712, 2020.
[23] Baoguo Yang, K. B. Letaief, R. S. Cheng, and Zhigang Cao, "Timing recovery for OFDM transmission," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 11, pp. 2278–2291, 2000.
[24] L. Chen, P. Thevenon, G. Seco-Granados, O. Julien, and H. Kuusniemi, "Analysis on the TOA Tracking With DVB-T Signals for Positioning," *IEEE Transactions on Broadcasting*, vol. 62, no. 4, pp. 957–961, 2016.
[25] Antennebureau. Dutch antenna register (Antenneregister). [Online]. Available: https://antenneregister.nl