Exploiting LTE Signals for Navigation: Theory to Implementation

Kimia Shamaei, *Student Member, IEEE*, Joe Khalife, *Student Member, IEEE*, and Zaher M. Kassas, *Senior Member, IEEE*

***Abstract*— Exploiting cellular long-term evolution (LTE) downlink signals for navigation purposes is considered. First, the transmitted LTE signal model is presented and relevant positioning and timing information that can be extracted from these signals are identified. Second, a software-defined receiver (SDR) that is capable of acquiring, tracking, and producing pseudoranges from LTE signals is designed. Third, a threshold-based approach for detecting the first peak of the channel impulse response is proposed in which the threshold adapts to the environmental noise level. This method is demonstrated to be robust against noise and interference in the environment. Fourth, an approach for estimating pseudoranges of multiple base stations by tracking only one base station is proposed. Fifth, a navigation framework based on an extended Kalman filter is proposed to produce the navigation solution using the pseudorange measurements obtained by the proposed SDR. Finally, the proposed SDR is evaluated experimentally on an unmanned aerial vehicle (UAV) and a ground vehicle. The root mean squared-error (RMSE) between the GPS navigation solution and LTE signals from three base stations produced by the proposed SDR for the UAV is shown to be 8.15 m with a standard deviation of 2.83 m. The RMSE between the GPS navigation solution and LTE signals from six base stations in a severe multipath environment for the ground vehicle is shown to be 5.80 m with a standard deviation of 3.02 m.**

***Index Terms*— Navigation, positioning, signals of opportunity, LTE, software-defined receiver.**

I. Introduction

THE Global Positioning System (GPS) has been at the core of virtually all navigation systems over the past few decades, providing accurate positioning and timing information for both military and civilian applications. However, GPS signals are severely attenuated indoors and in deep urban canyons and are susceptible to unintentional interference, intentional jamming, or malicious spoofing [1]–[4]. Recent approaches to overcome GPS drawbacks aimed at exploiting ambient signals of opportunity (SOPs). SOPs are radio frequency (RF) signals that are not designed for navigation purposes and are freely available when GPS signals are unusable [5]–[11].

The literature on SOPs answers theoretical questions on the observability and estimability of the SOPs landscape for various *a priori* knowledge scenarios [12] and prescribes receiver motion strategies for accurate receiver and SOP localization and timing estimation [13]–[15]. Moreover, a number of recent experimental results have demonstrated receiver localization and timing via different SOPs [16]–[20]. Cellular SOPs are particularly attractive for navigation purposes due to their abundance, geometric diversity, high transmitted power, and large bandwidth [21].

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 previous generations of wireless standards. The high bandwidths and data rates employed in LTE systems have made LTE signals attractive for navigation as well.

Two types of positioning techniques can be defined for LTE, namely network-based and user equipment (UE)-based positioning. The network-based positioning capabilities were enabled in LTE Release 9 by introducing a broadcast positioning reference signal (PRS). In positioning with the PRS, the dedicated resources to the PRS are free from the interference and the expected positioning accuracy is on the order of 50 m [22]. 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, UE-based positioning approaches that exploit the cell-specific reference signal (CRS) have been explored, where several advanced signal processing techniques exploited to achieve a performance similar to the PRS [24]–[28].

Software-defined receivers (SDRs) have been recently proposed in the literature for navigation using LTE signals [24], [28]. However, there are several challenges associated with navigating with these SDRs, which rely on acquiring the

Manuscript received August 5, 2017; revised October 30, 2017 and December 22, 2017; accepted December 23, 2017. Date of publication January 12, 2018; date of current version April 8, 2018. This work was supported by the Office of Naval Research under Grant N00014-16-1-2305. The associate editor coordinating the review of this paper and approving it for publication was R. Dinis. *(Corresponding author: Zaher M. Kassas.)*

The authors are with the Department of Electrical and Computer Engineering, University of California, Riverside, CA 92521 USA (e-mail: kimia.shamaei@email.ucr.edu; joe.khalife@email.ucr.edu; zkassas@ieee.org).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2018.2789882

primary synchronization signal (PSS) transmitted by the LTE base station (also known as eNodeB). The first challenge results from the near-far effect created by the strongest PSS, which makes it impossible for the receiver to individually acquire the remaining ambient PSSs. A simple solution would be to track only the strongest PSSs (up to three). This raises a second challenge: the number of intra-frequency eNodeBs that the receiver can simultaneously use for positioning is limited [29]. To circumvent this problem, 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 IDs, signal bandwidths, and the number of transmitting antennas. The literature on LTE-based navigation assumes this information to be known *a priori*, which raises the third challenge associated with the published SDRs. In practice, it is desirable to have a receiver that is capable of obtaining this information on-the-fly in unknown environments.

An initial study addressing these challenges was conducted in [30] in which an SDR was proposed for navigating with LTE signals. The proposed SDR acquires the transmitted signal from the eNodeBs with the highest power. Then, system information and the cell IDs of the neighboring eNodeBs are obtained on-the-fly, which enables the receiver to acquire all the eNodeBs in the environment. The secondary synchronization signal (SSS) is used to track the time-of-arrival (TOA) of each eNodeB. To improve TOA estimation in a multipath environment, the channel impulse response (CIR) is estimated using the CRS, then peaks are detected by assigning a threshold, and finally the TOA is obtained from the first detected peak. While the SDR design in [30] produced promising results, a number of issues were not addressed: (1) design and implementation of a robust and computationally efficient method to detect the first peak of the CIR, (2) tracking the highest number of eNodeBs in the environment to increase geometric diversity, and (3) estimating the clock biases of the receiver and eNodeBs. This paper addresses these issues.

Several studies have been conducted to tackle the first issue of estimating the first peak of the CIR [26], [28], [31]–[34]. In [31] and [32], a method to jointly estimate the CIR and the time delay was proposed. The CIR was modeled statistically by a skew-t distribution in [34], which improves TOA estimation for low bandwidth signals. A super resolution algorithm (SRA) was exploited in [28] to obtain the TOA, which resulted in a root mean squared-error (RMSE) of 31.09 m. Although these methods yielded a relatively good positioning accuracy, they are computationally expensive. A first arriving path detection using maximum likelihood in a correlation-based approach was discussed in [33]. A threshold-based approach was used in [26] and [35] to detect the first path. This method is computationally low-cost, but does not adapt to the environment, which causes significant errors when the noise level changes.

To the authors' knowledge, the second issue has not been addressed in the literature. To overcome the third issue, some approaches assume that the receiver has access to estimates of its own clock bias (from GPS signals), enabling the receiver to estimate the difference between its clock bias and the clock bias of the eNodeB in a post-processing fashion [26], [28]. In practice, the UE may not have access to estimates of its clock bias due to unavailability of GPS signals. Other approaches synchronize the receiver and transmitter through cables in the lab [35].

This paper extends [30] to address these issues and makes the following contributions:

- An SDR architecture for navigating with LTE signals is presented and the signal processing associated with its different stages are discussed.
- A TOA estimation method is presented. This method is highly robust against interference and noise and can be adapted to the particular environment in which the receiver is navigating.
- A method to estimate the TOA from multiple eNodeBs by tracking only one eNodeB is discussed. This enables the receiver to obtain CRS-based TOA measurements from eNodeBs that cannot be acquired and tracked due to their low carrier-to-noise ratio (C/N_0).
- A framework based on an extended Kalman filter (EKF) is discussed to estimate on-the-fly the position of the receiver along with the difference of the clock biases between the receiver and each eNodeB.

In addition, to evaluate the proposed approaches, results from two experimental demonstrations are presented. In the first demonstration, an unmanned aerial vehicle (UAV) is navigating exclusively with LTE signals from 3 eNodeBs. The trajectories corresponding to a GPS solution, which has a horizontal positioning accuracy of 5 m [36], are compared with the proposed LTE SDR solution. The RMSE between the trajectories is shown to be 8.15 m with a standard deviation of 2.83 m and a maximum difference of 12.38 m.

The second demonstration considers a ground vehicle in an urban environment in which the received LTE signal suffered from severe multipath. To alleviate the effect of multipath, the proposed method for detecting the first peak of the CIR is employed. The navigation solution from 6 LTE eNodeBs is compared to the GPS solution. The RMSE between the trajectories is shown to be 5.80 m with a standard deviation of 3.02 m and a maximum difference of 14.96 m. The proposed method is also compared to other methods from the literature.

Throughout the paper, italic small bold letters (e.g., $\boldsymbol{x}$) represent vectors in the time-domain, italic capital bold letters (e.g., $\boldsymbol{X}$) represent vectors in the frequency-domain, and capital bold letters represent matrices (e.g., $\mathbf{X}$).

The remainder of this paper is organized as follows. Section II provides an overview of LTE signals. Section III presents the LTE SDR architecture. Section IV discusses the proposed method for detecting the first peak of the CIR. Section V proposes a method for tracking multiple eNodeBs by tracking only one eNodeB. Section VI presents the framework to obtain the navigation solution. Section VII shows the experimental results. Concluding remarks are given in Section VIII.

II. LTE Frame and Reference Signals Structure

In this section, the architecture of an LTE frame is first discussed. Then, the structure of three main LTE signals which

can be used for navigation, namely the PSS, SSS, and CRS is explained.

A. LTE Frame Structure

In LTE downlink transmission, data is encoded using orthogonal frequency division multiplexing (OFDM). OFDM is a transmission method in which the symbols are mapped onto multiple carrier frequencies called subcarriers. The serial data symbols $\{S_1, \ldots, S_{N_r}\}$ are first parallelized in groups of length N_r, where N_r represents the number of subcarriers that carry data. Then, each group is zero-padded to length N_c, which is the total number of subcarriers, and an inverse fast Fourier transform (IFFT) is taken. The value of N_c is set to be greater than N_r to provide a guard band in the frequency-domain. Finally, to protect the data from multipath effects, the last L_{CP} elements of the obtained symbols are repeated at the beginning of the data, called the cyclic prefix (CP). The transmitted symbols can be obtained at the receiver by executing these steps in reverse order. Since the frequency reuse factor in LTE systems is one, all the eNodeBs of the same operator use the same frequency band. To reduce the interference caused by sharing the same frequency band, each signal is coded to be orthogonal to the transmitted signals from other eNodeBs. Using different frequency bands makes it possible to allocate the same cell IDs to the eNodeBs from different operators.

The obtained OFDM signals are arranged in multiple blocks, which are called frames. In an LTE system, the structure of the frame depends on the transmission type, which can be either frequency division duplexing (FDD) or time division duplexing (TDD). Due to the superior performance of FDD in terms of latency and transmission range, most network providers use FDD for LTE transmission. Hence, this paper considers FDD for LTE transmission and for simplicity an FDD frame is simply called a frame.

A frame is composed of 10 ms data, which is divided into either 20 slots or 10 subframes with a duration of 0.5 ms or 1 ms, respectively. A slot can be decomposed into multiple resource grids (RGs) and each RG has numerous resource blocks (RBs). Then, an RB is broken down into the smallest elements of the frame, namely resource elements (REs). The frequency and time indices of an RE are called subcarrier and symbol, respectively. The structure of the LTE frame is illustrated in Fig. 1 [37].

Note that N_c, N_r, and the total bandwidth W, are assigned by the network provider and can only accept a discrete set of values. The subcarrier spacing is typically $\Delta f = 15$ KHz.

When a UE receives an LTE signal, it must first convert the signal into the frame structure to be able to extract the transmitted information. This is achieved by first identifying the frame start time. Then, knowing the frame timing, the receiver can remove the CPs and take a fast Fourier transform (FFT) of each N_c symbols. The duration of a normal CP is 5.21 μs for the first symbol of each slot and 4.69 μs for the rest of the symbols [37].

B. Timing Signals

To provide symbol timing, the PSS is transmitted on the last symbol of slot 0 and repeated on slot 10. The PSS is a length-62 Zadoff-Chu sequence, which is located in the 62 middle subcarriers of the bandwidth, excluding the DC subcarrier [38]. The PSS is transmitted in only three possible sequences which map to an integer value $N_{ID}^{(2)} \in \{0, 1, 2\}$, representing the sector number of the eNodeB.

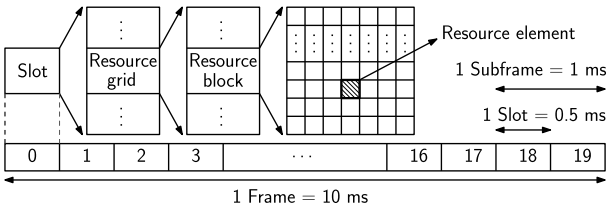

Fig. 1. LTE frame structure.

The SSS is an orthogonal length-62 sequence, which is transmitted in either slot 0 or 10 in the symbol preceding the PSS and on the same subcarriers as the PSS. The SSS is obtained by concatenating two maximal-length sequences scrambled by a third orthogonal sequence generated based on $N_{ID}^{(2)}$. There are 168 possible sequences for the SSS that are mapped to an integer number $N_{ID}^{(1)} \in \{0, \ldots, 167\}$ called the cell group identifier. After determining $N_{ID}^{(1)}$ and $N_{ID}^{(2)}$, the eNodeB's cell ID can be calculated as $N_{ID}^{Cell} = 3N_{ID}^{(1)} + N_{ID}^{(2)}$. The cell ID is used for data association purposes.

The CRS is an orthogonal sequence, which is mainly transmitted to estimate the channel frequency response (CFR). The transmitted OFDM signal from the u-th eNodeB at the k-th subcarrier and on the i-th symbol can be expressed as

$$\boldsymbol{Y}_i^{(u)}(k) = \begin{cases} \boldsymbol{S}_i^{(u)}(k), & \text{if } k \in N_{CRS}^{(u)}, \\ \boldsymbol{D}_i^{(u)}(k), & \text{otherwise}, \end{cases} \tag{1}$$

where $\boldsymbol{S}_i^{(u)}(k)$ represents the CRS sequence; $N_{CRS}^{(u)}$ denotes the set of subcarriers containing the CRS, which is a function of the symbol number, port number, and the cell ID; and $\boldsymbol{D}_i^{(u)}(k)$ represents some other data signals. Assuming that the transmitted signal propagated in an additive white Gaussian noise (AWGN) channel, the received signal in the i-th symbol will be

$$\boldsymbol{R}_i(k) = \sum_{u=0}^{U-1} \boldsymbol{H}_i^{(u)}(k) \boldsymbol{Y}_i^{(u)}(k) + \boldsymbol{W}_i(k), \tag{2}$$

where $\boldsymbol{H}_i^{(u)}(k)$ is the CFR, U is the total number of eNodeBs in the environment, and $\boldsymbol{W}_i(k)$ is a white Gaussian random variable representing the overall noise in the received signal.

III. Receiver Architecture

This section discusses the various stages of the proposed LTE SDR, depicted in Fig. 2.

A. Signal Acquisition

The first step in acquiring an LTE signal is to extract the transmitted frame timing and the eNodeB's cell ID [38]–[40]. These two parameters are obtained by the PSS and the SSS.

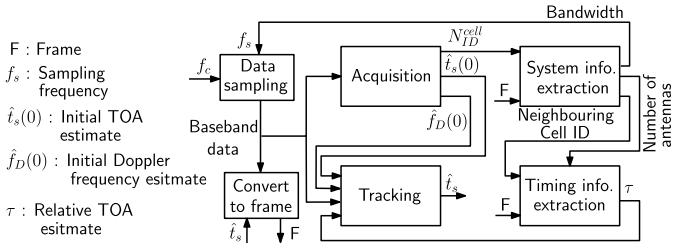

Fig. 2. High-level block diagram of the receiver architecture.

To detect the PSS, the UE exploits the orthogonality of the Zadoff-Chu sequences and correlates the received signal with all the possible choices of the PSS according to

$$\begin{aligned}\text{Corr}(\boldsymbol{r}, \boldsymbol{s}_{PSS})_m &= \sum_{n=0}^{N-1} \boldsymbol{r}(n)\boldsymbol{s}_{PSS}^*(n+m)_N \\ &= \boldsymbol{r}(m) \circledast_N \boldsymbol{s}_{PSS}^*(-m)_N, \end{aligned} \tag{3}$$

where $\boldsymbol{r}(n)$ is the received signal, $\boldsymbol{s}_{PSS}(n)$ is the receiver-generated PSS in time-domain, N is the frame length, $(\cdot)^*$ denotes the complex conjugate, $(\cdot)_N$ denotes the circular shift operator, and $\circledast_N$ represents the circular convolution operation. Taking the FFT and IFFT of (3) yields

$$\text{Corr}(\boldsymbol{r}, \boldsymbol{s}_{PSS})_m = \text{IFFT}\{\boldsymbol{R}(k)\boldsymbol{S}_{PSS}^*(k)\}, \tag{4}$$

where $\boldsymbol{R}(k) \triangleq \text{FFT}\{\boldsymbol{r}(n)\}$ and $\boldsymbol{S}_{PSS}(k) \triangleq \text{FFT}\{\boldsymbol{s}_{PSS}(n)\}$. The FFT-based correlation in (4) is also used to detect the SSS signal. Once the PSS and SSS are detected, the UE can estimate the frame start time.

The apparent Doppler frequency, including the carrier frequency offset due to clock drift and the Doppler shift, can be estimated by the CP as

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

where N_{CP} is the set of CP indices and T_s is the sampling interval [41]. Upon estimating the Doppler frequency, the acquisition of the LTE signal is complete. Fig. 3 summarizes the LTE signal acquisition process.

B. System Information Extraction

Parameters relevant for navigation purposes include the system bandwidth, number of transmitting antennas, and neighboring cell IDs. These parameters are provided to the UE in two blocks, namely the master information block (MIB) and the system information block (SIB). In this section, the decoding of each block is discussed.

1) MIB Decoding: In order to exploit the high-bandwidth CRS signal, which improves the navigation performance in multipath environments or in the presence of interference, the UE must first reconstruct the LTE frame from the received signal. To do so, the actual transmission bandwidth and number of transmitting antennas, which are provided in the MIB, must be decoded. The MIB is transmitted on the physical broadcast channel (PBCH) and consists of 24 bits of data: 3 bits for downlink bandwidth, 3 bits for frame number, and 18 bits for other information and spare bits. The MIB is coded

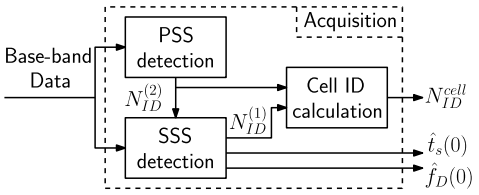

Fig. 3. Signal acquisition block diagram.

and transmitted on 4 consecutive symbols of a frame's second slot. However, it is not transmitted in REs reserved for the reference signals. Fig. 4 shows the steps the MIB message goes through before transmission [37], [42].

In the first step, a cyclic redundancy check (CRC) of length $L = 16$ is obtained using the cyclic generator polynomial $g_{CRC}(D) = D^{16} + D^{12} + D^5 + 1$. The number of transmitting antennas is not transmitted in the 24-bit MIB message. Instead, this information is provided in the CRC mask, which is a sequence used to scramble the CRC bits appended to the MIB. The CRC mask is either all zeros, all ones, or $[0, 1, 0, \ldots, 0, 1]$ for 1, 2, or 4 transmitting antennas, respectively. In order to obtain the number of transmitting antennas from the received signal, the UE needs to perform a blind search over the number of all possible transmitting antennas. Then, by comparing the locally-generated CRC scrambled by the CRC mask to the received CRC, the right number of transmitting antennas may be identified.

In the second step, channel coding is performed using a convolutional encoder with constraint length 7 and coding rate $1/3$. The configuration of the encoder is shown in Fig. 5. The initial value of the encoder is set to the value of the last 6 information bits in the input stream. The method illustrated in Fig. 6 is used to decode the received signal [43]. In this method, the received signal is repeated one time. Then, a Viterbi decoder is executed on the resulting sequence. Finally, the middle part of the sequence is selected and circularly shifted.

In the next step, the convolutional coded bits are rate-matched. In the rate matching step, the obtained data from channel coding is first interleaved. Then, the outcomes of interleaving each stream are repeated to obtain a 1920-bit long array [42]. Next, the output of the rate matching step is scrambled with a pseudo-random sequence, which is initialized with the cell ID, yielding unique signal detection for all eNodeBs. Subsequently, quadrature phase shift keying (QPSK) is performed on the obtained data, resulting in 960 symbols which are mapped onto different layers to provide transmission diversity. To overcome channel fading and thermal noise, space-time coding is utilized. This process is performed in the precoding step. Finally, the resulting symbols are mapped onto the predetermined subcarriers for MIB transmission [42].

2) SIB Decoding: When a UE performs acquisition, it obtains the cell ID of the ambient eNodeB with the highest power, referred to as the main eNodeB in this paper. For navigation purposes, the UE needs access to multiple eNodeBs' signals to estimate its state. One solution is to perform the acquisition for all the possible values of $N_{ID}^{(2)}$. However, this method limits the number of intra-frequency eNodeBs that a UE can simultaneously use for positioning. The second

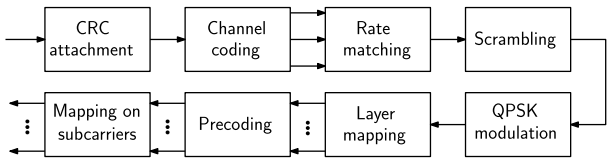

Fig. 4. MIB coding process.

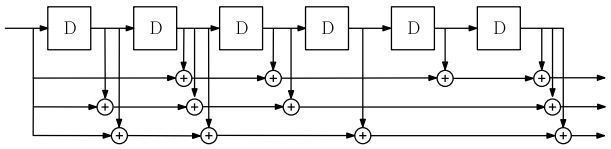

Fig. 5. Tail biting convolutional encoder with constraint length 7 and coding rate $1/3$.

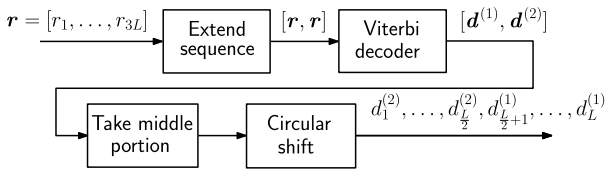

Fig. 6. MIB channel decoding method.

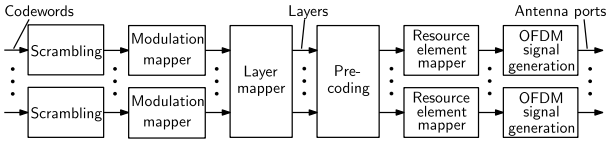

Fig. 7. General structure of downlink physical channels.

solution is to provide a database of the network to the UE. In this method, the UE needs to search over all possible values of the cell IDs to acquire the right ones unless the UE knows its current position, which is not a practical assumption. The other solution, which is more reliable and overcomes the aforementioned problem, is to extract the neighboring cell IDs using the information provided in the SIB transmitted by the main eNodeB. Since other operators transmit on different carrier frequencies, the same approach can be exploited to extract the cell IDs of the neighboring eNodeBs from other operators. Knowing the eNodeBs' cell IDs, the receiver only needs to know the position of the eNodeBs using a database or pre-mapping approaches.

The SIB contains information on (1) the eNodeB to which it is connected, (2) inter- and intra-frequency neighboring cells from the same operator, (3) neighboring cells from other networks (UMTS, GSM, and CDMA2000), and (4) other information. The SIB has 17 different forms called SIB1 to SIB17, which are transmitted in different schedules. SIB1, which is transmitted in subframe 5 of every even frame, carries scheduling information of the other SIBs. This information can be used to extract the schedule of SIB4, which has the intra-frequency neighboring cell IDs. To decode SIB1, the UE has to go through several steps. In each step, the UE needs to decode a physical channel to extract a parameter required to perform other steps.

In general, all the downlink physical channels are coded in a similar fashion before transmission, as shown in Fig. 7. Although all the physical channels have the same general structure, each step in Fig. 7 differs from one channel to another. In Subsection III-B.1, each step was discussed for the PBCH. Further details are given in [37] and [42].

In the following, the steps to retrieve information from SIB4 are briefly outlined:

3) PCFICH Decoding: The UE first obtains the control format information (CFI) from the physical control format indicator channel (PCFICH). The CFI indicates the number of REs dedicated to the downlink control channel and can take the values 1, 2, or 3. To decode the CFI, the UE first locates the 16 REs dedicated to the PCFICH. Then, it demodulates the obtained symbols by reverting the steps in Fig. 7, which results in a sequence of 32 bits. Finally, this sequence, which can be only one of three possible sequences, is mapped onto a CFI value.

4) PDCCH Decoding: The UE can identify the REs associated with the physical downlink control channel (PDCCH) and demodulate them by knowing the CFI. This results in a block of bits corresponding to the downlink control information (DCI) message. The DCI can be transmitted in several formats, which is not communicated with the UE. Therefore, the UE must perform a blind search over different formats to unpack the DCI. The right format is identified by a CRC.

5) PDSCH Decoding: The parsed DCI provides the configuration of the corresponding physical downlink shared channel (PDSCH) REs. The PDSCH, which carries the SIB, is then decoded, resulting in the SIB bits. Subsequently, these bits are decoded using an Abstract Syntax Notation One (ASN.1) decoder, which extracts the system information sent on SIBs by the eNodeB.

Fig. 8 summarizes all the aforementioned steps in this section.

C. Signal Tracking

After acquiring the LTE frame timing, a UE needs to keep tracking the frame timing for two reasons: (1) to produce a pseudorange measurement and (2) to continuously reconstruct the frame. The PSS and SSS are two possible sequences that a UE can exploit to track the frame timing. The PSS has only three different sequences, which causes two main problems in choosing the PSS for tracking: (1) the interference from neighboring eNodeBs with the same sector IDs is high and (2) the number of eNodeBs that the UE can simultaneously track is limited. The SSS is expressible in 168 different sequences, hence does not suffer from the same problems as the PSS. Therefore, the SSS will be exploited for tracking the frame timing. In this section, the components of the tracking loops are discussed, namely a frequency-locked loop (FLL)-assisted phase-locked loop (PLL) and a carrier-aided delay-locked loop (DLL).

1) FLL-Assisted PLL: The frequency reuse factor in LTE systems is set to be one, which results in high interference from neighboring cells. Under interference and dynamic stress, FLLs have better performance than PLLs. However, PLLs have significantly higher measurement accuracy compared to FLLs. An FLL-assisted PLL has both the dynamic and interference robustness of FLLs and the high accuracy of PLLs [44]. The main components of an FLL-assisted PLL are: a phase discriminator, a phase loop filter, a frequency

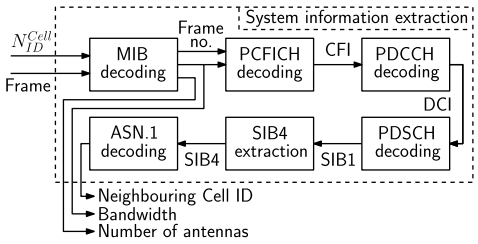

Fig. 8. System information extraction block diagram.

discriminator, a frequency loop filter, and a numerically-controlled oscillator (NCO). The SSS is not modulated with other data. Therefore, an `atan2` 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 designed to track the carrier phase, with a loop filter transfer function given by

$$F_{\text{PLL}}(s) = 2.4\,\omega_{n,p} + \frac{1.1\omega_{n,p}^2}{s} + \frac{\omega_{n,p}^3}{s^2}, \tag{5}$$

where $\omega_{n,p}$ is the undamped natural frequency of the phase loop, which can be related to the PLL noise-equivalent bandwidth $B_{n,\text{PLL}}$ by $B_{n,\text{PLL}} = 0.7845\,\omega_{n,p}$ [45]. 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 estimate. The phase loop filter transfer function in (5) is discretized and realized in state-space. 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 $S_{p_k} = I_{p_k} + j\,Q_{p_k}$ is the prompt correlation at time-step k and $T_{sub} = 10$ ms is the subaccumulation period, which is chosen to be one frame length. The transfer function of the frequency loop filter is given by

$$F_{\text{FLL}}(s) = 1.414\,\omega_{n,f} + \frac{\omega_{n,f}^2}{s}, \tag{6}$$

where $\omega_{n,f}$ is the undamped natural frequency of the frequency loop, which can be related to the FLL noise-equivalent bandwidth $B_{n,\text{FLL}}$ by $B_{n,\text{FLL}} = 0.53\,\omega_{n,f}$ [45]. 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 (6) is discretized and realized in state-space.

2) DLL: The carrier-aided DLL employs the non-coherent dot-product discriminator given by

$$e_{c_k} = C\left[(I_{e_k} - I_{l_k})I_{p_k} + (Q_{e_k} - Q_{l_k})Q_{p_k}\right],$$

where e_{c_k} is the code phase error and C is a normalization constant given by

$$C = \frac{T_c}{2(\mathbb{E}\{|S_{p_k}|^2\} - 2\sigma_{IQ}^2)},$$

where $S_{e_k} = I_{e_k} + j\,Q_{e_k}$ and $S_{l_k} = I_{l_k} + j\,Q_{l_k}$ are the early and late correlations, respectively, $T_c = \frac{1}{W_{SSS}}$ is the chip interval, $W_{SSS} = 63 \times 15 = 945$ KHz is the SSS bandwidth, $\mathbb{E}\{\cdot\}$ represents the expectation operator, and σ_{IQ}^2 is the interference-plus-noise variance. Section IV discusses how the overall noise level including interference and channel noise is calculated.

The DLL loop filter was chosen to be similar to (6), with a noise-equivalent bandwidth $B_{n,\text{DLL}}$ Hz. The output of the DLL loop filter v_{DLL} (in s/s) is the rate of change of the SSS code phase. Assuming low-side mixing, the code start time is updated according to

$$\hat{t}_s(k+1) = \hat{t}_s(k) - T_{sub}\,(v_{\text{DLL},k} + \hat{f}_D(k)/f_c).$$

The SSS code start time estimate is used to reconstruct the transmitted frame. Fig. 9 shows the block diagram of the tracking loops, where $\omega_c = 2\pi f_c$ and f_c is the carrier frequency (in Hz).

D. Timing Information Extraction

In LTE systems, the PSS and SSS are transmitted with the lowest possible bandwidth. The ranging precision and accuracy of the SSS is analyzed in [46], which shows that the SSS can provide very precise ranging resolution using conventional DLLs in an environment without multipath. However, because of its relatively low bandwidth, the SSS is extremely susceptible to multipath. To achieve more precise localization using LTE signals, the CRS can be exploited. Ranging precision of the SSS and the CRS in a semi-urban environment with multipath were compared experimentally in [47], which showed that the CRS is more robust to multipath.

In the timing information extraction stage of the receiver, the TOA is estimated by detecting the first peak of the CIR. The TOA estimate is then fed back to the tracking loops to improve SSS tracking. Fig. 10 shows the block diagram of the timing information extraction stage. A method for estimating the TOA is proposed in Section IV.

IV. Path Delay Estimation

In this section, a TOA estimation method is proposed. This method is a first-peak estimation algorithm in which the threshold adapts to the environmental noise.

A. Multipath Detection

The received signal model in the i-th symbol was presented in (2). The subscript i will be dropped in the sequel for simplicity of notation. The estimated CFR of the u-th eNodeB is given by

$$\hat{\boldsymbol{H}}^{(u)}(k) = \boldsymbol{S}^{(u)^*}(k)\boldsymbol{R}(k) = \boldsymbol{H}^{(u)}(k) + \boldsymbol{V}^{(u)}(k), \quad k \in N_{CRS}^{(u)}, \tag{7}$$

where $\boldsymbol{V}^{(u)}(k) \triangleq \boldsymbol{S}^{(u)^*}(k)\boldsymbol{W}(k)$. Equation (7) is obtained using the fact that $\left|\boldsymbol{S}^{(u)}(k)\right|^2 = 1$.

The CIR estimate is obtained by taking an IFFT from the estimated CFR given by

$$\hat{\boldsymbol{h}}^{(u)}(n) = \text{IFFT}\left\{\hat{\boldsymbol{H}}^{(u)}(k)\right\} = \boldsymbol{h}^{(u)}(n) + \boldsymbol{v}^{(u)}(n), \tag{8}$$

where $\boldsymbol{v}^{(u)}(n) \triangleq \text{IFFT}\{\boldsymbol{V}^{(u)}(k)\} \sim \mathcal{CN}(0, \sigma_h^2)$.

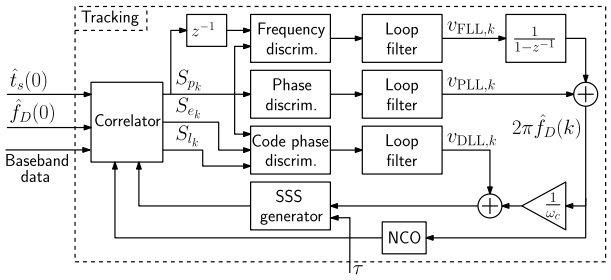

Fig. 9. Signal tracking block diagram.

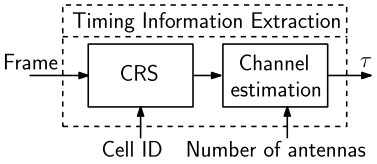

Fig. 10. Timing information extraction block diagram.

In general, a multipath CIR can be modeled as

$$\boldsymbol{h}^{(u)}(n) = \sum_{l=0}^{L^{(u)}-1} \boldsymbol{\alpha}^{(u)}(l)\delta[n - \boldsymbol{d}^{(u)}(l)], \quad \text{for} \quad n = 0, \ldots, N_h - 1,$$

where $\boldsymbol{\alpha}^{(u)}(l)$ and $\boldsymbol{d}^{(u)}(l)$ are the attenuation and the delay of the l-th path to the u-th eNodeB, respectively, $N_h = |N_{CRS}^{(u)}|$, and $L^{(u)}$ is the number of multipath components [48]. To simplify the derivation, it is assumed that the receiver's low-pass filter has infinite bandwidth. The goal is to estimate $\boldsymbol{d}^{(u)}(0)$, which represents the line-of-sight (LOS) TOA. In the absence of noise, $L^{(u)}$ will be the number of non-zero components in the estimated CIR, and the position of the non-zero components will be $\boldsymbol{d}^{(u)}$. In the presence of noise, the receiver must be able to distinguish between noise and multipath components at each specific n in the estimated CIR. This problem is similar to detecting the presence of a target, $\boldsymbol{h}^{(u)}(\boldsymbol{d}^{(u)})$ (not necessarily a single target), in a noisy environment. Therefore, the problem can be modeled as a binary hypothesis test, with H_1 indicating the presence of a target (LOS or multipath signal) and noise, and H_0 indicating the presence of only noise. The hypotheses can be expressed as

$$H_0 : \hat{\boldsymbol{h}}^{(u)}(n) = \boldsymbol{v}^{(u)}(n), \quad \text{for } n \neq \boldsymbol{d}^{(u)}(l),$$
$$H_1 : \hat{\boldsymbol{h}}^{(u)}(n) = \boldsymbol{\alpha}^{(u)}(l) + \boldsymbol{v}^{(u)}(n), \quad \text{for } n = \boldsymbol{d}^{(u)}(l),$$

where $l = 0, \ldots, L^{(u)} - 1$. It is worth mentioning that the receiver does not have any knowledge of $\boldsymbol{\alpha}^{(u)}(l)$, $\boldsymbol{d}^{(u)}(l)$, and $L^{(u)}$. Under H_0, $\hat{\boldsymbol{h}}^{(u)}(n) = \boldsymbol{v}^{(u)}(n)$; therefore, $|\hat{\boldsymbol{h}}^{(u)}(n)|$ has a Rayleigh distribution with a probability density function (pdf) given by

$$p\left(|\hat{\boldsymbol{h}}^{(u)}(n)| = r \middle| H_0\right) = \frac{2r}{\sigma_h^2} e^{\left(-\frac{r^2}{\sigma_h^2}\right)}.$$

Under H_1, $\hat{\boldsymbol{h}}^{(u)}(n) = \boldsymbol{\alpha}^{(u)}(l) + \boldsymbol{v}(n)$, where $\boldsymbol{\alpha}^{(u)}(l)$ is assumed to be a complex deterministic constant over a frame duration. Therefore, $|\hat{\boldsymbol{h}}^{(u)}(n)|$ has a Rician distribution with the pdf

$$p\left(|\hat{\boldsymbol{h}}^{(u)}(n)| = r \middle| H_1\right) = \frac{2r}{\sigma_h^2} e^{\left(-\frac{r^2+s^2}{\sigma_h^2}\right)} I_0\left(\frac{2rs}{\sigma_h^2}\right),$$

where $r \geq 0$, $I_0(\cdot)$ is the modified Bessel function of zeroth-order, and $s = |\boldsymbol{\alpha}^{(u)}(l)|$.

A Neyman-Pearson test is formulated to obtain the decision threshold, denoted η, where the probability of false alarm p_{FA} is set to a desired constant and is given by

$$p_{FA} = \int_{\eta}^{\infty} p\left(|\hat{\boldsymbol{h}}^{(u)}(n)| = r \middle| H_0\right) dr = e^{-\frac{\eta^2}{\sigma_h^2}}. \tag{9}$$

The threshold is then calculated as

$$\eta = \sqrt{-\sigma_h^2 \ln(p_{FA})}. \tag{10}$$

After determining the threshold, the detection probability is obtained using

$$p_D = \int_{\eta}^{+\infty} \frac{2r}{\sigma_h^2} e^{\left(-\frac{r^2+|\boldsymbol{\alpha}^{(u)}(l)|^2}{\sigma_h^2}\right)} I_0\left(\frac{2r|\boldsymbol{\alpha}^{(u)}(l)|}{\sigma_h^2}\right) dr.$$

Although it is not possible to obtain a closed-form expression for the probability of detection, numerical solutions for p_D have been tabulated and can also be computed with software packages [49]. Fig. 11 demonstrates the receiver operating characteristics (ROC) for different $C/N_0 \triangleq |\boldsymbol{\alpha}^{(u)}(l)|^2/N_0$, where $N_0 \triangleq 2\sigma_h^2/\Delta f$.

B. CFAR for Adaptive Threshold Calculation

The derived threshold equation in (10) showed that the threshold is dependent on the noise variance, σ_h^2. However, the noise variance continuously changes in a dynamic environment, and the threshold must be updated accordingly. Changing the threshold to keep a constant p_{FA} is defined as constant false alarm rate (CFAR). Cell-averaging CFAR (CA-CFAR), shown in Fig. 12, is one of the CFAR techniques [50].

In CA-CFAR, each cell is tested for the presence of a signal. For a given cell under test (CUT), a functional of N_t training cells separated from the CUT by N_g guard cells is computed. In a square-law detector, this functional will be the sum of $|\hat{\boldsymbol{h}}^{(u)}(n)|^2$, which is proportional to the background noise level given by

$$P_n = \sum_{m=1}^{N_t} x_m,$$

where x_m is the functional evaluated at the m-th training cell. A threshold can be obtained by multiplying P_n by a constant K, hence $\eta = KP_n$, which can be shown to have a non-central chi-square distribution with $2N_t$ degrees of freedom. The probability of false alarm for a specified threshold was calculated in (9). The p_{FA} in CA-CFAR can be obtained by taking the average of (9) over all possible values of the decision threshold. This yields

$$\eta = \left(p_{FA}^{-1/N_t} - 1\right) P_n,$$

which is used to compare the desired cell's value to the noise floor.

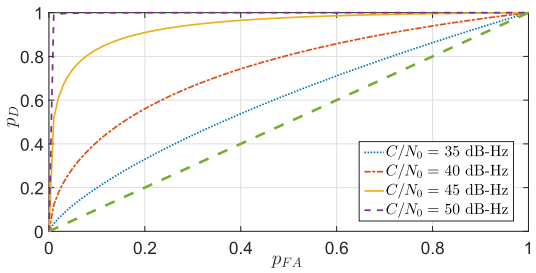

Fig. 11. ROC for different C/N_0.

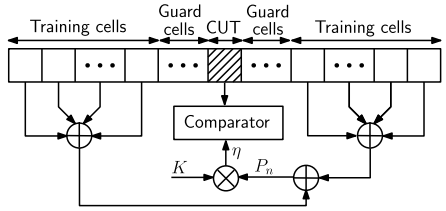

Fig. 12. Block diagram of the CA-CFAR.

To improve the probability of detection while maintaining a constant p_{FA}, a non-coherent integration can be used. For this purpose, it is proposed to integrate squared envelopes of $\hat{h}^{(u)}(n)$ at different slots and for different transmitting antennas (assuming that they have the same LOS path) in one frame duration. Defining n_i as the number of non-coherent integrations, averaging is performed over $n_i N_t$ training cells. Therefore, after integration, the threshold will have a non-central chi-square distribution with $2\,n_i N_t$ degrees of freedom. By taking the average of the probability of false alarm given the threshold presented in (9) over the new pdf of this threshold, it can be shown that [50]

$$p_{FA} = \frac{1}{(1+K)^{n_i N_t}} \sum_{k=0}^{n_i-1} \frac{1}{k!} \frac{\Gamma(n_i N_t + k)}{\Gamma(n_i N_t)} \left(\frac{K}{K+1}\right)^k, \quad (11)$$

where $\Gamma(n) = (n-1)!$ is the gamma function. By knowing p_{FA} and its relation to K according to (11), the value of K can be solved numerically (e.g. using Newton algorithm) and the threshold will be determined from $\eta = K P_n$.

Using the proposed method for tracking the TOA, the probability of false alarm in detecting the first peak means that noise is erroneously detected as a valid signal, which can cause significant errors and potentially loss of track. To resolve this problem, a low-pass filter is applied after the CFAR detector, which removes sudden changes in the estimated TOA. The localization error with the proposed method is acceptable for medium to high bandwidth LTE signals (e.g. above 10 MHz). For lower bandwidths, other methods could be exploited [34]. After detecting $\boldsymbol{d}^{(u)}(0)$, the residual TOA, $\tau = T_s\,\boldsymbol{d}^{(u)}(0)$, is fed-back to the tracking loops to improve the estimated frame start time $\hat{t}_s$.

V. Tracking Multiple eNodeBs

To estimate the position of the receiver in a two-dimensional (2-D) plane using a static estimator, the pseudoranges to at least three eNodeBs are required and can be obtained by tracking the signal of each eNodeB. However, tracking all signals is computationally involved and could prohibit real-time implementation. Besides, the received signal from an eNodeB may be highly attenuated; therefore, it may not be possible to track all ambient SSSs. In this section, a new method is proposed that exploits the frequency reuse factor of six in the LTE CRS signals to extract the pseudorange of multiple eNodeBs while tracking only one eNodeB. In this approach, the receiver may obtain a list of the neighboring eNodeBs by decoding the SIB of the main eNodeB. Once the neighboring eNodeBs cell IDs are known, the receiver may generate the CRS sequence transmitted by each neighboring eNodeB. With some assumption on the relative delay (including distance and clock bias) between eNodeBs, which will be discussed in this section, the receiver may be able to estimate the CIR of the neighboring eNodeBs in reference to the main eNodeB. Then, relative delay is calculated from the CIR for each new frame, which alleviates the need to track the SSS of the neighboring cell IDs.

The received symbol at the UE can be written as

$$\boldsymbol{r}(n) = \boldsymbol{r}^{(1)}(n) + \sum_{u=2}^{U} \boldsymbol{r}^{(u)}(n) + \boldsymbol{w}(n), \quad (12)$$

where $\boldsymbol{r}^{(1)}(n)$ is the received symbol from the main eNodeB, $\boldsymbol{r}^{(u)}(n)$ is the received signal from the u-th eNodeB at time n, and $\boldsymbol{w}(n)$ is modeled as an additive white Gaussian noise with variance σ^2_{IQ}. Defining the received time delay of the u-th eNodeB as $\boldsymbol{d}^{(u)}(0)$, which in effect measures the TOA and the clock biases (see Section IV), the signal will be received in one of three possible scenarios shown in Fig. 13. Fig. 13(a) shows the first scenario, which happens when the difference of the distances to the main eNodeB and to the neighboring eNodeB is less than the duration of the CP. For a CP of length 4.69 μs, this difference must be less than 1406 m. Fig. 13(b) shows the second scenario, where the difference is more than the length of a CP. Fig. 13(c) represents the third scenario, where the neighboring eNodeB is closer to the receiver than the main eNodeB. In the second scenario, the neighboring eNodeBs are significantly far, and it is assumed that the received signals from these eNodeBs are highly attenuated. It is also assumed that the third scenario does not happen since the main eNodeB is defined as the eNodeB with the highest power, which is usually the closest eNodeB to the receiver.

Defining $n_d^{(u)} \triangleq n^{(u)}(0) - n^{(1)}(0)$ as the time delay difference between the u-th eNodeB and the main eNodeB, it can be concluded that for $0 \le n_d^{(u)} \le L_{CP}$,

$$\boldsymbol{r}^{(u)}(n) = \boldsymbol{r}^{(u)}(n - n_d^{(u)})_{N_c}. \quad (13)$$

By taking the FFT of (12) and using (2) and (13), the received signal in the frequency-domain becomes

$$\boldsymbol{R}(k) = \boldsymbol{H}^{(1)}(k)\boldsymbol{Y}^{(1)}(k) + \sum_{u=2}^{U} \boldsymbol{H}^{(u)}(k)\boldsymbol{Y}^{(u)}(k) e^{-j\frac{2\pi n_d^{(u)} k}{N_c}} + \boldsymbol{W}(k).$$

For the symbols carrying the CRS, $\boldsymbol{Y}$ follows the definition in (1). Therefore, the CFR of the main eNodeB can be obtained from

$$\hat{\boldsymbol{H}}^{(1)}(k) = \boldsymbol{R}(k)\boldsymbol{S}^{(1)*}(k) = \boldsymbol{H}^{(1)}(k) + \boldsymbol{V}^{(1)}(k), \quad \text{for } k \in N_{CRS}^{(1)},$$

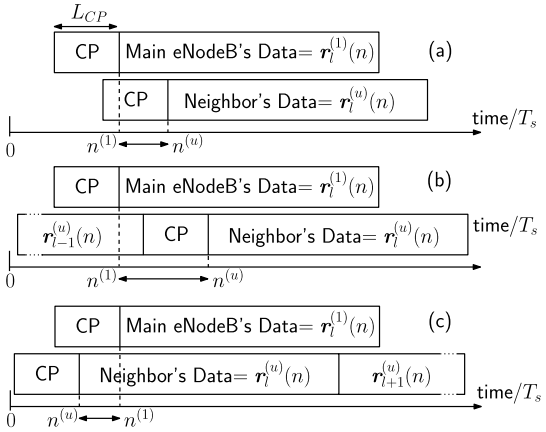

Fig. 13. The received symbols of the main and neighboring eNodeBs for: (a) $0 \le n_d^{(u)} \le L_{CP}$, (b) $n_d^{(u)} > L_{CP}$, and (c) $n_d^{(u)} < 0$.

and the estimated CFRs for other eNodeBs are obtained according to

$$\hat{\boldsymbol{H}}^{(u)}(k) = \boldsymbol{R}(k)\boldsymbol{S}^{(u)*}(k) = \boldsymbol{H}^{(u)}(k)e^{-\frac{j2\pi k n_d^{(u)}}{N_c}} + \boldsymbol{V}^{(u)}(k), \quad \text{for } k \in N_{CRS}^{(u)}.$$

Subsequently, the CIRs are calculated using

$$\begin{aligned} \hat{\boldsymbol{h}}^{(1)}(n) &= \boldsymbol{h}^{(1)}(n) + \boldsymbol{v}^{(1)}(n), \\ \hat{\boldsymbol{h}}^{(u)}(n) &= \boldsymbol{h}^{(u)}(n - n_d^{(u)}) + \boldsymbol{v}^{(u)}(n). \end{aligned} \tag{14}$$

After obtaining $\hat{\boldsymbol{h}}^{(u)}(n)$, the method proposed in Section IV can be exploited to determine the first peak of $\hat{\boldsymbol{h}}^{(u)}(n)$, which represents $n_d^{(u)}$. The u-th eNodeB TOA can be calculated as

$$\boldsymbol{d}^{(u)}(0) = \boldsymbol{d}^{(1)}(0) + n_d^{(u)}.$$

It is worth mentioning that in this method, the phase and frequency offsets of the neighboring eNodeBs are not tracked. The proposed approach is applicable when the carrier frequency offset between the eNodeBs is less than a subcarrier spacing. This is a practical assumption since the eNodeBs in LTE systems are tightly synchronized in frequency. The other challenge of using this method is that it depends on the relative location of the main eNodeB and the neighboring eNodeB, and it is applicable only when the condition $0 \le n_d^{(u)} \le L_{CP}$ is satisfied.

It is worth mentioning that in a conventional timing acquisition, all eNodeBs must be acquired and tracked separately. In the proposed approach, only the main eNodeB needs to be acquired and tracked, and TOA estimates from neighboring eNodeBs may be obtained by using timing and neighboring cell ID information obtained from the main eNodeB. The parameter n_d depends on the eNodeB clock as well as on the distance between the eNodeB and the receiver, and it must be calculated for every frame, regardless of the eNodeB clock.

VI. Navigation Solution

Sections III–V discussed how TOA estimates can be extracted from LTE signals. By multiplying the obtained TOA for the u-th eNodeB, $\hat{t}_s^{(u)}$, by the speed-of-light, c, pseudorange measurements are formed as

$$\rho_u(k) = ||\boldsymbol{r}_r(k) - \boldsymbol{r}_{s_u}||_2 + c \cdot \left[\delta t_r(k) - \delta t_{s_u}(k)\right] + \upsilon_u(k),$$

where k is the time-step; $\boldsymbol{r}_r = [x_r, y_r]^\mathsf{T}$ is the receiver's position vector; $\boldsymbol{r}_{s_u} = \left[x_{s_u}, y_{s_u}\right]^\mathsf{T}$ is the u-th eNodeB's position vector; δt_r and δt_{s_u} are the receiver's and u-th eNodeB's clock biases, respectively, and υ_u is the measurement noise and is modeled as a zero-mean Gaussian random variable with variance σ_u^2. This section discusses receiver state estimation from these measurements.

One of the main challenges in navigation with LTE signals is the lack of knowledge of the eNodeBs' positions and clock biases. It has been previously shown that an SOP's position can be mapped with a high degree of accuracy, whether collaboratively or non-collaboratively [51], [52]. Therefore, in this paper, it is assumed that the positions of the eNodeBs are known to the receiver. In some LTE deployments, the eNodeBs are required to be synchronized to within 3 μs [53]. Although this synchronization is sufficient for communications systems, it introduces significantly high error in navigation applications. Therefore, the eNodeBs' clock biases, which are stochastic and dynamic, must be continuously estimated using a dynamic estimator (e.g., an EKF). In this paper, an EKF is used to estimate the position of the receiver and the difference of the clock biases of the receiver and each eNodeB, simultaneously. Observability analysis of an environment comprising multiple receivers and transmitters has been thoroughly addressed in [12]. The receiver is assumed to have enough *a priori* knowledge to make this environment observable, namely its initial position and velocity, initial clock bias and drift, and the eNodeBs' locations. Knowing the receiver's *initial* position and velocity and its *initial* clock bias and drift could be obtained from GPS, for example, while the eNodeBs' locations could be mapped *a priori* or obtained from a database. Using the pseudoranges obtained from the proposed LTE navigation receiver, an estimator could estimate the state vector composed of the receiver's position and velocity as well as the difference between the clock bias of the receiver and each eNodeB and the difference between the clock drift of the receiver and each eNodeB, specifically

$$\boldsymbol{x} = \left[\boldsymbol{x}_{pv}^\mathsf{T}, \boldsymbol{x}_{clk_1}^\mathsf{T}, \ldots, \boldsymbol{x}_{clk_U}^\mathsf{T}\right]^\mathsf{T},$$

where $\boldsymbol{x}_{pv} \triangleq [\boldsymbol{r}_r^\mathsf{T}, \dot{\boldsymbol{r}}_r^\mathsf{T}]^\mathsf{T}$; $\dot{\boldsymbol{r}}_r$ is the receiver's velocity vector; $\boldsymbol{x}_{clk_u} \triangleq [(\delta t_r - \delta t_{s_u}), (\delta \dot{t}_r - \delta \dot{t}_{s_u})]^\mathsf{T}$; $\delta \dot{t}_r$ and $\delta \dot{t}_{s_u}$ are the receiver's and u-th eNodeB's clock drifts, respectively. The pseudorange measurements are obtained each T_{sub} second, which was defined to be the subaccumulation period. Assuming the receiver to be moving according to a velocity random walk, the system's dynamics after discretization at a uniform sampling period T_{sub} can be modeled as

$$\begin{aligned} \boldsymbol{x}(k+1) &= \mathbf{F}\boldsymbol{x}(k) + \boldsymbol{w}(k), \\ \mathbf{F} &= \begin{bmatrix} \mathbf{F}_{pv} & \mathbf{0}_{4\times 2U} \\ \mathbf{0}_{2U\times 4} & \mathbf{F}_{clk} \end{bmatrix}, \ \mathbf{F}_{clk} = \text{diag}\left[\mathbf{F}_{clk_1}, \ldots, \mathbf{F}_{clk_U}\right], \\ \mathbf{F}_{clk_u} &= \begin{bmatrix} 1 & T_{sub} \\ 0 & 1 \end{bmatrix}, \mathbf{F}_{pv} = \begin{bmatrix} \mathbf{I}_{2\times 2} & T_{sub}\mathbf{I}_{2\times 2} \\ \mathbf{0}_{2\times 2} & \mathbf{I}_{2\times 2} \end{bmatrix}, \end{aligned} \tag{15}$$

and $\boldsymbol{w}_k$ is a discrete-time zero-mean white noise sequence with covariance $\mathbf{Q} = \text{diag}[\mathbf{Q}_{pv}, \mathbf{Q}_{clk}]$. Defining $\tilde{q}_x$ and $\tilde{q}_y$ to be the power spectral densities of the acceleration in x and y directions, $\mathbf{Q}_{pv}$ and $\mathbf{Q}_{clk}$ are obtained as

$$\mathbf{Q}_{pv} = \begin{bmatrix} \tilde{q}_x \frac{T_{sub}^3}{3} & 0 & \tilde{q}_x \frac{T_{sub}^2}{2} & 0 \\ 0 & \tilde{q}_y \frac{T_{sub}^3}{3} & 0 & \tilde{q}_y \frac{T_{sub}^2}{2} \\ \tilde{q}_x \frac{T_{sub}^2}{2} & 0 & \tilde{q}_x T_{sub} & 0 \\ 0 & \tilde{q}_y \frac{T_{sub}^2}{2} & 0 & \tilde{q}_y T_{sub} \end{bmatrix},$$

$$\mathbf{Q}_{clk} = \begin{bmatrix} \mathbf{Q}_{clk_1} & \mathbf{Q}_{clk_r} & \cdots & \mathbf{Q}_{clk_r} \\ \mathbf{Q}_{clk_r} & \mathbf{Q}_{clk_2} & \cdots & \mathbf{Q}_{clk_r} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{Q}_{clk_r} & \mathbf{Q}_{clk_r} & \cdots & \mathbf{Q}_{clk_U} \end{bmatrix},$$

where $\mathbf{Q}_{clk_r}$ and $\mathbf{Q}_{clk_u}$ are defined as

$$\mathbf{Q}_{clk_u} \triangleq \mathbf{Q}_{clk_r} + \mathbf{Q}_{clk_{s_u}},$$

$$\mathbf{Q}_{clk_r} = \begin{bmatrix} S_{\tilde{w}_{\delta t_r}} T_{sub} + S_{\tilde{w}_{\dot{\delta} t_r}} \frac{T_{sub}^3}{3} & S_{\tilde{w}_{\dot{\delta} t_r}} \frac{T_{sub}^2}{2} \\ S_{\tilde{w}_{\dot{\delta} t_r}} \frac{T_{sub}^2}{2} & S_{\tilde{w}_{\dot{\delta} t_r}} T_{sub} \end{bmatrix},$$

where $S_{\tilde{w}_{\delta t_r}}$ and $S_{\tilde{w}_{\dot{\delta} t_r}}$ are the clock bias and drift process noise power spectra, respectively, and $\mathbf{Q}_{clk_{s_u}}$ has a structure similar to $\mathbf{Q}_{clk_r}$, except that $S_{\tilde{w}_{\delta t_r}}$ and $S_{\tilde{w}_{\dot{\delta} t_r}}$ are replaced with $S_{\tilde{w}_{\delta t_{s_u}}}$ and $S_{\tilde{w}_{\dot{\delta} t_{s_u}}}$, respectively.

Note that our estimator assumes the receiver to be mobile. For the stationary receiver case, a more advanced estimator (e.g., multiple model (MM)-type estimator [54]) could be employed. In this case, one mode of the estimator is matched to a velocity random walk dynamics, while the other mode is matched to a stationary dynamics. In practice, the receiver is typically coupled with an inertial measurement unit (IMU), which is used to propagate the estimator's state between measurement updates from eNodeBs [20].

VII. Experimental Results

In this section, the performance of the proposed SDR is evaluated. First, the output of each block of the receiver processing real LTE signals is provided. Then, experimental results for a UAV and a ground vehicle navigating exclusively with real LTE signals are presented. In each case, the details of the exploited hardware and software are provided. Finally, key concluding remarks are discussed.

A. Proposed SDR Outputs

This subsection presents the internal signals of the proposed receiver, which was implemented in LabVIEW and MATLAB. An experiment was performed with the proposed receiver, which was stationary and located close to an eNodeB. In the first stage of the receiver, acquisition was performed on the received signal, as discussed in Subsection III-A. The normalized correlation of the received LTE signal with locally generated PSS and SSS signals are presented in Fig. 14. It can be seen that since the PSS is transmitted twice per frame, the correlation result has two peaks in the duration of one frame, which is 10 ms. However, the SSS correlation result has only one peak, since the SSS is transmitted only once per frame. The result also showed that the highest PSS correlation peak was at $N_{ID}^{(2)} = 0$ and the highest SSS correlation peak was at $N_{ID}^{(1)} = 77$. Therefore, the cell ID was calculated to be $N_{ID}^{Cell} = 3 \times 77 + 0 = 231$.

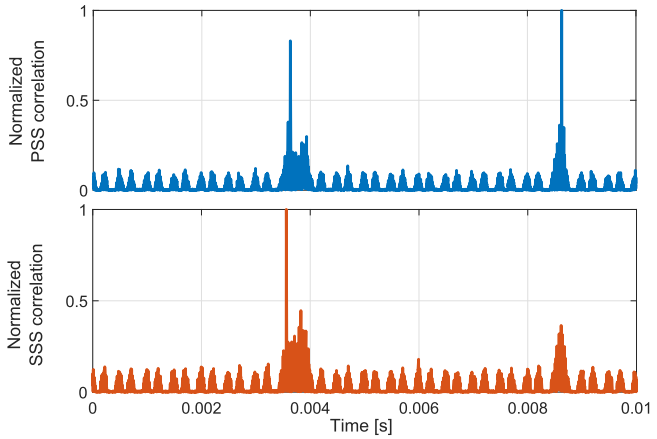

Fig. 14. PSS and SSS normalized correlation results with real LTE signals.

In the second stage, system information is extracted from the received signal according to Subsection III-B. The results showed that the LTE signal was transmitted at a bandwidth of 10 MHz with 2 transmitting antennas. The neighboring cell IDs were also obtained for this eNodeB. The rate at which information extraction must be performed depends on the receiver dynamics. A receiver that moves very fast may need to extract the information every few seconds since the environment is changing quickly; however, a static receiver may not need to extract the information frequently. One approach to obtain the rate at which system information is extracted can be based on the estimated C/N_0 of the eNodeBs. In the results provided in the next two subsections, the C/N_0 of the eNodeBs remains high during the test; therefore, information extraction is performed only once at the start position. Information extraction is not a time consuming process, and it can be performed in parallel with the tracking stage.

In the third stage, the received signal is tracked using the architecture discussed in Subsection III-C. The PLL, FLL, and DLL noise-equivalent bandwidths were set to 4, 0.2, and 0.001 Hz, respectively. To calculate the interference-plus-noise variance, the received signal was correlated with an orthogonal sequence that is not transmitted by any of the eNodeBs in the environment. Then, the average of the squared-magnitude of the correlation was assumed to be the interference-plus-noise variance. Fig. 15 shows the tracking results. Since the receiver was stationary and its clock was driven by a GPS-disciplined oscillator (GPSDO), the Doppler frequency was stable around zero.

B. UAV Experiment

In this subsection, the proposed LTE SDR and navigation framework are employed to navigate a UAV exclusively with

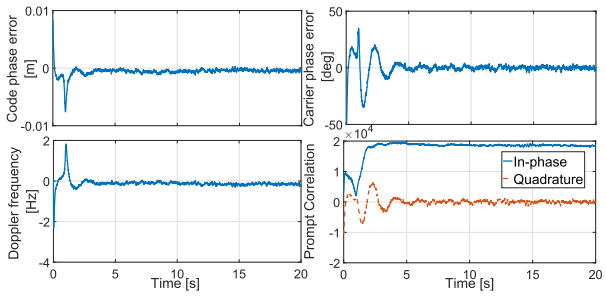

Fig. 15. Tracking results for a stationary receiver.

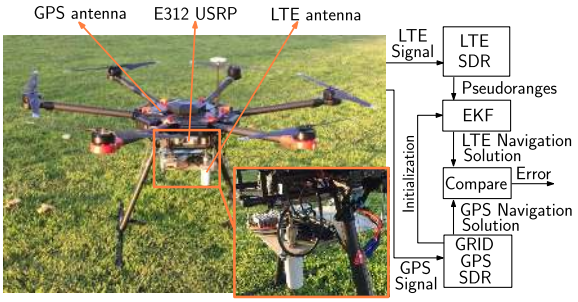

Fig. 16. UAV experimental hardware and software setup. The LTE and GPS antennas were connected to an Ettus E312 USRP driven by a GPSDO. The stored LTE and GPS signals were processed with the proposed SDR and GRID SDR, respectively. The LTE navigation solution was obtained from an EKF and compared to the GPS navigation solution.

LTE signals. To the author's knowledge, these results represent the first demonstration of a UAV navigating exclusively with LTE signals.

1) UAV Experimental Setup: When a UAV flies high enough, it can be assumed that the received signal to the UAV does not experience multipath from the surrounding environment, except from the UAV's body. In this paper, a UAV with body size less than 1 m was used; therefore, the effect of multipath from the UAV's body is neglected. In this case, tracking the SSS only yields good results; hence, the CRS was not used to improve the navigation solution. This will significantly decrease the computational cost of the receiver. It also reduces the need for high sampling rate, which results in lower hardware cost as well. Low sampling rates also allow for lightweight hardware, which is critical for UAVs with limited payload.

Fig. 16 shows the experimental setup used in performing the experiment with a UAV. In this experiment, a DJI Matrice 600 was equipped with:

- one consumer-grade 800/1900 MHz cellular omnidirectional Laird antenna to receive LTE signals at a frequency of 1955 MHz, which is used by AT&T (LTE network provider),
- an Ettus E312 universal software radio peripheral (USRP) driven by a GPSDO to down-mix and sample LTE signals,
- one small consumer-grade antenna for receiving GPS signals to discipline the URSP oscillator and to record the true trajectory.

For this particular experiment, the Ettus E312 offers three advantages over other USRPs: (1) it is lightweight, (2) it is battery operated, and (3) it has an SD Card slot which can be used to store LTE signals. Since the signals from all eNodeBs of the same operator are transmitted at the same frequency, it is possible to use one radio channel on the Ettus E312 USRP to receive signals from all eNodeBs. To store data for off-line post-processing, it was noticed that a sampling rate of 3 Msps or less is best suitable for the E312. This rate is acceptable for UAV navigation since it is assumed that multipath is negligible and only the SSS signal needs to be tracked.

The stored LTE signals were processed by the proposed LTE SDR, which was implemented in MATLAB. The stored GPS signals were processed by the Generalized Radionavigation Interfusion Device (GRID) SDR whose accuracy is consistent with the Standard Positioning Service GPS signal [55], [56]. The GPS navigation solution was used to initialize the states of the EKF, which was also implemented in MATLAB. The LTE navigation solution was obtained by the EKF using the pseudoranges produced by the LTE SDR, and the LTE and GPS navigation solutions were compared to calculate the estimation error.

Over the course of the experiment, the UAV was flying at the height of 40 m. The receiver was listening to 3 eNodeBs, each of which had 2 transmitting antennas with 20 MHz transmission bandwidth. The cell IDs of the eNodeBs were 300, 398 and 364, respectively. The positions of the eNodeBs were mapped prior to the experiment with approximately 2 m accuracy.

All measurements and trajectories were projected onto a 2-D plane. Subsequently, only the horizontal position of the receiver was estimated. It is assumed that the receiver had access to GPS, and GPS was cut off at the start time of the experiment. Therefore, the EKF's states were initialized with the values obtained from the GPS navigation solution. The standard deviation of the initial uncertainty of position and velocity were set to be 5 m and 0.01 m/s, respectively [36]. The standard deviation of the initial uncertainty of the clock bias and drift were set to be 0.1 m and 0.01 m/s, which were obtained empirically. The clock oscillators were modeled as oven-controlled crystal oscillators (OCXOs) with $S_{\tilde{w}_{\delta t_{s_i}}} \approx h_0/2$ and $S_{\tilde{w}_{\dot{\delta} t_{s_i}}} \approx 2\pi^2\, h_{-2}$, where $h_0 = 2.6 \times 10^{-22}$ and $h_{-2} = 4 \times 10^{-26}$. The power spectral densities $\tilde{q}_x$ and $\tilde{q}_y$ were set to 0.2 (m^2/s^3) and measurement noise covariance was set to be 10 m^2, which were obtained empirically.

2) UAV Experimental Results: Fig. 17 shows the obtained pseudoranges and the actual ranges with dashed and solid lines, respectively. To be able to plot all the pseudoranges in one figure, the initial value of each pseudorange is subtracted from the entire pseudorange time history. Therefore, all the pseudoranges in the figure start at zero. The same is performed to the actual ranges, which were obtained from GPS. The environment layout as well as the true and estimated receiver trajectories are shown in Fig. 18(a). It can be seen from Fig. 18(b) that the navigation solution obtained from LTE signals follows closely the GPS navigation solution. Over the course of the experiment, the UAV traversed a 426 m trajectory over 40 s with average speed of 38.34 Km/hr. The navigation performance including the RMSE, standard

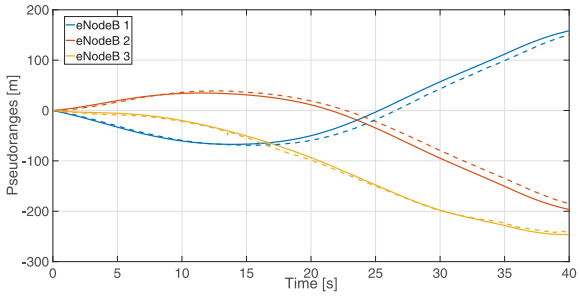

Fig. 17. Measured pseudoranges obtained by the LTE SDR and the actual ranges obtained by GPS for the UAV experiment. For the sake of comparison, the initial values were subtracted out. Dashed and solid lines represent the pseudoranges and actual ranges, respectively.

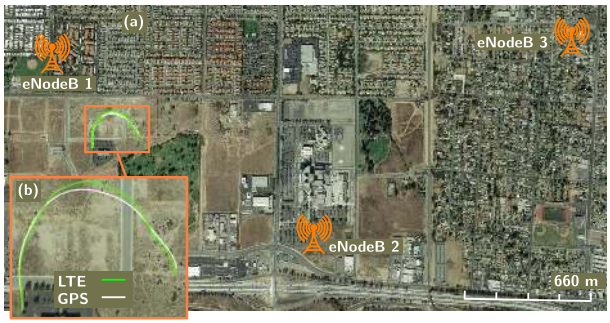

Fig. 18. (a) Environment layout, eNodeBs' locations, and the traversed trajectory. (b) The receiver's GPS trajectory estimate and the trajectory estimated using LTE signals. The RMSE between the GPS and LTE navigation solutions was calculated to be 8.15 m with an estimation error standard deviation of 2.83 m and a maximum error of 12.38 m. Image: Google Earth

deviation, and maximum error between GPS and LTE is summarized in Table I. The expected standard deviation of the horizontal error of a typical GPS navigation solution is 5 m [36].

Fig. 19(a) shows the distance estimation error. The initial value of the error is zero since the filter is initialized with true value of the receiver's position obtained from GPS. The experimental cumulative distribution function (CDF) of the error is plotted in Fig. 19(b) showing the 95-th error percentile to be 11.57 m.

C. Ground Vehicle Experiment

To evaluate the performance of the proposed methods for tracking multiple eNodeBs and exploiting CFAR to detect multipath components, a field test was conducted with a ground vehicle in an urban environment (downtown Riverside, CA, USA). The received signal to a ground vehicle suffers from severe multipath. The effect of multipath on an LTE signal may be worse than that of a GPS signal since LTE signals arrive at lower elevation angles than GPS signals. Therefore, higher bandwidth and the use of CRS to mitigate multipath are necessary. In this subsection, the experimental setup and results with a ground vehicle are provided. Finally, the performance of the receiver is compared with other methods.

1) Ground Vehicle Experimental Setup: Fig. 20 shows the experimental hardware and software setup. The equipment used in this experiment includes:

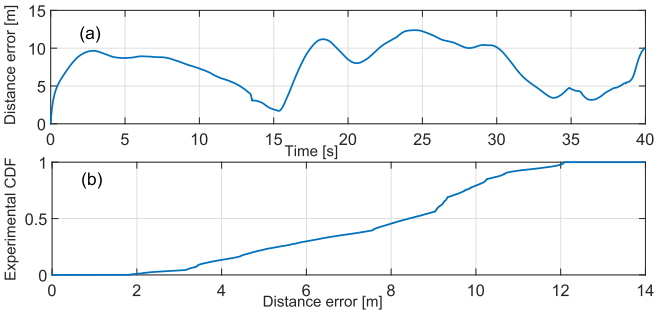

Fig. 19. (a) The navigation solution distance error. (b) Experimental CDF of the navigation solution distance error.

TABLE I
UAV NAVIGATION RESULTS

Performance Measure	Value
RMSE	8.15 m
Standard deviation	2.83 m
Maximum error	12.38 m

- two consumer-grade 800/1900 MHz cellular omnidirectional Laird antennas to receive LTE signals in frequencies 739 MHz and 1955 MHz, which are used by AT&T,
- a dual-channel national instruments (NI) USRP-2954R driven by a GPSDO to simultaneously down-mix and synchronously sample LTE signals with 20 Msps,
- a surveyor-grade Leica antenna to receive GPS signals to discipline the USRP oscillators and to obtain the ground truth,
- a single-channel NI USRP-2930 to down-mix and sample GPS signals,
- a laptop to store LTE and GPS signals for off-line post-processing.

The PLL, FLL, and DLL noise equivalent-bandwidths were set to 4, 0.2, and 0.001 Hz, respectively. The CFAR parameters were set to $N_t = 40$, $N_g = 100$, $p_{FA} = 0.01$, and non-coherent integration was performed over all the symbols and transmitting antennas in one frame, which results in $n_i = 80$. The EKF parameters were assigned similar to the UAV experiment. The vehicle traversed a total trajectory of 583 m in 39 s while listening to 6 eNodeBs whose position states were mapped prior to the experiment. The cell IDs of the eNodeBs were 216, 489, 457, 288, 232, and 152, respectively. The first 3 eNodeBs had 20 MHz and the rest of the eNodeBs had 10 MHz transmission bandwidth.

2) Ground Vehicle Experimental Results: The receiver was able to acquire and track all but the second eNodeB. Therefore, the proposed method in Section V was used to track the first eNodeB as the main eNodeB and obtain the pseudorange to the second eNodeB. Fig. 21(a) shows the measured pseudoranges and ranges, with initial values removed, with dashed and solid lines, respectively. The pseudorange error was obtained by subtracting the measured pseudorange for each eNodeB from its actual range. The average of the pseudorange error was assumed to be due to the clock bias and removed from the pseudorange error. Fig. 21(b) shows the experimental CDF of the pseudorange error for each eNodeB. Fig. 21(c) shows the measured C/N_0 obtained by the LTE SDR for

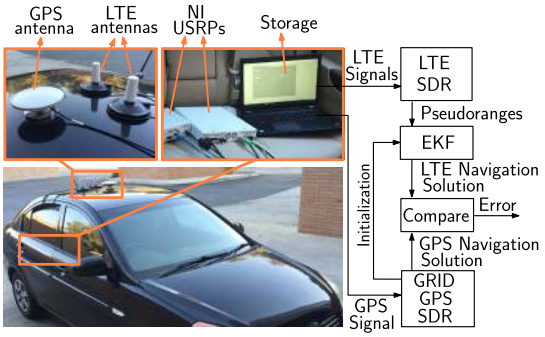

Fig. 20. Experimental hardware and software setup. The LTE antennas were connected to a dual-channel NI USRP-2954R driven by a GPSDO. The GPS antenna was connected to an NI-2930 USRP driven by a GPSDO. The stored LTE and GPS signals were processed with the proposed SDR and GRID SDR, respectively. LTE navigation solution was obtained by an EKF and compared with the GPS navigation solution.

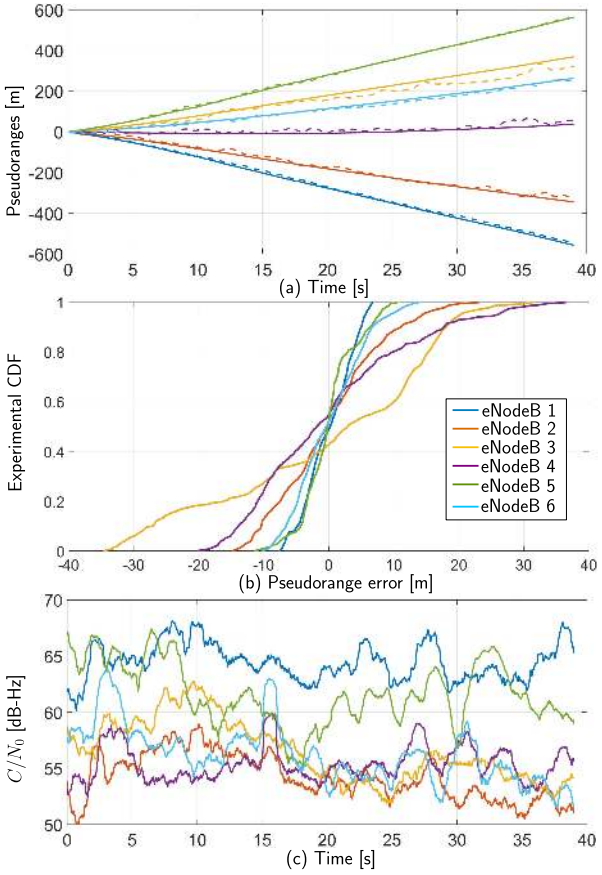

Fig. 21. (a) Measured pseudoranges obtained by the LTE SDR and actual ranges obtained by GPS for the ground vehicle experiment. For the sake of comparison, the initial values were subtracted out. Dashed and solid lines represent the pseudoranges and actual ranges, respectively. (b) Experimental CDF of the pseudorange error for each eNodeB. (c) Measured C/N_0 obtained by the LTE SDR for each eNodeB for the ground vehicle experiment.

each eNodeB over the course of the experiment. It can be seen that the pseudorange error for the eNodeBs with high C/N_0 is lower compared to the ones with low C/N_0. It is worth mentioning that low C/N_0 is one source of error in the estimated pseudorange. Short delay multipath can also increase the error on the estimated pseudorange.

Fig. 22 shows the amplitude of the estimated CIR, $|\hat{\boldsymbol{h}}^{(u)}(n)|$, from real LTE signals in a multipath environment at a given

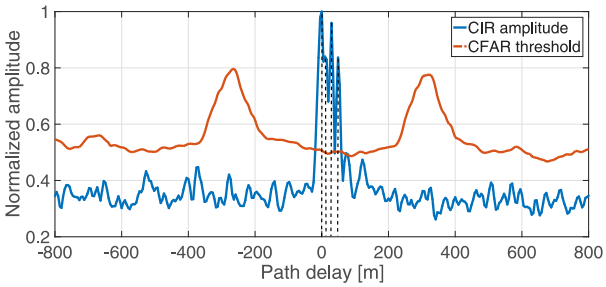

Fig. 22. The amplitude of the estimated CIR and the obtained threshold using the proposed CFAR method. The estimated threshold is used to differentiate the LOS peaks and strong multipath peaks from the noise level. The position of these peaks are shown in black dashed lines.

TABLE II
GROUND VEHICLE NAVIGATION RESULTS

Performance Measure	Value
RMSE	5.80 m
Standard deviation	3.02 m
Maximum error	14.96 m

time instant (blue). The proposed method in Section IV was used to obtain the threshold, η (red). Then, $\boldsymbol{d}^{(u)}(l)$ was set to be n_l, where $|\hat{\boldsymbol{h}}^{(u)}(n_l)| > \eta$ and $l = 0, \ldots, L^{(u)} - 1$. The position of the LOS peak (first peak) and the strong multipath peaks were set to be the peaks of $|\hat{\boldsymbol{h}}^{(u)}(\boldsymbol{d}^{(u)}(l))|$, which are shown in black dashed lines. It can be seen that the proposed method was able to isolate these peaks from the noise floor.

Fig. 23(a) shows the environment layout as well as the true and estimated receiver trajectory. It can be seen in Fig. 23(b) that the navigation solution obtained exclusively by LTE signals using the proposed LTE receiver and navigation framework follows closely the GPS solution. The navigation performance of the ground vehicle is summarized in Table II. Fig. 24 shows the distance estimation error and the experimental CDF of the error indicating a 95-th error percentile of 10.41 m.

In an urban environment, the pseudoranges received by a ground vehicle will suffer from more multipath-induced error compared to pseudoranges received by a UAV with LOS conditions. However, this comparison can be made as long as the ground vehicle and UAV are navigating in the same environment, using the same eNodeBs, and following the same trajectories, except for one being on the ground while the other being airborne. In this paper, the ground vehicle was equipped with a better USRP than the one on the UAV, due to payload limitations. The USRP on-board the ground vehicle was capable of sampling two different LTE channels at a sampling rate of 20 Msps, whereas the USRP on-board the UAV could only sample one LTE channel at 3 Msps. Consequently, the LTE receiver on-board the ground vehicle was able to listen to more eNodeBs than the receiver on-board the UAV, providing the former with more measurements at a better geometric diversity than the latter. Moreover, the ground vehicle-mounted receiver was able to produce more accurate TOA measurements, since it was sampling at more

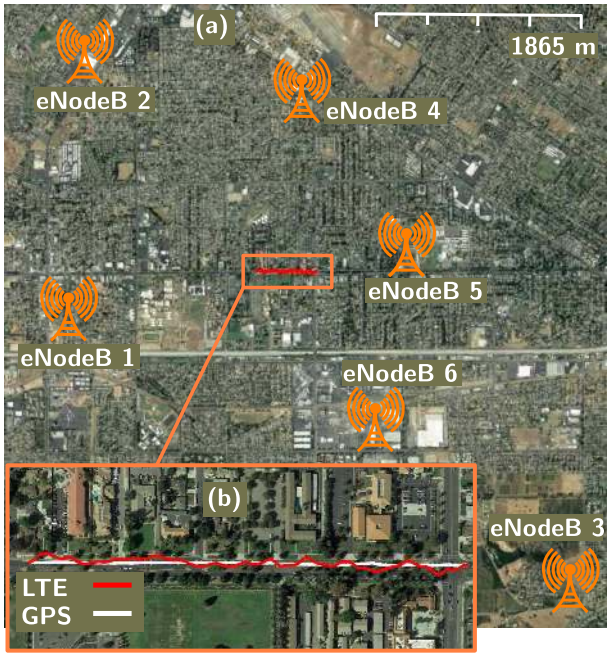

Fig. 23. (a) Environment layout in downtown Riverside, California: eNodeBs' locations and the traversed trajectory. (b) The receiver's GPS trajectory estimate and the trajectory estimated using LTE signals. The RMSE between the LTE and GPS navigation solutions was found to be 5.80 m, with an estimation error standard deviation of 3.02 m, and a maximum error of 14.96 m. Image: Google Earth.

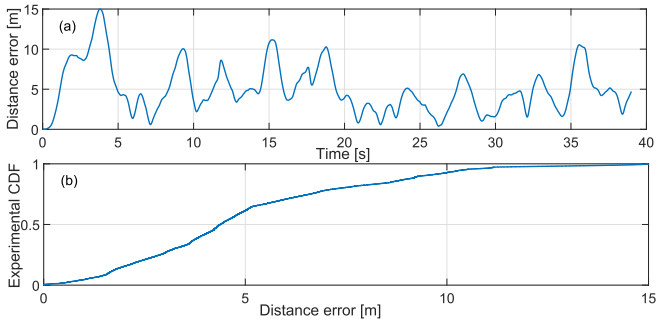

Fig. 24. (a) Distance estimation error. (b) Experimental CDF of the distance estimation error.

than six times the rate of the UAV-mounted receiver. These aforementioned factors resulted in the position RMSE of the ground vehicle being less than the position RMSE of the UAV.

3) Comparison With Other Methods: Prior solutions on navigating with LTE signals include: (1) detecting the first peak of the CIR using a constant threshold [26], [35] or an adaptive threshold [33], (2) estimating the CIR using estimation of signal parameters via rotational invariance techniques (ESPRIT) and Kalman filter, i.e., EKAT algorithm [28], and (3) tracking the CRS [24].

A constant threshold provides a computationally low-cost estimation of TOA; however, it has low accuracy when the C/N_0 is relatively low. In the adaptive threshold proposed in [33], the threshold is obtained based on the maximum of the CIR and the noise floor. The approach provide similar results to the proposed approach in this paper when the LOS signal has higher power than the multipath and the C/N_0 is relatively high. When the multipath signal has significantly higher power than the LOS (see the example in [47]), the approach in [33] cannot detect the LOS as the first peak of the CIR. In all threshold-based approaches including the proposed receiver in this paper, the accuracy of the TOA estimation depends on the transmission bandwidth. The EKAT algorithm proposed in [28] estimates the CIR using the ESPRIT algorithm, which is known to provide a relatively accurate estimate of the TOA when the length of the channel is known. To estimate the channel length, a minimum description length (MDL) criterion is used [28]. Since MDL tends to overestimate the CIR length, the TOA estimate has outliers. The outliers can be improved using a Kalman filter as discussed in [28]. The proposed SDR in [24] provides an accurate estimate of the TOA. However, in a multipath environment and for low C/N_0, the receiver may lose lock. The receiver proposed in this paper is an improvement over existing state-of-the-art approaches due to two main reasons: (1) it can estimate the first peak of the CIR even for low C/N_0 and (2) it can detect the first peak even for high multipath power.

Fig. 25 compares the error in estimating the eNodeB 3 pseudorange using (1) the proposed receiver in this paper, (2) the EKAT algorithm, (3) the SDR in [24], (4) a constant threshold-based algorithm (with threshold to be 4 dB lower than the maximum of the CIR), and (5) an adaptive threshold-based algorithm proposed in [33]. To be able to compare the results, the actual range obtained from GPS was subtracted from the pseudoranges obtained by each algorithm. Then, the average of each error over time, which is assumed to be the effect of clock bias, was removed. It is worth mentioning that the results are presented only for eNodeB 3 to show the effect of low C/N_0 and high multipath on the estimated pseudoranges by each method. Table III summarizes the standard deviation and maximum error for each method. It can be seen that the proposed method provides the most accurate results. Note that despite the high errors by the EKAT algorithm, the navigation performance in [28] shows a position RMSE of 31.09 m in an urban environment. It is worth mentioning that there are some considerations in the implementation of the EKAT algorithm (e.g., filter tuning). Perhaps with tuning, the performance of the EKAT algorithm could improve. However, no guidance on such tuning was provided in [28], so the same parameters provided in [28] were used to compare against the proposed method. This comparison also serves to highlight the importance of tuning in existing state-of-the-art, whereas the proposed method in this paper is mostly tune-free, except for the PLL and DLL bandwidth, which is stated how to choose in this manuscript.

It can be shown that the computational cost of the SRA method is proportional to $\mathcal{O}(N_r^3)$, which is mainly due to the singular value decomposition (SVD). However, the proposed algorithm, the SDR in [24], and the constant threshold method cost is $\mathcal{O}(N_c \log N_c)$, which is due to the FFT operator.

D. Remarks

This subsection summarizes key remarks concluded from the presented results.

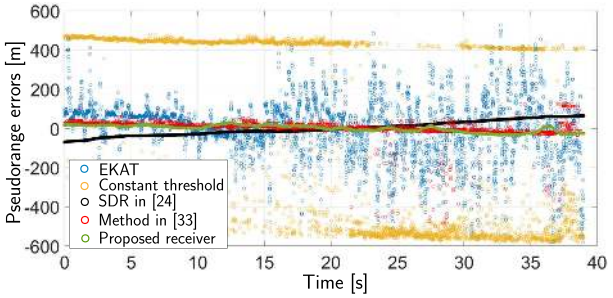

Fig. 25. Comparing the pseudorange errors obtained by EKAT, constant threshold, SDR in [24], adaptive threshold in [33], and the proposed method.

TABLE III
PSEUDORANGE ERROR COMPARISON OF DIFFERENT METHODS

	EKAT	Constant threshold	SDR in [24]	Method in [33]	Proposed receiver
Standard deviation [m]	152.39	472.70	35.80	49.68	16.80
Maximum error [m]	791.51	582.14	70.34	483.26	34.55

- A GPSDO allows modeling the receiver's clock by a known clock model as discussed in the navigation framework in Section VI. In an environment where GPS is not available and the receiver's clock is unknown, other navigation frameworks could be used, e.g., collaboration via mapping and navigating receivers [19].
- The GPS navigation solution is only used (1) as ground truth to obtain the estimation error for navigating with LTE signals and (2) to initialize the EKF.
- The choice of hardware and software is not unique. Any hardware that can sample in cellular bands can be used to record LTE signals and any software that has the processing capabilities (e.g. LabVIEW, MATLAB, and C++) can be used to implement the receiver.
- There is a slight mismatch between the vehicle's true dynamical model and the assumed model in (15). In the assumed model, the EKF might allow the vehicle's position and velocity estimates to move freely, as opposed to constraining them to a road segment. This model mismatch will cause the estimation error to become larger. In order to minimize the mismatch between the true and assumed model, multiple models for the vehicle's dynamics may be used to accommodate the different behaviors of the vehicle in different segments of the trajectory. Alternatively, an inertial measurement unit (IMU), which is available in many practical systems (e.g., UAV, cars, and smart phones), can be used to propagate the state of the vehicle [20]. This will also aid in alleviating multipath-induced errors.
- The estimation performance depends on the geometric diversity of the eNodeBs, the number of eNodeBs in the environment, the dynamical model, and the measurement accuracy.

VIII. CONCLUSION AND FUTURE WORK

This paper studied the exploitation of LTE signals for navigation purposes. A discussion of relevant signal models was presented and an SDR design for navigating with LTE signals was discussed. A method for timing information extraction was proposed. In addition, a method for tracking multiple eNodeBs by only tracking one reference eNodeB was proposed. Experimental results were presented demonstrating a UAV and a ground vehicle navigating exclusively with LTE signals via the proposed SDR. The RMSE between GPS and LTE navigation solutions was calculated to be 8.15 m (with 3 eNodeBs) and 5.80 m (with 6 eNodeBs) for the UAV and the ground vehicle, respectively.

Implementing the proposed receiver in hardware (e.g. digital signal processors (DSPs) and field-programmable gate arrays (FPGAs)) is one of the remaining challenges that needs to be addressed in the future. In this realm, the delay introduced by each part of the system, i.e., hardware and software, must be evaluated to analyze real-time feasibility.

Evaluating the proposed receiver in different environments over longer trajectories will be addressed in the future, upon having access to a database of the eNodeBs' positions.

REFERENCES

[1] A. Soloviev and J. Dickman, "Extending GPS carrier phase availability indoors with a deeply integrated receiver architecture," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 36–44, Apr. 2011.
[2] E. Costa, "Simulation of the effects of different urban environments on GPS performance using digital elevation models and building databases," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 819–829, Sep. 2011.
[3] J. C. Grabowski, "Personal privacy jammers: Locating Jersey PPDs jamming GBAS safety-of-life signals," *GPS World Mag.*, vol. 23, no. 4, pp. 28–37, Apr. 2012.
[4] C. Günther, "A survey of spoofing and counter-measures," *Navigation*, vol. 61, no. 3, pp. 159–177, 2014.
[5] J. Raquet and R. K. Martin, "Non-GNSS radio frequency navigation," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar./Apr. 2008, pp. 5308–5311.
[6] L. Merry, R. Faragher, and S. Schedin, "Comparison of opportunistic signals for localisation," in *Proc. 7th IFAC Symp. Intelli. Auto. Vehicles*, 2010, pp. 109–114.
[7] K. M. Pesyna, Jr., Z. M. Kassas, J. A. Bhatti, and T. E. Humphreys, "Tightly-coupled opportunistic navigation for deep urban and indoor positioning," in *Proc. ION GNSS Conf.*, 2011, pp. 1–12.
[8] P. Thevenon *et al.*, "Positioning using mobile TV based on the DVB-SH standard," *Navigation*, vol. 58, no. 2, pp. 71–90, 2011.
[9] K. M. Pesyna, Z. M. Kassas, and T. E. Humphreys, "Constructing a continuous phase time history from TDMA signals for opportunistic navigation," in *Proc. IEEE/ION Position Location Navigat. Symp.*, Apr. 2012, pp. 1209–1220.
[10] Z. M. Kassas, "Collaborative opportunistic navigation [student research highlight]," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 28, no. 6, pp. 38–41, Jun. 2013.
[11] Z. M. Kassas, "Analysis and synthesis of collaborative opportunistic navigation systems," Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. Texas Austin, Austin, TX, USA, 2014.
[12] Z. M. Kassas and T. E. Humphreys, "Observability analysis of collaborative opportunistic navigation with pseudorange measurements," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 260–273, Feb. 2014.
[13] Z. M. Kassas and T. E. Humphreys, "Motion planning for optimal information gathering in opportunistic navigation systems," in *Proc. AIAA Guid., Navigat., Control Conf.*, 2013, pp. 4551–4565.
[14] Z. M. Kassas, A. Arapostathis, and T. E. Humphreys, "Greedy motion planning for simultaneous signal landscape mapping and receiver localization," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 2, pp. 247–258, Mar. 2015.
[15] Z. M. Kassas and T. E. Humphreys, "Receding horizon trajectory optimization in opportunistic navigation environments," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 51, no. 2, pp. 866–877, Apr. 2015.
[16] F. Benedetto, G. Giunta, and S. Bucci, "A unified approach for time-delay estimators in spread spectrum communications," *IEEE Trans. Commun.*, vol. 59, no. 12, pp. 3421–3429, Dec. 2011.

[17] C. Yang, T. Nguyen, and E. Blasch, "Mobile positioning via fusion of mixed signals of opportunity," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 29, no. 4, pp. 34–46, Apr. 2014.
[18] C. Yang and T. Nguyen, "Tracking and relative positioning with mixed signals of opportunity," *Navigation*, vol. 62, no. 4, pp. 291–311, 2015.
[19] J. Khalife, K. Shamaei, and Z. M. Kassas, "A software-defined receiver architecture for cellular CDMA-based navigation," in *Proc. IEEE/ION Position, Location, Navigat. Symp.*, Apr. 2016, pp. 816–826.
[20] J. J. Morales, P. F. Roysdon, and Z. M. Kassas, "Signals of opportunity aided inertial navigation," in *Proc. ION GNSS Conf.*, 2016, pp. 1–10.
[21] Z. M. Kassas, J. Khalife, K. Shamaei, and J. J. Morales, "I hear, therefore I know where I am: Compensating for GNSS limitations with cellular signals," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 111–124, Sep. 2017.
[22] S. Fischer, "Observed time difference of arrival (OTDOA positioning in 3GPP LTE," Qualcomm, San Diego, CA, USA, White Paper, 2014.
[23] M. Hofer, J. McEachen, and M. Tummala, "Vulnerability analysis of LTE location services," in *Proc. Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2014, pp. 5162–5166.
[24] J. A. del Peral-Rosado *et al.*, "Software-defined radio LTE positioning receiver towards future hybrid localization systems," in *Proc. Int. Commun. Satellite Syst. Conf.*, Oct. 2013, pp. 14–17.
[25] J. A. del Peral-Rosado *et al.*, "Comparative results analysis on positioning with real LTE signals and low-cost hardware platforms," in *Proc. 7th ESA Satellite Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2014, pp. 1–8.
[26] F. Knutti, M. Sabathy, M. Driusso, H. Mathis, and C. Marshall, "Positioning using LTE signals," in *Proc. Eur. Navigat. Conf.*, 2015, pp. 1–8.
[27] M. Ulmschneider and C. Gentner, "Multipath assisted positioning for pedestrians using LTE signals," in *Proc. IEEE/ION Position, Location, Navigat. Symp.*, Apr. 2016, pp. 386–392.
[28] M. Driusso, C. Marshall, M. Sabathy, F. Knutti, H. Mathis, and F. Babich, "Vehicular position tracking using LTE signals," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3376–3391, Apr. 2017.
[29] Y. Shen, T. Luo, and M. Z. Win, "Neighboring cell search for LTE systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 908–919, Mar. 2012.
[30] K. Shamaei, J. Khalife, and Z. M. Kassas, "Performance characterization of positioning in LTE systems," in *Proc. ION GNSS Conf.*, 2016, pp. 1–9.
[31] J. A. del Peral-Rosado, J. López-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, "Joint channel and time delay estimation for LTE positioning reference signals," in *Proc. 6th ESA Satellite Navigat. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, Dec. 2012, pp. 1–8.
[32] J. A. del Peral-Rosado, J. López-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, "Joint maximum likelihood time-delay estimation for LTE positioning in multipath channels," *EURASIP J. Adv. Signal Process.*, vol. 2014, p. 33, Dec. 2014.
[33] W. Xu, M. Huang, C. Zhu, and A. Dammann, "Maximum likelihood TOA and OTDOA estimation with first arriving path detection for 3GPP LTE system," *Trans. Emerg. Telecommun. Technol.*, vol. 27, no. 3, pp. 339–356, 2016.
[34] P. Müller, J. A. del Peral-Rosado, R. Piché, and G. Seco-Granados, "Statistical trilateration with skew-t distributed errors in LTE networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 7114–7127, Oct. 2016.
[35] C. Gentner, E. Muñoz, M. Khider, E. Staudinger, S. Sand, and A. Dammann, "Particle filter based positioning with 3GPP-LTE in indoor environments," in *Proc. IEEE/ION Position, Location Navigat. Symp.*, Apr. 2012, pp. 301–308.
[36] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed. Nagpur, India: Ganga Jamuna Press, 2010.
[37] *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation*, document TS 36.211, 3rd Generation Partnership Project, Jan. 2011. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36211.htm
[38] F. Benedetto, G. Giunta, and E. Guzzon, "Initial code acquisition in LTE systems," *Recent Patents Comput. Sci.*, vol. 6, no. 1, pp. 2–13, 2013.
[39] I. Kim, Y. Han, and H. K. Chung, "An efficient synchronization signal structure for OFDM-based cellular systems," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 99–105, Jan. 2010.
[40] M. Morelli and M. Moretti, "A robust maximum likelihood scheme for PSS detection and integer frequency offset recovery in LTE systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1353–1363, Feb. 2016.
[41] J.-J. van de Beek, M. Sandell, and P. O. Borjesson, "ML estimation of time and frequency offset in OFDM systems," *IEEE Trans. Signal Process.*, vol. 45, no. 7, pp. 1800–1805, Jul. 1997.
[42] *Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and Channel Coding*, document TS 36.212, 3rd Generation Partnership Project, Jan. 2010. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36212.htm
[43] Y.-P. E. Wang and R. Ramesh, "To bite or not to bite-a study of tail bits versus tail-biting," in *Proc. 7th IEEE Int. Symp. Pers., Indoor Mobile Radio Commun.*, vol. 2. Oct. 1996, pp. 317–321.
[44] P. W. Ward, "Performance comparisons between FLL, PLL and a novel FLL-assisted-PLL carrier tracking loop under RF interference conditions," in *Proc. ION GNSS Conf.*, 1998, pp. 783–795.
[45] E. D. Kaplan and C. Hegarty, *Understanding GPS: Principles and Applications*, 2nd ed. Norwood, MA, USA: Artech House, 2005.
[46] K. Shamaei, J. Khalife, and Z. M. Kassas, "Ranging precision analysis of LTE signals," in *Proc. Eur. Signal Process. Conf. (EUSIPCO)*, Aug./Sep. 2017, pp. 2719–2723.
[47] K. Shamaei, J. Khalife, and Z. M. Kassas, "Comparative results for positioning with secondary synchronization signal versus cell specific reference signal in LTE systems," in *Proc. ION ITM Conf.*, 2017, pp. 1–13.
[48] X. Li and K. Pahlavan, "Super-resolution TOA estimation with diversity for indoor geolocation," *IEEE Trans. Wireless Commun.*, vol. 3, no. 1, pp. 224–234, Jan. 2004.
[49] N. A. Nechval, *Adaptive CFAR Tests for Detection of a Signal in Noise and Deflection Criterion*, T. Wysocki, H. Razavi, and B. Honary, Eds. Boston, MA, USA: Springer, 1997.
[50] B. R. Mahafza, *Radar Systems Analysis and Design Using MATLAB*, 1st ed. Boca Raton, FL, USA: CRC Press, 2000.
[51] Z. M. Kassas, V. Ghadiok, and T. E. Humphreys, "Adaptive estimation of signals of opportunity," in *Proc. ION GNSS Conf.*, 2014, pp. 1–11.
[52] J. J. Morales and Z. M. Kassas, "Optimal receiver placement for collaborative mapping of signals of opportunity," in *Proc. ION GNSS Conf.*, 2015, pp. 1–7.
[53] *Evolved Universal Terrestrial Radio Access (E-UTRA); Requirements for Support of Radio Resource Management*, document TS 36.133, 3rd Generation Partnership Project, Apr. 2010.
[54] Y. Bar-Shalom, X. R. Li, and T. Kirubarajan, *Estimation With Applications to Tracking and Navigation*. New York, NY, USA: Wiley, 2002.
[55] T. E. Humphreys, M. L. Psiaki, P. M. Kintner, Jr., and B. M. Ledvina, "GNSS receiver implementation on a DSP: Status, challenges, and prospects," in *Proc. ION GNSS Conf.*, 2006, pp. 1–13.
[56] T. E. Humphreys, J. A. Bhatti, T. Pany, B. M. Ledvina, and B. W. O'Hanlon, "Exploiting multicore technology in software-defined GNSS receivers," in *Proc. ION GNSS Conf.*, 2009, pp. 1–13.

Kimia Shamaei (S'15) received the B.S. and M.S. degrees in electrical engineering from the University of Tehran. She is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of California, Riverside, CA, USA. She is a member of the Autonomous Systems Perception, Intelligence, and Navigation Laboratory. Her research interests include the analysis and modeling of signals of opportunity and software-defined radio.

Joe Khalife (S'15) received the B.E. degree in electrical engineering and the M.S. degree in computer engineering from the Lebanese American University (LAU). He is currently pursuing the Ph.D. degree with the University of California, Riverside, CA, USA. From 2012 to 2015, he was a Research Assistant at LAU. He is a member of the Autonomous Systems Perception, Intelligence, and Navigation Laboratory. His research interests include opportunistic navigation, autonomous vehicles, and software-defined radio.

Zaher (Zak) M. Kassas (S'98–M'08–SM'11) received the B.E. degree in electrical engineering from the Lebanese American University, the M.S. degree in electrical and computer engineering from The Ohio State University, Columbus, OH, USA, and the M.S.E. degree in aerospace engineering and the Ph.D. degree in electrical and computer engineering from The University of Texas at Austin, Austin, TX, USA. From 2004 to 2010, he was a Research and Development Engineer with the LabVIEW Control Design and Dynamical Systems Simulation Group, National Instruments Corporation. He is currently an Assistant Professor at the University of California, Riverside, CA, USA, and the Director of the Autonomous Systems Perception, Intelligence, and Navigation Laboratory. His research interests include cyber-physical systems, estimation theory, navigation systems, autonomous vehicles, and intelligent transportation systems.