LTE Transmitter Location and Clock State Estimation: Simulated and Real Measurements Using the SSS and CRS Signals

Markel Arizabaleta-Diez, Muhammad Subhan Hameed, Thomas Pany

Universität der Bundeswehr München - Institute of Space Technology and Space Applications

BIOGRAPHY

Markel Arizabaleta-Diez studied his Master's degree in Telecommunication Engineering at Universidad del País Vasco (UPV-EHU) in Bilbao, Spain. He is currently a research associate at the Universität der Bundeswehr München at the Institute of Space Technology and Space Applications (ISTA). His research topics are GNSS receiver signal processing and authentication, and positioning with LTE signals.

Muhammad S. Hameed received a bachelor in Electrical Engineering in 2016 from the National University of Sciences and Technology (NUST), Pakistan and a master in Earth Oriented Space Science and Technology (ESPACE) in 2020 from the Technical University of Munich (TUM), Germany. He has been working as a research associate at the Institute of Space Technology and Space Applications of the Universität der Bundeswehr München. His current research interests include GNSS receiver technology, signal generation, tracking performance analysis and positioning using LTE signals.

Prof. Thomas Pany is with the Universität der Bundeswehr München at Space Systems Research Center (FZ-Space) where he leads the satellite navigation unit LRT 9.2 of the Institute of Space Technology and Space Applications (ISTA). He teaches navigation focusing on GNSS, sensors fusion and aerospace applications. Within LRT 9.2 a good dozen of full-time researchers investigate GNSS system and signal design, GNSS transceivers and high-integrity multi-sensor navigation (inertial, LiDAR) and is also developing a modular UAV-based GNSS test bed. ISTA also develops the MuSNAT GNSS software receiver and recently focuses on smartphone positioning and GNSS/5G integration. He has a PhD from the Graz University of Technology (sub auspiciis) and worked in the GNSS industry for seven years. He authored around 200 publications including one monography and received five best presentation awards from the US Institute of Navigation. Thomas Pany also organizes the Munich Satellite Navigation Summit.

ABSTRACT

The use of Long Term Evolution (LTE) communication signals has been extensively studied in literature as a complementary positioning system for GNSS in GNSS denied scenarios, such as urban canyons or indoor environments. However, in order to achieve accurate positioning with LTE signals, the transmitter location and clock state information is required, which is not provided by the system. This paper presents the estimation of the LTE transmitter position and clock states by using the LTE Secondary Synchronization Signals (SSS) and Cell-specific Reference Signal (CRS). Herewith, an analysis of the LTE SSS and CRS signals is done at a theoretical level to identify performance limitations when employed as 10 ms-long local replica in a GNSS-like processing and a comparison of transmitter localization results, obtained using these signals, is presented. Receiver optimizations for LTE signal compatibility are discussed within the context of extending the Multi-Sensor Analysis Tool (MuSNAT) software receiver for LTE SSS and CRS acquistion and tracking. The complete processing chain, which is based on MuSNAT and a MATLAB based LTE transmitter localization filter, has been validated based on simulation and is then employed for two commercial base stations and a research purposed Amarisoft LTE/5G base station.

I. INTRODUCTION

The use of only GNSS signals for navigation is prone to outages in challenging environments such as urban canyons or with dense foliage. In such environments, the GNSS signals suffer strong multipath, frequent non-line-of-sight (NLOS) instances, and other signal quality degrading effects. In such scenarios, for reliable and continuous positioning, mobile communication signals such as LTE or 5G are proposed as complementary systems to GNSS (Del Peral-Rosado et al., 2016; Knutti et al., 2015; Yang et al., 2022). However, as per design, the LTE system does not provide the base station (BS) location and clock information. Currently there are some crowd-based databases in which approximate locations of LTE BSs are provided, however, instead of the BS coordinates, they provide the address of the building in which the BS is located. By using the address instead the exact coordinates of the BS, a relevant error is obtained in the BS location, which directly impacts to the computation of the user position.

As an alternative, the LTE BS localization can be performed by using different signals, i.e., by means of the LTE synchronization or reference signals. In this context, previous work in literature (Shamaei et al., 2017) has presented preliminary results based on Secondary Synchronization Signal (SSS) and Cell-specific Reference Signal (CRS) signals and the comparison between them. However, instead of using a symbol-wise processing, the proposed architecture is based on a GNSS-like signal processing using 10 ms-long time-domain representation of the LTE signals as local replicas. The considered approach allows the possibility of extending GNSS receivers to be compatible with LTE signals keeping to a minimum the required modifications. With a receiver compatible with acquiring and tracking LTE SSS and CRS signals, a transmitter localization scheme can be employed based on receiver observations. Previous work by (Hameed et al., 2022) presented the preliminary results achieved in a 2D BS location and clock state estimation using the SSS signals only. This work first presents a theoretical analysis of the 10 ms-long time-domain representation of the SSS and CRS signals, then outlines the required receiver optimizations done for LTE signal compatibility and then provides the localization results for simulated and real test cases.

To perform the experiments a Universal Radio Peripheral (USRP) has been employed to record the GNSS and the LTE signals simultaneously. Then by using the Multi-Sensor Analysis Tool (MuSNAT) software receiver, which has been extended to perform LTE acquisition and tracking (Arizabaleta et al., 2021), the user dual-frequency position is computed by means of the L1 and L5 band GNSS signals, and the LTE pseudorange observations are produced. By using the user position retrieved from the processing of the GNSS signals, and by using a Kalman Filter (KF)-based transmitter location filter implemented in MATLAB, the inverse positioning is applied to estimate the BS location and the clock states.

The localization filter is firstly validated based on a simulated dataset. After the validation of the complete processing chain, the filter is applied on experimental datasets involving two commercial LTE BSs, located in an urban and suburban environment, and a research oriented Amarisoft BS (Amarisoft, 2021).

The work is presented in the following sections: Section II provides an overview of the LTE SSS and CRS signals, and analyse theoretical characteristics of the signals such as the cross- and auto-correlation functions (ACF), and the S-curve. The identified drawbacks for each signals are compensated within the MuSNAT software receiver by the optimizations indicated in Section III. Section IV introduces the transmitter location filter employed for the LTE transmitter location and clock estimation. Section V starts with the experimental set-up and then shows the results obtained based on simulations and experimental recordings. Finally, the conclusions of the work are presented in Section VI, where the future work is also discussed.

II. LTE SIGNAL STRUCTURE AND CHARACTERISTICS

The LTE signal is defined in the time domain in frames of 10 ms of duration. Each frame is subdivided into 10 sub-frames of 1 ms-long duration. Each sub-frame is further divided into two slots, with a duration of 0.5 ms per slot, and each slot contains 7 or 6 OFDM symbols based on the use of normal or extended cyclic prefix (CP), respectively. The current work focuses on LTE signals with normal CP, therefore each one of the OFDM symbols span a duration of 66.6 μs. Figure 1 provides an overview of the time domain structure of the LTE signal.

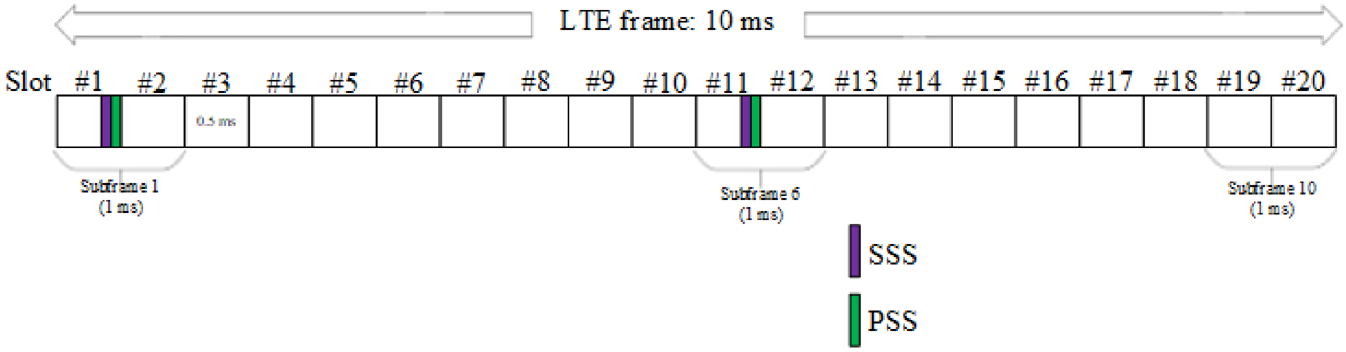


Figure 1: Frame structure and LTE PSS and SSS symbol location in the LTE FDD mode

In the frequency domain, the LTE signal is defined in terms of resource blocks (RB). Each RB is composed of 12 sub-carriers and 7 OFDM symbols considering normal CP. A resource element (RE), however, is presented as an OFDM symbol corresponding to a given sub-carrier. Figure 2 shows in an orange rectangle the representation of a RB, and with a grey square the representation of a RE. It also provides an overview of the allocation of the RE of the different CRS signals for different Antenna Ports (AP), which will be covered later in Section II.2.

LTE provides high flexibility allowing different downlink physical layer configurations. Table 1 provides an overview of the

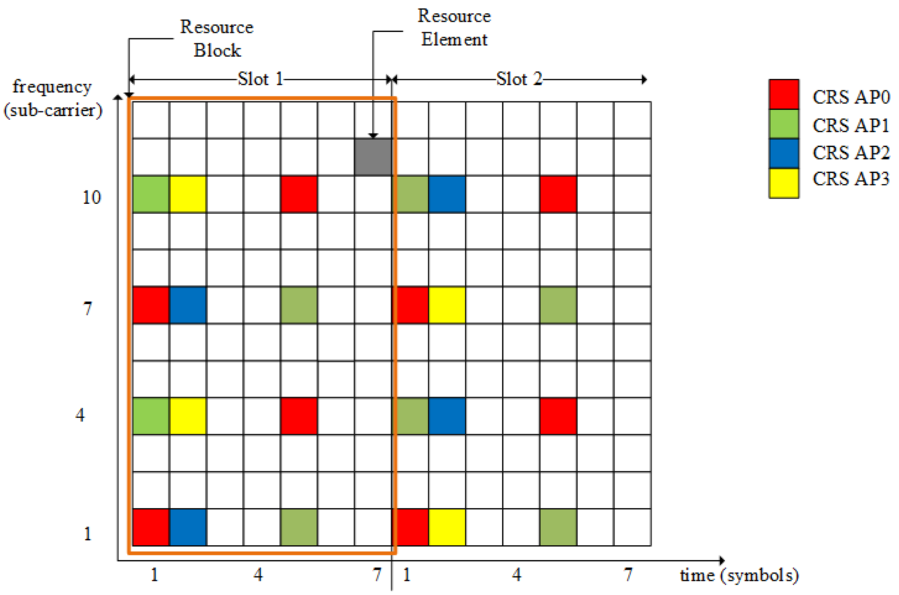


Figure 2: Graphic definition of a LTE RB and a RE and allocation of the CRS REs

downlink physical layer characteristics for the different available configurations based on the available transmission (channel) bandwidths (Innovations, 2010). The sampling frequency represents the frequency at which the user device needs to sample the incoming signal for the different configurations, and the FFT size provides the number of FFT sample points employed for each time symbol. These last two parameters are considered for generating the local replica for the SSS and CRS signals.

Table 1: LTE downlink parameters

Channel BW [MHz]	1.25	2.5	5	10	15	20
Sampling frequency [MHz]	1.92	3.84	7.68	15.36	23.04	30.72
FFT size	128	256	512	1024	1536	2048
N° RB	6	12	25	50	75	100
N° samples CP [samples] (1st symbol 5.2 μ s / 2nd to 7th symbol 4.69 μ s)	10 9	20 18	40 36	80 72	120 108	160 144
symbol duration (no CP)	66.67 μs					

The work presented here focuses mainly in the 10 MHz channel BW configuration due to the frequent transmission of this configuration around the UniBw M premises. It must be also taken into consideration that the parameters provided in Table 1 apply to normal CP, a sub-carrier spacing of 15 kHz, and frequency division duplex (FDD) transmission mode. The use of FDD means that different carrier frequencies are employed for the uplink and the downlink signals.

In contrast to the work presented in literature, where the processing of the LTE signals is done based on symbol-wise processing, the current work is based on using a 10 ms-long (i.e. 1 frame-long) time domain representation of the LTE SSS or CRS signals as local replicas. The local replicas are then used in a GNSS-like signal processing architecture to obtain the code and carrier based observations.

In the following subsections, the characteristics of the SSS and the CRS signals are presented in context of the generation of their local replicas and additional processing features such as the correlation metrics in time- and frequency-domain, as well as the S-curve. A point to be considered is that the local replicas are generated in the time-domain and span one complete frame (10 ms), and therefore, the parameters of Table 1 are invoked. The frequency domain generation of each symbol and the sub-carrier allocations of the SSS and CRS signals have been performed based on the 3GPP standard (3GPP, 2017).

1. SSS sequences

The Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS) sequences are synchronization signals transmitted every 5 ms, i.e., each one of the signals is transmitted twice per frame. The PSS helps to achieve subframe, slot, and symbol synchronization in the time domain. However, as the same sequence is transmitted every 5 ms, it does not allow to perform frame synchronization. For the frame synchronization, the SSS is employed, which consists of a different sequence for each occupied symbol within the frame. For a given sequence, each of the signals is identified by a different number, i.e., the PSS sequence is identified by three possible sequences, $\{0{,}2\}$, while the SSS sequence is identified between by one of 168 possible sequences, $\{0{,}167\}$. The combination of the sequence identifiers provides the Physical Cell Identification number (PCI = 3 SSS_{id}+PSS_{id}, where PSS_{id} and SSS_{id} is the PSS and SSS identification numbers, respectively).

The PSS and the SSS are transmitted in the center 62 sub-carriers of the transmitted LTE signal bandwidth, independently of the employed downlink physical layer configuration (see Table 1). However, due to the repeating of the PSS sequence every 5 ms, high secondary peaks can be found in the auto- and cross-correlation of the 10 ms-long PSS-SSS combined sequences (Hameed et al., 2022). Therefore, the PSS sequence is completely omitted to yield a 10 ms-long replica that shall contain only the SSS sequence (or the CRS sequence as it will be observed in Section II.2). Considering that the generation of the SSS sequence is impacted by PSS_{id}, a total of 504 different 10 ms-long SSS sequences can be generated, i.e., one 10 ms-long SSS-only sequence is obtained per PCI (Hameed et al., 2022).

As the SSS sequence is transmitted in the center 62 sub-carriers (independently of the transmitted signal bandwidth), to generate the 10 ms-long time domain representation of the SSS sequence, the lowest transmission bandwidth has been used, and therefore, the relevant parameters have been retrieved from the first column of Table 1, i.e., from the column corresponding to the 1.25 MHz of channel bandwidth. This means, that the complete replica has been generated at a rate of 1.92 MHz. Knowing the two locations of the symbols in which the SSS is transmitted and the sampling rate, the sample indexes in which both SSS sequences need to be located can be known. In these sample indexes, the time-domain representation of SSS sequences is inserted. To generate the time domain representation, the SSS frequency-domain sequences are generated and mapped based on the indications provided in the 3GPP standard (3GPP, 2017), and by then applying an Inverse Fast Fourier Transform (IFFT) of 128 points (size indicated in Table 1), the time-domain representation of each SSS sequence symbol is obtained. The samples not belonging to the SSS sequence within the 10 ms-long LTE replica, are set to 0, including the samples corresponding to all CPs. The time domain representation of the SSS sequence is provided in Figure 3.

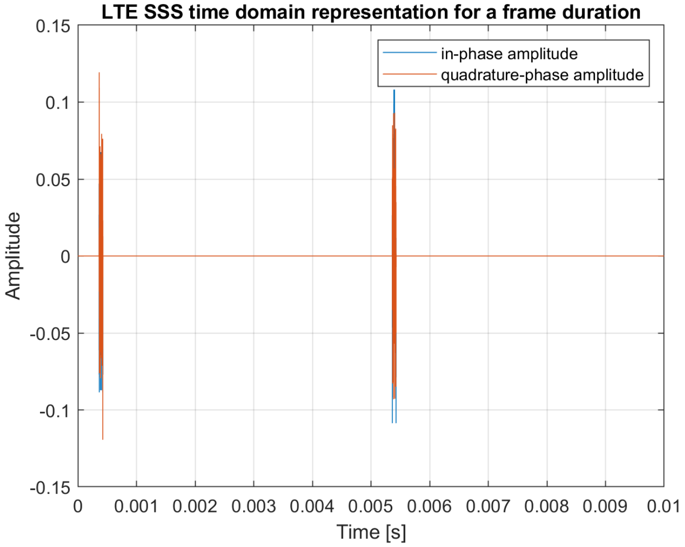
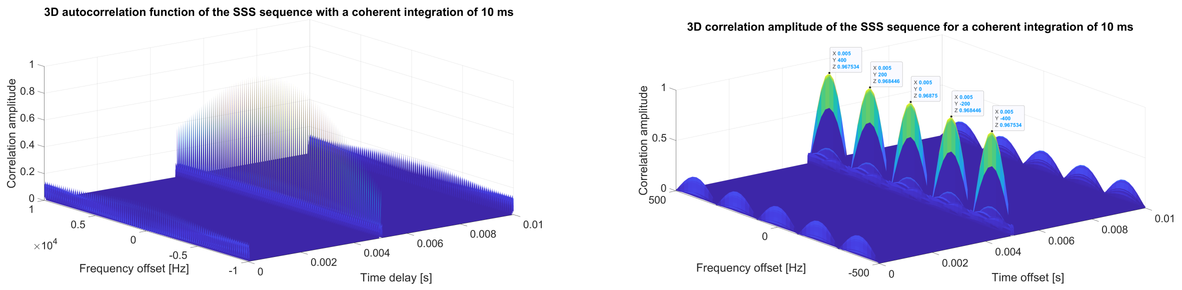


Figure 3: Time domain representation of the 10 ms-long LTE SSS replica

Once the local replica is generated, a 10 ms-long (i.e. 1 frame) LTE signal with 6 RB is simulated using the LTE waveform generator of MATLAB (Matlab, 2019). Using the simulated LTE signal and the generated local replica, the ACF has been applied at different delays and different Doppler offsets providing the 3D ACF plot as shown in Figure 4. As observed, a single main peak is detected in the time domain, however, a large number of secondary peaks are observed in the frequency domain of the ACF. Figure 4(b) is a zoomed version of the 3D ACF of the SSS signal, where it can be observed that a secondary peak is present in the frequency domain every 200 Hz. The main reason of these secondary peaks is the distance between consecutive symbols within the transmitted SSS sequence. This means that as the SSS is transmitted every 5 ms, a secondary peak is obtained every 1/5ms=200 Hz. The secondary peaks are present every 200 Hz within a frequency range of ±15 kHz, i.e., within a frequency range equivalent to the sub-carrier spacing.

The effects of the secondary peaks in the LTE ACF can be described by



(a) **(b)**

Figure 4: 3D correlation of the SSS signal. (a) Doppler range between ± 10 kHz, (b) Doppler range between ± 500 Hz

$$F(f) = sinc((f - \frac{n}{\Delta t_{symb}})T_{coh}) \times sinc(f \times \Delta f) \tag{1}$$

where Δt_{symb} is the time between occupied consecutive symbols in a sub-carrier, i.e. 5 ms for the SSS sequence. T_{coh} is the coherent time employed for the correlation function, 10 ms in this case, and its inverse, 100 Hz, provides the width of the $sinc$ lobes. Δf is the sub-carrier spacing, and finally, $n \in \mathbb{Z}$.

As we are working with a 10 ms-long time-domain representation of the SSS sequence, and performing a GNSS-like signal processing for computing the range observations, the S-curve needs to be taken into consideration for the 10 ms-long sequence. This has been computed using the Yet Another Signal Simulation Tool (YASST), which besides simulating signals, provides some theoretical characteristics of the generated signals. This tool has been employed to compute the S-curve of the LTE signal based on the characteristics of the employed configuration of the MuSNAT software receiver. The S-curve of the SSS sequence is provided in Figure 5. It must be noted that the S-curve is a characteristic of the code tracking loop, which is directly related to the early-late discriminator output and the shift of the local replica. In order to fix the early-late output within the linear range shown in Figure 5, an early-late spacing of 0.52 μs has been selected.

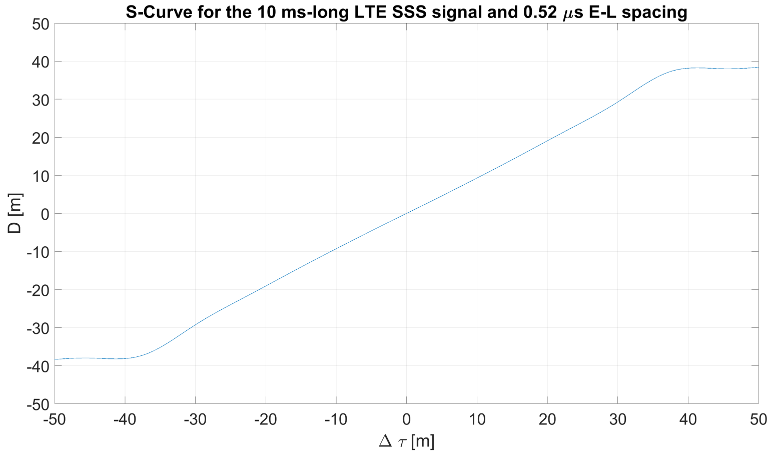


Figure 5: S-curve of the SSS sequence

2. CRS sequence

The Cell-specific Reference Signal (CRS) can be used for cell search and initial acquisition (usually this task is carried by the PSS and SSS sequences), downlink channel quality measurements and channel estimation. Based on the LTE 3GPP standard (3GPP, 2017), there are up to 4 different CRS signals per PCI, and they are differentiated based on the Antenna Port (AP) concept with indexes ranging from 0 to 3. The transmission of these signals is dependent on the service provider, however, a minimum of 1 CRS signal needs to be transmitted. The location of the REs of the LTE CRS signals depend on the AP index they are associated with, i.e., for CRS AP0 and CRS AP1, the REs are located in the symbols 1 and 5 of every slot, while for CRS

AP2 and CRS AP3, the REs are located only in the 2nd symbol of every slot. The frequency allocation of the CRS signals also differ based on the associated AP. In a single symbol, the REs of a given CRS AP signal are transmitted every 6 sub-carriers:

- For the CRS AP0, the sub-carriers 1 and 7 of each RB is employed for the REs transmitted in symbol 1, and sub-carriers 4 and 10 for the REs in symbol 5.
- For the CRS AP1, the sub-carriers 4 and 10 are employed in each RB for REs transmitted in symbol 1, and sub-carriers 1 an 7 for the REs in symbol 5.
- For the CRS AP2, the sub-carriers 1 and 7 of each RB is employed for the REs transmitted in symbol 2.
- For the CRS AP3, the sub-carriers 4 and 10 are employed in each RB for REs transmitted in symbol 2.

A better overview of the CRS signal allocation per RB for each AP is provided in Figure 2. Based on the signals observed in the surroundings of the UniBw M premises, the CRS for the AP0 is always transmitted, while the others (CRS AP1, CRS AP2, and CRS AP3) have been occasionally identified (Yang et al., 2020). Another consideration of the CRS signals is that they are transmitted over the whole LTE signal bandwidth, and as the observed signals around the university premises are most frequent in the frequency band of 796 MHz with a signal bandwidth of 10 MHz, the main focus of this section are LTE CRS signals for AP0 and 50 RBs, which correspond to signals with a bandwidth of 10 MHz (see Table 1).

The generation of the 10 ms-long local replica of the CRS AP0, has been done in the similar way to the one of the SSS presented in Section II.1. The main difference are the symbols and sub-carriers in which the REs of the CRS AP0 signal are transmitted. Based on the CRS AP0 structure, more frequent occupied symbols are observed, as shown in Figure 6. Similar to the case of the 10 ms-long time-domain representation of the SSS signal, the samples of all REs that do not correspond to the CRS AP0 and all samples corresponding to the CP are set to 0. The sampling rate employed for the CRS AP0 and 50 RBs is 15.36 MHz following the indications of Table 1.

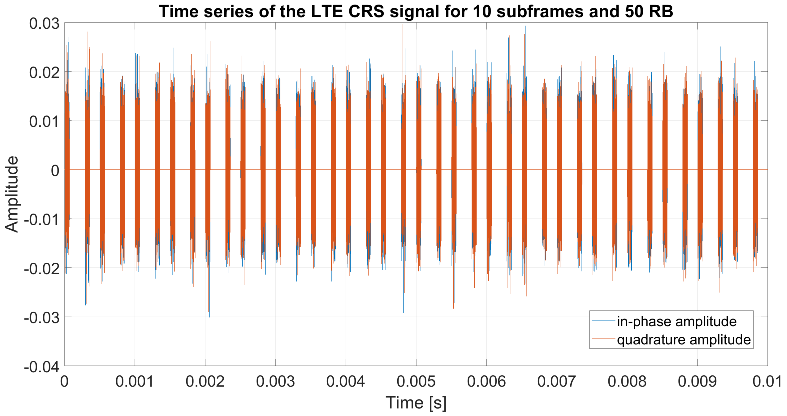
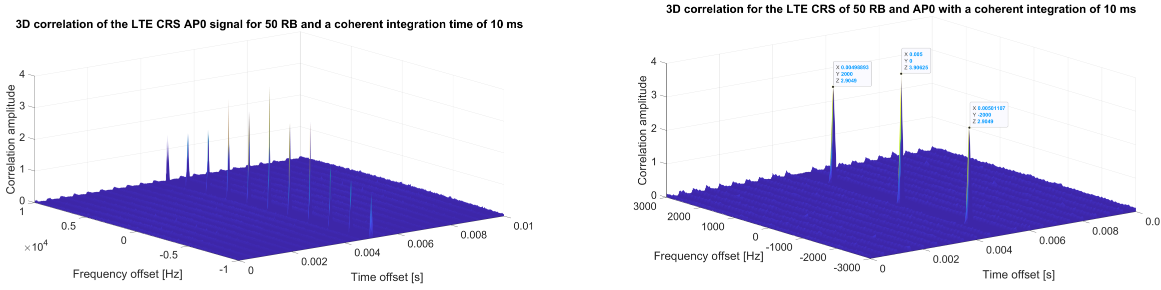


Figure 6: Time domain representation of the LTE CRS for AP0 and 50 RBs

Once the local replica is generated, the correlation properties of the CRS signal are anlayzed using a MATLAB based simulated signal. The MATLAB LTE Waveform Generator Toolbox (Matlab, 2019) is employed to generate a 10 ms-long LTE signal with 50 RB for a certain PCI. Then, the correlation between the simulated signal and the 10 ms-long time-domain representation of the CRS is done for different delays of the local replica and Doppler offsets providing the results as shown in Figure 7. As in the case of the SSS 3D correlation case (see Figure 4), it is observed that there are several secondary peaks in the frequency domain, and it can be mathematically represented as indicated in (1). The difference is that in the case of CRS, the time delay between two occupied symbols for a specific sub-carrier, Δt_{symb}, is 0.5 ms instead of 5 ms for the SSS signal. This reduction in Δt_{symb} by a factor of 10 directly affects to the distance between secondary peaks in the frequency domain, i.e., the secondary peaks in the frequency domain are 2 kHz apart (see right figure in Figure 7). This means that the risk of locking onto a secondary frequency peak during acquisition and tracking of the 10 ms-long local replica is reduced when employing the CRS signal.

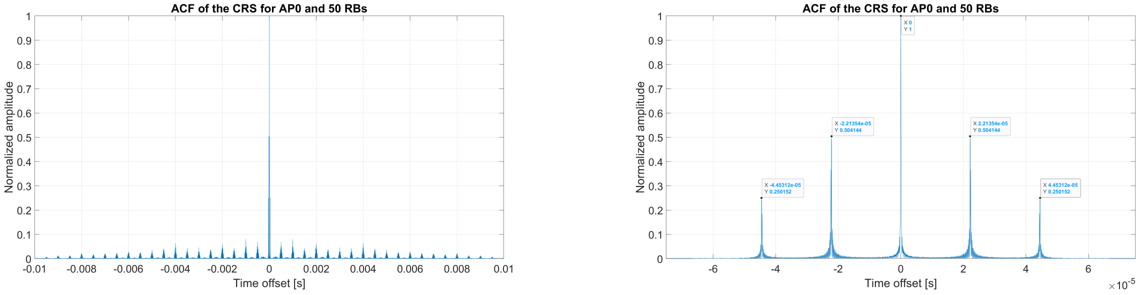
The ACF of the time domain representation of the CRS signal for AP0 and 50 RBs also indicate the presence of secondary peaks in the time domain. Figure 8 shows the time domain representation of the ACF of the CRS local replica. Figure 8(a) shows the complete ACF while Figure 8(b) shows a zoomed version of the ACF, where the distance of the secondary peaks are better observed. The secondary peaks in time-domain are far away from each other, i.e, the secondary peaks are 22.1354 μs apart (it is reminded that the local replica is generated at a sampling rate of 15.36 MHz as per Table 1, and therefore, a spacing of 340 samples between consecutive peaks is obtained). Therefore, the secondary peaks in time-domain can be detected by using the already known Bump Jump technique (see Section III.3).



(a)

(b)

Figure 7: 3D correlation of the SSS signal. (a) Doppler range between ± 10 kHz, (b) Doppler range between ± 3 kHz



(a)

(b)

Figure 8: Time domain ACF for the LTE CRS signal for AP0 and 50 RBs

Finally, by using the YASST tool, as it was done for the SSS signal, the S-curve has been generated, and represented in Figure 9. To analyse the curve, a E-L spacing of 50 ns has been set, which correspond to 14.99 m between the early and late correlators.

3. SSS vs. CRS: summary

This section aims to provide a brief comparison between the SSS and the CRS signals based on the results already presented in the previous sections. The main issue observed for the generated 10 ms-long time-domain SSS and CRS representations is the presence of secondary peaks, specially in the frequency domain. However, the secondary frequency peaks are much further away for the CRS case (2 kHz) than for the SSS case (200 Hz). This means that there exists a lower risk for the CRS to lock onto a secondary frequency peak during acquisition. However, the CRS signal presents secondary peaks in the time-domain representation of the ACF, which are far from each other (340 samples considering a signal generation rate of 15.36 MHz). A lock into a secondary time-domain peak can be easily resolved by using the Bump Jump technique already used for dealing with the secondary peaks of the Galileo E1-B/C ACF.

Regarding the bandwidth of the signals, it must be considered that while the SSS signal occupies always the middle 62 sub-carriers of the LTE signal bandwidth, the CRS occupies the full transmission bandwidth. Considering that the work is carried with a 10 MHz signal, the CRS signal shows a wider bandwidth, which is translated into a narrower main ACF peak, and therefore, a lower tracking jitter for the CRS. Figure 10 shows the difference in the main correlation peak for the CRS and the SSS sequences.

Finally, if we observe the cross-correlation properties of the SSS and the CRS signals, then it can also be observed that the cross-correlation amplitude is much lower for the CRS case than for the SSS case. This is shown in Figure 10(b).

III. RECEIVER OPTIMIZATION

The MuSNAT SDR is optimized for LTE signal acquisition and tracking in two folds - implementing a complex acquisition scheme by further developing the source code (Arizabaleta et al., 2021) and tailoring MuSNAT configuration parameters to adapt to LTE signal structure. This section describes the optimizations performed to adapt MuSNAT for processing LTE signals.

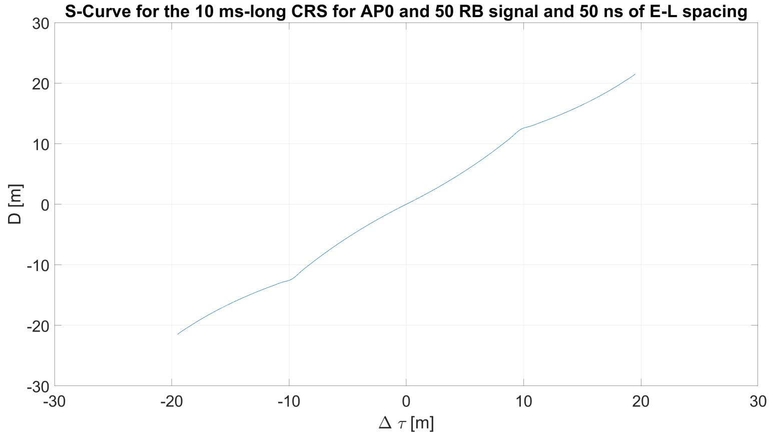
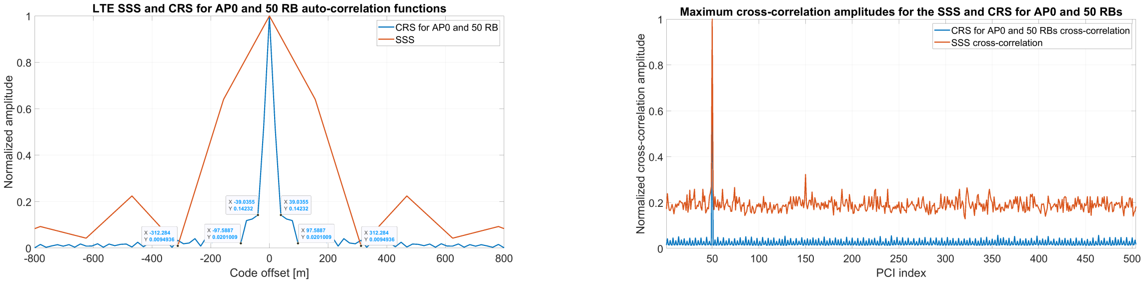


Figure 9: S-curve representation for the LTE CRS for AP0 and 50 RB.



(a) **(b)**

Figure 10: Time domain representation of (a) the main ACF peak for the LTE SSS and CRS for AP0 and 50 RB and (b) the maximum cross-correlations for SSS and CRS signals.

1. Fine tuning of correlator spacing

For the measurements of GNSS and LTE signals, a front-end IQ sampling rate of 20 MHz is selected to cover the L5 signal bandwidth. MuSNAT internally converts complex IQ samples to real IF samples and hence, maintains an IF sampling frequency of 40 MHz yielding an IF sample length of 7.4948 meters. A MATLAB based signal simulator called YASST is used to derive the early-late scale factor required for a ±1 IF sample correlator spacing for CRS and ±5 IF samples correlator spacing for SSS.

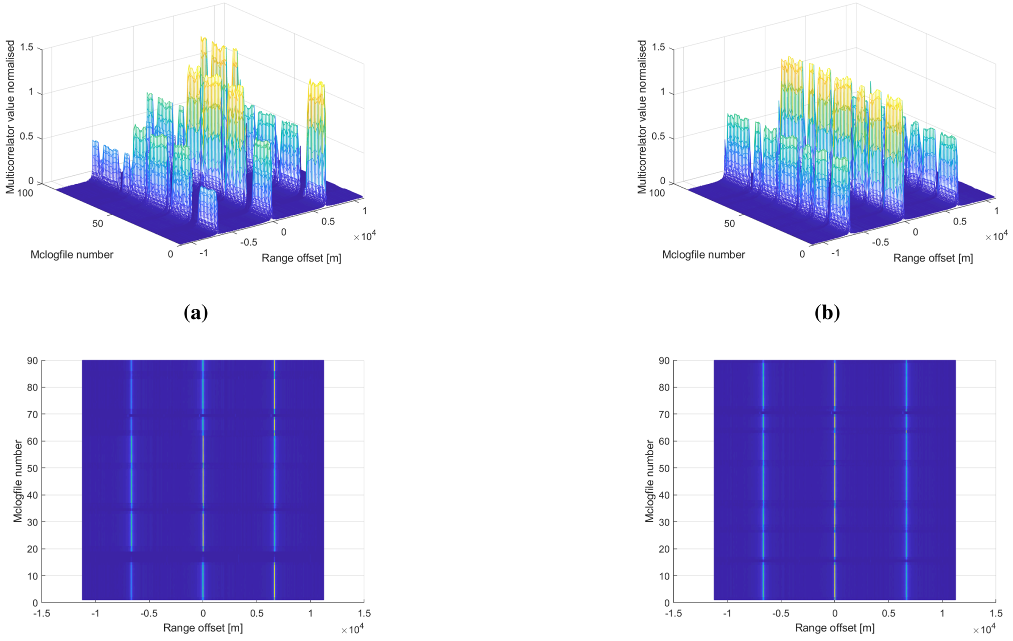
2. Warm acquisition for LTE

The LTE signal acquisition Doppler search space is narrowed by doing a warm acquisition in which the signal is acquired after a GNSS position fix is achieved. A coarse LTE transmitter position is provided to MuSNAT in the form of Earth-Centered-Earth-Fixed (ECEF) coordinates along with the expected standard deviation. MuSNAT uses the Single Point Positioning (SPP) receiver position and clock drift along with a coarse LTE transmitter position to compute the expected Doppler search space for the signal. Furthermore, a long coherent integration time of 80 ms is used for acquisition to increase the Doppler search resolution, or equivalently, to reduce the Doppler frequency bin size. These two optimizations potentially reduce the chance of having false frequency locks during the LTE signal acquisition process.

3. Bump Jump for CRS

As highlighted in Section II.2, the CRS correlation function contains side-peaks in the code phase domain which can potentially cause the receiver Delay Lock Loop (DLL) to falsely lock onto a side-peak. For an IF sampling rate of 40 MHz, the first side-peaks exist at ±6647.9 m which correspond to ±887 IF samples. To avoid side-peak tracking, a Bump Jump (Fine and Wilson, 1999) is configured in MuSNAT by placing 11 Very-Early (VE) correlators at consecutive IF samples ranging from -895 to -885 and 11 Very-Late (VL) correlators at consecutive IF samples ranging from +885 to +895 IF samples. The Bump Jump attempts to detect jumps greater than a threshold equals to three quarters of the first side-peak distance which amounts to

5109 subchips. Figure 11 shows the measured CRS correlation function for a dataset in which several re-acquisitions take place where McLogfile number represent the time in seconds. Figure 11(a) and (c), show the results with the Bump Jump deactivated, where it can be observed for $t < 15$ s and $t > 70$ s the DLL is locked onto a side-peak. With the Bump Jump activated, it can be seen in Figure 11(b) and (d) that the DLL locks onto the main peak each time an acquisition takes place throughout the complete dataset time duration.



(a)

(b)

(c)

(d)

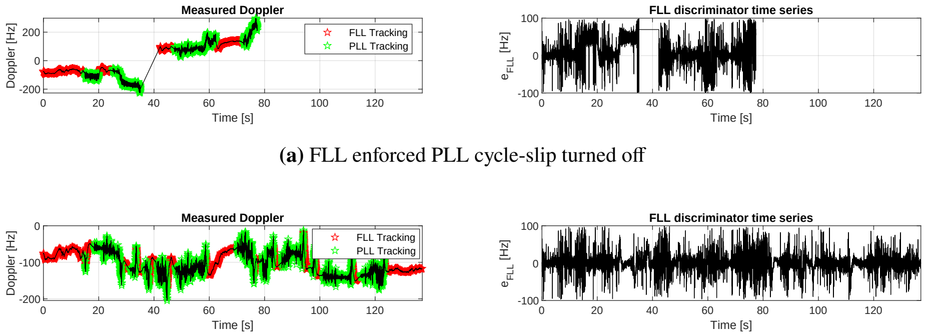
Figure 11: (a)(c) - Bump Jump deactivated, (b)(d) - Bump Jump activated

4. FLL enforced PLL cycle-slip for SSS

As highlighted in Section II.1, the SSS correlation function has side-peaks in the frequency domain with an interval of 200 Hz. It is observed in dynamic measurements that the receiver Frequency Lock Loop (FLL) can potentially deviate to a side-peak tracking despite having a low FLL bandwidth. While already in phase-lock, such a deviation appears as a bias in the FLL discriminator time series and causes the PLL to hold onto a track with an incorrect Doppler, which eventually leads to a loss-of-lock of the signal. This can be observed in Figure 12(a), where a bias within the FLL discriminator can be seen at $t = 30$ s. To avoid this, MuSNAT is configured to perform a PLL cycle-slip whenever such a bias is detected and return to FLL tracking for frequency recovery of the incoming signal. The cycle-slip is configured by computing the average of 10 previous FLL discriminator values and comparing it against a fixed threshold. Figure 12(b) shows the SSS Doppler tracking results for a threshold of 50 Hz. It can be observed that after a temporary phase loss-of-lock, the signal frequency is recovered and PLL tracking is achieved for a longer duration for the same dataset.

5. LTE code replica scaling

With the optimized LTE configuration, MuSNAT is able to track LTE signals by generating a pre-computed code replica which is multiplied by a locally generated carrier and is then correlated with the incoming signal. As the generated LTE code replica contains floating values between [-1,1], and MuSNAT requires *int8* integer values, the amplitude of replicas are converted to the nearest integer between [-127, +127]. This causes the local replica to contain high amplitude values, and occasionally to exceed the standard range of *int16* within the Intel IPP multiplication routine, which is employed within MuSNAT, producing a register over-flow which eventually stops the tracking channel. To overcome this issue, a scaling factor called $CorrelatorScaleFactor$ has been introduced within the MuSNAT configuration to scale the output of the Intel IPP multiplication sub-routine by $(1/2^{CorrelatorScaleFactor})$ so that it falls within the range of *int16*. The code replica amplitude is then scaled up by $2^{CorrelatorScaleFactor}$ before it is assigned to the complex signal container which is of type *double*. A typical value of 3 for the $CorrelatorScaleFactor$ has been tested to successfully eliminate the register overflow issue.



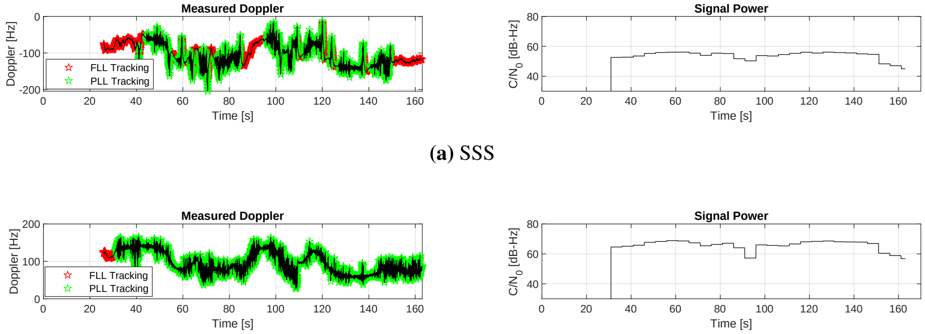
(a) FLL enforced PLL cycle-slip turned off

(b) FLL enforced PLL cycle-slip turned on with threshold equal to 50 Hz

Figure 12: FLL enforced PLL cycle-slip for SSS tracking

6. CUDA based correlator for LTE

With the Bump Jump optimization done for CRS, the MuSNAT LTE receiver consists a total of 50 correlators, from which 25 correlators correspond to the real part and 25 correlators corresponds to the imaginary part of the correlation function. Having 50 correlators imposes a high-computational load on the processor. To avoid this, the CUDA support for MuSNAT (Pany et al., 2019) was extended to incorporate typical LTE signal correlation amplitude values to offload the correlation process load to an on-board GPU. The GPU offloading is especially useful when monitoring the shape of the LTE correlation function over time such as shown in Figure 11 where 3000 correlators have been used.



(a) SSS

(b) CRS

Figure 13: Dynamic receiver SSS and CRS tracking results

IV. TRANSMITTER LOCALIZATION FILTER

Using the time-domain code replicas of SSS and CRS, as described in Section II.1 and II.2, the LTE signals can be tracked within a GNSS-like signal processing architecture within MuSNAT SDR. The results of SSS and CRS tracking for a dynamic receiver measurement is shown in Figure 13 which shows the CRS signal being tracked with a higher C/N_0 and having less frequent loss-of-locks than SSS. From the DLL output of the LTE signal, code phase observations can be obtained to produce pseudorange measurements. These pseudorange measurements can be used for navigation given that the LTE base station position and clock offset are also known. However, the latter is a priori unknown for the commercial cellular base stations. Hence, as part of this paper, a base station localization scheme is employed in which a ground receiver tracks both GNSS and LTE signals using the same antenna module. The GNSS PVT solutions are used to correct LTE pseudoranges and then to estimate the LTE transmitter position and clock offset (Hameed et al., 2022).

1. Observation Model

We consider a system with K valid satellites and L valid LTE base stations visible to the receiver in the observation window. It is assumed that when $K \geq 4$ the receiver is able to compute PVT solutions, which renders the receiver position $\vec{\mathbf{r}_r}$ and clock offset $\delta\tau_r$ to be known as a prior for the estimation problem. The localization scheme is applied for one BS at a time, hence we consider the case $L = 1$. For this system, a simplified code observation model as given in (2) is considered where ρ_r^l is the measured LTE code pseudorange, $\vec{\mathbf{r}}^l$ is the LTE transmitter position, c is the speed of light, $\delta\tau^{l,clk}$ is the LTE transmitter clock offset and η represents the LTE code measurement noise. The LTE transmitter clock offset $\delta\tau^{l,clk}$ is modeled using a two-state model having a clock bias $\delta\tau^l$ and a clock drift $\delta\dot{\tau}^l$ component. The receiver and LTE transmitter position can be expressed in the ECEF coordinate system as shown in (3) and (4), respectively. The GNSS Position, Velocity and Time (PVT) solutions are used to correct LTE pseudoranges and then to estimate the LTE transmitter position and clock offset as expressed in (5).

$$\rho_r^l = \left|\vec{\mathbf{r}_r} - \vec{\mathbf{r}}^l\right| + c\left(\delta\tau_r - \delta\tau^{l,clk}\right) + \eta \tag{2}$$

$$\vec{\mathbf{r}_r} = [x_r, y_r, z_r]^T \tag{3}$$

$$\vec{\mathbf{r}}^l = [x^l, y^l, z^l]^T \tag{4}$$

$$\begin{pmatrix} \hat{\vec{\mathbf{r}}}^l \\ \delta\tau^{\hat{l},clk} \end{pmatrix} = \underset{\vec{\mathbf{r}}^l,\delta\tau^{l,clk}}{\arg\min} \, ||\rho_r^l - \left|\vec{\mathbf{r}_r} - \vec{\mathbf{r}}^l\right| - c\left(\delta\tau_r - \delta\tau^{l,clk}\right)|| \tag{5}$$

2. Kalman Filter

As part of this work, the estimation problem given in (5) is alternatively approached using a Kalman Filter (KF), which is used to estimate the absolute LTE transmitter position, clock bias and clock drift in each epoch i with a sampling time interval T. The filter state-vector $\mathbf{x}$ is given in (6) where x^l, y^l and z^l are the LTE position states, and $\delta\tau^l$ and $\delta\dot{\tau}^l$ are the LTE clock bias and drift states, respectively. In each epoch, a time-update step propagates the state-vector using the state transition matrix $\mathbf{B}$ which models for the transmitter a static position and a clock offset steered by the clock drift. The state-covariance $\mathbf{P}$ is propagated to the current time step with the addition of the filter process noise $\mathbf{Q}$. The process noise matrix $\mathbf{Q}$ models zero process noise for the position states and a noise model realized by $\mathbf{Q}_{clk}$, which is inherited from (Kassas and Humphreys, 2013), for the clock bias and clock drift states. $\mathbf{Q}_{clk}$ models zero-mean and mutually independent white noise processes with power spectra $S_{\delta\dot{\tau}_s}$ and $S_{\delta\dot{\tau}_s}$ for the clock bias and drift, respectively. The values of the power spectra $S_{\delta\dot{\tau}_s}$ and $S_{\delta\dot{\tau}_s}$ are calculated using the typical values of the power-law coefficients h_0 and h_{-2} as given in (Kassas, 2020). The filter observation matrix $\mathbf{H}$ is given in (9) where $(\vec{\mathbf{e}^l})^T$ is the unit vector pointing from the receiver to LTE transmitter. A measurement update step computes the filter residual $\mathbf{z}$ by using the current pseudorange measurement. The residual is scaled by the filter gain $\mathbf{K}$ to eventually update the state-vector $\mathbf{x}$. The state-vector, at the end of each measurement update step, contains the estimates for the state-variables.

$$\mathbf{x} = \begin{pmatrix} \vec{\mathbf{r}^l} \\ \delta\tau^l \\ \delta\dot{\tau}^l \end{pmatrix} \tag{6}$$

$$\mathbf{B} = diag[\mathbf{I}_{3x3}, \mathbf{B}_{clk}]^T \tag{7}$$

$$\mathbf{B}_{clk} = \begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix} \tag{8}$$

$$\mathbf{H} = \begin{pmatrix} -(\vec{\mathbf{e}^l})^T & -c & 0 \end{pmatrix} \tag{9}$$

$$\mathbf{P}_0 = diag[\sigma_x^2, \sigma_y^2, \sigma_z^2, \sigma_{\delta\tau}^2, \sigma_{\delta\dot{\tau}}^2]^T \tag{10}$$

$$\mathbf{R} = \sigma_\rho^2 \tag{11}$$

$$\mathbf{Q} = diag[\mathbf{0}_{3x3}, \mathbf{Q}_{clk}]^T \tag{12}$$

$$\mathbf{Q}_{clk} = \begin{pmatrix} S_{\delta\tau_s}T + S_{\delta\dot{\tau}_s}\frac{T^3}{3} & S_{\delta\dot{\tau}_s}\frac{T^2}{2} \\ S_{\delta\dot{\tau}_s}\frac{T^2}{2} & S_{\delta\dot{\tau}_s}T \end{pmatrix} \tag{13}$$

$$\mathbf{x}_i^- = \mathbf{B}\mathbf{x}_{i-1} \tag{14}$$

$$\mathbf{P}_i^- = \mathbf{B}\mathbf{P}_{i-1}\mathbf{B^T} + \mathbf{Q} \tag{15}$$

$$\mathbf{z}_i = \mathbf{y}_i - \mathbf{H}\mathbf{x}_i^- \tag{16}$$

$$\mathbf{K}_i = \mathbf{P}_i^-\mathbf{H}\left(\mathbf{H}\mathbf{P}_i^-\mathbf{H}^T + \mathbf{R}\right)^{\mathbf{-1}} \tag{17}$$

$$\mathbf{x}_i^+ = \mathbf{x}_i^- + \mathbf{K}_i\mathbf{z}_i \tag{18}$$

$$\mathbf{P}_i^+ = \left(\mathbf{I} - \mathbf{K}_i\mathbf{H}\right)\mathbf{P}_i^- \tag{19}$$

V. TRANSMITTER LOCALIZATION RESULTS

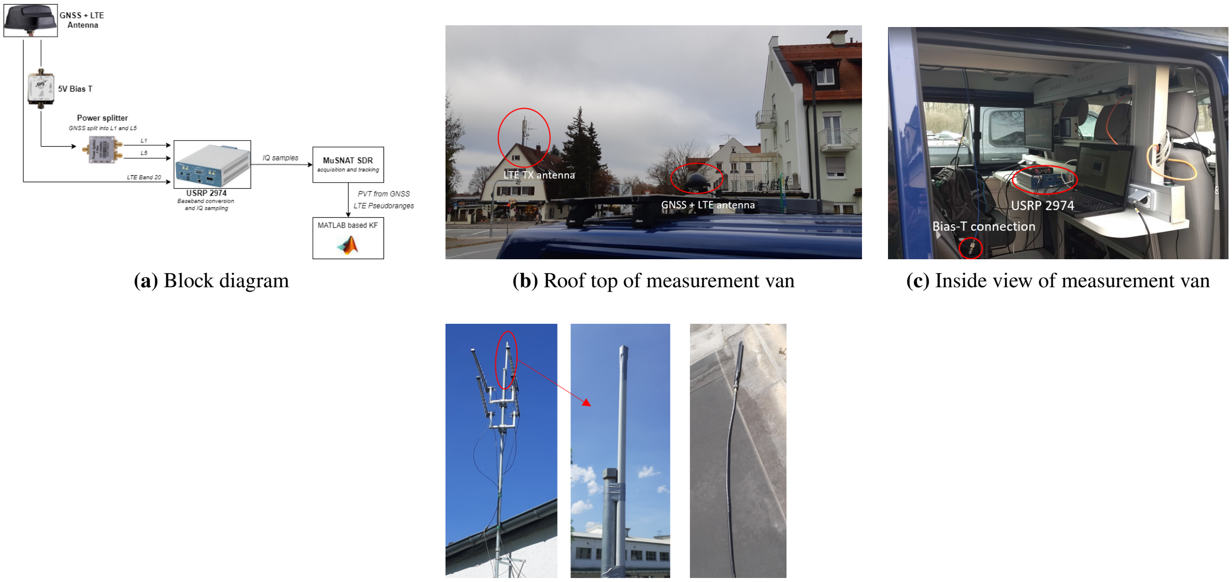
1. Experimental set-up

The experimental setup is illustrated in Figure 14. A multi-band PCTEL GL125-DLTEMIMO-SM antenna (PCTEL, 2021) is used to capture both the GNSS and LTE signals. A power splitter is used to dedicate one RF channel for the GNSS L1 and one for the L5 frequency band signals. The LTE signal is recorded at the base station downlink frequency. For baseband conversion and digital sampling, the National Instrument's USRP-2974 (NI, 2022b) front-end is used. A proprietary software is used to record each signal in the form of 16-bit digital IQ samples at 20 MHz sampling frequency. The IQ samples are post-processed using MuSNAT for acquisition, tracking, and PVT computation for the GNSS signals and for acquisition and tracking of the LTE signal.

The receiver antenna is placed on the roof-top of a measurement bus (see Figure 14(b)), which is driven around a candidate LTE base station along a trajectory that attempts to cover the orthogonal axes for a better spatial distribution of measurement points. The cellular base station archive CellMapper (CellMapper, 2022) is used to select two commercial base stations. The selection criteria for a base station focuses on the base station downlink frequency to be 796 MHz and around which a suitable trajectory can be made. The selected commercial base stations correspond to two distinct signal reception environments - Urban and Suburban. The Urban BS exists in an environment where there is higher multipath and frequent signal blockages due to surrounding buildings. The Suburban BS exists in an environment with higher LOS conditions and reduced multipath. A third test case is realized by recording the LTE signal from a research purposed Amarisoft base station (Amarisoft, 2021), operated by the institute Electrical Engineering and Computer Engineering (ETTI) within the premises of the UniBw M campus. This base station is equipped with an omni-directional LTE transmitter antenna as shown in Figure 14(d) to transmit a single PCI, and is driven by a GPS-synchronized reference clock signal derived from a NI OctoClock device (NI, 2022a). A downlink frequency of 2.665 GHz is chosen for the Amarisoft BS and it broadcasts all the standard LTE synchronization and reference signals but no data symbols.

The MuSNAT software receiver is used for acquisition and tracking of the LTE signals and for producing GNSS PVT solutions. A Trimble NetR9 receiver, placed on the roof-top of a nearby building, is used as a reference receiver to compute the GNSS Real-Time Kinematic (RTK) trajectory in post-processing to minimize forwarding the receiver state-errors into the localization filter. It is to note, however, that within the results presented, the RTK data from this reference receiver is available only for the Urban BS and Amarisoft BS test cases but not for the Suburban test case.

Finally, the GNSS PVT solutions and the measured LTE code pseudoranges are provided to the MATLAB based localization filter as input. The localization filter uses GNSS RTK for Urban BS and Amarisoft BS and GNSS SPP for Suburban BS. The filter estimates the LTE transmitter position, clock offset and drift over time.



(a) Block diagram

(b) Roof top of measurement van

(c) Inside view of measurement van

(d) Amarisoft BS transmit antenna

Figure 14: Experimental Setup

2. Simulation results

The localization filter is validated using a simulated dataset which contains GNSS and LTE signal simulated at the bit-true level using the MuSNAT-SigGen signal simulator. Figure 15 shows the ground track of the simulated receiver trajectory. The trajectory begins with a linear path, progresses onto a circular trajectory and then again follows a linear path. The LTE transmitter is simulated to be located at the center of the circular trajectory and is simulated to have zero clock bias and drift. The filter is provided an initial LTE transmitter position that is offset in the X and Y coordinates by 10 m to obtain a convergence to the true position. Figure 15(b)-(c) show the filter residuals and Figure 15(d)-(i) show the convergence results for the filter states and position error. For this simulated test case, the filter uses as well the carrier phase measurements, and hence, includes the carrier-phase float ambiguity within the state-vector. Overall, the filter position states converge to a cm level error with respect to the true LTE transmitter position.

3. Experimental Results

This section presents the localization results for the three real-base station test cases. Table 2 lists the Kalman filter parameters chosen for each test case. The initial clock bias state variance is set significantly higher for the Amarisoft BS than for the Urban and Surban BS to obtain filter convergence. The initial position of the LTE base station is set to the coordinates as obtained from Google Maps biased by an offset of 10 m in both X and Y directions. As part of this analysis, the inter-PCI clock bias and transmitter antenna position offset is not taken into consideration within the localization filter.

Figure 16, 17 and 18 show the localization results for the Urban BS, Suburban BS and Amarisoft BS, respectively. Within Figure 16(a-b), 17(a-b), and 18(a), the receiver trajectory as obtained from GNSS PVT is shown in blue, the trajectory points at which the LTE CRS signal is tracked is shown in magenta and the trajectory points at which the LTE SSS signal is tracked is shown in cyan. Overall, a greater concentration of the CRS track points directly indicate its superior tracking performance to the SSS signal which exhibits a sparse density of track points that directly influences the filter state convergence results with less measurements available over the observation window. Figure 16(e-f), 17(e-f), and 18(d-e) show the convergence of the clock bias and clock drift states. Figure 16(g-j), 17(g-j) and 18(f-i) show the convergence of the position difference with respect to the Google Maps coordinates in the East-North-Up (ENU) frame. Figure 16(d), 17(d), and 18(c) show the corrected LTE pseudorange, which after filter pull-in, represent the geometric range between the LTE transmitter and receiver.

Also shown, both for CRS and SSS, is the final estimated position of the LTE transmitter bounded by an error ellipse constructed using the diagonal terms of the final filter state convariance matrix. It can be observed that for each test case, the volume of the error ellipse is smaller for CRS than for SSS. It is also observable that the coarse LTE transmitter position, denoted by the magenta colored marker, resides within the error ellipse bounds for each test case.

Table 3 and 4 provide the final filter state results for each test case. It can be seen that for all test cases, the absolute position difference obtained for CRS is less than for SSS. Furthermore, the absolute position difference for Suburban BS is highest amongst all test cases, which can be associated to the unavailability of RTK data for the Suburban case.

The results presented are for a ground-based reception scenario in which the measurement bus is the antenna payload vehicle. Due to the surrounding buildings and foliage, this ground-based reception is prone to high code multipath as it can be seen in the Code-minus-Carrier (CMC) time series obtained for the Amarisoft BS signal. This is shown in Figure 19(a), which has an RMS CMC value of 5.38 m for the phase-lock samples. To avoid such high code multipath, a UAV can be used instead as the user antenna payload vehicle. Figure 19(b) shows the CMC time series for a UAV-based measurement done for a commercial BS. It can be observed that the CMC variation is within 1.81 m indicating less multipath within the LTE code pseudorange measurements.

Table 2: Kalman filter parameters

Parameter	Symbol	Value	
		Suburban, Urban	**Amarisoft**
Initial x, y, z position state variance [m^2]	$\sigma_x^2, \sigma_y^2, \sigma_z^2$	5x10^1	5x10^1
Initial clock bias state variance [m^2]	$\sigma_{\delta\tau}^2$	2x10^6	2x10^{12}
Initial clock drift state variance [m^2]	$\sigma_{\dot{\delta\tau}}{}^2$	2x10^1	2x10^1
Measurement noise variance [m^2]	σ_ρ^2	50^2	50^2

VI. CONCLUSIONS AND FUTURE WORK

Overall, this paper presents the implementation of the LTE synchronization and CRS signals within a GNSS-based signal processing architecture, and provides a comparison of CRS based tracking against SSS based tracking of the LTE signal. The paper outlines identifies the observed implementation issues and provides the optimizations done to extend the MuSNAT SDR for LTE signal compatibility and highlights the merits of using the CRS signal for LTE transmitter localization due to its superior

Table 3: Final states results for SSS tracking

Parameter	Symbol	SSS Results		
		Amarisoft	**Suburban**	**Urban**
Pos. diff. X [m]*	δx	6.758	5.818	-10.05
Pos. diff. Y [m]*	δy	-5.489	-0.0923	-0.2240
Pos. diff. Z [m]*	δz	-7.606	-15.93	2.504
Absolute pos. diff.[m]*	Δ	11.56	16.96	10.36
Clock Bias [ms]	$\delta\tau$	$4.49e6$	-4.210	-4.955
Clock Drift [ns/s]	$\delta\dot{\tau}$	3.736	-0.4114	0.6022

*Pos. differences with respect to Google Maps coordinates.

Table 4: Final states results for CRS tracking

Parameter	Symbol	CRS Results		
		Amarisoft	**Suburban**	**Urban**
Pos. diff. X [m]*	δx	4.324	0.2020	-5.148
Pos. diff. Y [m]*	δy	0.5632	-2.626	4.693
Pos. diff. Z [m]*	δz	-4.982	-9.741	0.0871
Absolute pos. diff.[m]*	Δ	6.621	10.09	6.966
Clock Bias [ms]	$\delta\tau$	$4.49e6$	-4.210	-4.955
Clock Drift [ns/s]	$\delta\dot{\tau}$	2.089	-0.3345	0.5511

*Pos. differences with respect to Google Maps coordinates.

tracking performance compared to the SSS, which is mainly because of its narrower main correlation peak in the time-domain and more distant Doppler side-peaks in the frequency domain.

The paper presents the localization results of 3 real LTE base stations by using GNSS PVT solutions and LTE pseudoranges recorded using the same antenna module. Overall, CRS is observed to provide less steady-state absolute position difference than SSS for all the considered test cases.

For achieving cm level accuracy, it is important to consider the transmission of one PCI signal per antenna element and to model the inter-PCI clock biases. Thirdly, the model can be extended to include carrier phase measurements which exhibit a much lower measurement noise.

The LTE localization filter can be refined by further investigating the Amarisoft BS using UAV-based measurements and by obtaining a ground truth for the base station transmit antenna. The Amarisoft BS inherently offers some advantages over commercial base stations for this activity. Firstly, the base station is set-up to transmit one PCI using an omni-directional antenna, thereby, eliminating inter-PCI clocks biases and transmitter antenna position offsets. Secondly, the base station clock can be regulated to ensure GPS synchronization. Thirdly, a ground truth for the precise coordinates of the transmit antenna can be obtained by using GNSS RTK and a Leica Multi-station (Leica, 2022) device. Hence, as part of the future work the Amarisoft BS shall be further investigated using UAV-based measurements.

ACKNOWLEDGEMENTS

This activity was carried out at Institute of Space Technology and Space Applications (ISTA) at Universität der Bundeswehr München as part of the projects ”*Forschungs- und Studienvorhaben für Innovationen des Galileo GNSS-Systems (GalileoFusion)*” and ”*Firefly - Mobiles und vernetztes Positionierungssystem zur gestützten Navigation in urbanen Umgebungen*, funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) and administered by the project Management Agency for Aeronautics Research of the German Space Agency (DLR) in Bonn, Germany (grant no. 50NA2001 and no. 50NA2102). The authors are also grateful for Christian Menzel and his supervisor Prof. Petra Weitkemper from the Institute for communications engineering and data transmission technology (ETTI) of the Universität der Bundeswehr München for their support setting up the Amarisoft BS to transmit the test signal, from which the results shown in Figure 18 and discussed in Section V.3 were obtained.

REFERENCES

3GPP (2017). Evolved universal terrestrial radio access (e-utra); physical channels and modulation. Technical report, 3GPP. 3GPP TS 36.211 version 14.2.0 Release 14.

Amarisoft (2021). Amarisfot lte/5g base station. `https://www.amarisoft.com/app/uploads/2022/03/AMARI-Callbox-Advanced.pdf`. Last accessed: 2022-09-22.

Arizabaleta, M., Ernest, H., Dampf, J., Kraus, T., Sanchez-Morales, D., Dötterböck, D., Schütz, A., and Pany, T. (2021). Recent enhancements of the multi-sensor navigation analysis tool (musnat). In *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, pages 2733–2753.

CellMapper (2022). Map of cell tower positions. https://www.cellmapper.net.

Del Peral-Rosado, J. A., I Castillo, R. E., Mıguez-Sanchez, J., Navarro-Gallardo, M., Garcıa-Molina, J. A., Lopez-Salcedo, J. A., Seco-Granados, G., Zanier, F., and Crisci, M. (2016). Performance analysis of hybrid gnss and lte localization in urban scenarios. In *2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pages 1–8.

Fine, P. and Wilson, W. (1999). Tracking algorithm for gps offset carrier signals. In *Proceedings of the 1999 national technical meeting of The Institute of Navigation*, pages 671–676.

Hameed, M. S., Arizabaleta-Diez, M., and Pany, T. (2022). Lte transmitter position estimation through combined gnss and lte tracking using a software receiver.

Innovations, T. (2010). Lte in a nutshell: the physical layer. Technical report, Telesystem Innovations. White paper. Last accessed: 2022-09-22.

Kassas, Z. M. (2020). Navigation with cellular signals of opportunity. *Position, Navigation, and Timing Technologies in the 21st Century*.

Kassas, Z. M. and Humphreys, T. E. (2013). Observability analysis of collaborative opportunistic navigation with pseudorange measurements. *IEEE Transactions on Intelligent Transportation Systems*, 15(1):260–273.

Knutti, F., Sabathy, M., Driusso, M., Mathis, H., and Marshall, C. (2015). Positioning using lte signals. In *Proceedings of Navigation Conference in Europe*, pages 1–8.

Leica (2022). Leica nova ms60 multistation. https://leica-geosystems.com/products/total-stations/multistation/leica-nova-ms60. Last accessed: 27-09-2022.

Matlab (2019). Matlab's lte waveform generator. https://www.mathworks.com/help/lte/ref/ltewaveformgenerator-app.html?searchHighlight=lte%20waveform%20generator&s_tid=srchtitle_lte%20waveform%20generator_1. Last accessed: 2022-09-22.

NI (2022a). National instruments octoclock cda-2990. https://www.ettus.com/all-products/octoclock. Last accessed: 27-09-2022.

NI (2022b). National instruments usrp 2974. https://www.ni.com/docs/de-DE/bundle/guid-2c77f3ed-2df7-488d-9a36-f36457b9e6a8/page/specs.html. Last accessed: 26-09-2022.

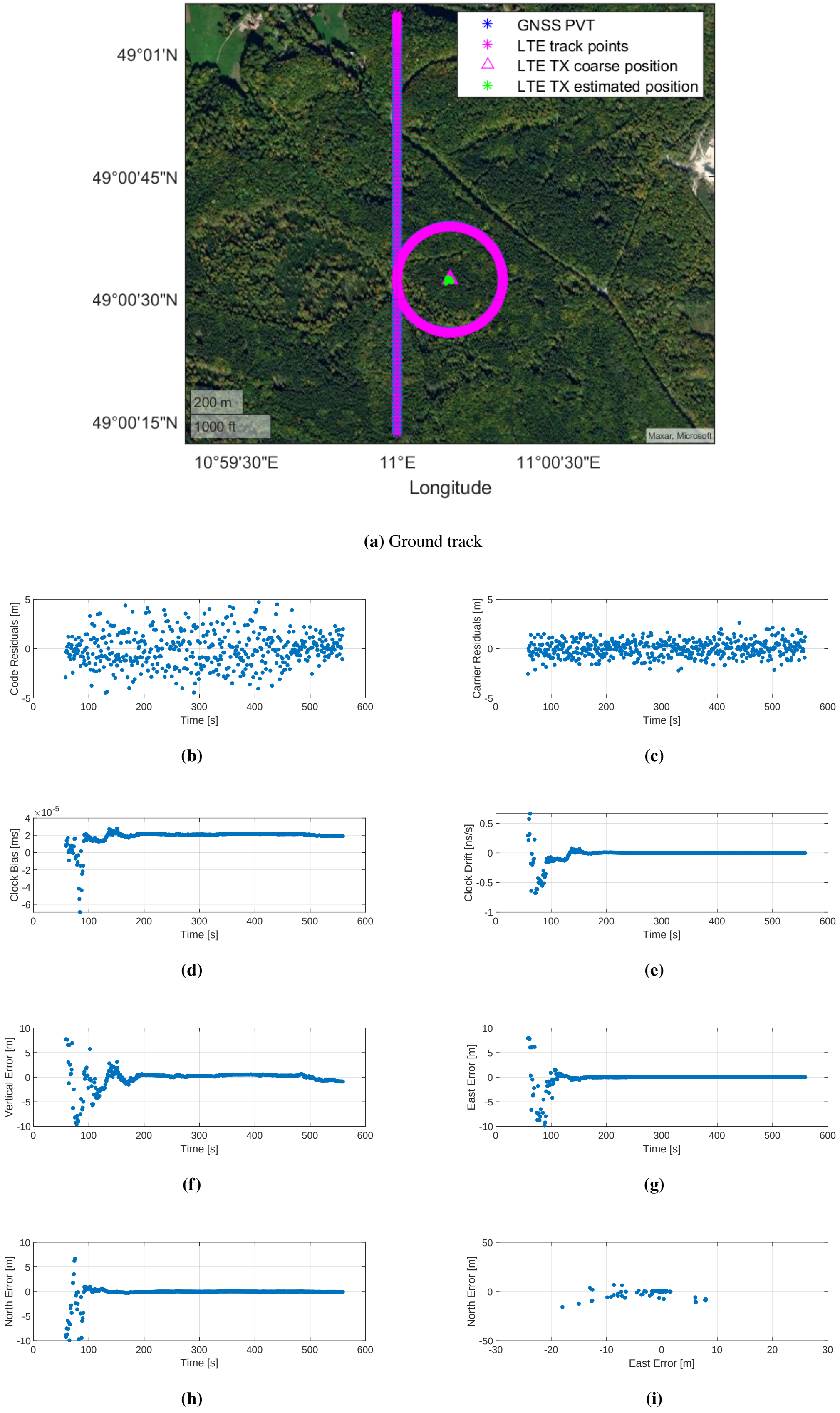
Pany, T., Dötterböck, D., Gomez-Martinez, H., Hammed, M. S., Hörkner, F., Kraus, T., Maier, D., Sánchez-Morales, D., Schütz, A., Klima, P., et al. (2019). The multi-sensor navigation analysis tool (musnat)–architecture, lidar, gpu/cpu gnss signal processing. In *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, pages 4087–4115.

PCTEL (2021). Coach™ ii 5g cellular gnss multiband antenna. https://d3dqzy9ky05fbv.cloudfront.net/wp-content/uploads/2020/06/GL125-DLTEMIMO-SM.pdf. Last accessed: 26-09-2022.

Shamaei, K., Kalife, J., and Kassas, Z. M. (2017). Comparative results for positioning with secondary synchronization signals vs cells specific reference signal in lte systems. In *Proceedings of the 2017 International Technical Meeting of The Institute of Navigation*, pages 1256–1268.

Yang, C., Arizabaleta-Diez, M., Weitkemper, P., and Pany, T. (2022). An experimental analysis of cyclic and reference signals of 4g lte for toa estimation and positioning in mobile fading environments. *IEEE Aerospace and Electronic Systems Magazine*, 37(9):16–41.

Yang, C., Pany, T., and Weitkemper, P. (2020). Effect of antenna ports on toa estimation with 4g lte signals in urban mobile environments. In *Proceedings of the 33rd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2020)*, pages 2166–2181.



(**a**) Ground track

(**b**)

(**c**)

(**d**)

(**e**)

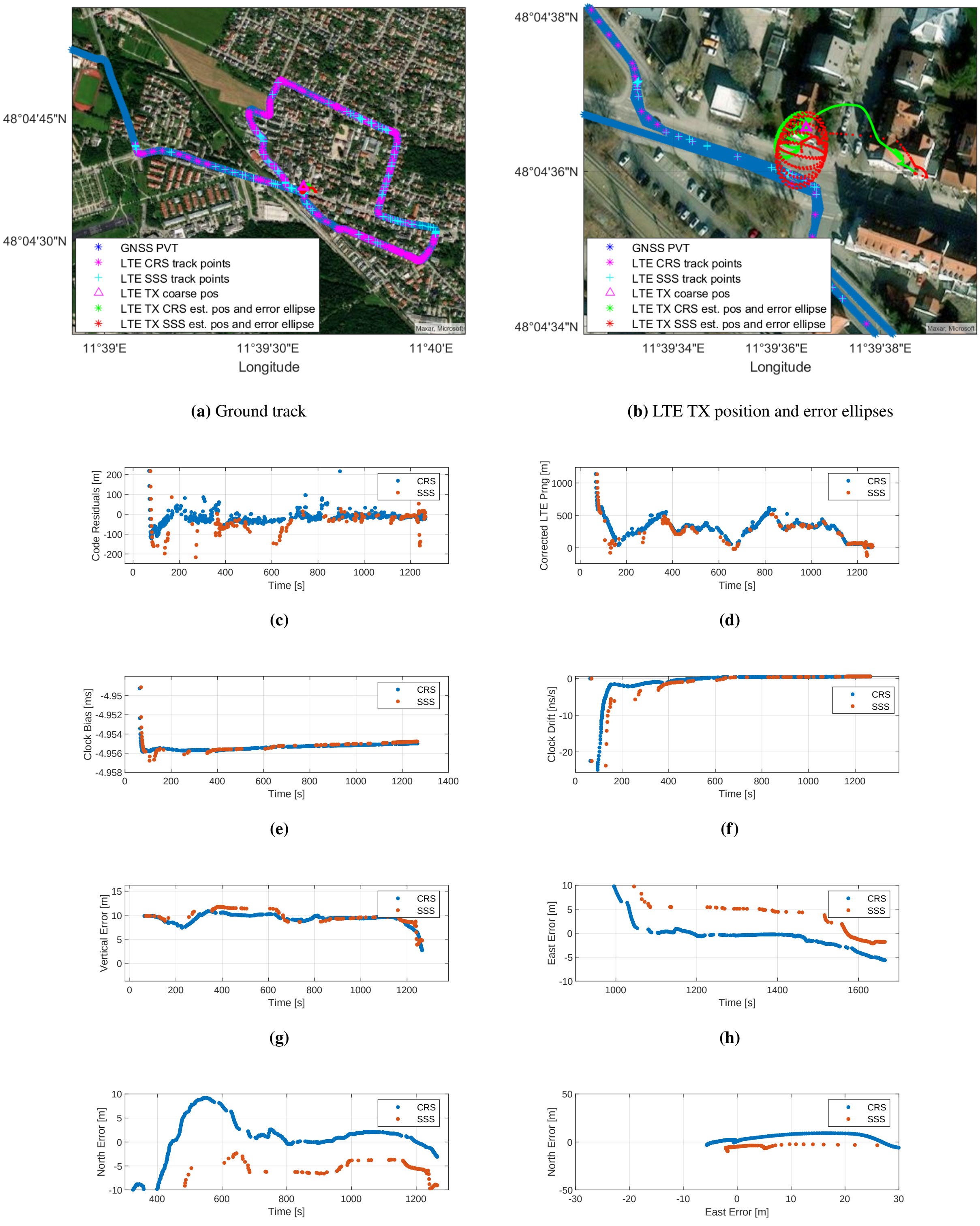
(**f**)

(**g**)

(**h**)

(**i**)

Figure 15: Simulated dataset results



(a) Ground track

(b) LTE TX position and error ellipses

(c)

(d)

(e)

(f)

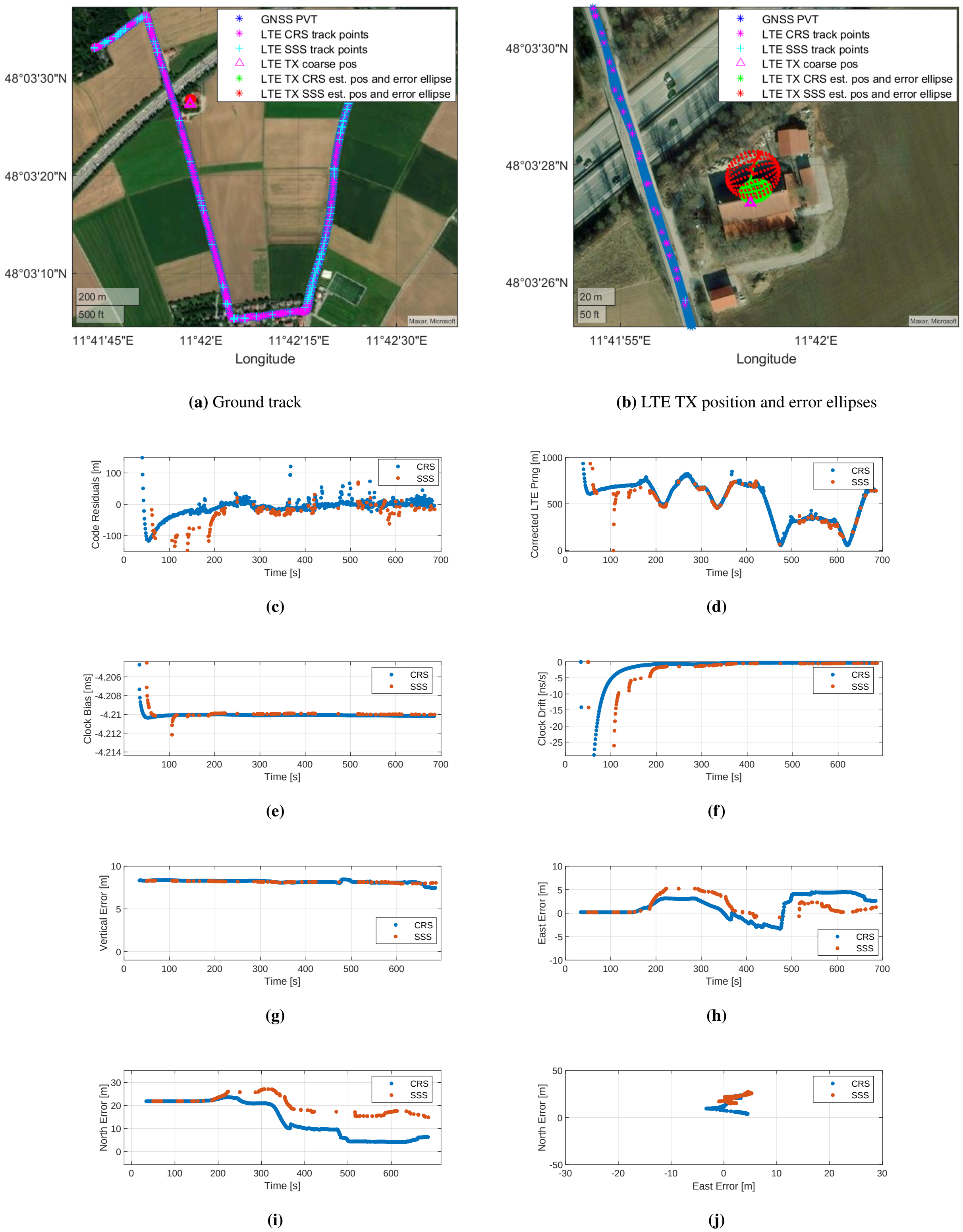
(g)

(h)

(i)

(j)

Figure 16: Localization results for Urban BS



(a) Ground track

(b) LTE TX position and error ellipses

(c)

(d)

(e)

(f)

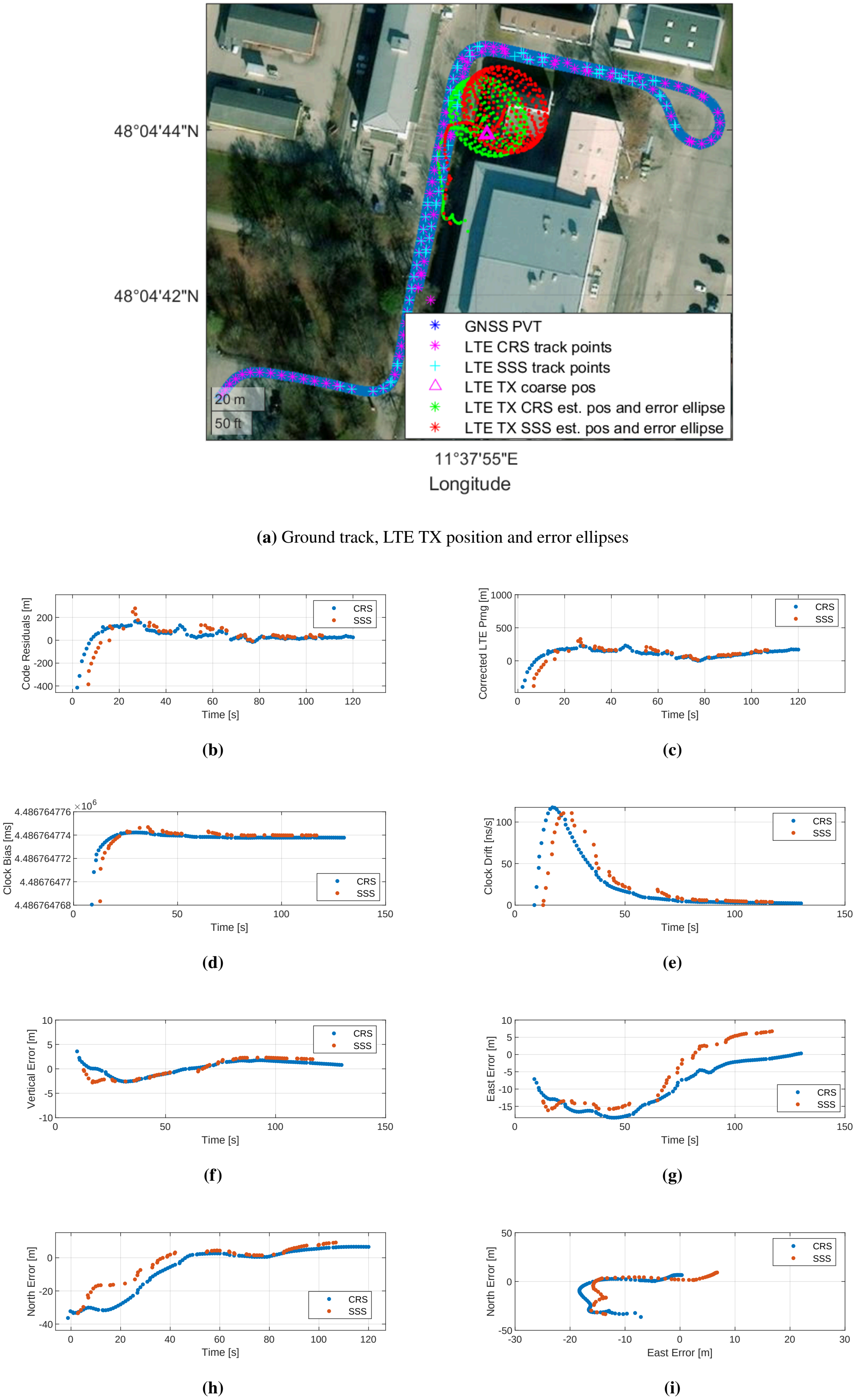
(g)

(h)

(i)

(j)

Figure 17: Localization results for Suburban BS



(a) Ground track, LTE TX position and error ellipses

(b)

(c)

(d)

(e)

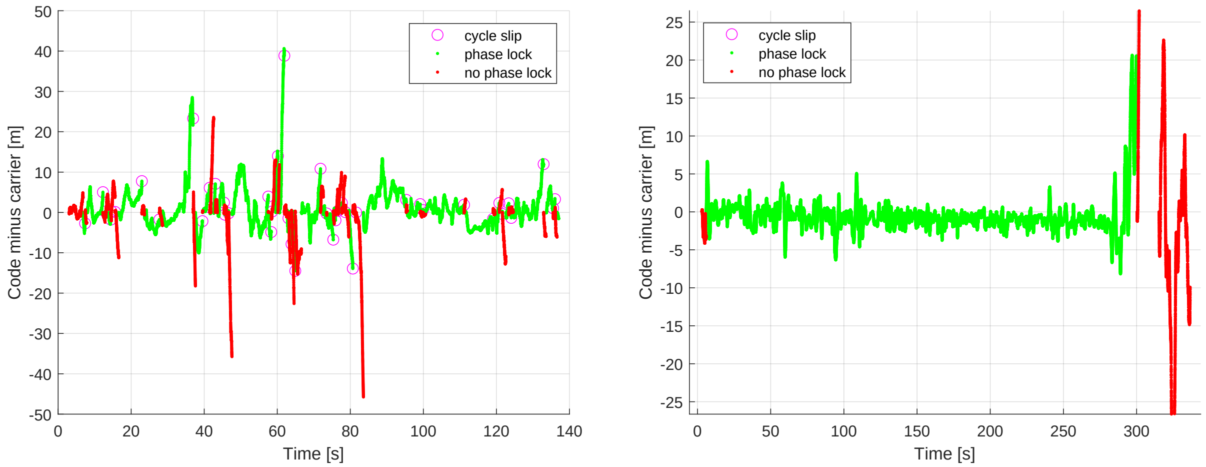
(f)

(g)

(h)

(i)

Figure 18: Localization results for Amarisoft BS



(a) Amarisoft BS CRS tracking using Measurement Bus

(b) Commercial BS CRS tracking using a UAV

Figure 19: Code-minus-Carrier Plots