A Software-Defined Receiver Architecture for Cellular CDMA-Based Navigation

Joe Khalife, Kimia Shamaei, and Zaher M. Kassas
Department of Electrical and Computer Engineering
University of California, Riverside
{joe.khalife@email.ucr.edu, kimia.shamaei@email.ucr.edu, zkassas@ieee.org}

***Abstract*—A detailed software-defined receiver (SDR) architecture for navigation using cellular code division multiple access (CDMA) signals is presented. The cellular forward-link signal structure is described and models for the transmitted and received signals are developed. Particular attention is paid to relevant information that could be extracted and subsequently exploited for navigation and timing purposes. The differences between a typical GPS receiver and the proposed cellular CDMA receiver are highlighted. Moreover, a framework that is based on a mapping/navigating receiver scheme for navigation in a cellular CDMA environment is studied. The position and timing errors arising due to estimating the base transceiver station clock biases in different cell sectors are also analyzed. Experimental results utilizing the proposed SDR are presented demonstrating a mean distance difference of 5.51 m from a GPS navigation solution.**

***Index Terms*—Navigation, signals of opportunity, cellular CDMA, software-defined radio.**

I. Introduction

Over the past decade, research in navigation via signals of opportunity (SOPs) has revealed their potential as an alternative or a complement to global navigation satellite system GNSS) [1], [2]. Such signals include AM/FM radio signals [3], [4], iridium satellite signals [5], [6], cellular signals [7], [8], digital television signals [9], [10], and Wi-Fi signals [11], [12]. The literature on SOP-based navigation answers theoretical questions on the observability and estimability of the signal landscape map for a different number of receivers, a different number of SOPs, and various *a priori* knowledge scenarios [13], [14]. Moreover, experimental results have demonstrated receiver localization and timing via SOPs [2], [8], [15].

There are two main challenges associated with using SOPs for navigation: (1) the unavailability of appropriate precise, low-level signal models for optimal extraction of states and parameters of interest for navigation and timing purposes and (2) the absence of published receiver architectures capable of producing navigation observables. This paper addresses these two challenges for cellular CDMA signals. These signals are abundant, are transmitted at high power, and have a structure that is similar to the well-understood GPS signals, which renders them good candidates for navigation. To the authors' knowledge, while previous work demonstrated experimental results for navigation via cellular CDMA signals, neither of these two challenges has been fully addressed.

Unlike GNSS, the states of a cellular CDMA base transceiver station (BTS) are unknown to a navigating receiver and need to be estimated. Although, the IS-95 standard states that a CDMA BTS should transmit its position, local wireless providers do not usually transmit such information [16], [17]. Hence, the position of the BTSs need to be manually surveyed or estimated on-the-fly individually or collaboratively [18], [19]. Nevertheless, while the position states of a BTS are static, the clock error states of the BTS are dynamic and need to be continuously estimated via (1) a mapping receiver, which shares such estimates with the navigating receiver or (2) by the navigating receiver itself by adopting a simultaneous localization and mapping approach [20], [21], [22].

Whether it is for navigation or mapping purposes, a specialized receiver is needed to process the received cellular CDMA signal and extract relevant positioning and timing observables. Cellular CDMA receivers are routinely implemented in hardware in mobile phones; however, hardware implementations limits the ability to extract or modify information within the receiver. As such, software-defined radio (SDR) becomes an attractive platform of choice for implementing a cellular CDMA receiver for navigation purposes, because of its inherent advantages: (1) flexibility: designs are hardware independent, (2) modularity: different functions can be implemented independently, and (3) upgradability: minimal changes are needed to improve designs. Although most SDRs used to be limited to post-processing applications, processor-specific optimization techniques allow for real-time operation [23]. Consequently, SDR implementations are becoming more prevalent. Moreover, graphical programming languages such as LabVIEW and Simulink offer the advantage of a one-to-one correspondence between the architectural conceptualization of the SDR and software implementation [24].

This paper makes two contributions. First, it presents a detailed and reproducible navigation cellular CDMA SDR architecture along with precise, low-level signal models for optimal extraction of relevant navigation and timing information from received signals. Second, the paper studies a navigation framework in which a mapping receiver estimates the states of BTSs and shares such estimates with a navigating receiver, which navigates exclusively with cellular CDMA signals. The paper analyzes the induced error in the navigation solution due to having the mapping and navigating receivers listening to different sectors within a BTS cell. The paper also presents experimental results comparing the trajectories corresponding to a navigation solution from GPS and that of the proposed

cellular CDMA SDR. The mean distance difference between the trajectories is shown to be 5.51 m with a standard deviation of 4.01 m and a maximum difference of 11.11 m.

The remainder of the paper is organized as follows. Section II provides an overview of the cellular CDMA forward link signal structure. Section III presents a complete LabVIEW-based implementation of the navigation cellular CDMA SDR. Section IV analyzes a mapping/navigating receiver framework for navigation with celluar CDMA signals. Experimental results are given in Section V and concluding remarks are discussed in Section VI.

II. Cellular CDMA Forward Link Signal Structure

In a cellular CDMA communication system, 64 logical channels are multiplexed on the forward link channel: a pilot channel, a sync channel, 7 paging channels and 55 traffic channels [25]. In the following subsection, the modulation process of the forward link channel is presented. Next, a brief overview of the pilot, sync, and paging channels, from which timing and positioning information can be extracted, is provided. Finally, models of the transmitted and received signals are given.

A. Modulation of Forward Link CDMA Signals

The data transmitted on the forward link channel in cellular CDMA systems (i.e., BTS to mbile) is modulated through quadrature phase shift keying (QPSK) and then spread using direct-sequence CDMA (DS-CDMA). However, for the channels of interest in this work, the in-phase and quadrature components, I and Q, respectively, carry the same message $m(t)$ as shown in Fig. 1. The spreading sequences c_I and c_Q, called the short code, are maximal-length pseudorandom noise (PN) sequences that are generated using 15 linear feedback shift registers (LFSRs). Hence, the length of c_I and c_Q is $2^{15}-1 = 32,767$ chips [16]. The characteristic polynomials of the short code I and Q components, $P_I(D)$ and $P_Q(D)$, are given by

$$P_I(D) = D^{15}+D^{13}+D^9+D^8+D^7+D^5+1$$
$$P_Q(D) = D^{15}+D^{12}+D^{11}+D^{10}+D^6+D^5+D^4+D^3+1,$$

where D is the delay operator. It is worth noting that an extra zero is added after the occurrence of 14 consecutive zeros to make the length of the short code a power-of-two. In order to distinguish the received data from different BTSs, each station uses a shifted version of the PN codes. This shift, known as the pilot offset, is unique for each BTS and is an integer multiple of 64 chips. The cross-correlation of the same PN sequence with different pilot offsets can be shown to be negligible [25]. Each individual logical channel is spread by a unique 64-chip Walsh code [26]. Therefore, at most 64 logical channels can be multiplexed at each BTS. Spreading by the short code enables multiple access for BTSs over the same carrier frequency, while the orthogonal spreading by the Wlash codes enables multiple access for users over the same BTS. The CDMA signal is subsequently filtered using a digital pulse shaping filter that limits the bandwidth of the transmitted CDMA signal according to the IS-95 standard. The signal is finally modulated by the carrier frequency ω_c to produce $s(t)$.

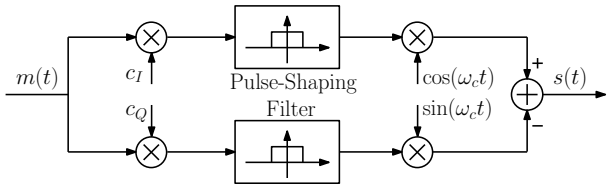

Fig. 1. Forward-link modulator.

B. Pilot Channel

The message transmitted by the pilot channel is a constant stream of binary zeros and is spread by Walsh code zero, which also consists of 64 binary zeros. Therefore, the modulated pilot signal is nothing but the short code. The proposed receiver will utilize the pilot signal to detect the presence of a CDMA signal and then track it, as will be discussed in Section III. The fact that the pilot signal is data-less allows for longer integration time. The receiver differentiates between the BTSs based on their pilot offsets.

C. Sync Channel

The sync channel is used to provide time and frame synchronization to the receiver. The cellular CDMA system uses GPS as the reference timing source and the BTS sends the system time to the receiver over the sync channel. Other information such as the pilot PN offset and the long code state are also provided on the sync channel [16]. The long code is a PN sequence and is used to spread the reverse-link signal (i.e., receiver to BTS) and the paging channel message. The long code has a chip rate of 1.2288 Mcps and is generated using 42 LFSRs. The output of the registers are masked and modulo-two added together to form the long code. The latter has a period of more than 41 days; hence, the states of the 42 LFSRs and the mask are transmitted to the receiver so that it can readily achieve long code synchronization. The sync message encoding before transmission is shown in Fig. 2.

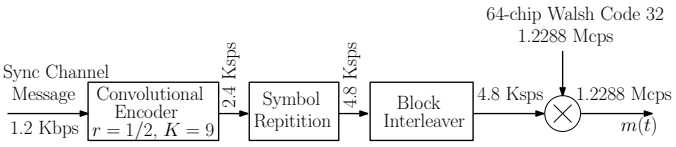

Fig. 2. Forward-link sync channel encoder.

The initial message, which is at 1.2 Kbps, is convolutionally encoded at a rate $r = (1/2)$ with generator functions $g_0 = 753$ (octal) and $g_1 = 561$ (octal) [26]. The state of the encoder is not reset during the transmission of a message capsule. The resulting symbols are repeated twice and the resulting frames, which are 128-symbols long, are block interleaved using the bit reversal method [16]. The modulated symbols, which have a rate of 4.8 Ksps, are spread with Walsh code 32.

The sync message is divided into 80 ms superframes, and each superframe is divided into three frames. The first bit of each frame is called the start-of-message (SOM). The beginning of the sync message is set to be on the first frame of each superframe, and the SOM of this frame is set to one. The BTS sets the other SOMs to zero. The sync channel message capsule is composed of the message length, the message body, cyclic redundancy check (CRC), and zero padding. The length of the zero padding is such that the message capsule extends up to the start of the next superframe. A 30-bit CRC is computed for each sync channel message with the generator polynomial

$$\begin{aligned} g(x) &= x^{30} + x^{29} + x^{21} + x^{20} + x^{15} + x^{13} \\ &\quad + x^{12} + x^{11} + x^{8} + x^{7} + x^{6} + x^{2} + x + 1. \end{aligned}$$

The SOM bits are dropped by the receiver and the frames bodies are combined to form a sync channel capsule. The sync message structure is summarized in Fig. 3.

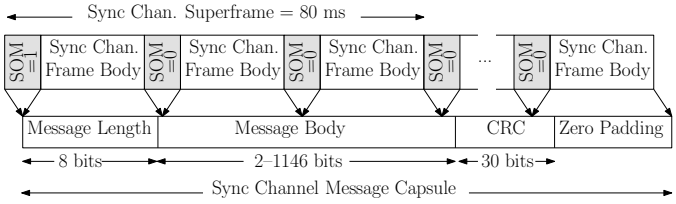

Fig. 3. Sync channel message structure.

D. Paging Channel

The paging channel transmits all the necessary overhead parameters for the receiver to register into the network [25]. Some mobile operators also transmit the BTS latitude and longitude on the paging channel, which can be exploited for navigation. The major cellular CDMA providers in the United States, Sprint and Verizon, do not transmit the BTS latitude and longitude. US Cellular used to transmit the BTS latitudes and longitude, but this provider does not operate anymore. The paging channel message encoding before transmission is illustrated in Fig. 4.

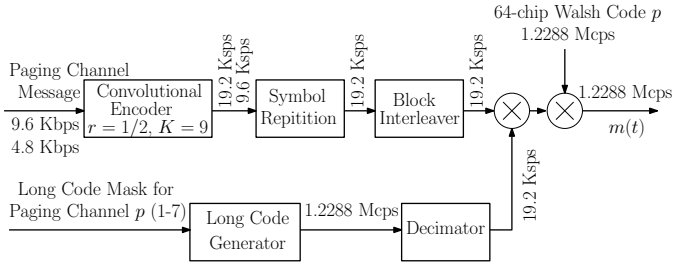

Fig. 4. Forward-link paging channel encoder.

The initial bit-rate of the paging channel message is either 9.6 Kbps or 4.8 Kbps and is provided in the sync channel message. Next, the data is convolutionally encoded in the same way as that of the sync channel data. The output symbols are repeated twice only if the bit rate is less than 9.6 Kbps. After symbol repetition, the resulting frames, which are 384-symbols long, are block interleaved one frame at a time. The interleaver is different than the one used for the sync channel because it operates on 384-symbols instead of 128-symbols. However, both interleavers use the bit reversal method. Finally, the paging channel message is scrambled by modulo-two addition with the long code sequence.

The paging channel message is divided into 80 ms time slots, where each slot is composed of eight half-frames. All the half-frames start with a synchronized capsule indicator (SCI) bit. A message capsule can be transmitted in both a synchronized and an unsynchronized manner. A synchronized message capsule starts exactly after the SCI. In this case, the BTS sets the value of the first SCI to one and the rest of the SCIs to zero. If by the end of the paging message capsule there remains less than 8 bits before the next SCI, the message is zero padded to the next SCI. Otherwise, an unsynchronized message capsule is sent immediately after the end of the previous message [25]. The paging channel structure is summarized in Fig. 5.

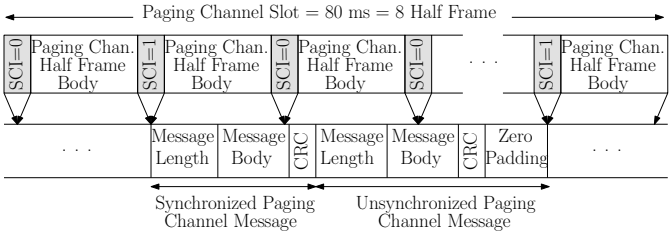

Fig. 5. Paging channel message structure.

E. Transmitted Signal Model

The pilot signal, which is purely the PN sequence, is used to acquire and track a cellular CDMA signal. The acquisition and tracking will be discussed in Section III. Demodulating the other channels becomes an open-loop problem, since no feedback is taken from the sync, paging, nor any of the other channels for tracking. Since all the other channels are synchronized to the pilot, only the pilot needs to be tracked. In fact, it is required by the IS-95 specification that all the coded channels be synchronized with the pilot to within ± 50 ns [27]. Although signals from multiple BTSs could be received simultaneously, a receiver could associate each individual signal with the corresponding BTS, since the offsets between the transmitted PN sequences are much larger than one chip. The normalized transmitted pilot signal $s(t)$ by a particular BTS can be expressed as

$$\begin{aligned} s(t) &= c'_I[t-\Delta(t)]\cos(\omega_c t) - c'_Q[t-\Delta(t)]\sin(\omega_c t) \\ &= \Re\left\{\left(c'_I[t-\Delta(t)] + jc'_Q[t-\Delta(t)]\right)\cdot e^{j\omega_c t}\right\} \\ &= \frac{1}{2}\left\{c'_I[t-\Delta(t)] + jc'_Q[t-\Delta(t)]\right\}\cdot e^{j\omega_c t} \\ &\quad + \frac{1}{2}\left\{c'_I[t-\Delta(t)] - jc'_Q[t-\Delta(t)]\right\}\cdot e^{-j\omega_c t}, \end{aligned}$$

where $c'_I(t) = c_I(t) * h(t)$ and $c'_Q(t) = c_Q(t) * h(t)$; h is the continuous-time impulse response of the pulse shaping filter; c_I and c_Q are the in-phase and quadrature PN sequences, respectively; $\omega_c = 2\pi f_c$ with f_c being the carrier frequency;

and Δ is the absolute clock bias of the BTS from GPS time. The total clock bias Δ is defined as

$$\Delta(t) = 64 \cdot (PN_{\text{offset}}\, T_c) + \delta t_s(t),$$

where PN_{offset} is the PN offset of the BTS, $T_c = \frac{1\times10^{-6}}{1.2288}$ s is the chip interval, and δt_s is the BTS clock bias. Since the chip interval is known and the PN offset can be decoded by the receiver, only δt_s needs to be estimated. It is worth noting that the cdma2000 standard requires the BTS's clock to be synchronized with GPS to within 10 μs, which translates to a range of approximately 3 km (the average cell size) [27]. This requirement is enough to prevent severe interference between the short codes transmitted from different BTSs and maintains the CDMA system's capability to perform soft hand-offs [16]. The clock bias of the BTS can therefore be neglected for communication purposes. However, ignoring δt_s in navigation applications can be disastrous, and it is therefore crucial for the receiver to know the BTS's clock bias. Estimation of δt_s is discussed in Section IV.

F. Received Signal Model After Front-End Processing

Assuming the transmitted signal to have propagated through an additive white Gaussian noise channel, a model of the received discrete-time signal $r[k]$ after radio frequency (RF) front-end processing: downmixing, a quadrature approach to bandpass sampling [28], and quantization can be expressed as

$$r[k] = \frac{1}{2}\left\{c'_I[t_k - t_s(t_k)] - jc'_Q[t_k - t_s(t_k)]\right\}\cdot e^{j\theta(t_k)} + n[k], \quad (1)$$

where $t_s(t_k) \triangleq \delta t_{TOF} + \Delta(t_k - \delta t_{TOF})$ is the PN code phase of the BTS, $t_k = kT_s$ is the sample time expressed in receiver time, T_s is the sampling period, δt_{TOF} is the time-of-flight (TOF) from the BTS to the receiver, $\theta(t_k)$ is the beat carrier phase of the received signal, and $n[k] = n_I[k] + jn_Q[k]$ with $n_I[k]$ and $n_Q[k]$ being independent, identically-distributed (i.i.d.) Gaussian random sequences with zero-mean and variance σ_n^2. The receiver developed in Section III will operate on the samples of $r[k]$ in (1).

III. Cellular CDMA Receiver Architecture

The cellular CDMA receiver consists of three main stages: signal acquisition, tracking, and decoding. The first subsection gives a brief description of the correlation process in the cellular CDMA navigation receiver. The following subsections present a detailed software implementation of the three receiver stages. The main differences between a GPS receiver and the developed cellular CDMA receiver are highlighted.

A. Cellular CDMA Receiver Correlator

Given samples of the baseband signal exiting the RF front-end, defined in (1), the cellular CDMA receiver first wipes-off the residual carrier phase and match-filters the resulting signal. The output of the matched-filter can be expressed as

$$x[k] = \left[r[k] \cdot e^{-j\hat{\theta}(t_k)}\right] * h[-k], \quad (2)$$

where $\hat{\theta}$ is the beat carrier phase estimate and $h[k]$ is a pulse shaping filter, which is a discrete-time version of the one used to shape the spectrum of the transmitted signal, with a finite-impulse response specified in [16]. Next, $x[k]$ is correlated with a local replica of the spreading PN sequence. The resulting correlation is used as a measure of the quality of the code phase and the beat carrier phase estimates. In a digital receiver, the correlation operation is expressed as

$$S_i = \sum_{k=i}^{i+N_s-1} x[k]\left\{c_I[t_k - \hat{t}_s(t_k)] + jc_Q[t_k - \hat{t}_s(t_k)]\right\}, \quad (3)$$

where S_i is the ith subaccumulation, N_s is the number of samples per subaccumulation, and $\hat{t}_s(t_k)$ is the code start time estimate over the ith subaccumulation. The code phase can be assumed to be approximately constant over a short subaccumulation interval T_{sub}; hence, $\hat{t}_s(t_k) \approx \hat{t}_{s_i}$. It is worth mentioning that T_{sub} can be made arbitrarily large, theoretically, since no data is transmitted on the pilot channel. Practically, T_{sub} is mainly limited by the stability of the BTS and receiver oscillators [29]. In this paper, T_{sub} is set to one PN code period. The carrier phase estimate is modeled as $\hat{\theta}(t_k) = 2\pi\hat{f}_{D_i}t_k + \theta_0$, where $\hat{f}_{D_i}$ is the apparent Doppler frequency estimate over the ith subaccumulation, and θ_0 is the initial beat carrier phase of the received signal. As in a GPS receiver, the value of θ_0 is set to zero in the acquisition stage and is subsequently maintained in the tracking stage. The apparent Doppler frequency is assumed to be constant over a short T_{sub}. Substituting for $r[k]$ and $x[k]$, defined in (1)-(2), into (3), it can be shown that

$$S_i = N_s\, R_c(\Delta t_i)\left[\sum_{k=i}^{i+N_s-1} e^{j\Delta\theta(t_k)}\right] + n_i, \quad (4)$$

where R_c is the autocorrelation function of the PN sequences c_I and c_Q, $\Delta t_i \triangleq t_{s_i} - \hat{t}_{s_i}$ is the code phase error, $\Delta\theta(t_k) \triangleq \theta(t_k) - \hat{\theta}(t_k)$ is the carrier phase error, and $n_i \triangleq n_{I_i} + jn_{Q_i}$ with n_{I_i} and n_{Q_i} being i.i.d. Gaussian random sequences with zero-mean and variance $N_s\sigma_n^2$. The expression of S_i in (4) assumes that the locally generated c_I and c_Q have the same code phase. To ensure this, both sequences must begin with the first binary one that occurs after 15 consecutive zeros; otherwise, $|S_i|$ will be halved. Fig. 6 shows $|S_i|^2$ for unsynchronized and synchronized c_I and c_Q code phases (i.e., shifted by 34 chips). The correlation peak for the synchronized codes is four-times the peak for the unsynchronized case.

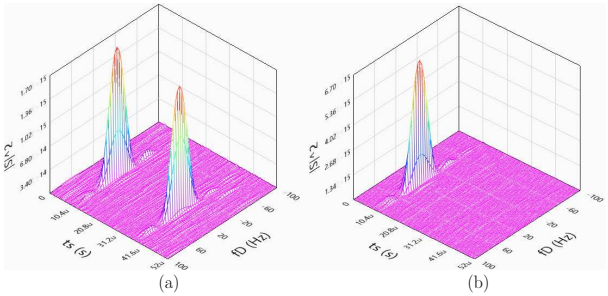

Fig. 6. $|S_i|^2$ for (a) unsynchronized and (b) synchronized c_I and c_Q codes.

The carrier wipe-off and correlation stages are illustrated in Fig. 7.

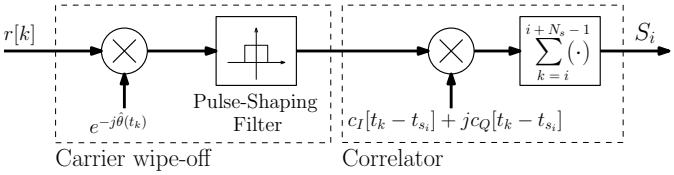

Fig. 7. Carrier wipe-off and correlator diagram. Thick lines indicate a complex-valued variable.

B. Acquisition

The objective of this stage is to determine which BTSs are in the receiver's proximity and to obtain a coarse estimate of their corresponding code start times and Doppler frequencies. For a particular PN offset, a search over the code start time and Doppler frequency is performed to detect the presence of a signal. To determine the range of Doppler frequencies to search over, one must consider the relative motion between the receiver and the BTS and the stability of the receiver's oscillator. For instance, a Doppler shift of 122 Hz will be observed for a cellular CDMA carrier frequency of 822.75 MHz at a mobile receiver with a receiver-to-BTS line-of-sight velocity of 150 km/h. Furthermore, a Doppler shift up to 250 Hz was experimentally observed for a stationary receiver equipped with a poor temperature-compensated crystal oscillator (TCXO). Therefore, the Doppler frequency search window is chosen to be between -500 and 500 Hz at a carrier frequency of 882.75 MHz. The frequency spacing Δf_D must be a fraction of $1/T_{sub}$, which implies that $\Delta f_D \ll 37.5$ Hz, if T_{sub} is assumed to be one PN code period. In this paper, Δf_D is chosen to be between 8 and 12 Hz. The code start time search window is naturally chosen to be one PN code interval with a delay spacing of one sample.

Similar to GPS signal acquisition, the search could be implemented either serially or in parallel, which in turn could be performed over the code phase or the Doppler frequency. The proposed receiver performs a parallel code phase search by exploiting the optimized efficiency of the fast Fourier transform (FFT) [30]. If a signal is present, a plot of $|S_i|^2$ will show a high peak at the corresponding code start time and Doppler frequency estimates. A hypothesis test could be performed to decide whether the peak corresponds to a desired signal or noise. Since there is only one PN sequence, the search needs to be performed once. Then, the resulting surface is subdivided in the time-axis into intervals of 64 chips, each division corresponding to a particular PN offset. The PN sequences for the pilot, sync, and paging channels could be generated off-line and stored in a binary file to speed-up the processing. Fig. 8 corresponds to the front panel of the acquisition stage of the LabVIEW cellular CDMA SDR showing $|S_i|^2$ along with $\hat{t}_{s_i}$, $\hat{f}_{D_i}$, PN offset, and carrier-to-noise ratio C/N_0 for a particular BTS.

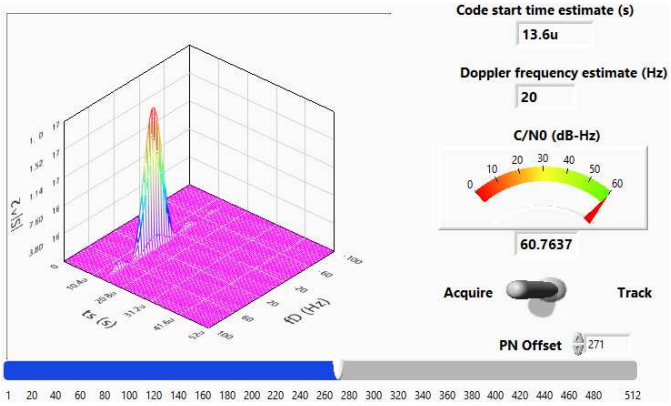

Fig. 8. Cellular CDMA signal acquisition front panel showing $|S_i|^2$ along with $\hat{t}_{s_i}$, $\hat{f}_{D_i}$, PN offset, and C/N_0 for a particular BTS.

C. Tracking

After obtaining an initial coarse estimate of the code start time and Doppler frequency, the receiver refines and maintains these estimates via tracking loops. In the proposed design, a phase-locked loop (PLL) is employed to track the carrier phase and a carrier-aided delay-locked loop (DLL) is used to track the code phase. The PLL and DLL are discussed next.

1) PLL: The PLL consists of a phase discriminator, a loop filter, and a numerically-controlled oscillator (NCO). Since the receiver is tracking the data-less pilot channel, 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. In contrast, a GPS receiver cannot use this discriminator unless the transmitted data bit values of the navigation message are known [31]. Furthermore, while GPS receivers require second- or higher-order PLLs due to the the high dynamics of GPS satellite vehicles (SVs), lower-order PLLs could be used in cellular CDMA navigation receivers. It was found that the receiver could easily track the carrier phase with a second-order PLL with a loop filter transfer function given by

$$F_{\mathrm{PLL}}(s) = \frac{2\zeta\omega_n s + \omega_n^2}{s}, \tag{5}$$

where $\zeta \equiv \frac{1}{\sqrt{2}}$ is the damping ratio and ω_n is the undamped natural frequency, which can be related to the PLL noise-equivalent bandwidth $B_{n,\mathrm{PLL}}$ by $B_{n,\mathrm{PLL}} = \frac{\omega_n}{8\zeta}(4\zeta^2+1)$ [32]. The output of the loop filter v_{PLL} is the rate of change of the carrier phase error, expressed in rad/s. The Doppler frequency is deduced by dividing v_{PLL} by 2π. The loop filter transfer function in (5) is discretized and realized in state-space. The noise-equivalent bandwidth is chosen to range between 4 and 8 Hz.

2) DLL: The carrier-aided DLL employs the non-coherent dot product discriminator. In order to compute the code phase error, the dot product discriminator uses the prompt, early and late correlations, denoted by S_{p_i}, S_{e_i}, and S_{l_i}, respectively. The prompt correlation was described in Subsection III-A. The early and late correlations are calculated by correlating the received signal with an early and a delayed version of the

prompt PN sequence, respectively. The time shift between S_{e_i} and S_{l_i} is defined by an early-minus-late time t_{eml}, expressed in chips. Since the autocorrelation function of the transmitted cellular CDMA pulses is not triangular as in the case of GPS, a wider t_{eml} is preferable in order to have a significant difference between S_{p_i}, S_{e_i}, and S_{l_i} [25]. Fig. 9 shows the autocorrelation function of the cellular CDMA PN code as specified by the IS-95 standard and that of the C/A code in GPS. It can be seen from Fig. 9 that for $t_{eml} \leq 0.5$ chips, $R_c(\tau)$ in the IS-95 standard has approximately a constant value, which is not desirable for precise tracking. In this paper, a t_{eml} of 1 to 1.2 chips is chosen.

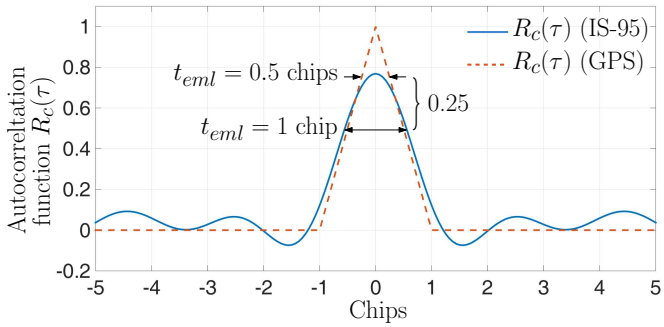

Fig. 9. Autocorrelation function of GPS C/A code and cellular CDMA PN sequence according to the IS-95 standard.

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

$$\hat{t}_{s_{i+1}} = \hat{t}_{s_i} - (v_{\mathrm{DLL},i} + \hat{f}_{D_i}/f_c) \cdot N_s T_s.$$

Fig. 10 depicts a diagram of the tracking loops.

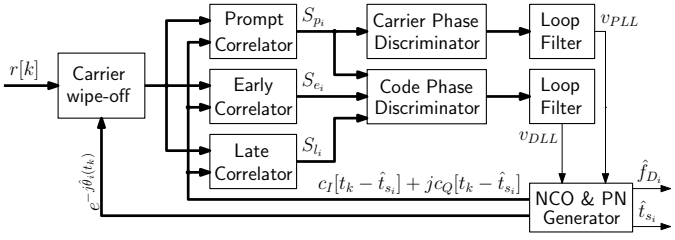

Fig. 10. Tracking loops in the navigation cellular CDMA receiver.

In a GPS receiver, the pseudorange is calculated based on the time a navigation message subframe begins in order to eliminate ambiguities due to the relative distance between GPS SVs [32]. This necessitates the decoding of the navigation message in order to detect the start of a subframe. These ambiguities do not exist in a cellular CDMA system. This follows from the fact that a PN offset of one translates to a distance greater than 15 km between BTSs, which is beyond the size of a typical cell [33]. The pseudorange can therefore be deduced by multiplying the code start time by the speed-of-light. Fig. 11 shows the intermediate signals produced within the tracking loops of the LabVIEW cellular CDMA navigation receiver: code error; phase error; Doppler frequency; early, prompt, and late correlations; pseudorange; and in-phase and quadrature components of the correlation function.

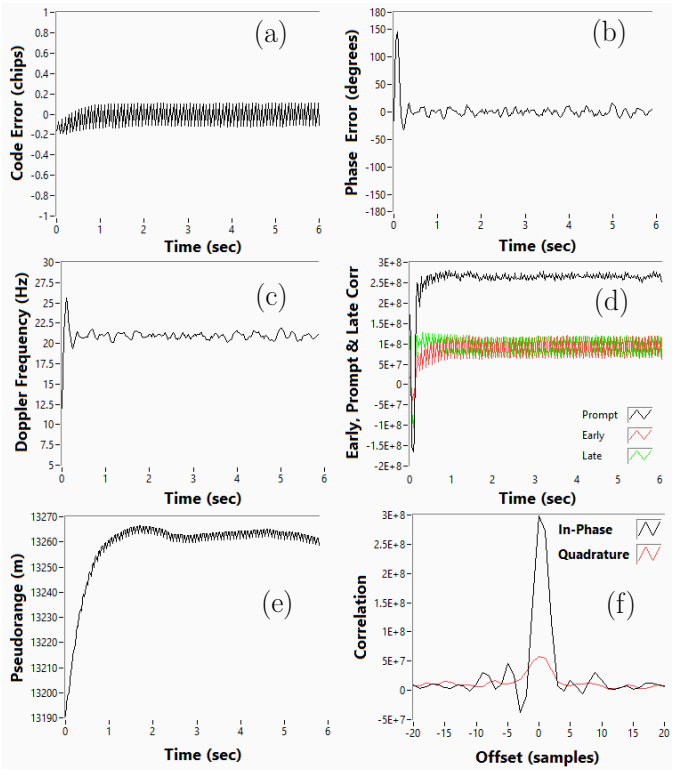

Fig. 11. Cellular CDMA signal tracking: (a) Code phase error (chips), (b) carrier phase error (degrees), (c) Doppler frequency estimate (Hz), (d) prompt (black), early(red), and late (green) correlation, (e) measured pseudorange (m), and (f) correlation function

D. Message Decoding

Demodulating the sync and paging channel signals is performed similarly to the pilot signal but with two major differences: (1) the locally generated PN sequence is furthermore spread by the corresponding Walsh code and (2) the subaccumulation period is bounded by the data symbol interval. In contrast to GPS signals in which a data bit stretches over twenty C/A codes, a sync data symbol comprises only 256 PN chips and a paging channel data symbol comprises 128 chips. After carrier wipe-off, the sync and paging signals are processed in the reverse order of the steps illustrated in Fig. 2 and Fig. 4, respectively. It is worth noting that the start of the sync message always coincides with the start of the PN code and the corresponding paging channel message starts after 320 ms minus the PN offset (expressed in seconds), as shown in Fig. 12. The long code state decoded from a sync message is valid at the beginning of the corresponding paging channel message.

The long code is generated by masking the outputs of the 42 registers and computing the modulo-two sum of the resulting bits. In contrast to the short code generator in cellular CDMA and to the C/A code generator in GPS, the 42 long code

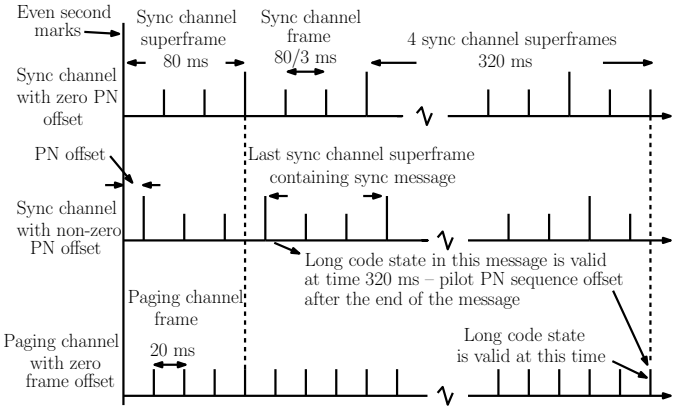

Fig. 12. Sync and paging channel timing.

generator registers are configured to satisfy a linear recursion given by

$$\begin{aligned} p(x) &= x^{42}+x^{35}+x^{33}+x^{31}+x^{27}+x^{25}+x^{22} \\ &\quad +x^{21}+x^{19}+x^{18}+x^{17}+x^{16}+x^{10}+x^{7} \\ &\quad +x^{6}+x^{5}+x^{3}+x^{2}+x+1. \end{aligned}$$

The long code mask is obtained by combining the PN offset and the paging channel number p as shown in Fig. 13.

41 — 29	28 — 24	23 — 21	20 — 9	8 — 0
1100011001101	00000	p	000000000000	PN offset

Fig. 13. Long code mask structure.

Subsequently, the sync message is decoded first and the PN offset, the paging channel number, and the long code state are then used to descramble and decode the paging message. It is important to note that the long code is first decimated at a rate of 1/64 to match the paging channel symbol rate. More details are specified in [16]. Fig. 14 shows the demodulated sync signal as well as the final information decoded from the sync and paging channels. Note that the Verizon BTS position information (latitude and longitude) are not broadcasted. Moreover, note that the last digit in the BTS ID corresponds to the sector number of the BTS cell.

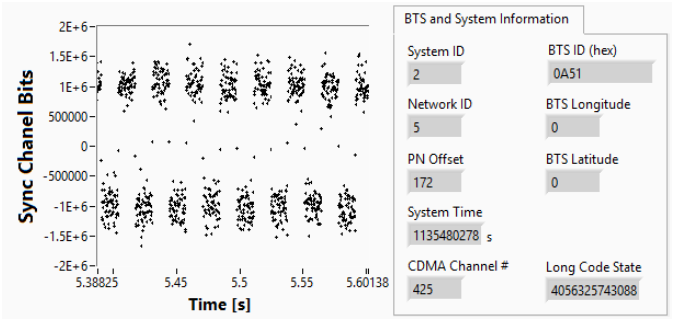

Fig. 14. Message decoding: demodulated sync channel signal (left) and BTS and system information decoded from sync and paging channels (right).

E. Cellular CDMA Navigation SDR Realization

The acquisition, tracking, and signal decoding stages of the cellular CDMA navigation SDR were developed in LabVIEW. Each stage was expressed as a separate so-called virtual instrument (VI), whose inputs and outputs are illustrated in Fig. 15.

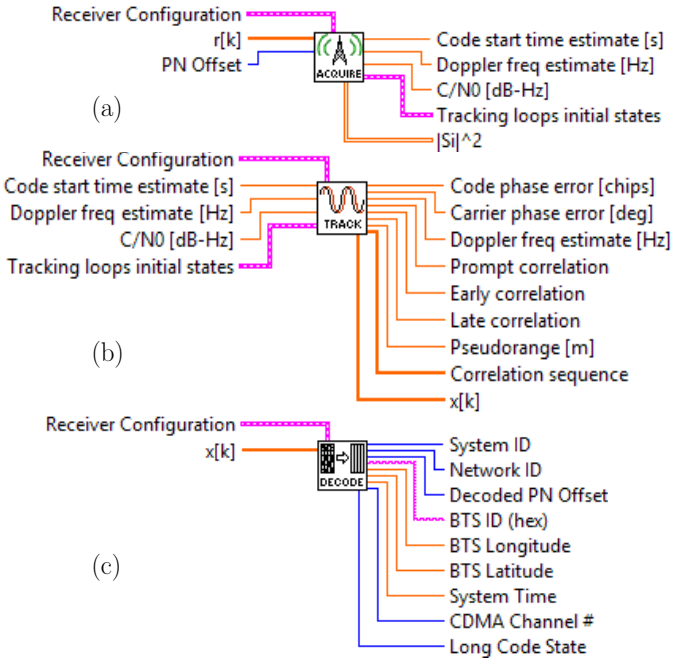

Fig. 15. Navigation Cellular CDMA LabVIEW VIs: (a) acquisition, (b) tracking, and (c) signal decoding.

IV. Navigation With Cellular CDMA Signals

By making pseudorange observations via the cellular CDMA navigation SDR presented in Section III to 4 or more BTSs, one may estimate the position and clock bias of the SDR, provided that the BTS locations and their clock biases are known. The observability of environments comprising multiple receivers making pseudorange observations on terrestrial SOPs was studied in [14] and the estimation of unknown cellular CDMA SOP states was addressed in [18]. This section describes a framework for navigating with cellular CDMA signals. The framework consists of two receivers: a mapping receiver and a navigating receiver, each equipped with the proposed cellular CDMA SDR. The mapping receiver is assumed to have knowledge of its own state vector (by having access to GPS signals, for example) and is estimating the states of the unknown SOP BTS. These estimates are shared with the navigating receiver, which has no knowledge of its own states. This section considers the estimation of receiver and SOP states in a static framework. As such, the time argument will be dropped for simplicity of notation.

A. Pseudorange Measurement Model

The state of the receiver is defined as $\boldsymbol{x}_r \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, c\delta t_r\right]^{\mathsf{T}}$, where $\boldsymbol{r}_r = [x_r, y_r, z_r]^{\mathsf{T}}$ is the position vector of the re-

ceiver, δt_r is the receiver's clock bias, and c is the speed-of-light. Similarly, the state of the ith BTS is defined as $\boldsymbol{x}_{s_i} \triangleq \left[\boldsymbol{r}_{s_i}^{\mathsf{T}}, c\delta t_{s_i}\right]^{\mathsf{T}}$, where $\boldsymbol{r}_{s_i} = [x_{s_i}, y_{s_i}, z_{s_i}]^{\mathsf{T}}$ is the position vector of the ith BTS and δt_{s_i} is the clock bias. The pseudorange measurement to the ith BTS, ρ_i, can be therefore expressed as

$$\rho_i = h_i(\boldsymbol{x}_r, \boldsymbol{x}_{s_i}) + v_i,$$

where $h_i(\boldsymbol{x}_r, \boldsymbol{x}_{s_i}) \triangleq \|\boldsymbol{r}_r - \boldsymbol{r}_{s_i}\|_2 + c \cdot [\delta t_r - \delta t_{s_i}]$ and v_i is the observation noise, which is modeled as a zero-mean Gaussian random variable with variance σ_i^2 [14]. Assuming that the receiver is drawing pseudoranges to $N \geq 4$ BTSs with known states, the receiver's state can be estimated by solving a weighted nonlinear least-squares (WNLS) problem, as discussed in Subsection IV-C. The next subsection discusses estimating the states of the BTS.

B. BTS State Estimation

Consider a mapping receiver with knowledge of its own state vector (by having access to GPS signals, for example) to be present in the navigating receiver's environment as depicted in Fig. 16. The mapping receiver's objective is to estimate the BTSs' position and clock bias states and share these estimates with the navigating receiver through a central database. If the mapping receiver has been estimating the SOP BTSs' states for a sufficiently long period of time, the position state estimate uncertainties will be negligible. Moreover, the position state estimates are physically verifiable (through surveying or satellite images, for example), at which point these estimates are assumed to match the true states and are subsequently stored in the database. Unlike the position state estimates, the clock bias state estimates are more difficult to verify and are time-varying. Therefore, in the sequel, it is assumed that the mapping receiver is only estimating the BTSs' clock bias states.

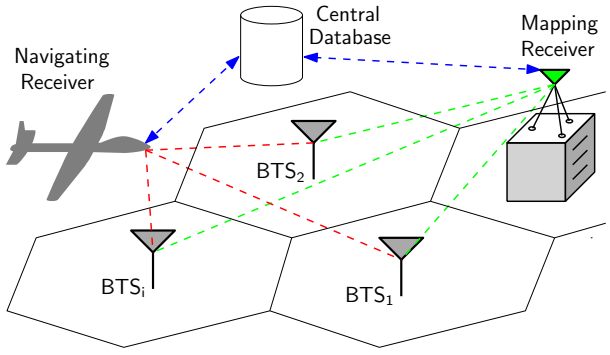

Fig. 16. Mapping receiver and navigating receiver in SOP environment.

Considers M mapping receivers and N SOP BTSs. Denote the state vector of the jth receiver by $\boldsymbol{x}_{r_j}$, the pseudorange measurement by the jth receiver on the ith BTS by $\rho_i^{(j)}$, and the corresponding measurement noise by $v_i^{(j)}$. Assume $v_i^{(j)}$ to be independent for all i and j with a corresponding variance ${\sigma_i^{(j)}}^2$. Define the set of measurements made by all receivers on the ith BTS as

$$\boldsymbol{z}_i = \begin{bmatrix} \|\boldsymbol{r}_{r_1} - \boldsymbol{r}_{s_i}\| + c\delta t_{r_1} - \rho_i^{(1)} \\ \vdots \\ \|\boldsymbol{r}_{r_M} - \boldsymbol{r}_{s_i}\| + c\delta t_{r_M} - \rho_i^{(M)} \end{bmatrix} = \begin{bmatrix} c\delta t_{s_i} - v_i^{(1)} \\ \vdots \\ c\delta t_{s_i} - v_i^{(M)} \end{bmatrix}$$
$$= c\delta t_{s_i} \mathbf{1}_M + \boldsymbol{v}^{(j)},$$

where $\mathbf{1}_M \triangleq [1, \ldots, 1]^{\mathsf{T}}$ and $\boldsymbol{v}^{(j)} \triangleq -\left[v_1^{(j)}, \ldots, v_N^{(j)}\right]^{\mathsf{T}}$.The clock bias δt_{s_i} is estimated by solving a weighted least-squares (WLS) problem, resulting in the estimate $\hat{\delta t}_{s_i} = \frac{1}{c}\left(\mathbf{1}_M^{\mathsf{T}}\mathbf{W}\mathbf{1}_M\right)^{-1}\mathbf{1}_M^{\mathsf{T}}\mathbf{W}\boldsymbol{z}$ and its associated error variance $\sigma^2_{\delta t_{s_i}} = \left(\mathbf{1}_M^{\mathsf{T}}\mathbf{W}\mathbf{1}_M\right)^{-1}$, where $\mathbf{W} = \text{diag}\left[\frac{1}{{\sigma_i^{(1)}}^2}, \ldots, \frac{1}{{\sigma_i^{(M)}}^2}\right]$ is the weighting matrix. The true clock bias of the ith BTS can now be expressed as $\delta t_{s_i} = \hat{\delta t}_{s_i} + w_i$, where w_i is a zero-mean Gaussian random variable with variance $\sigma^2_{\delta t_{s_i}}$.

C. Fusion of BTS Clock State Estimates into the Navigation Solution

Since the navigating receiver is using the estimate of the BTS clock bias, which is produced by the mapping receiver, the pseudorange measurement made by the navigating receiver on the ith BTS becomes

$$\rho_i = h_i(\boldsymbol{x}_r, \hat{\boldsymbol{x}}_{s_i}) + \eta_i,$$

where $\hat{\boldsymbol{x}}_{s_i} = \left[\boldsymbol{r}_{s_i}^{\mathsf{T}}, c\hat{\delta t}_{s_i}\right]^{\mathsf{T}}$ and $\eta_i \triangleq v_i - w_i$ models the overall uncertainty in the pseudorange measurement. Hence, the vector $\boldsymbol{\eta} \triangleq [\eta_1, \ldots, \eta_N]^{\mathsf{T}}$ is a zero-mean Gaussian random vector with a covariance matrix $\boldsymbol{\Sigma} = \mathbf{C} + \mathbf{R}$, where $\mathbf{C} = \text{diag}\left[\sigma^2_{\delta t_{s_1}}, \ldots, \sigma^2_{\delta t_{s_N}}\right]$ is the covariance matrix of $\boldsymbol{w} \triangleq [w_1, \ldots, w_N]^{\mathsf{T}}$ and $\mathbf{R} = \text{diag}\left[\sigma_1^2, \ldots, \sigma_N^2\right]$ is the covariance of the measurement noise vector $\boldsymbol{v} = [v_1, \ldots, v_N]^{\mathsf{T}}$. The Jacobian matrix $\mathbf{H}$ of the set of observation functions $\boldsymbol{h} \triangleq [h_1(\boldsymbol{x}_r, \hat{\boldsymbol{x}}_{s_1}), \ldots, h_N(\boldsymbol{x}_r, \hat{\boldsymbol{x}}_{s_N})]^{\mathsf{T}}$ with respect to $\boldsymbol{x}_r$ is given by $\mathbf{H} = [\mathbf{G} \quad \mathbf{1}_N]$, where

$$\mathbf{G} \triangleq \begin{bmatrix} \frac{x_r - x_{s_1}}{\|\boldsymbol{r}_r - \boldsymbol{r}_{s_1}\|} & \frac{y_r - y_{s_1}}{\|\boldsymbol{r}_r - \boldsymbol{r}_{s_1}\|} & \frac{z_r - z_{s_1}}{\|\boldsymbol{r}_r - \boldsymbol{r}_{s_1}\|} \\ \vdots & \vdots & \vdots \\ \frac{x_r - x_{s_N}}{\|\boldsymbol{r}_r - \boldsymbol{r}_{s_N}\|} & \frac{y_r - y_{s_N}}{\|\boldsymbol{r}_r - \boldsymbol{r}_{s_N}\|} & \frac{z_r - z_{s_N}}{\|\boldsymbol{r}_r - \boldsymbol{r}_{s_N}\|} \end{bmatrix}.$$

The navigating receiver's state can now be estimated by solving a WNLS problem, where the incremental change in the state vector estimate per iteration is given by $\delta\boldsymbol{x}_r = \left[\delta\boldsymbol{r}_r^{\mathsf{T}}, \delta(c\delta t_r)\right]^{\mathsf{T}}$, where $\delta\boldsymbol{r}_r$ and $\delta(c\delta t_r)$ are the incremental change in the position and the clock bias states, respectively, and $\delta\boldsymbol{x}_r = \left(\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}(\boldsymbol{\rho} - \boldsymbol{h})$, where $\boldsymbol{\rho} \triangleq [\rho_1, \rho_2, \ldots, \rho_N]^{\mathsf{T}}$ and $\mathbf{H}$ and $\boldsymbol{h}$ are evaluated at the current iteration of the state estimate $\hat{\boldsymbol{x}}_r$ and the BTS state estimates $\{\hat{\boldsymbol{x}}_{s_i}\}_{i=1}^N$.

D. Clock Biases of Different Sectors of a BTS

A typical CDMA BTS transmits into three different sectors within a particular cell. Ideally, all sectors' clocks should be driven by the same oscillator, which implies that the same

clock bias (after correcting for the PN offset) should be observed in all sectors of the same cell. However, factors such as unknown distance between the phase-center of the sector antennas, delays due to RF connectors and other components (e.g., cabling, filters, amplifiers, etc.) cause the clock biases corresponding to different BTS sectors to be slightly different. This behavior was consistently observed experimentally and is depicted in Fig. 17.

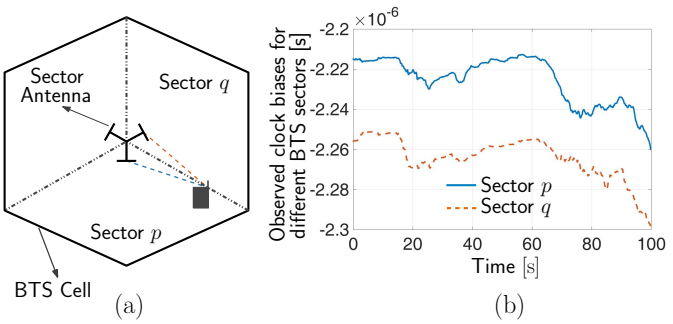

Fig. 17. (a) A receiver placed at the border of two sectors of a cell, making pseudorange observations on both sector antennas simultaneously. The receiver has knowledge of its own states (from GPS signals) and has knowledge of the BTS position states. (b) Observed BTS clock bias for the two sectors (after correcting for the PN offset).

Fig. 17 suggest that the clock biases $\delta t_{s_i}^{(p)}$ and $\delta t_{s_i}^{(q)}$ of sectors p and q, respectively, of the ith BTS are related through

$$c\delta t_{s_i}^{(q)} = c\delta t_{s_i}^{(p)} + \epsilon_i^{(p,q)},$$

where $\epsilon_i^{(p,q)}$ is a random variable that models the discrepancy between the sectors' clock biases. The discrepancy $\epsilon_{i_{p,q}}$ can be particulary harmful if the mapping and navigating receivers are listening to two different sectors of the same BTS cell. In the following subsection, a bound on the error introduced in the navigation solution due to the sector clock discrepancy is characterized.

E. Navigation Solution Error Characterization Due to Presence of Discrepancy in BTS Sectors' Clock Biases

The pseudorange measured by the navigating receiver in sector q of the ith BTS is given by $\rho_i^{(q)} = \|\boldsymbol{r}_r - \boldsymbol{r}_{s_i}\| + c \cdot \left[\delta t_r - \delta t_{s_i}^{(q)}\right] + v_i$. If the navigating receiver uses $\hat{\delta t}_{s_i}^{(p)}$, which is produced by the mapping receiver in sector p, as an estimate of $\delta t_{s_i}^{(q)}$, the pseudorange model becomes $\rho_i'^{(q)} = \|\boldsymbol{r}_r - \boldsymbol{r}_{s_i}\| + c\cdot\left[\delta t_r - \hat{\delta t}_{s_i}^{(q)}\right] + \eta_i + \epsilon_i^{(p,q)} = \rho_i^{(q)} + \epsilon_i^{(p,q)}$. Generalizing this expression to the case of N SOP BTS cells with each mapping receiver listening to a different sector than the navigating receiver yields $\boldsymbol{\rho}' = \boldsymbol{\rho} + \boldsymbol{\epsilon}$, where $\boldsymbol{\rho}' \triangleq \left[\rho_1'^{(q)}, \ldots, \rho_N'^{(q)}\right]^{\mathsf{T}}$ and $\boldsymbol{\epsilon} \triangleq \left[\epsilon_1^{(p,q)}, \ldots, \epsilon_N^{(p,q)}\right]^{\mathsf{T}}$. The effect of $\boldsymbol{\epsilon}$ on the incremental change $\delta\boldsymbol{x}_r$ is $\left(\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\boldsymbol{\epsilon}$. In general, the discrepancy vector $\boldsymbol{\epsilon}$ can be expressed as

$$\boldsymbol{\epsilon} = b\mathbf{1}_N + \boldsymbol{\psi}, \tag{6}$$

where $b \triangleq \frac{1}{N}\sum_{i=1}^{N}\epsilon_i^{(p,q)} = \frac{1}{N}\mathbf{1}_N^{\mathsf{T}}\boldsymbol{\epsilon}$, and $\boldsymbol{\psi} \triangleq \left[\epsilon_1^{(p,q)} - b, \ldots, \epsilon_N^{(p,q)} - b\right]^{\mathsf{T}}$. The term b is referred to as the common error and the vector $\boldsymbol{\psi}$ as the uncommon error. It follows from this definition that $\sum_{i=1}^{N}\psi_i = 0$. By replacing the expression of $\boldsymbol{\epsilon}$ in a WNLS step, the incremental change in the receiver state estimate can be expressed as $\delta\boldsymbol{x}_r = \delta\boldsymbol{x}_r^{(b)} + \delta\boldsymbol{x}_r^{(\psi)}$, where $\delta\boldsymbol{x}_r^{(b)} = b\left(\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\mathbf{1}_N$ is the effect of the common error and $\delta\boldsymbol{x}_r^{(\psi)} = \left(\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\boldsymbol{\psi}$ is the effect of the uncommon error.

1) Effect of Common Error on Navigation Solution: The common error term will only affect the receiver clock bias estimate. This can be shown by realizing that

$$\mathbf{H}\boldsymbol{e}_4 = [\mathbf{G} \quad \mathbf{1}_N]\,\boldsymbol{e}_4 = \mathbf{1}_N, \tag{7}$$

where $\boldsymbol{e}_4 = [0,0,0,1]^{\mathsf{T}}$. Then, using (7), the incremental change due to the common term becomes

$$\begin{aligned}\delta\boldsymbol{x}_r^{(b)} &= b\left(\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\mathbf{1}_N \\ &= b\left(\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\mathbf{H}\boldsymbol{e}_4 = b\boldsymbol{e}_4,\end{aligned} \tag{8}$$

which has a non-zero component only in the clock bias state. Thus, if the individual errors $\epsilon_i^{(p,q)}$ happen to be all equal, the receiver's position estimate will be unaffected.

2) Effect of Uncommon Error on Navigation Solution: Unlike the common error, the uncommon error will affect all receiver states. Next, a bound on the error introduced by the uncommon error in the receiver's position estimate is derived. The incremental change in the receiver position state can be expressed as $\delta\boldsymbol{r}_r = \mathbf{T}\delta\boldsymbol{x}_r = \mathbf{T}\delta\boldsymbol{x}_r^{(b)} + \mathbf{T}\delta\boldsymbol{x}_r^{(\psi)}$, where $\mathbf{T} = [\mathbf{I}_{3\times 3} \quad \mathbf{0}_{3\times 1}]$. By replacing $\delta\boldsymbol{x}_r^{(b)}$ with its expression from (8), the change in position becomes

$$\delta\boldsymbol{r}_r = b\mathbf{T}\boldsymbol{e}_4 + \mathbf{T}\delta\boldsymbol{x}_r^{(\psi)} = \mathbf{T}\delta\boldsymbol{x}_r^{(\psi)}. \tag{9}$$

Taking the 2-norm on both sides of (9) yields

$$\begin{aligned}\|\delta\boldsymbol{r}_r\| &= \left\|\mathbf{T}\delta\boldsymbol{x}_r^{(\psi)}\right\| \\ &\leq \|\mathbf{T}\| \cdot \left\|\delta\boldsymbol{x}_r^{(\psi)}\right\| = \left\|\delta\boldsymbol{x}_r^{(\psi)}\right\|,\end{aligned} \tag{10}$$

since $\|\mathbf{T}\| = 1$. Replacing $\delta\boldsymbol{x}_r^{(\psi)}$ by its expression in the WNLS update, (10) becomes

$$\begin{aligned}\|\delta\boldsymbol{r}_r\| &\leq \left\|\left(\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\left(\boldsymbol{\epsilon} - b\mathbf{1}_N\right)\right\| \\ &\leq \gamma\left\|\boldsymbol{\epsilon} - b\mathbf{1}_N\right\|,\end{aligned} \tag{11}$$

where $\gamma \triangleq \left\|\left(\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathsf{T}}\boldsymbol{\Sigma}^{-1}\right\|$. Therefore, to determine the upper bound of (11), the term $\|\boldsymbol{\epsilon} - b\mathbf{1}_N\|$, or equivalently its square, must be maximized, leading to

$$\underset{\boldsymbol{\epsilon}}{\text{maximize}} \quad \|\boldsymbol{\epsilon} - b\mathbf{1}_N\|^2 = \|\mathbf{A}\boldsymbol{\epsilon}\|^2, \tag{12}$$

$$\mathbf{A} \triangleq \begin{bmatrix} (1-\frac{1}{N}) & -\frac{1}{N} & \cdots & -\frac{1}{N} \\ -\frac{1}{N} & (1-\frac{1}{N}) & \cdots & -\frac{1}{N} \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{1}{N} & -\frac{1}{N} & \cdots & (1-\frac{1}{N}) \end{bmatrix}.$$

Motivated by experimental data collected in different BTS cell sectors and for various cells, it is reasonable to assume that

$$|\epsilon_i^{(p,q)}| \leq \alpha, \quad \forall\, i, \tag{13}$$

where α is some positive constant. As such, the maximization problem in (12) becomes constrained by (13). The function in (12) is convex, since it is the composition of the norm with a linear mapping, and the box constraints in (13) form a convex set. Therefore, the maximizer of (12) subject to the constraints (13) lies on the extreme points of the feasibility region, namely $\left|\left(\epsilon_i^{(p,q)}\right)^\star\right| = \alpha,\ \forall\ i$.

If N is even, the maximum is achieved whenever $\sum_{i=1}^{N} \epsilon_i^{(p,q)} = 0$; hence, the maximizer is $\left(\epsilon_i^{(p,q)}\right)^\star = (-1)^i\, \alpha,\ \forall\ i$. If N is odd, the maximum is achieved whenever $\sum_{i=1}^{N} \epsilon_i^{(p,q)} = |\alpha|$; hence, the maximizer is $\left(\epsilon_i^{(p,q)}\right)^\star = (-1)^i\, \alpha$ for $i = 1, \ldots, N-1$, and $\left(\epsilon_N^{(p,q)}\right)^\star = \pm\alpha$. Therefore, the maximum error introduced in the receiver's position is bounded by

$$\|\delta \boldsymbol{r}_r\| \leq \begin{cases} \sqrt{N}\alpha\,\gamma, & \text{if } N \text{ is even,} \\ \sqrt{\frac{N^2-1}{N}}\alpha\,\gamma, & \text{if } N \text{ is odd.} \end{cases}$$

V. Experimental Results

Navigation using the proposed mapper/navigater framework discussed in Section IV was tested experimentally with the cellular CDMA SDR developed on Section III. For this purpose, a mapping receiver and a navigating receiver were equipped with two antennas each to acquire and track: 1) GPS signals and 2) signals from nearby cellular CDMA BTSs. The receiver CDMA antennas used for the experiment were consumer-grade 800/1900 MHz cellular antennas, and the GPS antennas were surveyor-grade Leica antennas. The GPS and cellular signals were simultaneously down-mixed and synchronously sampled via two universal software radio peripherals (USRPs) driven by the same GPS-disciplined oscillator. The receivers were tuned to a 882.75 MHz carrier frequency, which is a channel allocated for Verizon Wireless. Samples of the received signals were stored for off-line post-processing. The GPS signal was processed by a Generalized Radionavigation Interfusion Device (GRID) SDR [34] and the cellular CDMA signals were processed by the proposed LabVIEW-based SDR. Fig. 18 shows the experimental hardware setup

Over the course of the experiment, both receivers were listening to the same 3 BTSs of which the position states were mapped prior to the experiment according to the framework discussed in [35]. The mapping receiver and the navigating receiver were listening to the same sectors; hence, there were no additional errors due to the discrepancies between sector clocks. The mapping receiver was stationary during the experiments and was estimating the clock biases of the 3 known BTSs. The measurement noise variance for the mapping and navigating receivers was calculated from [36]

$$\sigma_i^2 = \frac{c^2\, t_{eml}\, B_{n,\mathrm{DLL}}\, T_c^2}{2\,(C/N_0)_i}\left[1 + \frac{1}{T_{CO}\,(C/N_0)_i}\right],$$

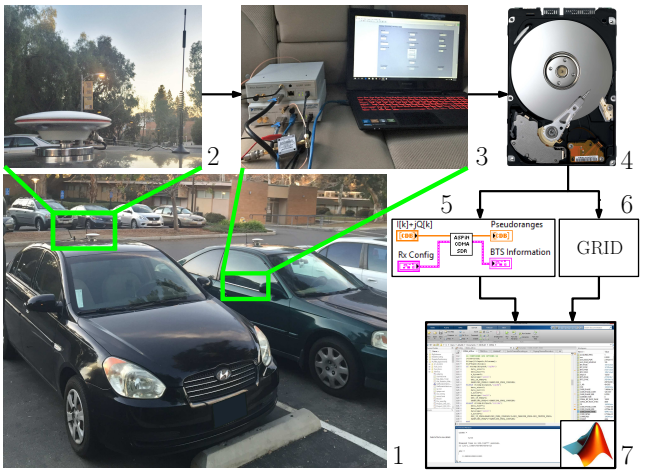

Fig. 18. Experimental hardware setup. 1: Vehicle-mounted receivers. 2: GPS and cellular CDMA antennas. 3: USRPs. 4: Storage device. 5: LabVIEW-based cellular CDMA SDR. 6: GRID GPS SDR. 7: MATLAB-based estimator.

where $(C/N_0)_i$ is the measured carrier-to-noise ratio for the ith BTS and $T_{CO} = \frac{1}{37.5}$ s is the predetection coherent integration time. The weighting matrices for the WNLS were calculated accordingly.

Since measurements to only 3 BTSs were available, all measurements and trajectories were projected onto a two-dimensional (2-D) space. Subsequently, only the horizontal position and the clock bias of the navigating receiver were being estimated. The environment layout as well as the true and estimated receiver trajectories are shown in Fig. 19.

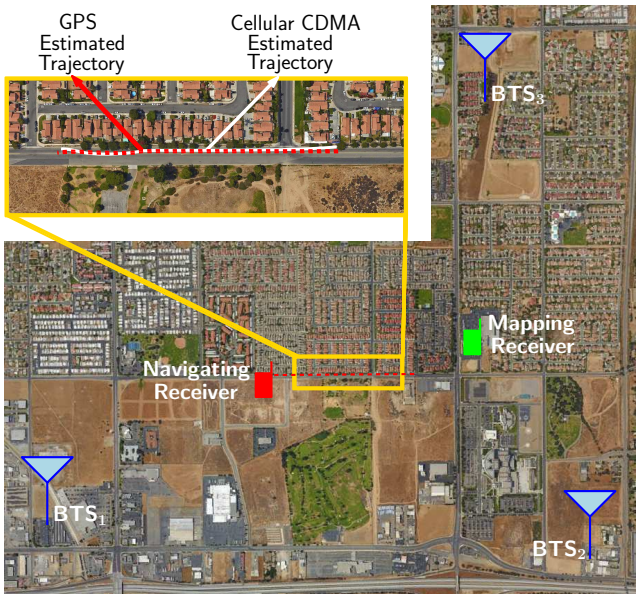

Fig. 19. Navigating receiver trajectory and mapping receiver and BTS locations.

It can be seen from Fig. 19 that the navigation solution obtained from the cellular CDMA signals follows closely the navigation solution obtained using GPS signals. The mean distance difference along the traversed trajectory between the GPS and CDMA navigation solutions was calculated to be

5.51 m with a standard deviation of 4.01 m and a maximum error of 11.11 m. The mean receiver clock estimate difference between the GPS and CDMA navigation solutions was calculated to be -45 ns with a standard deviation of 23.03 ns.

VI. Conclusion

This paper presented an SDR architecture for cellular CDMA-based navigation. Models of the cellular CDMA signals were first developed and optimal extraction of relevant positioning and timing information was discussed. Next, a detailed description of the various stages of a LabVIEW-based SDR was presented. Furthermore, a navigation framework consisting of a mapping/navigating receiver in a cellular CDMA environment was studied. The induced error in the navigation solution due to having the mapping and navigating receivers listen to different sectors of the BTS cell was analyzed. Finally, experimental results comparing the navigation solution from GPS versus that of cellular CDMA utilizing the developed SDR showed a mean distance difference of 5.51 m.

Acknowledgment

This work was supported in part by the Office of Naval Research (ONR) under Grant N00014-16-1-2305. This work was also supported in part by a grant from the National Center for Sustainable Transportation (NCST), supported by the U.S. Department of Transportation (USDOT) through the University Transportation Centers Program. The authors would also like to thank Souradeep Bhattacharya, Yuanqi Gao, and Keshav Narayan for their help in data collection.

References

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

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

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

[4] S. Fang, J. Chen, H. Huang, and T. Lin, "Is FM a RF-based positioning solution in a metropolitan-scale environment? A probabilistic approach with radio measurements analysis," *IEEE Transactions on Broadcasting*, vol. 55, no. 3, pp. 577–588, September 2009.

[5] M. Joerger, L. Gratton, B. Pervan, and C. Cohen, "Analysis of Iridium-augmented GPS for floating carrier phase positioning," *NAVIGATION, Journal of the Institute of Navigation*, vol. 57, no. 2, pp. 137–160, 2010.

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

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

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

[9] M. Rabinowitz and J. Spilker, Jr., "A new positioning system using television synchronization signals," *IEEE Transactions on Broadcasting*, vol. 51, no. 1, pp. 51–61, March 2005.

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

[11] J. Khalife, Z. Kassas, and S. Saab, "Indoor localization based on floor plans and power maps: Non-line of sight to virtual line of sight," in *Proceedings of ION GNSS Conference*, September 2015, pp. 2291–2300.

[12] R. Faragher and R. Harle, "Towards an efficient, intelligent, opportunistic smartphone indoor positioning system," *NAVIGATION, Journal of the Institute of Navigation*, vol. 62, no. 1, pp. 55–72, 2015.

[13] Z. Kassas and T. Humphreys, "Observability and estimability of collaborative opportunistic navigation with pseudorange measurements," in *Proceedings of ION GNSS Conference*, September 2012, pp. 621–630.

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

[15] K. Pesyna, K. Wesson, R. Heath, and T. Humphreys, "Extending the reach of GPS-assisted femtocell synchronization and localization through tightly-coupled opportunistic navigation," in *Proceedings of IEEE GLOBECOM Workshops*, December 2011, pp. 242–247.

[16] TIA/EIA-95-B, "Mobile station-base station compatibility standard for dual-mode spread spectrum systems," October 1998.

[17] B. Horn. (2014) How to install a cellular repeater. [Online]. Available: http://people.csail.mit.edu/bkph/CellTracker

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

[19] J. Morales and Z. Kassas, "Collaborative mapping of terrestrial signals of opportunity," *IEEE Transactions on Aerospace and Electronic Systems*, 2015, in preparation.

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

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

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

[23] T. Humphreys, M. Psiaki, P. Kintner, and B. Ledvina, "GNSS receiver implementation on a DSP: Status, challenges, and prospects," in *Proceedings of ION GNSS Conference*, September 2006, pp. 1567–1575.

[24] Z. Kassas, J. Bhatti, and T. Humphreys, "A graphical approach to GPS software-defined receiver implementation," in *Proceedings of IEEE Global Conference on Signal and Information Processing*, December 2013, pp. 1226–1229.

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

[26] A. Viterbi, *CDMA: Principles of Spread Spectrum Communication*. Redwood City, CA, USA: Addison Wesley Longman Publishing Co., 1995.

[27] 3GPP2, "Recommended minimum performance standards for cdma2000 spread spectrum base stations," December 1999.

[28] R. Vaughn, N. Scott, and D. White, "The theory of bandpass sampling," *IEEE Transactions on Signal Processing*, vol. 39, no. 9, pp. 1973–1984, September 1991.

[29] K. Wesson, K. Pesyna, J. Bhatti, and T. Humphreys, "Opportunistic frequency stability transfer for extending the coherence time of GNSS receiver clocks," in *Proceedings of ION GNSS Conference*, September 2010, pp. 2959–2968.

[30] D. van Nee and A. Coenen, "New fast GPS code-acquisition technique using FFT," *Electronics Letters*, vol. 27, no. 2, pp. 158–160, January 1991.

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

[32] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed. Ganga-Jamuna Press, 2010.

[33] ETSI, "Universal mobile telecommunications system (UMTS); base station (BS) radio transmission and reception (FDD)," 2015.

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

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

[36] M. S. Braasch and A. J. van Dierendonck, "GPS receiver architectures and measurements," in *Proceedings of the IEEE*, vol. 87, no. 1, January 1999, pp. 48–64.