LTE transmitter position estimation through combined GNSS and LTE tracking using a software receiver

Muhammad S. Hameed, Markel Arizabaleta-Diez, Thomas Pany

Institute of Space Technology and Space Applications
Universität der Bunderwehr München
85577 Neubiberg, Germany

ABSTRACT

The increasing incidences of Global Navigation Satellite System (GNSS) denial due to signal jamming or spoofing [1] and the limited access to GNSS signals in challenging environments (e.g.urban canyons and indoors) has instigated interest in realizing localization through cellular LTE signals by using them as Signal of Opportunity (SoO) [2]. The high transmission power of these signals and a dense terrestrial network of transmitting base stations together formulate an environment where high signal availability is ensured which renders these signals as an alternative to GNSS signals in times where GNSS signals are not trackable. LTE signals, originally designed for cellular communications, do not provide information about the precise position and clock characteristics of the transmitting base stations which is a key information required to compute the user position. The unavailability of these two parameters can be treated as two separate problems. This paper addresses the first problem by assuming a model for the LTE clock and hence, estimating the LTE transmitter position by applying a Kalman Filter (KF) over GNSS conditioned LTE code pseudorange measurements. The measurements are obtained by tracking GNSS and LTE signals through the same antenna module and are processed using the Multi Sensor Navigation Analysis Tool (MuSNAT) software receiver [3]. In addition, this paper provides some overview of the implementation of the LTE synchronization signals in a GNSS-based signal processing architecture, where time domain replica signals are used for acquisition and tracking.

INTRODUCTION

In the last 20 years, there has been a proliferation of applications which require Position, Navigation and Timing (PNT) functions. Among the technologies available to achieve this, the most developed and accurate stand-alone technology is GNSS. However, the technology presents heavy limitations in scenarios where Non-Line-Of-Sight (NLOS) occurrences and multipath signals are common (e.g. urban canyons and indoors). Moreover, despite the availability, GNSS signals may not be trackable in scenarios where there is high signal interference (e.g. jamming). To overcome the GNSS limitations, the Third Generation Partnership Project (3GPP) released positioning methods employed within the Long Term Evolution (LTE) mobile communication standard [4]. These methods are expected to be used as complementary signals to GNSS.

The LTE standard was primarily defined for communication purposes and it was later modified to allow positioning capabilities by means of the Positioning Reference Signal (PRS). This technology uses network based Observed Time Difference Of Arrival (OTDOA) techniques to realise positioning by employing two-way communication in which a location server computes the user position and then provides it to the user [5]. The transmission of the PRS is optional and depends on the service provider, who usually decides not to transmit such reference signals so that the bandwidth is instead utilized for data communication [5, 6]. Besides the PRS signal, additional techniques are available in literature in which the LTE synchronization (i.e. Primary Synchronization Signal and Secondary Synchronization Signal, namely PSS and SSS, respectively) and reference signals are used for positioning by measuring the Time Of Arrival (ToA) [6, 7]. For real-time use of these techniques, however, the user requires to know the location and time information of the transmitting base station (BS), which is not transmitted as part of the signal.

This paper firstly explores the use of a combination of the PSS-SSS signals for LTE signal tracking against the use of only SSS signals for ToA. The definition of the employed LTE signal configuration and its implementation in MuSNAT software receiver [3] is described as a GNSS-like time domain spreading code signal. Secondly, it presents a calibration procedure to estimate an approximate location of the LTE transmitter antenna by correcting LTE pseudorange measurements using the

receiver position and clock offset as obtained from GNSS PVT Single Point Positioning (SPP) solutions. The estimation problem is formulated with a simplified LTE code observation model which is used within a KF. Then the paper highlights the experimental setup used to do dynamic signal recordings for two selected LTE BSs and presents the results for calibrating the selected base stations. Finally, the conclusions of the activity is presented with considerations for the way forward.

LTE SIGNAL DEFINITION

The LTE data transmission is performed in frames, each frame having a duration of 10 ms. Each frame is divided into 10 subframes of 1 ms long duration, or 20 slots with a duration of 0.5 ms. The data within a frame is divided into Resource Blocks (RB). Each RB consists of 6 or 7 symbols and 12 subcarriers. The number of symbols in an RB depends on whether the extended or normal Cyclic Prefix (CP) is used. In the case of normal CP, 7 symbols are used in an RB and otherwise 6 symbols. This Orthogonal Frequency Division Multiplexing (OFDM) signal uses a subcarrier spacing of 15 kHz with the symbol duration being 66.6 μs. The possible bandwidths to be used in LTE depends on the number of RBs employed, which can be 6, 12, 25, 50, 75 or 100 RB, and therefore the bandwidth ranges from 1.4 MHz to 20 MHz [8].

Among the transmitted LTE signals, two synchronization signals, the PSS and SSS, are used to (i) perform symbol and frame synchronization, (ii) identify the Physical Cell Identity (PCI), (iii) identify the frame type (Time Domain Duplex (TDD) or Frequency Domain Duplex (FDD)), and (iv) coarsely estimate the Fractional Frequency Offset (FFO). In addition to these two signals, the LTE frames contain some reference signals such as the Cell-specific Reference Signals (CRS) or the Channel-State Information Reference Signal (CSI-RS).

The work presented is based on the synchronization signals, PSS and SSS, which are generated as indicated in [9], using an FDD frame type and normal CP length. The characteristics of such signals is that regardless of the total LTE signal bandwidth, the synchronization signals are transmitted in the center 1.08 MHz of the total bandwidth and are transmitted every 5 ms. In the case of the PSS the same sequence is used, however for the SSS, the sequence in the subframe 5 differs from the sequence in the subframe 0. The PSS is a length-62 Zadoff-Chu sequence spread in the frequency domain, i.e. it has a 1 symbol duration (66.6 μs), and it is located in the last symbol (7th symbol) of the slot numbers 0 and 10. There are only 3 possible PSS sequences ($PSS_{id} \in [0,2]$, where PSS_{id} is the PSS identifier). The SSS sequence, however, is a concatenation of two length-31 m-sequences. As the PSS, it is defined in the frequency domain with a duration of one symbol (66.6 μs). The location of the SSS sequence, in a FDD frame type, is one symbol prior to the PSS for both slot number 0 and 10. The SSS sequence is different based on the PSS_{id} and the subframe location, providing 168 sequences for the subframe 0 and additional 168 for subframe 5 per PSS_{id}. The synchronization sequences to be employed depends on a Physical Cell Identification (PCI) number, which can take a value between 0 and 503 (PCI = 3 SSSid+PSS_{id}, where SSS_{id} is the SSS identification).

Software implementation of the LTE synchronization signals

The extension of MuSNAT for LTE signal processing [3] has been implemented by using a time domain representation of the PSS and SSS signals. As MuSNAT has been developed with a GNSS signal processing architecture, the use of the frequency domain synchronization signals would require a complete modification of the acquisition and tracking methods. Instead, the synchronization signals have been defined to last 1 frame, i.e. 10 ms, and their time domain representations have been used. This section defines how the LTE signals have been defined based on a combined PSS-SSS representation. However, the technique is also applicable to generate the SSS-only signal by omitting the PSS sequences.

The generation of the time domain PSS-SSS sequences has been performed by considering the LTE signal characteristics for a bandwidth of 1.4 MHz, indicated in Table 1, which is the minimum LTE downlink bandwidth that can be allocated [8]. This implies, that after generating the PSS and SSS separately in the frequency domain, as indicated in [9], an Inverse-Fast Fourier Transform (IFFT) of 128 points has been employed to obtain the time domain sequences for the PSS and SSS. The combined sequence is then an all-zero sequence with a rate of 1.92 MHz, a duration of 10 ms, and the time domain PSS and SSS sequences are placed in the desired locations. Therefore, the samples belonging to the last symbol of slot 0 and 10 contain the PSS sequences and the samples of the symbols preceding the PSS contain the SSS sequences. The remaining samples are assigned to be zero and they correspond to the CP and to the data symbols in each subcarrier. An assignment of zero is done to avoid a cross-correlation against these samples so that they reduce the impact during the correlation process allowing a more distinct peak detection.

Table 1: LTE downlink parameters

Channel BW [MHz]	1.4	3	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]	10	20	40	80	120	160
(1st symbol / 2nd to 7th symbol)	9	18	36	72	108	144
symbol duration (no CP)	16.67 μs					

Combined PSS-SSS vs SSS-only signals

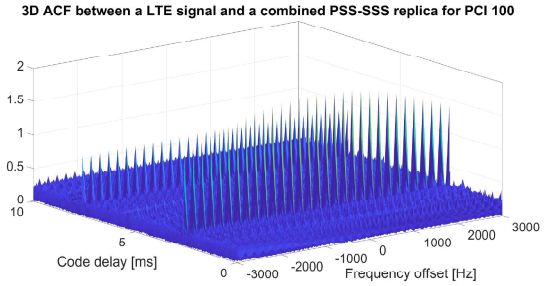
To analyse the effects of combining the PSS and SSS sequences in time domain as a local replica, a 10 ms signal has been generated with the LTE Waveform Generation Matlab toolbox. The generated sequence contained 6 RB, in FDD mode and the example of the PCI 100 has been analysed. This signal is correlated with the combined PSS-SSS replica in time domain, and the results are shown in Fig. 1. The correlation has been performed for different frequency offsets [-3,3] kHz, with frequency bins of 100 Hz. The 3D correlation is shown in Fig. 1a. There are two observations that can be made. Firstly, there exists multiple peaks in the frequency domain (see Fig. 1b) and secondly, there exists a secondary peak in the time domain correlation output (see Fig. 1c).

The presence of multiple peaks in the frequency domain is the direct effect of using a 10 ms long sequence as replica where the non PSS-SSS samples and the CP samples are set to 0, which help to reduce cross-correlation issues in the time domain. This means that there are almost 5 ms of zeros in the combined PSS-SSS replica, resulting in a frequency spacing of 200 Hz (1/5 ms = 200 Hz) between the frequency domain peaks. To limit the effect of the secondary peaks in the frequency domain, the Doppler search range has been limited during the LTE signal acquisition process. As the effect relies in the duration of the zero padding, when using the SSS-only sequence, this effect persists. When correlating the incoming signal with the combined PSS-SSS sequence, a secondary peak is shown in the time domain of the correlation output, with a separation of 5 ms (i.e. at half code duration), see Fig. 1c. This is caused by the repetition of the PSS sequence every 5 ms. As already discussed, the SSS does not show this behaviour due to the different sequence in the subframes 0 and 5. As a consequence of this repetition of the PSS, the secondary peak maintain an amplitude which is approximately half of the amplitude of the main peak. An alternative to remove the secondary peak in the time domain is to use only the SSS contribution as the 10 ms long replica.

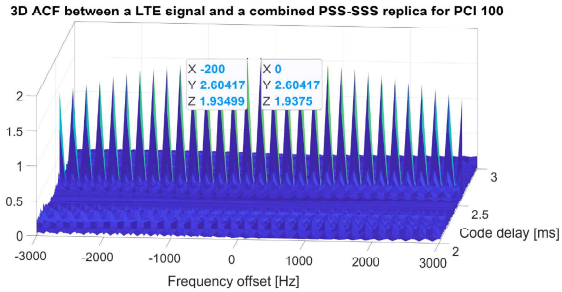
The repetition of the PSS is further investigated. Every 3 PCIs the PSS sequence repeats, e.g. the PCI 100, 103, and 106 share the same PSS sequence. This also causes sequences sharing the PSS to show a high cross-correlation peak. Fig. 2 shows the normalized amplitudes of the cross-correlation peaks for the combined PSS-SSS and for the SSS-only sequence. Regarding the cross-correlation amplitudes for the PCI 100 for the combined PSS-SSS sequence is shown in 2a. It can be observed that the cross-correlations are high, showing a mean value around 0.5 for the normalized amplitude, which implies that the secondary peak is around 3 dB below the main peak. This means that the signal detection and loss-of-lock thresholds need to be carefully´configured to reduce false acquisitions and tracking of cross-correlation peaks. By removing the PSS sequence from the replica, it is observed that the cross-correlation effects get considerably reduced. Fig. 2b shows a cross-correlation amplitude of around 0.2 which is lower than that for the combined PSS-SSS sequence. This reduction still requires to carefully configure the detection and loss-of-lock thresholds.

ESTIMATION PROBLEM

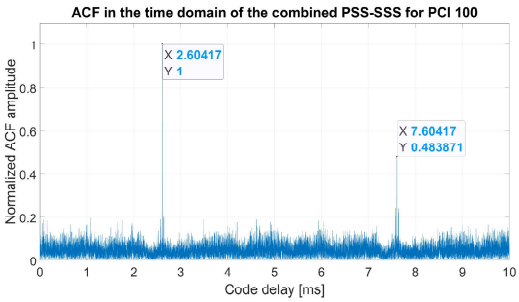
By using the IFFT to obtain the time domain representation of the LTE replica, there is a need to use a complex signal acquisition and tracking scheme within a conventional GNSS receiver. With the use of such a tracking scheme, from the Delay Locked Loop (DLL) output, code phase observations can be obtained to eventually produce code pseudorange measurements. These pseudorange measurements can potentially 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 BSs. Even if a GNSS antenna, equipped on-board the BS is used to compute the BS position, the obtained position solution will be at a baseline to the LTE transmission antenna and shall not take into account its phase center. Hence, as part of this paper, a base station calibration scheme is employed in which a ground receiver tracks both GNSS and LTE signals using the same antenna module. The GNSS SPP solutions are used to correct LTE pseudoranges and to then estimate the LTE transmitter position and clock offset.



(a) 3D view of the combined PSSS-SSS ACF

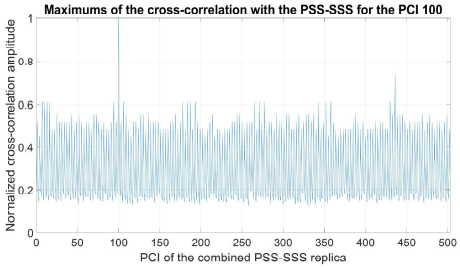


(b) Frequency domain secondary peaks in the combined PSS-SSS ACF

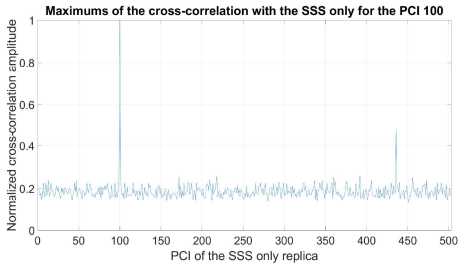


(c) Time domain secondary peaks in the combined PSS-SSS ACF

Figure 1: Secondary effects in the combined PSS-SSS ACF



(a) Normalized amplitudes of the cross-correlation with the PSS-SSS sequences



(b) Code delays of the maximum peaks of the cross-correlation with the PSS-SSS sequences

Figure 2: Maximum amplitudes of the cross-correlation for the PSS-SSS and SSS-only replica for the LTE PCI 100 signal

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 $\vec{\mathbf{r}}_r$ and $\delta\tau_r$ to be known as a prior for the estimation problem which is shown in Equation 4. The calibration scheme is applied for one BS at a time, hence we consider the case $L = 1$. For this system, the simplified code observation model given in Equation 1 is considered where ρ_r^l is the measured LTE code pseudorange, $\vec{\mathbf{r}}_r$ is the receiver position, $\vec{\mathbf{r}}_l$ is the LTE transmitter position, c is the speed of light, $\delta\tau_r$ is the receiver clock offset, $\delta\tau_l$ is the LTE transmitter clock offset which is modeled using a two-state model and η represents the LTE code measurement noise. The receiver and LTE transmitter position can be expressed in the xy plane as shown in Equation 2 and Equation 3 respectively.

$$\rho_r^l = \left|\vec{\mathbf{r}}_r - \vec{\mathbf{r}}_l\right| + c\left(\delta\tau_r - \delta\tau_l\right) + \eta \tag{1}$$

$$\vec{\mathbf{r}}_r = [x_r, y_r]^T \tag{2}$$

$$\vec{\mathbf{r}}_l = [x_l, y_l]^T \tag{3}$$

$$\begin{pmatrix} \hat{\vec{\mathbf{r}}}_l \\ \hat{\delta\tau_l} \end{pmatrix} = \underset{\vec{\mathbf{r}}_l, \delta\tau_l}{\arg\min} \left|\left|{\rho_r}^k - \left|\vec{\mathbf{r}}_r - \vec{\mathbf{r}}_l\right| - c\left(\delta\tau_r - \delta\tau_l\right)\right|\right| \tag{4}$$

Kalman Filter

A Kalman Filter (KF) is used to estimate the absolute LTE transmitter position, the LTE clock bias and clock drift in each epoch i with a sampling time interval $T = 1$ sec. The filter state-vector $\mathbf{x}$ is given in Equation 5 where x_l and y_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 $\mathbf{Q}_{clk}$ and inherited from [10] 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 [11]. The filter system matrix $\mathbf{F}$ is given in Equation 8 where $(\vec{\mathbf{e}}^l)^T$ is the unit vector pointing from the LTE transmitter to the receiver. 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.

$$\mathbf{x} = \begin{pmatrix} \vec{\mathbf{r}}_l \\ \delta\tau_l \\ \delta\dot{\tau}_l \end{pmatrix} \tag{5}$$

$$\mathbf{B} = diag[\mathbf{I}_{2x2}, \mathbf{B}_{clk}]^T \tag{6}$$

$$\mathbf{B}_{clk} = \begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix} \tag{7}$$

$$\mathbf{F} = \begin{pmatrix} (\vec{\mathbf{e}}^l)^T & -c & 0 \end{pmatrix} \tag{8}$$

$$\mathbf{P}_0 = diag[\sigma_x^2, \sigma_y^2, \sigma_{\delta\tau}^2, \sigma_{\delta\dot{\tau}}^2]^T \tag{9}$$

$$\mathbf{R} = \sigma_\rho^2 \tag{10}$$

$$\mathbf{Q} = diag[\mathbf{0}_{2x2}, \mathbf{Q}_{clk}]^T \tag{11}$$

$$\mathbf{Q}_{clk} = \begin{pmatrix} S_{\delta\tau_s} T + S_{\delta\dot{\tau}_s} \frac{T^3}{3} & S_{\delta\dot{\tau}_s} \frac{T^2}{2} \\ S_{\delta\dot{\tau}_s} \frac{T^2}{2} & S_{\delta\dot{\tau}_s} T \end{pmatrix} \tag{12}$$

$$\mathbf{z}_i = \mathbf{y}_i - \mathbf{F}\mathbf{x}_i^- \tag{15}$$

$$\mathbf{x}_i^- = \mathbf{B}\mathbf{x}_{i-1} \tag{13}$$

$$\mathbf{K}_i = \mathbf{P}_i^- \mathbf{F} \left(\mathbf{F}\mathbf{P}_i^- \mathbf{F}^T + \mathbf{R} \right)^{-1} \tag{16}$$

$$\mathbf{P}_i^- = \mathbf{B}\mathbf{P}_{i-1}\mathbf{B}^\mathbf{T} + \mathbf{Q} \tag{14}$$

$$\mathbf{x}_i^+ = \mathbf{x}_i^- + \mathbf{K}_i \mathbf{z}_i \tag{17}$$

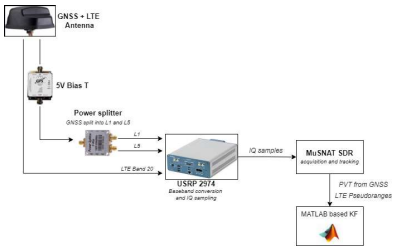
$$\mathbf{P}_i^+ = (\mathbf{I} - \mathbf{K}_i \mathbf{F})\, \mathbf{P}_i^- \tag{18}$$

EXPERIMENTAL SET-UP

The experimental setup is illustrated in Fig. 3. A multi-band PCTEL GL125-DLTEMIMO-SM antenna [12] is used to capture both the GNSS and LTE signals. For GNSS, a 5V inline bias-T is used to provide power to the internal Low Noise Amplifier (LNA) of the antenna. A power splitter is used to dedicate one RF channel for L1 and one for L5 frequency. For LTE, since the reception power is much higher than GNSS, no signal amplification is sought. The recorded LTE signal corresponds to the band 20 with a center frequency of 796 MHZ and 10 MHz bandwidth. For baseband conversion and digital sample recording, the National Instrument's USRP2974 [13] front-end is used. A proprietary software is used to record each signal in the form of 16-bit digital IQ samples. The digital samples are stored in the internal hardrive of USRP2974. The recording software currently does not support an Automatic Gain Control (AGC) configuration and hence all the recordings are done at a constant gain value. The MuSNAT software receiver is used for acquisition, tracking and PVT computation for the GNSS signals. The calibration procedure is performed using GNSS SPP solutions as computed in MuSNAT based on code pseudoranges. Additionally, the receiver is used for acquisition and tracking of LTE signals. MuSNAT hence provides the PVT solutions computed from GNSS signals and the measured LTE code pseudoranges as inputs to a MATLAB based KF. The KF estimates the LTE transmitter position, clock offset and drift over time.

The receiver antenna is placed on the roof-top of a measurement bus (see Fig. 3b) 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 measurements points. The cellular base station archive [14] is used to select the candidate base stations. The selection criteria for a candidate base station focuses on the availability of 3 PCIs transmitted at 796 MHz from different sectors of the transmitting LTE antenna and around which a suitable trajectory can be made. Considering this, two base stations were

selected corresponding to two distinct signal reception environments - Urban and Suburban. The Urban candidate base station exists in an environment where there is higher multipath and frequent signal blockages due surrounding buildings. The Suburban candidate base station exists in an environment with higher LOS conditions and reduced multipath.

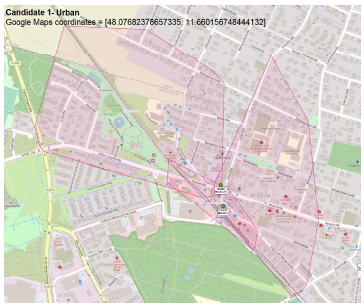


(a) Block diagram

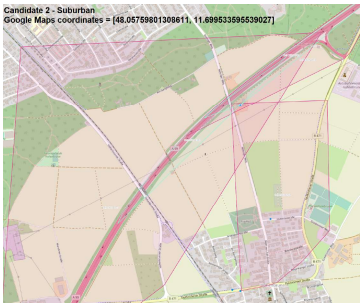
(b) Roof top of measurement van

(c) Inside view of measurement van

Figure 3: Experimental Setup



(a) Candidate 1 - Urban



(b) Candidate 2 - Suburban

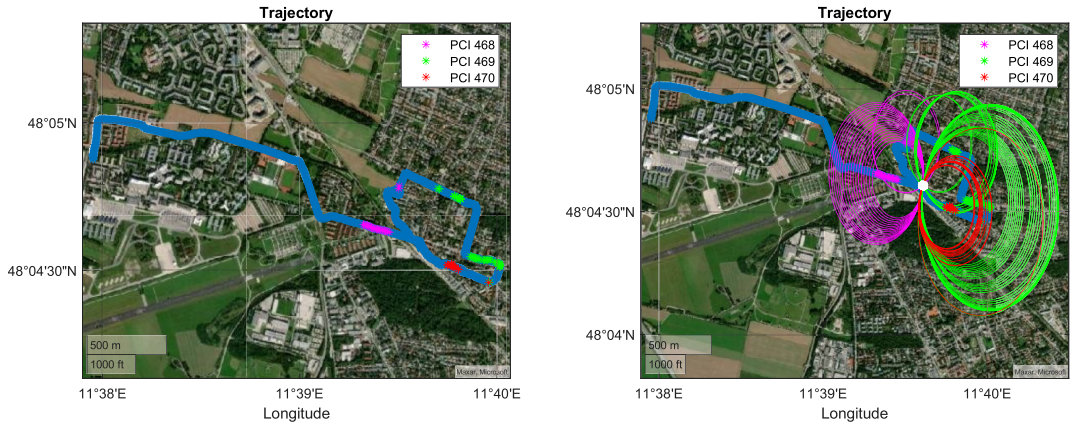
Figure 4: Candidate LTE base stations

EXPERIMENTAL RESULTS

In this section, the results of the calibration exercise of the two candidate LTE BSs are presented. Fig. 5(a) and 6(a) show the receiver trajectory, as taken from MuSNAT SPP solutions, for candidate BS 1 and 2 respectively. Also indicated within Fig. 5(a) and 6(a) are the trajectory points at which the LTE signal was successfully tracked with different colors corresponding to different PCIs. It can be observed that there exists a correlation between the spatial distribution of the PCI coverage areas, as indicated in Fig. 4, and the spatial distribution of the trajectory points at which different PCIs are tracked. This can be associated with the typical uniform cell coverage strategy of a cellular BS in which the cellular signal is transmitted using 3 antenna elements, each spanning an angle of 120° [15]. Fig. 5(b) and 6(b) show the filtered LTE range, computed as the difference between the SPP receiver position and the estimated LTE transmitter position, as a locus around each LTE track point. The intersection region of all the loci bound the estimated LTE transmitter position which is depicted by the white colored points. In comparison to Fig. 6(a), Fig. 5(a) shows a larger concentration of LTE track points along the trajectory paths where the LTE signal was successfully received. This can be justified by considering the receiver velocity across the Urban and Suburban landscapes. Since, the velocity of the measurement bus was much higher on the highway road tracks of the Suburban landscape, we see a less concentration of LTE track points. The LTE signal visibility is however better in the Suburban landscape where the LTE signal is tracked for a larger portion of the whole trajectory.

Table 2 shows the filter parameters used for each candidate BS. The initial position of the LTE base station was set to the Google Maps coordinates biased by an offset of 10 m in both X and Y directions. Table 3 summarizes the final filter state results for both the candidate BS. For each case, the position difference is computed against the Google Maps coordinates as given in Fig. 4. For the Urban case, it can be observed that the position difference in the Y direction is much less than the position difference in the X direction. This can be justified by analyzing the trajectory of the receiver around the BS which is highly co-linear along the Y axis and covers both the positive and negative sides of the axis with respect to the base station as origin. For the Suburban case, the position error in both X and Y directions is within ±5 m. This can be

associated to the trajectory of the receiver as covering both the orthogonal axes with similar distributions. The clock bias for both the base stations is estimated to be within ±6 ms. The estimated clock drift for the Suburban base station is four times higher than the Urban station. With the absence of a prior knowledge and hence a ground truth about the base station clocks, the accuracy of the estimated clock solutions cannot be justifiably inferred.



(a) Receiver trajectory from GNSS SPP

(b) Locus applied on each LTE received point with radius equal to modeled LTE range

Figure 5: LTE base station calibration results

(a) Receiver trajectory from GNSS SPP

(b) Locus applied on each LTE received point with radius equal to modeled LTE range

Figure 6: Suburban LTE base station calibration results

Table 2: Kalman filter parameters

Parameter	Symbol	Value	
		Urban	Suburban
Initial position state variance [m^2]	σ_x^2, σ_y^2	1x10^3	1x10^3
Initial clock bias state variance [m^2]	$\sigma_{\delta\tau}^2$	3x10^4	2x10^4
Initial clock drift state variance [m^2]	$\sigma_{\dot{\delta\tau}^2}$	2x10^1	2x10^1
Measurement noise variance [m^2]	σ_ρ^2	30^2	30^2

Table 3: Final states results

State-variable	Symbol	Value	
		Urban	Suburban
Pos. diff. X [m]*	δx	−8.9161	−0.2260
Pos. diff. Y [m]*	δy	0.2613	−4.7613
Clock bias [ms]	$\delta\tau_l$	−4.9553	5.7900
Clock drift [ns/s]	$\delta\dot{\tau}_l$	2.5906	12.1354

*Pos. differences with respect to Google Maps coordinates.

CONCLUSIONS AND WAY FORWARD

Overall, this paper presents the implementation of the LTE synchronization signal within a GNSS-based signal processing architecture, and provides a comparison of a 10 ms long combined PSS-SSS signal as local replica against a 10 ms long SSS only replica, showing that the latter presents better cross-correlation performance with respect to the combined PSS-SSS sequence, and therefore is the way forward. In future, the implementation of the CRS signals is expected to be employed as a higher bandwidth can potentially provide better LTE ranging results [7]. Additionally, the paper presents the preliminary results of calibrating LTE base stations using GNSS PVT solutions and LTE pseudoranges recorded using the same antenna module. The results indicate a convergence of state-variables, validating the positive observability of the estimation problem. However, the accuracy of the final solution can be further improved by considering multiple modifications. Firstly, the GNSS PVT solution is computed using SPP which contributes to a forward carrying error within the filter inputs. For future experiments, a PVT solution computed using GNSS Real Time Kinematic shall be sought to minimize this forward carrying error. Secondly, the filter uses a very simple model for the estimation process which assumes the signal for all PCIs to be transmitted by the same antenna element and hence also disregards the small clock biases that can practically exist between the received PCI signals [11]. 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. Furthermore, the proprietary software is sought to be extended with AGC control to account for a larger dynamic gain for receiving LTE signals without saturation of the front-end.

ACKNOWLEDGEMENTS

This activity was carried out at Institute of Space Technology and Space Applications (ISTA) at Universität der Bundeswehr München as part 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).

References

[1] Stars, Above Us Only, "Exposing gps spoofing in russia and syria," 2019. [Online]. Available: https://www.c4reports.org/aboveusonlystars

[2] K. Shamaei, J. Khalife, and Z. M. Kassas, "Exploiting lte signals for navigation: Theory to implementation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2173–2189, 2018.

[3] M. Arizabaleta, H. Ernest, J. Dampf, T. Kraus, D. Sanchez-Morales, D. Dötterböck, A. Schütz, and T. Pany, "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)*, 2021, pp. 2733–2753.

[4] 3GPP consortium. Home page. [Online]. Available: https://www.3gpp.org

[5] S. Fischer, "Observed time difference of arrival (otdoa) positioning in 3gpp lte," *Qualcomm White Pap*, vol. 1, no. 1, pp. 1–62, 2014.

[6] M. Driusso, F. Babich, F. Knutti, M. Sabathy, and C. Marshall, "Estimation and tracking of lte signals time of arrival in a mobile multipath environment," in *2015 9th International Symposium on Image and Signal Processing and Analysis (ISPA)*, 2015, pp. 276–281.

[7] 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 *Proceedings of the 2017 International Technical Meeting of the Institute of Navigation*, 2017, pp. 1256–1268.

[8] 3GPP Consortium. Evolved universal terrestrial radio access (e-utra); base station (bs) radio transmission and reception. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2412

[9] 3GPP consortium. Evolved universal terrestrial radio access (e-utra); physical channels and modulation. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2425

[10] Z. M. Kassas and T. E. Humphreys, "Observability analysis of collaborative opportunistic navigation with pseudorange measurements," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 260–273, 2013.

[11] Z. M. Kassas, "Navigation with cellular signals of opportunity," *Position, Navigation, and Timing Technologies in the 21st Century*, 2020.

[12] PCTEL, "Coach™ ii 5g cellular gnss multiband antenna." [Online]. Available: https://www.pctel.com/antenna-product/coach-ii-gnss-multi-band-antenna-dual-port/

[13] N. Instruments, "Usrp 2974." [Online]. Available: https://www.ni.com/de-de/support/model.usrp-2974.html

[14] Cell mapper. [Online]. Available: https://www.cellmapper.net/

[15] Evolved Universal Terrestrial Radio Access (E-UTRA), "3rd generation partnership project: Technical specification group radio access network (release 8)," 2007-02.