Comparative Results Analysis on Positioning with Real LTE Signals and Low-Cost Hardware Platforms

José A. del Peral-Rosado, Juan M. Parro-Jiménez,
José A. López-Salcedo and Gonzalo Seco-Granados
Universitat Autònoma de Barcelona (UAB)
Bellaterra, Spain
Email: {JoseAntonio.DelPeral, JuanManuel.Parro,
Jose.Salcedo, Gonzalo.Seco}@uab.cat

Paolo Crosta, Francesca Zanier
and Massimo Crisci
European Space Agency (ESA)
Noordwijk, The Netherlands
Email: {Paolo.Crosta, Francesca.Zanier,
Massimo.Crisci}@esa.int

***Abstract*—Long Term Evolution (LTE) networks are rapidly deploying around the world, covering the needs of high data rates demanded by many applications. Still, less attention is paid on the positioning capabilities specified in the LTE standard. Thus, an experimental LTE positioning receiver is presented to assess the positioning accuracy in commercial LTE deployments. This receiver is based on a software defined radio (SDR) and a low-cost radio-frequency (RF) front-end, such as the universal software radio peripheral (USRP) or a DVB-T dongle with the Realtek RTL2832U chipset. These two platforms are then used to capture and post-process real LTE signals generated in the laboratory. The positioning results obtained show the viability on the use of this experimental SDR LTE positioning receiver with low-cost hardware platforms for commercial LTE networks.**

I. Introduction

The adoption and demand of localization applications is notably increasing due to the massive use of mobile devices every day. Most of these devices are usually connected to cellular networks that provide communication services, such as messaging, calls or Internet access with high data rates. But, many applications also require the support of location-based services (LBS). These services typically rely on Global Navigation Satellite Systems (GNSS) or WiFi-based positioning systems. However, the reduced satellite signal availability in urban and indoor environments, or the reliability and accuracy issues of WiFi databases prevent these systems from achieving ubiquitous and precise positioning. Therefore, complementary technologies need to be adopted to fulfil the positioning requirements of the LBS applications. This is the case of the Long Term Evolution (LTE), which is the current standard for mobile communication systems. The LTE standard [1] already specifies a positioning method based on the observed time difference of arrival (OTDoA) technique, in order to improve the positioning capabilities of cellular networks. In addition, this method uses dedicated and synchronised OFDM (Orthogonal Frequency Division Multiplexing) signals, called positioning reference signals (PRS). Thus, the combined use of the available positioning technologies leads to the concept of hybrid navigation, as a means to provide anywhere and anytime positioning.

The hybridisation of GNSS with cellular technologies has been actively studied, such as from using the Global System for Mobile communications (GSM) in [2] to LTE in [3]. However, few of these hybrid positioning systems have been successfully implemented in commercial deployments, and none of them considering a hybrid GNSS and LTE OTDoA solution. An example is the combination of the assisted Global Positioning System (A-GPS) and CDMA (Code Division Multiple Access) cellular systems [4], which adopt the advanced forward link trilateration (AFLT) technique. Still, these commercial systems cannot cope with the new challenges imposed by user applications and legal mandates. For instance, they cannot identify the specific building and floor corresponding to a mobile device location, as it is reported in [5], which may be one of the future requirements of the enhanced 911 (E911) mandate for indoor location [6]. Thus, the attractive features of LTE for positioning [7] are expected to enhance current commercial hybrid systems.

Despite the rapid commercial deployment of LTE networks around the world, few contributions have studied standalone OTDoA positioning with real LTE signals, such as [8] in a field demonstration and [9] in a laboratory test. Therefore, the aim of this paper is to assess an experimental OTDoA positioning platform for commercial LTE deployments. For this purpose, a software-defined radio (SDR) receiver is used in order to obtain a very flexible architecture. The SDR platform is typically formed by a reconfigurable radio-frequency (RF) front-end, which can have multiple operating bands. This feature is especially convenient for LTE because of the high number of operating bands specified in the standard [10], which are up to 40 in its Release 9. For instance, the SDR LTE positioning receiver can be used with the universal software radio peripheral (USRP) [11], as in [9]. Although the USRP is already an inexpensive platform, a very low-cost solution can be found by using a DVB-T (Digital Video Broadcasting–Terrestrial) dongle equipped with the Realtek RTL2832U chipset. This chipset can be reconfigured in order to capture RF signals at carrier frequencies from few MHz up to 1.7 GHz (depending on the tuner). Given this functionality, the DVB-T dongle can be used with different SDR receivers for multiple purposes, being this system called RTL-SDR. Therefore, this paper assesses the positioning performance of these low-cost hardware platforms for their use in commercial LTE networks. Indeed, the flexibility of these platforms has interesting applications, such as prototyping of mass-market receivers, testing or educational purposes. These capabilities could also be exploited to integrate both GNSS and LTE receivers towards an experimental solution for hybrid navigation.

978-1-4799-6529-8/14/$31.00 ©2014 IEEE

This paper is structured as follows. The fundamentals of SDR receivers and a brief description of the hardware platforms is provided in Section II. The experimental SDR LTE positioning receiver is presented in Section III. The performance results of the receiver using the USRP and the DVB-T dongle are assessed in Section IV, before drawing the conclusions in Section V.

II. Fundamentals of SDR Receivers

A software-defined radio is a RF equipment with most of its signal treatment performed by a digital signal processor (DSP) that can be controlled and configured by software. In this sense, common functionalities, such as filtering, demodulation or mixing, are implemented in a digital manner instead of in an analogue circuit.

In general, the design goal of a SDR hardware is to be as reconfigurable as possible at the lowest cost. To achieve this, most of the SDR platforms use an homodyne concept that consists in reducing the RF adaptation chain by converting the signal directly from/to baseband. Note that any intermediate conversion step is skipped in this architecture thus reducing the number of elements to be included in the RF chain. The RF chain of a SDR receiver is typically divided in two different stages. Firstly, a RF front-end amplifies, mixes and filters the signal. Note that these functions can be configured by selecting the gain, the frequency of the local oscillator (LO) or the filter bandwidth. Once the signal has been adapted, it is sampled and passed to a DSP module that consists of a field-programmable gate array (FPGA) and/or a host computer. A FPGA is commonly required to carry out high rate operations, such as filtering and decimation of signals at high sampling frequencies. The lower rate operations or storage are implemented in the host computer.

Due to the lack of intermediate stages for signal adaptation, the SDR architectures suffer from different problems, such as LO leakage caused by a bad isolation between the LO and the low-noise amplifier (LNA), which in turn results in a DC offset in the baseband signal. Another common problem is occasioned by the non-linearity of the components of the RF chain that produces harmonic signals, which are added to the final signal. On the other hand, the use of SDR presents several benefits that make them attractive in several applications. For instance, their large degree of reconfigurability makes them suitable for research or prototyping.

A. USRP platform

The USRP is a family of SDR products manufactured by Ettus [11] that has become one of the most popular in the recent years. Although they are intended to be a low-cost SDR solution, there are also high performance products designed for more demanding applications. Most of the USRP are computer-hosted devices for post-processing of the recorded signals. For the sake of reconfigurability, this SDR consists of two different blocks. The first is a RF front-end chain that is responsible of the up/down-conversion of the signals, including amplification and filtering. This part, known as daughterboard, is interchangeable for the different user needs, such as frequency band, gain or number of channels. The daughterboard is attached to a second board that carries out the sampling of the signals and incorporates a FPGA for signal processing. This board, known as motherboard, also includes the corresponding interface with the host. The user is able to receive baseband signals using this SDR with a configurable sampling rate up to 25 MSps and different resolution from 8 to 32 bits per sample. The center frequency of the signal will depend on the chosen daughterboard.

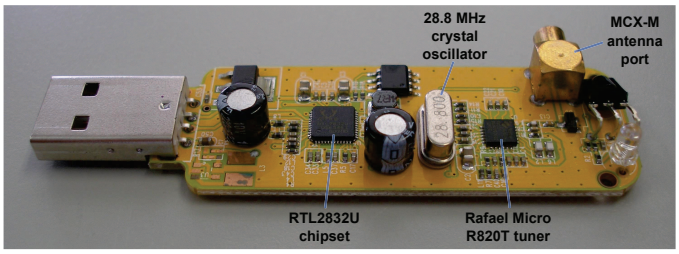


Fig. 1. DVB-T dongle with RTL2832U and Rafael Micro R820T tuner.

B. DVB-T dongle with Realtek RTL2832U chipset

The RTL2832U is a chipset manufactured by Realtek as DVB-T COFDM (Coded OFDM) demodulator that is present in a great number of the DVB-T dongles available in the market, such as the one shown in Figure 1. However, it was discovered by reverse engineering that the chip allows sending the raw baseband samples with the objective of receiving the DVB-T signals. The chip is able to stream the I/Q samples at a maximum rate of 3 MSps and with a precision of 8 bits per sample. This sampling rate is sufficient for receiving LTE, DVB-T, FM or some satellite navigation signals. The frequency range of the device depends on the tuner used. For instance, the Rafael Micro R820T tuner (shown in Figure 1) has a frequency range from 24 MHz to 1766 MHz.

C. Usage considerations of the USRP and RTL-based dongle

The resulting performance of a certain application is highly dependent on the components of the SDR hardware. While a USRP N210 plus a DBSRX2 daughterboard costs around 1.9K$, a RTL2832U-based dongle costs only 20$. Therefore, the performance of the USRP is expected to be much above the RTL-based dongle. The specifications of each SDR are in line with this statement. According to the datasheet of the USRP N210 [11], its clock has an accuracy of ± 2.5 ppm. In the case of a RTL2832U-based dongle with a Rafael Micro 820T tuner [12], the typical clock accuracy is ± 30 ppm. However, the reduced price of the Realtek chipset makes it attractive for research applications, such as in [13], and could be taken as a reference for the performance of a mass-market receiver. In addition, the dongle is more portable than the USRP, because it is fully powered through the USB port.

III. Experimental SDR LTE Positioning Receiver

The hardware platforms presented in the previous section can be used as a low-cost solution to demonstrate the positioning capabilities of the LTE technology. Thus, an experimental SDR LTE positioning receiver is designed and developed in MATLAB to post-process the recorded samples using a low-cost RF front-end. This prototype receiver is able to acquire and track the received signals from the different base stations

(BSs), in order to later calculate the position. In this section, the LTE received signal and the main synchronization errors are described, and the receiver architecture is presented.

A. LTE received signal and synchronisation errors

The LTE standard [1] specifies multicarrier signals based on the OFDM modulation for the downlink transmission, defined as

$$x_{\mathrm{c}}(t) = \sqrt{\frac{2C}{N}} \sum_{n=0}^{N-1} b(n) \cdot \exp\left(j \frac{2\pi n t}{T}\right), \quad 0 < t < T, \quad (1)$$

where C is the power of the band-pass signal, N is the total number of subcarriers, $b(n)$ is the complex-valued symbol transmitted at the n-th subcarrier, and the OFDM symbol period T is equal to 66.67 µs, which corresponds to a subcarrier spacing $F_{\mathrm{sc}} = 1/T$ of 15 kHz. Considering the normal cyclic prefix (CP) configuration, the minimum resource allocation in LTE, called resource block (RB), is formed by 7 OFDM symbols and 12 subcarriers. The system bandwidth is scalable from 1.4 MHz to 20 MHz. In this paper, only the LTE pilot signals, formed by synchronisation and reference signals, are considered for acquisition, tracking and positioning purposes.

Given the wide adoption of OFDM signals in wireless communications systems, the synchronization errors and their effects are well studied in the literature, such as in [14] and [15]. The three main synchronization errors are:

- the symbol timing offset τ_ϵ, produced by the propagation delay and the clock time difference between transmitter and receiver,
- the sampling clock offset f_{s} with respect to the sampling frequency F_{s}, and
- the carrier frequency offset f_0, formed by an initial offset F_0 and the frequency drift f_ϵ, which is the residual frequency deviation f_{c} of the oscillator from the carrier center frequency F_{c} plus the Doppler frequency shift f_{D} caused by the relative motion between transmitter and receiver.

Let us consider an additive white Gaussian noise (AWGN) channel, the LTE received signal is modelled in the frequency domain as

$$r(n) = \mathcal{F}\left\{x(m - \tau_0(m)) \cdot e^{j\theta(m)}\right\} + w(n), \quad (2)$$

where $\mathcal{F}\{\cdot\}$ is the discrete-time Fourier transform operator, $x(m)$ is the sampled version of the transmitted signal $x_{\mathrm{c}}(t)$ given F_{s}, $\tau_0(m)$ is the time delay, $\theta(m)$ is the phase shift, and $w(n)$ are the noise frequency samples, which are statistically uncorrelated with $w(n) \sim \mathcal{CN}\left(0, \sigma^2_{\mathbf{W}}\right)$. As it can be noticed in (2), both time delay and phase shift are varying over time due to the clock drift and the motion of the receiver. The time delay is modelled as

$$\tau_0(m) = \tau_\epsilon(m) + \tau_{\mathrm{f}}(m), \quad (3)$$

where $\tau_{\mathrm{f}}(m)$ is the time shift resulting from the sampling clock offset and the carrier frequency drift, defined as

$$\tau_{\mathrm{f}}(m) = (f_{\mathrm{s}}(m) + f_\epsilon(m)) \cdot \frac{F_{\mathrm{s}}}{F_{\mathrm{c}}}, \quad (4)$$

being the variation of f_{s} very small with respect to the variation of f_ϵ. The phase shift is expressed as

$$\theta(m) = \theta_0 + \frac{2\pi m f_0(m)}{N}, \quad (5)$$

where θ_0 is the initial phase shift and the frequency shift $f_0(m)$ is denoted as

$$f_0(m) = F_0 + f_\epsilon(m) = F_0 + f_{\mathrm{c}}(m) + f_{\mathrm{D}}(m). \quad (6)$$

Symbol timing, sampling clock and carrier frequency offsets may produce intersymbol interference (ISI) and/or interchannel interference (ICI), resulting in a severe degradation of the received signal, as it is described in [14] and [15]. Thus, time and frequency synchronization is required to avoid these effects. The following section presents the acquisition and tracking stages used to achieve coarse and fine synchronization of the signal, respectively.

B. Receiver architecture

The architecture of the SDR receiver is based on the cell detection, signal acquisition, signal tracking, and OTDoA positioning. Similarly to the platform described in [9], this architecture is completely independent of the RF front-end used, being only necessary to adjust few parameters, such as the format of the input samples. Thus, the SDR receiver can be tested with different hardware platforms in order to assess the quality of the captured signal.

1) Cell detection: The cell identification is the first step to access a LTE network. The pilot signals are dependant on the physical cell identity $N_{\mathrm{ID}}^{\mathrm{cell}}$ (cell ID) of the BSs. Thus, the cell ID has to be detected in order to coherently synchronize the received signal. The LTE standard [1] specifies

$$N_{\mathrm{ID}}^{\mathrm{cell}} = 3 \cdot N_{\mathrm{ID}}^{(1)} + N_{\mathrm{ID}}^{(2)}, \quad (7)$$

where $N_{\mathrm{ID}}^{(1)}$ is the cell ID group and $N_{\mathrm{ID}}^{(2)}$ is the cell ID sector within the group. The cell detection is performed by using the primary and secondary synchronization signals (PSS and SSS, respectively), as it is shown in Figure 2. First, the start of the PSS symbol is found by using the autocorrelation of the received signal in the time domain, as it is proposed in [16], which exploits the symmetry of the PSS. Once the CP is removed and the fast Fourier transform (FFT) is computed, the cell ID sector is detected with the maximum of the cross-correlation between the received samples and the PSS sequences in the frequency domain. Then, the subframe and cell ID group is jointly detected by using the SSS sequences with a serial search algorithm, such as in [17, p. 76], where frequency shifts (with a resolution of one subcarrier) are considered. Finally, the cell ID is obtained with (7).

2) Signal acquisition: The coarse time and frequency synchronization is performed with the signal acquisition, shown in Figure 2. For this purpose, the synchronization signals and the cell-specific reference signals (CRS) are used given that the cell ID and start of the radio frame are already detected. The time delay and frequency shift are jointly estimated with the maximum likelihood (ML) criterion as

$$\begin{bmatrix}\hat{\tau}_0 \\ \hat{f}_0\end{bmatrix} = \arg\max_{\tau_0, f_0} \left\{ \left| \sum_{n=0}^{N-1} r(n - f_0) \cdot d^*(n) \cdot e^{j\frac{2\pi n \tau_0}{N}} \right|^2 \right\}, \quad (8)$$

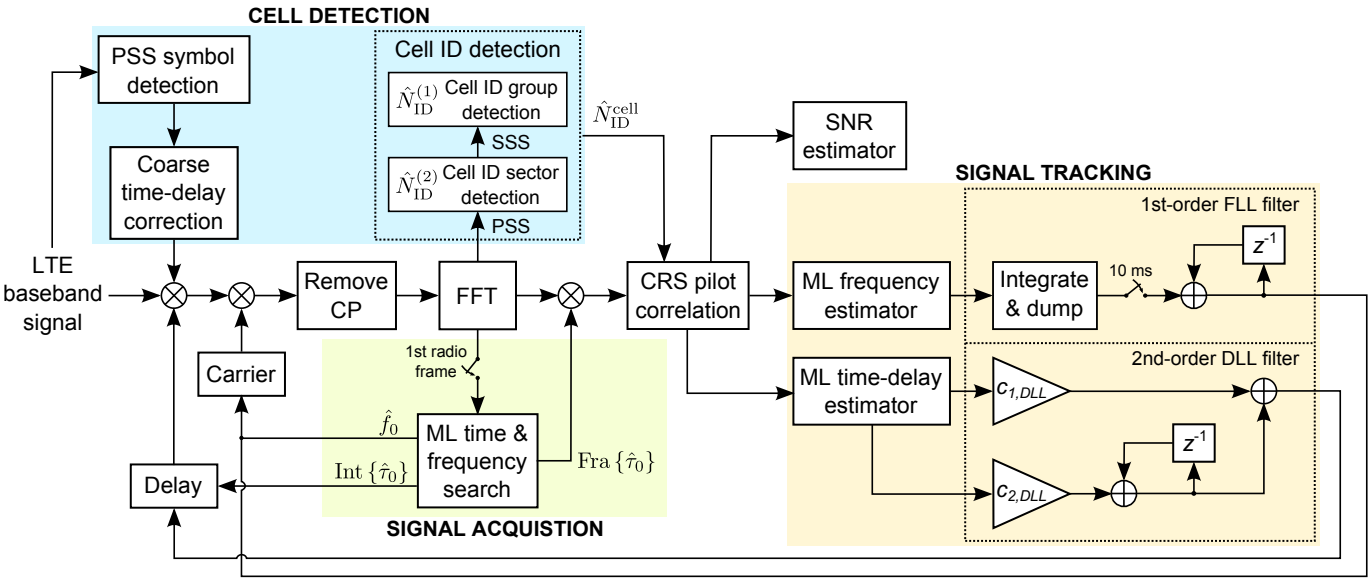


Fig. 2. Cell detection, signal acquisition and signal tracking stages of the experimental SDR LTE receiver.

where $d^*(n)$ is the conjugate pilot signal (formed by the pilot sequence and empty subcarriers). Both parameters are estimated for each pilot symbol during one radio frame of 10 ms, i.e. 44 symbols out of 140 symbols per radio frame. Then, these time-delay and frequency estimates are averaged. The acquisition is completed by compensating $\hat{f}_0$ and $\mathrm{Int}\{\hat{\tau}_0\}$ (integer part of $\hat{\tau}_0$) in the time domain, and $\mathrm{Fra}\{\hat{\tau}_0\}$ (fractional part of $\hat{\tau}_0$) in the frequency domain.

3) Signal tracking: Fine synchronization of the received signal is achieved by signal tracking. Time delay and frequency shift are estimated and filtered by using a tracking architecture based on a second-order delay lock loop (DLL) and a first-order frequency lock loop (FLL), as it is shown in Figure 2. Using one CRS symbol every slot of 0.5 ms, the time delay is estimated with the matched filter, and the frequency shift is estimated with the ML frequency estimator proposed in [18]. The coefficients of the DLL filter are calculated as in [17, p. 91]. A low-pass filter is implemented in the FLL by averaging the frequency estimates over one radio frame. Thus, the time delay is corrected every slot and the frequency shift every radio frame.

In parallel to the signal tracking, the signal-to-noise ratio (SNR) is estimated in order to be used as a metric of the receiver performance. The non-data-aided SNR estimator presented in [19] is implemented by taking advantage of the empty and pilot subcarriers of the LTE signal. Its SNR estimation $\hat{\rho}$ is written as

$$\hat{\rho} = \frac{\sum_{n\in\mathcal{N}_{\mathrm{a}}} |r(n)|^2}{\sum_{n\in\mathcal{N}_{\mathrm{e}}} |r(n)|^2} \cdot \eta - 1, \tag{9}$$

where the indexes of the N_{a} active pilot subcarriers are within the subset $\mathcal{N}_{\mathrm{a}}$, the indexes of the N_{e} empty subcarriers are within the subset $\mathcal{N}_{\mathrm{e}}$, and η denotes the noise-to-noise ratio (NNR). The empty subcarriers are located in the guard bands of the system bandwidth, e.g. $N_{\mathrm{e}} = F_{\mathrm{s}}/F_{\mathrm{sc}} - 12\cdot N_{\mathrm{RB}} - 1 = 55$ subcarriers for a sampling frequency F_{s} equal to 1.92 MHz and 6 RB. Considering the AWGN channel, the expected value of the NNR is defined by

$$\bar{\eta} = \frac{N_{\mathrm{e}}}{N_{\mathrm{a}}}. \tag{10}$$

4) OTDoA positioning: The determination of the position is based on the difference in the arrival times of the downlink radio signals from multiple BSs, in this case, between the serving BS (i.e. most powerful BS) and the neighbour BSs. OTDoA positioning is then computed with the output of the ML time-delay estimates by means of a trilateration technique, based on Fletcher's version of the Levenberg-Marquardt algorithm [20]. This technique is already implemented in MATLAB [21], and provides an independent position for every time differences.

C. Cramér-Rao bound for ranging

The Cramér-Rao bound (CRB) is used to assess the achievable ranging accuracy of the ML estimator implemented in the SDR receiver. This bound is derived from the general definition given by [22], and it is attainable for moderate to high SNR levels. Thus, considering equi-powered CRS, the CRB for time-delay estimation over AWGN channel is expressed as

$$\mathrm{CRB}(\tau) = \frac{T^2}{8\pi^2 \cdot \mathrm{SNR} \cdot \sum_{n\in\mathcal{N}_{\mathrm{a}}} n^2}. \tag{11}$$

IV. Results and Performance Assessment

The performance of the experimental SDR receiver with two low-cost hardware platforms, i.e. based on the URSP and the DVB-T dongle, is assessed in this section by using real LTE signals emulated in the laboratory. These RF signals are generated with a LTE network emulator, then they are captured with the USRP and with the DVB-T dongle, and finally they are post-processed with the SDR receiver in MATLAB. The tracking and ranging results obtained using both hardware platforms are compared and analysed considering their tentative application for positioning in commercial LTE networks.

A. Test-bed description

The experimental test-bed is based on the emulation of a LTE network with a static user equipment and AWGN channel. These conditions are set in order to strictly assess the performance obtained using each hardware platform. In addition, the capabilities of the USRP are aided with an external reference clock. The setup is performed with equipment of the European Navigation Laboratory (ENL) at the European Space Agency (ESTEC, The Netherlands). The test-bed is based on the Spirent E2010S network emulator, Spirent VR5 HD spatial channel emulator, a splitter, an active hydrogen maser to generate 10-MHz reference signal, USRP equipped with DBSRX2 daughterboard, DVB-T dongle with the RTL2832U chipset and the Rafael Micro R820T tuner, and a host computer.

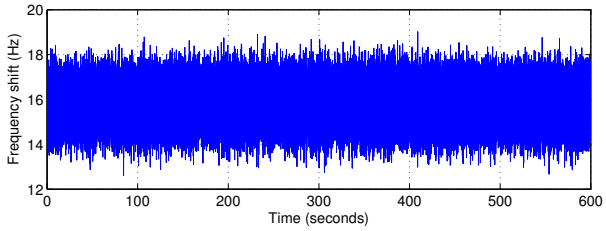
First, the LTE network emulator generates the RF signal of one or multiple BSs with a system bandwidth of 1.4 MHz. Then, the channel emulator introduces power and delay differences among the RF signals of the different BSs according to a certain scenario. The carrier center frequency F_{c} is set to 806 MHz or to 816 MHz, which correspond to band 20 and E-UTRA absolute radio frequency channel numbers (EARFCN) equal to 6300 and 6400, respectively. These specifications are already used in deployed LTE networks and fit with the operation range of both hardware platforms. The signal power at the output of the network emulator is set by considering the reference signal transmit power (RSTP), which is the average power of the CRS within a subframe [23]. The resulting signal is split in order to feed the USRP and the dongle (connected with a MCX-M to SMA-F cable). The insertion losses of the splitter and the cables are estimated to be around 8 dB. Then, both equipment are connected to the host computer, i.e the USRP through the Gigabit Ethernet port, and the dongle through the USB port. Finally, the USRP is controlled by using an example application of the USRP hardware driver (UHD), called `rx_samples_to_file` [24], and the dongle is controlled by using the RTL-SDR driver `rtl_sdr` developed by Osmocom [25]. The sampling frequency is set in both drivers to 2 MHz, and the gain is adjusted manually.

Once the RF signal is captured and stored in the host computer, the post-processing starts by loading the received signal in MATLAB. A few seconds at the beginning of the file are skipped in order to avoid instabilities of the local oscillator. The real and imaginary parts of the signal are deinterleaved, and the sampling frequency of 2 MHz is downsampled to 1.92 MHz, which preserves the LTE subcarrier spacing of $F_{\mathrm{sc}} = 15$ kHz. The SDR receiver is then executed in order to acquire and track the LTE signal, and finally calculate the user position.

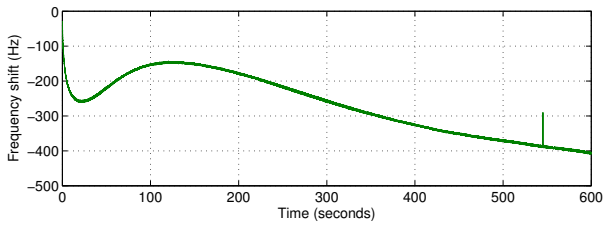
B. Frequency stability

Given this test-bed, the frequency stability of both hardware platforms is compared in this section. The capabilities of the USRP are fully exploited by enabling the external clock reference, which can be obtained by using a very stable clock (as in this case) or using a GNSS receiver. In contrast, the DVB-T dongle uses a crystal oscillator with a poor frequency stability. Thus, the comparison between platforms is aimed to determine if both solutions can be used for accurate positioning.

For this test, the network emulator is configured with a RSTP power of -50 dBm for only one BS, and the RF gain



(a) USRP (RF gain = 16 dB)



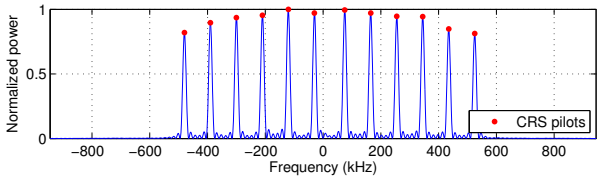
(b) Dongle (RF gain = 2.7 dB)

Fig. 3. Comparison of frequency estimates averaged over a 10-ms radio frame using (a) USRP and (b) dongle hardware platforms.

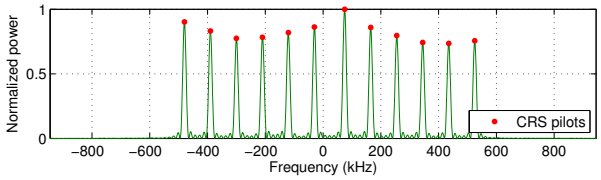
is set to 16 dB for the USRP and 2.7 dB for the dongle. After a successful cell detection, the signal acquisition is performed during one radio frame of 10 ms. The coarse frequency synchronization results in an initial carrier frequency offset F_0 of 133 Hz or 0.17 ppm by using the USRP, and -55.6 kHz or -68.99 ppm by using the dongle. Since this high frequency offset is expected from the dongle, the frequency search is performed within 6 subcarriers from the central frequency. Fine frequency synchronization is then obtained in the tracking stage. The sampling period T_{L} of the DLL is equal to 0.5 ms, and its noise bandwidth B_{L} is set to 5 Hz. As it is shown in Figure 3, the frequency shift is tracked over 10 minutes using the same SDR receiver for both hardware platforms. Since the signal is emulated in static conditions, the deviation of the frequency shift is completely produced by the oscillator of the equipment. In the USRP case, there is almost no frequency deviation from the initial offset due to the high stability of both network emulator and active hydrogen maser (used as external reference clock). In contrast, the crystal oscillator used in the dongle has a high frequency drift, as it can be seen during the first three minutes. Once the oscillator is more warm after five minutes, the carrier frequency offset of the dongle is more stable. Still, a frequency deviation equal to 150 Hz is obtained over five minutes. In addition, a sporadic frequency glitch is found around 545 second of the signal capture.

C. Normalized CRS frequency response

Once the SDR receiver is tracking the signal, the frequency response of the CRS symbols can be computed in the same test-bed. This response is important in order to assess the time-delay estimates obtained by using the CRS pilots with respect to the expected ranging accuracy. The frequency response is estimated with the power of the received signal after the FFT. To obtain this result, the FFT is computed with $10N$ samples, i.e. the received signal is oversampled ten times. Using 16 CRS symbols over one radio frame, the signal is squared and averaged in the frequency domain between the same subcarriers of the different symbols. The resulting normalized average signal power is shown in Figure 4. As it can be seen,



(a) USRP (RF gain = 16 dB)



(b) Dongle (RF gain = 2.7 dB)

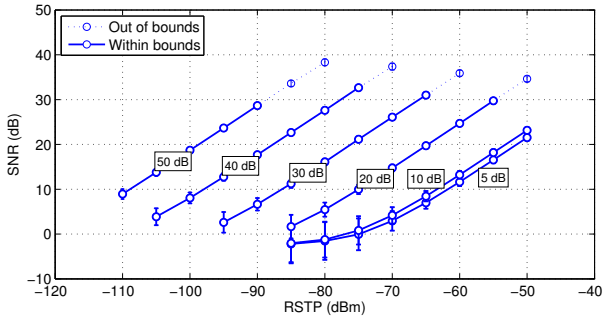
Fig. 4. Comparison of the normalized and averaged signal power of CRS symbols over a radio frame using (a) USRP and (b) dongle hardware platforms.

the frequency response is different for each platform, and the CRS pilots are not equi-powered. This is the result of the RF filter response that modifies the flat spectrum expected. These frequency responses should be considered for the assessment of the positioning accuracy obtained with each platform.

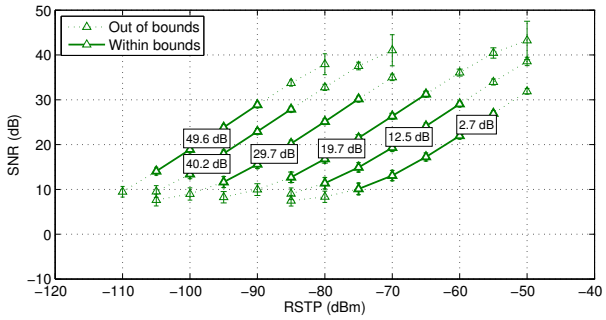
D. Gain performance

An important aspect on the use of the USRP and the dongle is the minimization of the quantization error produced by the ADC for a certain received signal power. The ADC has a range of input values that are quantized with a certain granularity or precision, which is defined by the number of quantization bits used per sample. Thus, there is a trade-off between the accuracy of the quantization and the amount of data generated by the ADC. The precision of the dongle is fixed to 8 bits per sample, while the ADC of the USRP N210 (with DBSRX2 daughterboard) allows 8 bits and 16 bits per sample. In order to minimize the round-off error, the USRP is configured with 16-bit option, even if it implies the double amount of data with respect to the 8-bit option. The rest of the quantization error is produced due to the truncation of those input values out of the range of the ADC. The automatic gain control (AGC) is aimed to detect the input signal level and to set the gain before the ADC, in order to reduce this quantization error. The USRP and the dongle have built-in AGC modules. However, they have problems due to the presence of blank symbols during the LTE signal transmission. Since no user data is transmitted in this test-bed, there are unused symbols during the radio frame. The detection of these blank symbols and a large response time may lead the AGC to set inappropriate gain levels. Thus, this section is aimed to characterize the adequate gain value that maximize the SNR. In this sense, upper and lower SNR thresholds or bounds can be defined for an implementation of the AGC in the SDR receiver.

The characterization of the gain performance is computed by setting several input signal levels for every gain in both platforms. The input levels are defined by a range of RSTP between -50 dBm and -110 dBm with steps of 5 dB in the network emulator. For each input level, a gain between 0 and 50 dB is set in both platforms. The gains defined in the USRP are $G = \{5, 10, 20, 30, 40, 50\}$ dB, and in the dongle are $G = \{2.7, 12.5, 19.7, 29.7, 40.2, 49.6\}$ dB. In order to simplify the experiment, the signal is acquired for the highest input level, and the RSTP is decreased 5 dBm every ten seconds during signal tracking. Then, the SNR estimates are averaged over five seconds for each RSTP value. The resulting mean and standard deviation of the SNR estimates are shown in Figure 5 for every RSTP and gain using both platforms. These results can be divided into a linear SNR region, where the SNR decreases linearly with the input signal level, and upper and lower SNR regions, where the SNR estimation is degraded with respect to the expected value. This is because the SDR receiver is upper bounded by the saturation of the amplifier, and it is lower bounded by the loss of lock of the tracking loops. These two bounds can be set by assessing the standard deviation of the SNR estimates. Comparing the different values, the expected standard deviation should be lower for a higher RSTP value. In case this condition is not fulfilled, the SDR receiver is out of the SNR bounds. The SNR upper bound is around 30 dB in both platforms, but the SNR lower bound is around 0 dB for the USRP and around 10 dB for the dongle. This shows the higher sensitivity offered by the USRP in comparison with the dongle. Therefore, these bounds should be considered for an implementation of the AGC in the SDR receiver, i.e. by increasing the gain when SNR estimates are below 30 dB.



(a) USRP



(b) Dongle

Fig. 5. Comparison of SNR estimates averaged over five seconds with respect to the RSTP using (a) USRP and (b) dongle hardware platforms. Error bars depict the standard deviation of the SNR estimates over five seconds. Every gain value is specified in a box over the resulting curve.

E. Ranging performance

The ranging performance of the SDR receiver is assessed in this section by computing the root-mean-square error (RMSE) of the ML time-delay estimates obtained during the previous experiment. The results of both platforms are compared with the CRB expression in (11), by sorting the average SNR

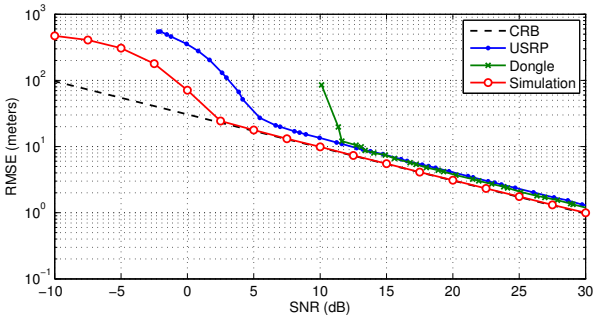


Fig. 6. RMSE of the time-delay estimates obtained over five seconds using both hardware platforms as a function of the SNR.

values for every gain and RSTP. As a reference, the RMSE of the time-delay estimates is also obtained for a LTE signal simulated in MATLAB. The resulting RMSE values are shown in Figure 6. As it can be seen, the ML estimator attains the CRB when using the simulated signal, in contrast there is a gap of around 2 dB between the CRB and the RMSE obtained with the USRP and the dongle. This is mainly due to the ideal rectangular shape of the spectrum generated in MATLAB, which differs from the frequency response obtained with both platforms, as it was discussed in Section IV-C. In addition, the RMSE obtained with the dongle is slightly lower than the RMSE obtained with the USRP. However, the SNR threshold of the USRP platform is between 0 and 5 dB, being lower than the SNR threshold of the dongle plaform, which is between 10 and 15 dB. These results are in accordance with the SNR lower bound shown in the previous section.

F. Positioning performance

The positioning capabilities of the low-cost hardware platforms are finally assessed by computing the position errors in a realistic scenario. For this purpose, a commercial LTE network in the municipality of Leiden, The Netherlands, is emulated in the laboratory. This network is chosen given the information provided in [26], such as location of BSs, aiming direction of the antennas or carrier center frequency. Considering four BSs transmitting at 816 MHz, the LTE scenario emulated is shown in Figure 7. In order to focus on the performance of the hardware platforms, multipath is not considered, thus there is only line-of-sight (LoS) propagation between BSs and user. This assumption can be realistic if the location of the receiver antenna is assumed to be on the roof of a high building, such as *Pieterskerk* in Leiden, as in this case.

The scenario is emulated by using two E2010S network emulators to generate the RF signals of four BSs, and the VR5 channel emulator to set the power and delay of the received signals. These power and delay values are determined by considering the network topology shown in Figure 7 and assuming the propagation models recommended in [27] for a macro cellular deployment in urban areas. The transmit power of the BSs is assumed to be equal to 25 dBm, and log-normally distributed shadowing with standard deviation of 10 dB is added to the path loss model. The received power results in $P_{\mathrm{rx},k} = \{-75.7, -80.8, -89, -97.3\}$ dBm from each BS, where $k = \{1, 2, 3, 4\}$, leading to $\mathrm{SNR}_k = \{29.2, 24.1, 16, 7.6\}$ dB for a 6-RB CRS bandwidth of 1.02 MHz. The relative delays between BSs are calculated as

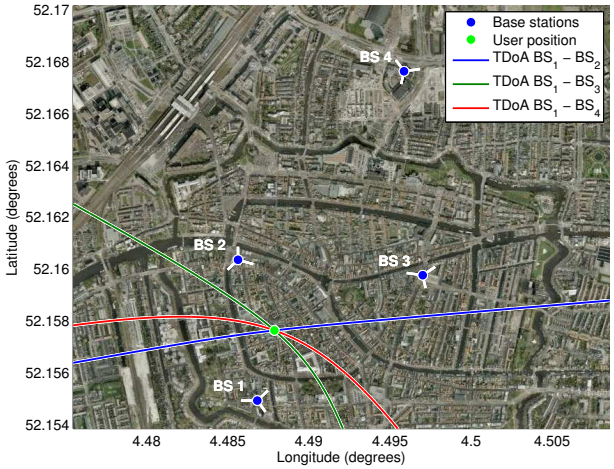


Fig. 7. Scenario emulated based on a commercial LTE network in the municipality of Leiden, The Netherlands.

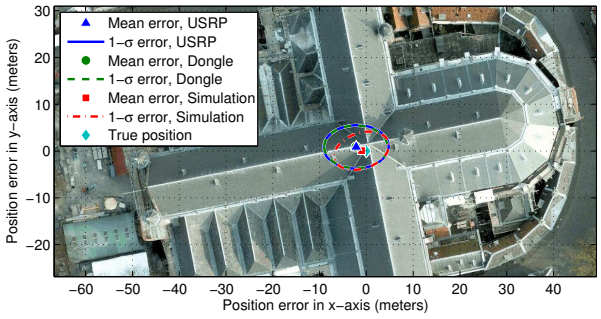


Fig. 8. Position errors of the SDR receiver with respect to the user position.

$t_d = (d_i - d_1)/c$, where the distances between BSs and user position are $d_k = \{309.5, 339.9, 668.4, 1238.8\}$ meters, $i = \{2, 3, 4\}$, and c is the speed of light. Since the interface of the equipment has a delay resolution of 100 ns, the time differences between signals are approximated to $t_d \simeq \{0.1, 1.2, 3.1\}$ μs, which results in a position error of 1.03 meters.

Once the RF signals are generated, the SDR receiver is aided with the cell identities of the BSs. Then, the serving BS (i.e. one) is successfully acquired and tracked. The noise bandwidth B_{L} of the DLL is maintained to 5 Hz, but the sampling period T_{L} is increased to 10 ms, using only one CRS symbol with low interference every radio frame. The rest of BSs are tracked by using the same updates of the tracking loops corresponding to the serving BS, taking advantage of the network synchronization. The OTDoA measurements are obtained with the time-delay estimates for every BS. In absence of noise, these time differences draw hyperbolas that intersect in the user position, as it can be seen in Figure 7. The position errors obtained with both platforms are shown in Figure 8, in terms of mean and standard deviation of the position estimates with respect to the true position. The mean error using the USRP and using the dongle is equal to 2.36 and 2.4 meters, respectively. In addition, the ellipses drawn by the standard deviation for both platforms are very similar. In Figure 8, the results obtained with LTE signals simulated in MATLAB are also shown, confirming a mean error of 1.03 meters, due to the approximation of the relative delays introduced in the equipment. The position accuracy of the

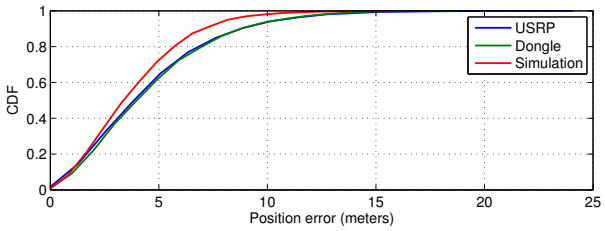


Fig. 9. CDF of the position errors using both hardware platforms in the LTE scenario emulated.

SDR receiver is finally obtained by computing the cumulative distribution function (CDF) of the position errors, as it is shown in Figure 9. In this emulated scenario, the receiver is able to achieve position errors around 5 and 10 meters for the 67% and 95% of the cases, respectively. The difference on the accuracy achieved with both equipments is almost negligible. The results obtained through MATLAB simulation indicate a slightly better accuracy, because it does not account for quantization, filtering and calibration errors found with real LTE signals. The positioning performance obtained show the viable use of these low-cost hardware platforms in commercial LTE networks, such as the network emulated in Leiden. Thus, it is left for future work the use of the SDR positioning receiver with LTE field measurements.

V. Conclusions

This paper has compared the positioning performance of a software-defined radio (SDR) receiver using real signals from a Long Term Evolution (LTE) system by means of two low-cost hardware platforms, in order to assess their potential use in commercial LTE networks. The LTE signals are emulated in the laboratory and are captured in parallel with the universal software radio peripheral (USRP) hardware and a DVB-T dongle with the Realtek RTL2832U chipset. The results have shown the higher sensitivity of the USRP with respect to the dongle. Tracking can be maintained below 10 dB using the USRP, while loss-of-lock is produced between 10 dB and 15 dB with the dongle. Signs of amplifier saturation have been noticed in both platforms for SNR values above 30 dB. The SDR receiver is able to attain the Cramér-Rao bound (CRB) for ranging with simulated signal, but the use of both low-cost hardware platforms degrades the accuracy in about 2 dB. In order to validate the positioning capabilities of these platforms, a real LTE network has been emulated in the laboratory by considering a system bandwidth of 1.4 MHz and standard path loss models (without multipath). Using both platforms, the SDR receiver have achieved position errors around 5 and 10 meters for the 67% and 95% of the cases, respectively. Thus, the USRP and the DVB-T dongle are viable tools to assess the positioning performance in deployed LTE networks. Their use in field measurements is proposed for future work.

Acknowledgment

The content of the present article reflects solely the authors view and by no means represents the official European Space Agency (ESA) view. This work was supported by the ESA under the NPI programme No. 4000110780/14/NL/AK, and by the Spanish Ministry of Science and Innovation projects TEC 2011-28219 and EIC-ESA-2011-0079.

References

[1] 3GPP TS 36.211, *Evolved universal terrestrial radio access (E-UTRA); Physical channels and modulation*, Std., Rel. 9, V9.1.0, March 2010.

[2] I. Martin-Escalona, F. Barceló, and J. Paradells, "Delivery of non-standardized assistance data in E-OTD/GNSS hybrid location systems," in *Proc. IEEE Int. Symp. on PIMRC*, vol. 5, Sept. 2002, pp. 2347–2351.

[3] C. Gentner, J.-M. Rawadi, E. Muñoz, and M. Khider, "Hybrid positioning with 3GPP-LTE and GPS employing particle filters," in *Proc. ION GNSS*, Sep. 2012, pp. 473–481.

[4] Z. Biacs, G. Marshall, M. Moeglein, and W. Riley, "The Qualcomm/SnapTrack wireless-assisted GPS hybrid positioning system and results from initial commercial deployments," in *Proc. ION GPS*, Sep. 2002, pp. 378–384.

[5] CSRIC III Working Group 3, "E9-1-1 location accuracy: Indoor location test bed report," Final Report, March 2013.

[6] FCC, "Third futher notice of proposed rulemaking on wireless E911 location accuracy requirements," Tech. Rep., Feb. 2014.

[7] J. A. del Peral-Rosado, J. A. López-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, "Joint maximum likelihood time-delay estimation for LTE positioning in multipath channels," *EURASIP Journal on Advances in Signal Processing*, vol. 2014, no. 33, p. 13, Feb. 2014.

[8] J. Medbo, I. Siomina, A. Kangas, and J. Furuskog, "Propagation channel impact on LTE positioning accuracy: A study based on real measurements of observed time difference of arrival," in *Proc. IEEE Int. Symp. on PIMRC*, Sep. 2009, pp. 2213–2217.

[9] J. A. del Peral-Rosado, J. A. López-Salcedo, G. Seco-Granados, F. Zanier, P. Crosta, R. Ioannides, and M. Crisci, "Software-defined radio LTE positioning receiver towards future hybrid localization systems," in *Proc. AIAA ICSSC*, Oct. 2013.

[10] 3GPP TS 36.101, *E-UTRA; User equipment (UE) radio transmission and reception*, Std., Rel. 9, V9.18.0, Jan. 2014.

[11] Ettus Research LLC. [Online]. Available: http://www.ettus.com

[12] Rafael Microelectronics, Inc., "R820T high performance low power advanced digital TV silicon tuner datasheet," 2011.

[13] C. Fernández-Prades, J. Arribas, and P. Closas, "Turning a television into a GNSS receiver," in *Proc. ION GNSS*, Sep. 2013, pp. 1492–1507.

[14] M. Speth, S. A. Fechtel, G. Fock, and H. Meyr, "Optimum receiver design for wireless broad-band systems using OFDM – Part I," *IEEE Trans. on Communications*, vol. 47, no. 11, pp. 1668–1677, 1999.

[15] B. Yang, K. B. Letaief, R. S. Cheng, and Z. Cao, "Timing recovery for OFDM transmission," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 11, pp. 2278–2291, 2000.

[16] Z. Zhang, J. Liu, and K. Long, "Low-complexity cell search with fast PSS identification in LTE," *IEEE Trans. on Vehicular Technology*, vol. 61, no. 4, pp. 1719–1729, 2012.

[17] K. Borre, D. Akos, N. Bertelsen, P. Rinder, and S. Jensen, *A software-defined GPS and Galileo receiver: a single-frequency approach*. Birkhauser, 2007.

[18] P. Moose, "A technique for orthogonal frequency division multiplexing frequency offset correction," *IEEE Trans. on Communications*, vol. 42, no. 10, pp. 2908–2914, 1994.

[19] Y. Li, "Blind SNR estimation of OFDM signals," in *Proc. ICMMT*, 8–11 May 2010, pp. 1792–1796.

[20] R. Fletcher, "A modified Marquardt subroutine for non-linear least squares." AERE, Harwell, UK, Tech. Rep., 1971.

[21] M. Balda, "LMFsolve.m: Levenberg-Marquardt-Fletcher algorithm for nonlinear least squares problems," MathWorks, File Exchange, 2007.

[22] S. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice-Hall PTR, 1993–1998.

[23] 3GPP TS 36.141, *BS conformance testing*, Std., Rel. 9, Sep. 2012.

[24] Ettus Research LLC, "Examples provided with the USRP hardware driver," Application Note, 2012.

[25] Osmocom. [Online]. Available: http://sdr.osmocom.org/trac/wiki/rtl-sdr

[26] Antenna Bureau, "Location and details of all antennas in The Netherlands," 2014. [Online]. Available: http://www.antenneregister.nl/register

[27] 3GPP TR 36.942, *E-UTRA; Radio frequency (RF) system scenarios*, Std., Rel. 9, V9.3.0, July 2012.