Performance Characterization of Positioning in LTE Systems

Kimia Shamaei, Joe Khalife, and Zaher M. Kassas
University of California, Riverside

BIOGRAPHIES

Kimia Shamaei is a Ph.D. student at the University of California, Riverside. She received her B.S. and M.S. in electrical engineering from the University of Tehran. Her current research interests include analysis and modeling of signals of opportunity and software-defined radio.

Joe J. Khalife is a Ph.D. student at the University of California, Riverside. He received a B.E. in electrical engineering and an M.S. in computer engineering from the Lebanese American University (LAU). From 2012 to 2015, he was a research assistant at LAU. His research interests include opportunistic navigation, autonomous vehicles, and software-defined radio.

Zaher (Zak) M. Kassas is an assistant professor at the University of California, Riverside and director of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He received a B.E. in Electrical Engineering from the Lebanese American University, an M.S. in Electrical and Computer Engineering from The Ohio State University, and an M.S.E. in Aerospace Engineering and a Ph.D. in Electrical and Computer Engineering from The University of Texas at Austin. From 2004 through 2010 he was a research and development engineer with the LabVIEW Control Design and Dynamical Systems Simulation Group at National Instruments Corp. His research interests include estimation, navigation, autonomous vehicles, and intelligent transportation systems.

ABSTRACT

This paper presents low-level models of cellular LTE signals along with an architecture for a software-defined radio (SDR) that is capable of (1) extracting the essential parameters for navigation from the received LTE signals and (2) acquiring and tracking real LTE signals transmitted from multiple base stations. Moreover, a method for obtaining time-of-arrival (TOA) estimates that is highly robust against interference and noise in the environment is presented. This method relies on estimating the channel impulse response from the received LTE signal. The proposed LTE SDR is evaluated on a ground vehicle in an urban environment with real LTE signals. Experimental results show a mean distance difference of 11.96 m between the proposed LTE SDR and the GPS solutions over a 1.42 Km with a standard deviation of 6.83 m and a maximum distance difference of 40.42 m.

I. INTRODUCTION

Research in navigation via signals of opportunity (SOPs) has revealed their potential as an alternative or a complement to global navigation satellite system (GNSS) [1–9]. The literature on SOPs answers theoretical questions on the observability and estimability of the SOPs landscape for various *a priori* knowledge scenarios [10–12] and prescribe receiver motion strategies for accurate receiver and SOP localization and timing estimation [13–16]. Moreover, a number of recent experimental results have demonstrated receiver localization and timing via different SOPs [7, 17–21]. Cellular SOPs are particulary attractive due to the large number of base transceiver stations in environments where GNSS signals are typically challenged. Navigation frameworks and receiver architectures were developed for cellular code division multiple access (CDMA) based navigation, where experimental results showed meter-level accuracy [22].

In recent years, interest in long term evolution (LTE) signals as SOPs has emerged. LTE has become the prominent standard for fourth generation (4G) communication systems. Its multiple-input multiple-output (MIMO) capabilities allowed higher data rates to be achieved compared to the previous generations of wireless standards. The high bandwidths and data rates employed in LTE systems have made LTE signals attractive for navigation as well. In LTE Release 9, a broadcast positioning reference signal (PRS) was introduced to enable network-based positioning capabilities within the LTE protocol. However, PRS-based positioning suffers from a number of drawbacks: (1) the user's privacy is compromised since the user's location is revealed to the network [23], (2) localization services are limited only to paying subscribers and from a particular cellular provider, (3) ambient LTE signals transmitted by other cellular providers are not exploited, and (4) additional bandwidth is required to accommodate the PRS, which caused the majority of cellular providers to choose not to transmit the PRS in favor of dedicating more bandwidth for traffic channels. To circumvent these drawbacks, user equipment (UE)-based positioning approaches that exploit the cell-specific reference signal (CRS) have been explored. While, several papers demonstrated experimental results for positioning using real LTE signals [24, 25], they did not discuss the design or architecture of a receiver that is capable of extracting navigation observables from LTE signals. Other paper proposed SDRs for navigation

**Preprint of the 2016 ION GNSS+ Conference
Portland, Oregon, September 12–16, 2016**

using LTE signals [26–28]; however, only experimental results using LTE signals emulated in the laboratory were presented. There are several challenges associated with navigating with these proposed SDRs, which rely on tracking the primary synchronization signal (PSS) transmitted by the LTE base station, or eNodeB. The first challenge results from the near-far effect created by the strongest PSS, which makes it impossible for the receiver to individually track the remaining ambient PSSs. A simple solution would be to track only the strongest PSSs (up to three), which raises a second challenge: the number of intra-frequency eNodeBs that the receiver can simultaneously use for positioning is limited. Alternatively, other cell-specific signals can be tracked, in which case the receiver must obtain high-level information of the surrounding eNodeBs, such as their cell ID, signal bandwidth, and the number of transmitting antennas. In the LTE-based navigation literature, this information is assumed to be known *a priori*. In practice, the receiver must be able to obtain this information in unknown environments, which is the third challenge associated with using these existing SDRs.

This paper addresses the challenges mentioned above. First, it presents a cellular LTE SDR along with low-level signal models for optimal extraction of relevant navigation and timing information from received signals. Then, it provides experimental results comparing the trajectories corresponding to a navigation solution from GPS and those of the proposed LTE SDR. The mean distance difference between the trajectories is shown to be 11.96 m with a standard deviation of 6.83 m and a maximum difference of 40.42 m.

The remainder of this paper is organized as follows. In Section II, an overview of LTE signals is provided, and the signal acquisition process is discussed. Section III presents the steps to extract relevant eNodeB information. Section IV discusses signal tracking. Section V describes timing information extraction from received eNodeB signals. Section VI presents the framework used to obtain the navigation solution. Section VII presents experimental results demonstrating a ground vehicle navigation with LTE signals through the LTE SDR developed in this paper. Concluding remarks are discussed in Section VIII.

II. SIGNAL ACQUISITION

When a UE enters an unknown LTE environment, the first step it performs to establish communication with the network is synchronizing with the surrounding eNodeBs. This is achieved by acquiring the PSS and the secondary synchronization signal (SSS) transmitted by the eNodeB. In this section, the steps taken by the UE to acquire these LTE signals are presented. First, a brief summary of the LTE frame structure is provided. Then, the PSS and SSS acquisition process is discussed.

A. LTE Frame Structure

A frame, which is a major component in LTE communication, is a two-dimensional grid representing time and frequency. The elementary block of an LTE frame is a complex symbol, defined as a resource element (RE). The frequency index of an RE maps to an LTE subcarrier, and its time index maps to an LTE symbol. The REs are grouped into resource blocks (RBs), which are further grouped into resource grids (RGs). The RGs are then grouped into slots, which constitute a type 1 LTE frame. This type of frame is suitable for frequency division duplex (FDD) transmission, which is considered in this paper. A frame consists of 20 slots of duration 0.5 ms each. Subsequently, an LTE frame will have a duration of 10 ms, and an LTE subframe, which is defined as two consecutive slots, will have a duration of 1 ms. The structure of the FDD LTE frame is illustrated in Fig. 1 [29].

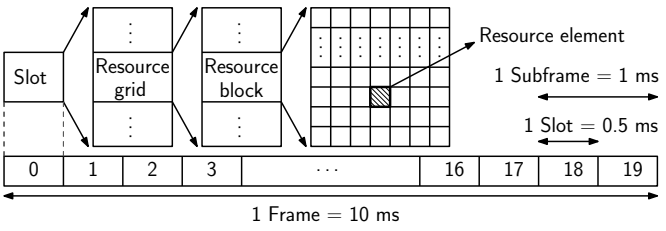

Fig. 1. FDD frame structure.

The subcarriers in an LTE frame are typically separated by $\Delta f = 15$ KHz, and the total number of subcarriers, N_c, is set by the operator. This implies that different LTE systems may have different bandwidths, which are summarized in Table I. It is worth mentioning that the unused subcarriers create a guardband between LTE bands.

TABLE I
LTE SYSTEM BANDWIDTHS AND NUMBER OF SUBCARRIERS.

Bandwidth (MHz)	Total number of subcarriers	Number of subcarriers used
1.4	128	72
3	256	180
5	512	300
10	1024	600
15	1536	900
20	2048	1200

In order to transmit data, data symbols are first mapped onto the frame REs. Then, the inverse fast Fourier transform (IFFT) is applied to each LTE symbol across all the subcarriers. The resulting signal is serialized and appended with a cyclic prefix (CP) before transmission over the wireless channel. This process is called orthogonal frequency division multiplexing (OFDM). The LTE receiver will then reverse these steps in order to reconstruct the LTE frame [29]. However, it must first determines the

frame timing, which is achieved by acquiring the PSS and SSS as will be discussed in the next subsection.

B. PSS and SSS Acquisition

PSS is a length-62 Zadoff-Chu sequence mapped to 62 subcarriers in slot 0 of the LTE frame and is repeated in slot 10. It is important to note that the DC subcarrier and the rest of the subcarriers in the symbols where PSS is transmitted are filled with zeros. Each eNodeB's sector transmits only one of three possible PSS sequences, each of which maps to an integer between 0 and 2, denoted by $N_{ID}^{(2)}$. The UE correlates the received LTE signal with all three possible PSS sequences that are generated locally. Due to the orthogonality properties of Zadoff-Chu sequences, a peak in the correlation will be seen only when the eNodeB's and UE's PSS sequences match. By detecting these peaks, the UE will be able to determine the LTE symbol timing as well as the integer $N_{ID}^{(2)}$.

SSS is detected in a similar way as PSS. It is a length-62 orthogonal sequence, obtained by concatenating two maximal-length sequences scrambled by a third orthogonal sequence generated based on $N_{ID}^{(2)}$. SSS is transmitted only once in the symbol preceding the PSS directly, either in slot 0 or 10. There are 168 possible SSS sequences, each mapped to an integer between 0 and 167, denoted $N_{ID}^{(1)}$. Once the PSS and SSS are detected, the UE can produce an estimate of the frame start time $\hat{t}_s$, as well as determine the cell ID, which is given by $N_{ID}^{cell} = 3N_{ID}^{(1)} + N_{ID}^{(2)}$ [29].

After obtaining the frame timing, the UE estimates the frequency shift (Doppler frequency), using the CP in the received signal $r(n)$ [30]. The Doppler frequency estimate $\hat{f}_D$ is given by

$$\hat{f}_D = \frac{1}{2\pi N_c T_s} \arg\left\{ \sum_{n \in \mathcal{N}_{\mathcal{CP}}} r(n) r^*(n + N_c) \right\},$$

where $(\cdot)^*$ is the complex conjugate operator, $\mathcal{N}_{\mathcal{CP}}$ is the set of CP indices, N_c is the total number of subcarriers, and T_s is the sampling interval.

Fig. 2 summarizes the signal acquisition steps and Fig. 3 shows the PSS and SSS correlation with real LTE signals.

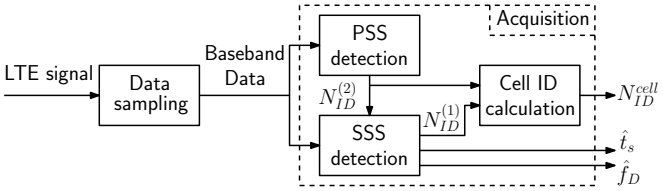

Fig. 2. Signal acquisition block diagram.

III. SYSTEM INFORMATION EXTRACTION

After acquiring the LTE signal, the UE needs to determine several parameters of the LTE network in order to successfully communicate with the eNodeBs. These parameters

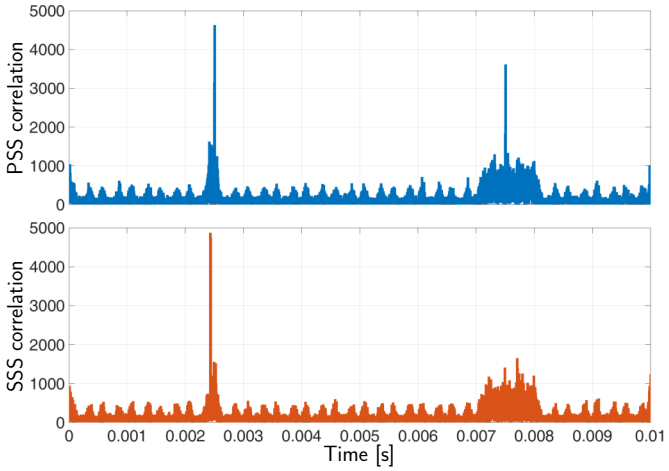

Fig. 3. PSS and SSS correlation results with real LTE signals.

are transmitted on the downlink physical channels, which can be control, broadcast or shared channels. This section briefly discusses the structure of these channels and shows how the system parameters are provided in two information blocks, namely the master information block (MIB) and the system information block (SIB).

A. LTE Downlink Physical Channels

A downlink physical channel corresponds to a set of REs carrying high level system information and/or communication data. There are typically seven physical channels in the LTE downlink. The MIB is transmitted on the physical broadcast channel (PBCH), and the SIB is transmitted on the physical downlink shared channel (PDSCH). The physical control format indicator channel (PCFICH) and the physical downlink control channel (PDCCH) must also be decoded in order to extract the SIB, as it will be explained in Subsection III-C. All the downlink physical channels are processed in a similar fashion before transmission, as it is shown in Fig. 4 . The codewords are first scrambled and mapped for modulation, which can be either quadrature phase-shift keying (QPSK), 16 quadrature amplitude modulation (QAM), 64QAM, or 256QAM. Then, layer mapping for spatial and transmit diversity is performed and the resulting layers are precoded for transmit diversity as well. Finally, the blocks of symbols are mapped to REs, from which the OFDM signal is generated. Although all the physical channels have the same general structure, each step in Fig. 4 differs from one channel to another. Further details are discussed in [29] and [31].

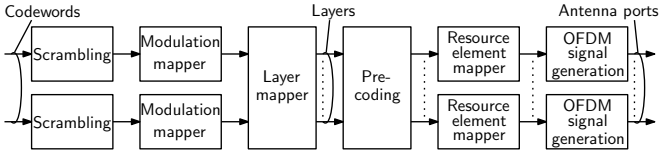

Fig. 4. General structure of downlink physical channels.

B. MIB Structure

As mentioned in Section II, there is no unique bandwidth for LTE systems. It is therefore important for the UE to determine the bandwidth of the system it is trying to connect to. Furthermore, to provide higher transmission rates, LTE systems employ a MIMO structure where the number of transmitting antennas could be either 1, 2 or 4. Subsequently, to decode the LTE signal correctly, the UE must know the number of transmitting antennas. Fortunately, this information is provided to the UE in the MIB, which is transmitted in the second slot of the first subframe. It is mapped to the first 6 RBs around the carrier frequency and the first four symbols of the slot. Note that the MIB symbols are not transmitted on the subcarriers reserved for the reference signals, which will be discussed in section V.

C. SIB Structure

The SIB transmitted by the eNodeB contains information on (1) the cell it is servicing, (2) inter- and intra-frequency neighboring cells, (3) neighboring cells from other networks (UMTS, GSM, and CDMA2000), (4) other warning and alert system information. The transmitted SIB can be in the form of one out of seventeen blocks, numbered SIB1 to SIB17. SIB1 is transmitted in subframe 5 of every even frame, and it contains scheduling information for the other SIBs, which can be subsequently decoded. Decoding the SIB involves a several complicated steps. For the purpose of this paper, these steps are summarized and listed in the order in which the UE executes them, excluding the technical details which can be found in [29, 31]. In order to decode the SIB, the UE first decodes the control format information (CFI) from the PCFICH. Then, it decodes the downlink control information (DCI) from the PDCCH, which will allow it to extract the SIB bits from the PDSCH. Finally, an Abstract Syntax Notation One (ASN.1) decoder is used to recover the system information sent by the eNodeB. These steps are summarized in Fig. 5.

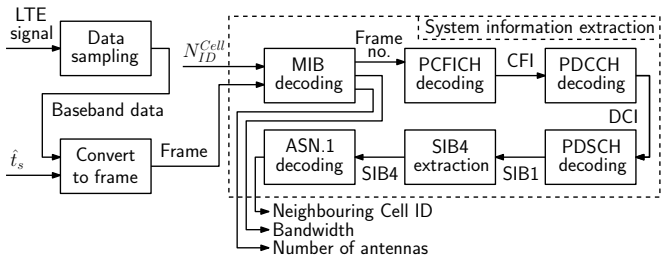

Fig. 5. System information extraction block diagram.

C.1 PCFICH Demodulation and CFI Decoding

The CFI is transmitted on the PCFICH. It indicates the number of OFDM symbols dedicated for the downlink control channel, and can take the values 1, 2, or 3. In order to decode the CFI, the UE first locates the 16 PCFICH REs and demodulates them by reversing the steps in Fig. 4, resulting in a sequence of 32 bits. This sequence can be only one of three possible sequences, each of which is mapped to a CFI value.

C.2 PDCCH Demodulation and DCI Decoding

Knowing the CFI, the UE can identify the REs associated with the PDCCH and demodulate them, resulting in a block of bits corresponding to the DCI message. The packing of these bits can take one of several formats, and it is not communicated with the UE. A blind search over the different formats must therefore be performed by the UE to unpack these bits. The "candidate" formats are either on the common search space or on the UE-specific search space. Fortunately, for the SIBs, there are only two candidate formats, which are both located on the common search space. A cyclic redundancy check (CRC) is obtained to identify the right format.

C.3 PDSCH Demodulation and SIB Decoding

The DCI is next parsed to give the configuration of the corresponding PDSCH REs carrying the SIB, which are then demodulated. Next, the received bits are downlink-shared channel (DL-SCH) decoded, resulting in the SIB bits. Subsequently, these bits are decoded using an ASN.1 decoder, which will extract the system information sent on the SIB by the eNodeB.

D. System Information Extraction and Neighboring Cells Identification

During signal acquisition, the frame timing and the eNodeB cell ID are determined. Then, the MIB is decoded and the bandwidth of the system as well as the frame number are extracted. This will allow the UE to demodulate the OFDM signal across the entire bandwidth and locate the SIB1 REs. The UE moves on to decode the SIB1 message, from which the scheduling for SIB4 is deduced and, subsequently, decoded. SIB4 contains the cell ID of intra-frequency neighboring cells as well as other information pertaining to these cells. Decoding this information gives the UE the ability to simultaneously track signals from different eNodeBs and produce time-of-arrival (ToA) estimates from each of these eNodeBs. Signal tracking and ToA estimation will be thoroughly discussed in the next two sections.

IV. SIGNAL TRACKING

Section II discussed how to obtain the eNodeB's cell ID and the transmitted LTE frame. In order to be able to continuously reconstruct the LTE frame, the UE must be synchronized with the eNodeB at all time. This can be achieved by tracking the PSS or SSS. However, it is important to note that there are only 3 possible PSS sequences; thus, there will be a high level of interference from neighboring cells. The interference level is much lower for the

SSS, which can be one of 168 possible sequences. Hence, SSS will be tracked instead of PSS. In this section, the components of the tracking loop employed to track the SSS are discussed, namely a frequency-locked loop (FLL) assisted phase-locked loop (PLL) and a carrier-aided delay-locked loop (DLL).

A. FLL-Assisted PLL

The FLL-assisted PLL consists of a phase discriminator, a phase loop filter, a frequency discriminator, a frequency loop filter, and a numerically-controlled oscillator (NCO). Since there is no data modulated on the SSS, an `atan2` phase discriminator, which remains linear over the full input error range of $\pm\pi$, could be used without the risk of introducing phase ambiguities. A third-order PLL was used to track the carrier phase, with a loop filter transfer function given by

$$F_{\mathrm{PLL}}(s) = 2.4\omega_{n,p} + \frac{1.1\omega_{n,p}^2}{s} + \frac{\omega_{n,p}^3}{s^2}, \tag{1}$$

where $\omega_{n,p}$ is the undamped natural frequency of the phase loop, which can be related to the PLL noise-equivalent bandwidth $B_{n,\mathrm{PLL}}$ by $B_{n,\mathrm{PLL}} = 0.7845\omega_{n,p}$ [32, 33]. The output of the phase loop filter is the rate of change of the carrier phase error $2\pi\hat{f}_{D_k}$, expressed in rad/s, where $\hat{f}_{D_k}$ is the Doppler frequency. The phase loop filter transfer function in (1) is discretized and realized in state-space. The noise-equivalent bandwidth $B_{n,\mathrm{PLL}}$ is chosen to range between 4 and 8 Hz. The PLL is assisted by a second-order FLL with an `atan2` discriminator for the frequency as well. The frequency error at time step k is expressed as

$$e_{f_k} = \frac{\texttt{atan2}\left(Q_{p_k}I_{p_{k-1}} - I_{p_k}Q_{p_{k-1}}, I_{p_k}I_{p_{k-1}} + Q_{p_k}Q_{p_{k-1}}\right)}{T_{sub}},$$

where $S_{p_k} = I_{p_k} + jQ_{p_k}$ is the prompt correlation at time step k and $T_{sub} = 0.01$s is the subaccumulation period, which is chosen to be one frame length. The transfer function of the frequency loop filter is given by

$$F_{\mathrm{FLL}}(s) = 1.414\omega_{n,f} + \frac{\omega_{n,f}^2}{s}, \tag{2}$$

where $\omega_{n,f}$ is the undamped natural frequency of the frequency loop, which can be related to the FLL noise-equivalent bandwidth $B_{n,\mathrm{FLL}}$ by $B_{n,\mathrm{FLL}} = 0.53\omega_{n,f}$ [32]. The output of the frequency loop filter is the rate of change of the angular frequency $2\pi\hat{\dot{f}}_{D_k}$, expressed in rad/s^2. It is therefore integrated and added to the output of the phase loop filter. The frequency loop filter transfer function in (2) is discretized and realized in state-space. The noise-equivalent bandwidth $B_{n,\mathrm{FLL}}$ is chosen to range between 1 and 4 Hz.

B. DLL

The carrier-aided DLL employs the non-coherent dot product discriminator. In order to compute the SSS code phase error, the dot product discriminator uses the prompt, early, and late correlations, denoted by S_{p_k}, S_{e_k}, and S_{l_k}, respectively. The early and late correlations are calculated by correlating the received signal with an early and a delayed version of the prompt SSS sequence, respectively. The time shift between S_{e_k} and S_{l_k} is defined by an early-minus-late time t_{eml}, expressed in chips. The chip interval T_c for SSS (and PSS), can be expressed as $T_c = \frac{1}{BW}$, where BW is the bandwidth of the synchronization signal. Since the SSS and PSS occupy only 62 subcarriers, the BW is calculated to be $BW = 62 \times 15 = 930$ KHz, which gives $T_c \approx 1.0752\mu$s. The autocorrelation function of the transmitted LTE SSS is wide at its peak and therefore a wider t_{eml} is preferable in order to have a significant difference between S_{p_k}, S_{e_k}, and S_{l_k} [34].

The DLL loop filter is a simple gain K, with a noise-equivalent bandwidth $B_{n,\mathrm{DLL}} = \frac{K}{4} \equiv 0.5$ Hz. The output of the DLL loop filter v_{DLL} is the rate of change of the SSS code phase, expressed in s/s. Assuming low-side mixing, the code start time is updated according to

$$\hat{t}_{s_{k+1}} = \hat{t}_{s_k} - (v_{\mathrm{DLL,k}} + \hat{f}_{D_k}/f_c) \cdot T_{sub}.$$

Finally, the SSS code start time estimate is used to reconstruct the transmitted LTE frame. Fig. 6 shows the block diagram of the tracking loops and Fig. 7 shows the tracking results for a stationary receiver.

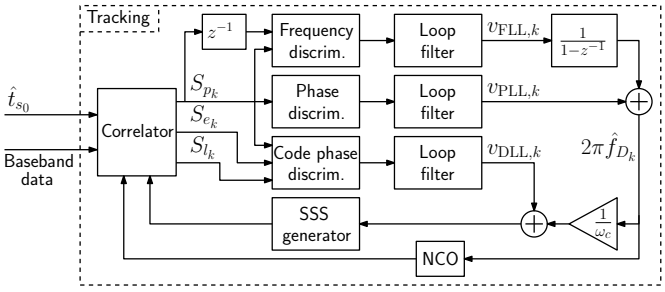

Fig. 6. Signal tracking block diagram.

V. TIMING INFORMATION EXTRACTION

In LTE systems, the PSS and SSS are transmitted with the lowest possible bandwidth. Consequently, the timing resolution obtained from these signals is low. For more precise navigation using LTE signals, the cell-specific reference signal (CRS) is used. This section discusses the CRS and how timing information can be deduced from it.

A. Received CRS Model

The CRS is a pseudo-random sequence which is uniquely defined by the eNodeB's cell ID. It is spread across the entire bandwidth and is transmitted mainly to estimate the channel frequency response. The CRS subcarrier allocation depends on the cell ID, and it is designed to keep the interference with CRSs from other eNodeBs to a minimum.

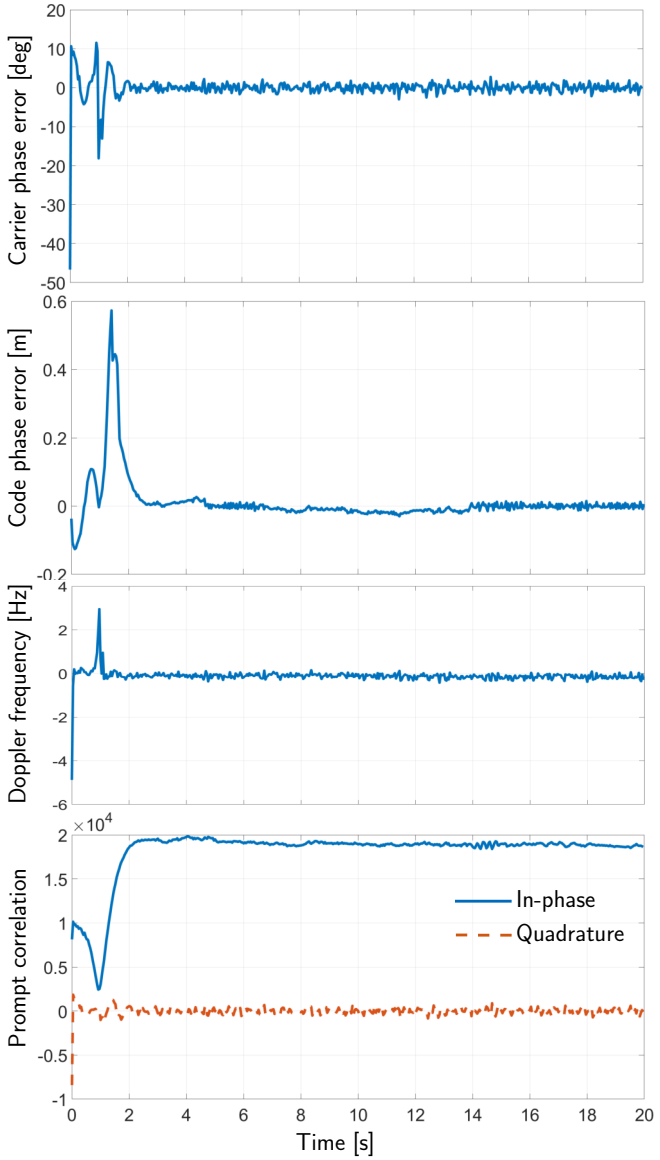

Fig. 7. Tracking results for a stationary receiver.

The transmitted OFDM signal from the u-th eNodeB at the k-th subcarrier, $Y^{(u)}(k)$, can be expressed as

$$Y^{(u)}(k) = \begin{cases} S^{(u)}(k), & \text{if } k \in A^{(u)}, \\ D^{(u)}(k), & \text{otherwise,} \end{cases}$$

where $S^{(u)}(k)$ is the u-th eNodeB's CRS sequence, $A^{(u)}$ is the set of subcarriers in which $S^{(u)}(k)$ is transmitted, and $D^{(u)}(k)$ represents some other data signals. Assuming that the transmitted signal propagates in an additive white Gaussian noise (AWGN) channel, the received signal will be

$$R(k) = \sum_{u=0}^{U-1} \left(H^{(u)}(k) Y^{(u)}(k) + w^{(u)}(k) \right),$$

where $H^{(u)}(k)$ is the channel frequency response at the k-th subcarrier and $w^{(u)}(k)$ is a white Gaussian sequence.

B. Channel Impulse Response Estimation

The channel frequency response estimate of the desired eNodeB, u', is obtained according to

$$\begin{aligned} \hat{H}^{(u')}(k) &= S^{(u')^*}(k) R(k) \\ &= H^{(u')}(k) \left| S^{(u')}(k) \right|^2 + I^{(u')}(k) + V(k), \end{aligned} \tag{3}$$

where $k \in A^{(u')}$, $I^{(u')} = S^{(u')^*}(k) \sum_{\substack{u=0 \\ u \neq u'}}^{U-1} H^{(u)}(k) D^{(u)}(k)$, and $V(k) = S^{(u')^*}(k) \sum_{u=0}^{U-1} w^{(u)}(k)$. From the properties of the CRS sequence, $\left| S^{(u')}(k) \right|^2 = 1$, hence

$$\hat{H}^{(u')}(k) = H^{(u')}(k) + I^{(u')}(k) + V(k).$$

Moreover, the data transmitted by each eNodeB is scrambled by a pseudo-random sequence that is orthogonal to the sequences of other eNodeBs, which means that $I^{(u')}$ must be zero. However, since the DC component of the transmitted data is removed, the orthogonality between different pseudo-random codes is lost, and the resulting correlation can be modeled as a zero-mean Gaussian random variable. Let $\Gamma(k) \triangleq I^{(u')}(k) + V(k)$, then

$$\hat{H}^{(u')}(k) = H^{(u')}(k) + \Gamma(k),$$

where $\Gamma(k)$ is a zero-mean Gaussian random variable as well. The channel impulse response estimate is given by

$$\hat{h}^{(u')}(n) = \mathsf{IFFT}\left\{ \hat{H}^{(u')}(k) \right\} = h^{(u')}(n) + \gamma(n), \tag{4}$$

where $\gamma(n) = \mathsf{IFFT}\{\Gamma(k)\}$ is a complex Gaussian random variable.

C. Path Delay Estimation

In general, a multipath channel can be modeled as

$$h^{(u)}(n) = \sum_{l=0}^{L^{(u)}-1} \alpha^{(u)}(l) \delta[n - n^{(u)}(l)],$$

where $\alpha^{(u)}(l)$ and $n^{(u)}(l)$ are the attenuation and delay of the l-th path to the u-th eNodeB, respectively. Estimating $n^{(u')}(l)$ can be achieved through the following hypothesis test

$$\begin{aligned} H_0: &\quad \hat{h}^{(u')}(n) = \gamma(n), && \text{for } n \neq n^{(u')}(l), \\ H_1: &\quad \hat{h}^{(u')}(n) = \alpha^{(u')}(l) + \gamma(n), && \text{for } n = n^{(u')}(l), \end{aligned}$$

where $l = 0, \ldots, L-1$. It can be shown that $|\hat{h}^{(u')}(n)|$ has a Rayleigh distribution under H_0 and a Rician distribution under H_1. Finally, in order to increase the probability of detection, the channel impulse response estimates at different slots can be added non-coherently. Similarly, the

channel impulse response estimates for different transmitting antennas can also be added non-coherently, assuming that they have the same line-of-sight (LOS) path. In this paper, the channel frequency response estimates are accumulated across the entire frame to improve the detection performance. Fig. 8 illustrates the timing information extraction process.

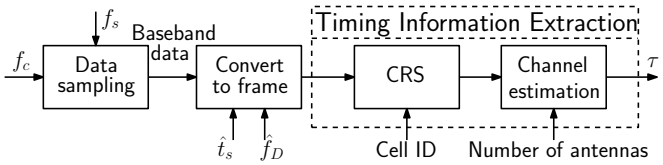

Fig. 8. Timing information extraction block diagram.

VI. NAVIGATION SOLUTION

Sections II through V discussed how TOA can be extracted from LTE signals. By multiplying the obtained TOA to the speed of light, the pseudorange measurements can be formed. This section discusses receiver state estimation from these measurements. The receiver state is defined by $\boldsymbol{x}_r = \left[\boldsymbol{r}_r^{\mathsf{T}}, c\delta t_r\right]^{\mathsf{T}}$, where $\boldsymbol{r}_r = [x_r, y_r, z_r]^{\mathsf{T}}$ is the receiver's position vector, δt_r is the receiver's clock bias, and c is the speed-of-light. Similarly, the state of the i-th eNodeB is defined as $\boldsymbol{x}_{s_i} = \left[\boldsymbol{r}_{s_i}^{\mathsf{T}}, c\delta t_{s_i}\right]^{\mathsf{T}}$, where $\boldsymbol{r}_{s_i} = [x_{s_i}, y_{s_i}, z_{s_i}]^{\mathsf{T}}$ is the eNodeB's position vector and δt_{s_i} is its clock bias. Subsequently, the pseudorange measurement to the i-th eNodeB at time t, ρ_i, can be expressed as

$$\rho_i = \|\boldsymbol{r}_r - \boldsymbol{r}_{s_i}\|_2 + c \cdot [\delta t_r - \delta t_{s_i}] + v_i,$$

where v_i is the measurement noise, which is modeled a zero-mean Gaussian random variable with variance σ_i^2 [9]. By drawing pseudorange measurements to four or more eNodeBs, the UE can estimate its state, provided that the position and the clock bias of the eNodeBs are known. It has been previously shown that the SOP position can be mapped with a high degree of accuracy whether collaboratively or non-collaboratively [35–37]. Moreover, the location of LTE base stations can be obtained from online databases, ground surveys, or even satellite imagery. Here, it is assumed that the position of the eNodeBs is perfectly known to the UE. However, the clock bias of these base stations is a stochastic dynamic process and needs to be estimated at all times [12]. In this paper, only the difference $\delta t_i \triangleq \delta t_r - \delta t_{s_i}$ is considered, instead of the receiver and eNodeB's individual clock biases. This difference is modeled as a first order polynomial [24], i.e., $\delta t_i(t) = a_i\, t + b_i$, where a_i is the clock drift between the receiver and the i-th eNodeB and b_i is the corresponding constant bias. The coefficients of δt_i are calculated from GPS data and the measured pseudoranges using a least-squares (LS) estimator. Consequently, the pseudorange at time t is re-expressed as $\rho_i \approx h_i\left(\boldsymbol{r}_r, \boldsymbol{r}_{s_i}\right) + v_i$, where $h_i\left(\boldsymbol{r}_r, \boldsymbol{r}_{s_i}\right) \triangleq \|\boldsymbol{r}_r - \boldsymbol{r}_{s_i}\|_2 + c \cdot [a_i\, t + b_i]$. Then, by making pseudorange measurements to $N \geq 3$ eNodeBs with known position states, the receiver can estimate its position state using an iterative weighted nonlinear LS (WNLS) solver. The receiver's position estimate update at the l-th iteration is given by

$$\hat{\boldsymbol{r}}_r^{(l+1)} = \hat{\boldsymbol{r}}_r^{(l)} + \left(\mathbf{H}^{\mathsf{T}}\mathbf{R}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathsf{T}}\mathbf{R}^{-1}\left(\boldsymbol{\rho} - \hat{\boldsymbol{h}}^{(l)}\right),$$

where, $\hat{\boldsymbol{h}}^{(l)} = \left[h_1\left(\hat{\boldsymbol{r}}_r^{(l)}, \boldsymbol{r}_{s_1}\right), \ldots, h_N\left(\hat{\boldsymbol{r}}_r^{(l)}, \boldsymbol{r}_{s_N}\right)\right]^{\mathsf{T}}$, $\boldsymbol{\rho} = [\rho_1, \ldots, \rho_N]^{\mathsf{T}}$, $\mathbf{R} = \mathsf{diag}\left[\sigma_1^2, \ldots, \sigma_{\mathsf{N}}^2\right]$ is the measurement noise covariance matrix, and $\mathbf{H}$ is the Jacobian matrix with respect to the receiver's position, given by

$$\mathbf{H} \triangleq \left[\frac{\hat{\boldsymbol{r}}_r^{(l)} - \boldsymbol{r}_{s_1}}{\left\|\hat{\boldsymbol{r}}_r^{(l)} - \boldsymbol{r}_{s_1}\right\|_2} \quad \cdots \quad \frac{\hat{\boldsymbol{r}}_r^{(l)} - \boldsymbol{r}_{s_N}}{\left\|\hat{\boldsymbol{r}}_r^{(l)} - \boldsymbol{r}_{s_N}\right\|_2}\right]^{\mathsf{T}},$$

evaluated at $\hat{\boldsymbol{r}}_r^{(l)}$.

VII. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed LTE SDR, a field test was conducted with real LTE signals in an urban environment. For this purpose, a mobile ground receiver was equipped with three antennas to acquire and track: (1) GPS signals and (2) LTE signals in two different bands from nearby eNodeBs. The receiver LTE antennas were consumer-grade 800/1900 MHz cellular omnidirectional antennas, and the GPS antenna was a surveyor-grade Leica antenna. The LTE signals were simultaneously down-mixed and synchronously sampled via a dual-channel universal software radio peripheral (USRP) driven by a GPS-disciplined oscillator. The GPS signals were collected on a separate single-channel USRP also driven by a GPS-disciplined oscillator. The LTE receiver was tuned to 739 and 1955 MHz carrier frequencies, both of which are allocated for AT&T. Samples of the received signals were stored for off-line post-processing. The GPS signal was processed by a Generalized Radionavigation Interfusion Device (GRID) SDR [38] and the LTE signals were processed by the proposed LTE SDR. Fig. 9 shows the experimental hardware and software setup.

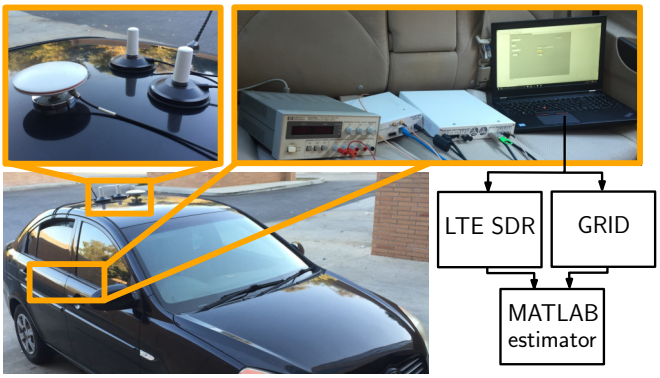

Fig. 9. Experimental setup.

Over the course of the experiment, the receiver was listening to the same 3 eNodeBs listed in Table II. The position states of these eNodeBs were mapped prior to the experiment. Moreover, all measurements and trajectories were projected onto a two-dimensional (2-D) plane. Subsequently, only the horizontal position of the receiver was estimated.

TABLE II
eNodeB characteristics

eNodeB	f_c (MHz)	N_{ID}^{Cell}	BW (MHz)	Number of antennas
1	739	288	10	2
2	1955	216	20	2
3	739	232	10	2

The environment layout as well as the true and estimated receiver trajectories are shown in Fig. 10. It can be seen from Fig. 10 that the navigation solution obtained from the LTE signals follows closely the navigation solution obtained using GPS signals. The root mean squared error between the GPS and LTE navigation solutions along the traversed 1.42 Km trajectory was calculated to be 11.96 m with a standard deviation of 6.83 m and a maximum error of 40.42 m.

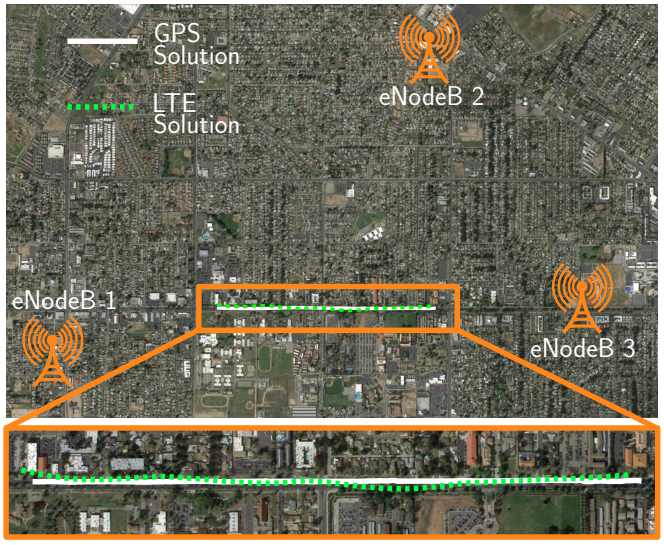

Fig. 10. Receiver trajectory and eNodeB locations.

VIII. CONCLUSION

This paper presented an SDR design for LTE-based navigation. A relevant description of the LTE signal structure is first discussed. Next, the various stages of an LTE SDR was presented. Furthermore, optimal extraction of timing information from LTE signals was studied. Finally, experimental results comparing the navigation solution from GPS versus that of LTE utilizing the developed SDR showed a mean distance difference of 11.96 m over a 1.42 Km trajectory.

ACKNOWLEDGMENT

This work was supported in part by the Office of Naval Research (ONR) under Grant N00014-16-1-2305.

References

[1] K. Fisher, "The navigation potential of signals of opportunity-based time difference of arrival measurements," Ph.D. dissertation, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA, 2005.

[2] J. McEllroy, "Navigation using signals of opportunity in the AM transmission band," Master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA, 2006.

[3] J. Raquet and R. Martin, "Non-GNSS radio frequency navigation," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, March 2008, pp. 5308–5311.

[4] L. Merry, R. Faragher, and S. Schedin, "Comparison of opportunistic signals for localisation," in *Proceedings of IFAC Symposium on Intelligent Autonomous Vehicles*, September 2010, pp. 109–114.

[5] K. Pesyna, Z. Kassas, J. Bhatti, and T. Humphreys, "Tightly-coupled opportunistic navigation for deep urban and indoor positioning," in *Proceedings of ION GNSS Conference*, September 2011, pp. 3605–3617.

[6] P. Thevenon, S. Damien, O. Julien, C. Macabiau, M. Bousquet, L. Ries, and S. Corazza, "Positioning using mobile TV based on the DVB-SH standard," *NAVIGATION, Journal of the Institute of Navigation*, vol. 58, no. 2, pp. 71–90, 2011.

[7] K. Pesyna, Z. Kassas, and T. Humphreys, "Constructing a continuous phase time history from TDMA signals for opportunistic navigation," in *Proceedings of IEEE/ION Position Location and Navigation Symposium*, April 2012, pp. 1209–1220.

[8] Z. Kassas, "Collaborative opportunistic navigation," *IEEE Aerospace and Electronic Systems Magazine*, vol. 28, no. 6, pp. 38–41, 2013.

[9] ——, "Analysis and synthesis of collaborative opportunistic navigation systems," Ph.D. dissertation, The University of Texas at Austin, USA, 2014.

[10] Z. Kassas and T. Humphreys, "Observability analysis of opportunistic navigation with pseudorange measurements," in *Proceedings of AIAA Guidance, Navigation, and Control Conference*, vol. 1, August 2012, pp. 1209–1220.

[11] ——, "Observability and estimability of collaborative opportunistic navigation with pseudorange measurements," in *Proceedings of ION GNSS Conference*, September 2012, pp. 621–630.

[12] ——, "Observability analysis of collaborative opportunistic navigation with pseudorange measurements," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 260–273, February 2014.

[13] ——, "Motion planning for optimal information gathering in opportunistic navigation systems," in *Proceedings of AIAA Guidance, Navigation, and Control Conference*, August 2013, 551–4565.

[14] Z. Kassas, J. Bhatti, and T. Humphreys, "Receding horizon trajectory optimization for simultaneous signal landscape mapping and receiver localization," in *Proceedings of ION GNSS Conference*, September 2013, pp. 1962–1969.

[15] Z. Kassas, A. Arapostathis, and T. Humphreys, "Greedy motion planning for simultaneous signal landscape mapping and receiver localization," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 2, pp. 247–258, March 2015.

[16] Z. Kassas and T. Humphreys, "Receding horizon trajectory optimization in opportunistic navigation environments," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 51, no. 2, pp. 866–877, April 2015.

[17] C. Yang, T. Nguyen, and E. Blasch, "Mobile positioning via fusion of mixed signals of opportunity," *IEEE Aerospace and Electronic Systems Magazine*, vol. 29, no. 4, pp. 34–46, April 2014.

[18] C. Yang and T. Nguyen, "Tracking and relative positioning with mixed signals of opportunity," *NAVIGATION, Journal of the*

Institute of Navigation, vol. 62, no. 4, pp. 291–311, December 2015.

[19] J. Morales, P. Roysdon, and Z. Kassas, "Signals of opportunity aided inertial navigation," in *Proceedings of ION GNSS Conference*, September 2016, 1492–1501.

[20] J. Morales, J. Khalife, and Z. Kassas, "Opportunity for accuracy," *GPS World Magazine*, vol. 27, no. 3, pp. 22–29, March 2016.

[21] ——, "GNSS vertical dilution of precision reduction using terrestrial signals of opportunity," in *Proceedings of ION International Technical Meeting Conference*, January 2016, pp. 664–669.

[22] J. Khalife, K. Shamaei, and Z. Kassas, "A software-defined receiver architecture for cellular CDMA-based navigation," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2016, pp. 816–826.

[23] M. Hofer, J. McEachen, and M. Tummala, "Vulnerability analysis of LTE location services," in *Proceedings of Hawaii International Conference on System Sciences*, January 2014, pp. 5162–5166.

[24] F. Knutti, M. Sabathy, M. Driusso, H. Mathis, and C. Marshall, "Positioning using LTE signals," in *Proceedings of Navigation Conference in Europe*, April 2015.

[25] 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 *Proceedings of International Symposium on Image and Signal Processing and Analysis*, September 2015, pp. 276–281.

[26] J. del Peral-Rosado, J. Parro-Jimenez, J. Lopez-Salcedo, G. Seco-Granados, P. Crosta, F. Zanier, and M. Crisci, "Comparative results analysis on positioning with real LTE signals and low-cost hardware platforms," in *Proceedings of Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing*, December 2014, pp. 1–8.

[27] J. del Peral-Rosado, J. Lopez-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 *Proceedings of International Communication Satellite Systems Conference*, October 2013, pp. 14–17.

[28] M. Ulmschneider and C. Gentner, "Multipath assisted positioning for pedestrians using LTE signals," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2016, pp. 386–392.

[29] 3GPP, "Evolved universal terrestrial radio access (E-UTRA); physical channels and modulation," 3rd Generation Partnership Project (3GPP), TS 36.211, January 2011. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36211.htm

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

[31] 3GPP, "Evolved universal terrestrial radio access (E-UTRA); multiplexing and channel coding," 3rd Generation Partnership Project (3GPP), TS 36.212, January 2010. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36212.htm

[32] E. Kaplan and C. Hegarty, *Understanding* GPS*: Principles and Applications*, 2nd ed. Artech House, 2005.

[33] W. Ward, "Performance comparisons between FLL, PLL and a novel FLL-assisted-PLL carrier tracking loop under RF interference conditions," in *Proceedings of ION GNSS Conference*, September 1998, pp. 783–795.

[34] J. Lee and L. Miller, *CDMA Systems Engineering Handbook*, 1st ed. Norwood, MA, USA: Artech House, 1998.

[35] Z. Kassas and T. Humphreys, "The price of anarchy in active signal landscape map building," in *Proceedings of IEEE Global Conference on Signal and Information Processing*, December 2013, pp. 165–168.

[36] Z. Kassas, V. Ghadiok, and T. Humphreys, "Adaptive estimation of signals of opportunity," in *Proceedings of ION GNSS Conference*, September 2014, pp. 1679–1689.

[37] J. Morales and Z. Kassas, "Optimal receiver placement for collaborative mapping of signals of opportunity," in *Proceedings of ION GNSS Conference*, September 2015, pp. 2362–2368.

[38] T. Humphreys, J. Bhatti, T. Pany, B. Ledvina, and B. O'Hanlon, "Exploiting multicore technology in software-defined GNSS receivers," in *Proceedings of ION GNSS Conference*, September 2009, pp. 326–338.