Navigation With Cellular CDMA Signals—Part I: Signal Modeling and Software-Defined Receiver Design

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

***Abstract*—A software-defined receiver (SDR) 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 positioning and timing purposes. The pseudorange from the proposed receiver is modeled and the pseudorange error is studied in an additive white Gaussian channel. Experimental results with aerial and ground vehicles utilizing the proposed SDR are presented demonstrating a close match between the variation in pseudoranges and the variation in true ranges between the receiver and two cellular CDMA base transceiver stations (BTSs). Moreover, the dynamics of the discrepancy between the observed clock biases of different sectors of the same BTS cell is modeled and validated experimentally. The consistency of the obtained model is analyzed through experimental tests in different locations, at different times, and for different cellular providers.**

***Index Terms*—Radionavigation, signals of opportunity, opportunistic navigation, direct-sequence code-division multiple access, software radio, system identification.**

I. Introduction

TRADITIONAL approaches to enable navigation in global navigation satellite system (GNSS)-challenged environments (e.g., indoors, deep urban canyons, and intentionally jammed and spoofed environments) have focused on coupling GNSS receivers with inertial navigation systems and advanced signal processing algorithms [1]–[4]. Recently, considerable attention has been devoted to exploiting ambient radio frequency (RF) signals of opportunity (SOPs) as a stand-alone alternative to GNSS or to complement GNSS-based navigation [5]–[8].

Different studies have been conducted for specific types of SOPs including AM/FM radio [9], [10], iridium satellites [11], [12], digital television (DTV) [13], [14], cellular [15]–[19], and Wi-Fi [20]–[22]. It has been demonstrated that AM signals could potentially provide 20 meter positioning accuracy [9]. A better localization performance could be achieved using DTV signals, where the average positioning error becomes less than 4 meters in certain favorable environments [13]. Experimental results for navigation using cellular code-division multiple access (CDMA) fused with DTV signals showed a navigation solution within 2 meters from that of a GPS solution and a maximum difference of 12 meters [17]. SOPs have also been used for indoor positioning, where it has been shown that an average positioning error of 4 meters could be achieved by coupling Wi-Fi and inertial measurement units (IMUs) in a SLAM framework [20]. Coupling observables from other signals such as GSM, digital audio broadcasting, and cellular 3G with IMU measurements also showed promising results [6]. Moreover, iridium satellite signals were considered to improve navigation performance in deep urban and indoor environments [23]. SOPs were also employed in timing applications, such as enabling longer integration time for GPS-assisted femtocells in indoor environments [24]. Besides these experimental studies, the literature on SOPs answers theoretical questions on the observability and estimability of the SOP signal landscape [25], [26], motion planning in the SOP landscape for optimal information gathering [27]–[29], and collaborative SOP landscape map building [30], [31].

There are three main challenges associated with using SOPs for navigation: (1) the unavailability of appropriate low-level signal models for optimal extraction of states and parameters of interest for positioning and timing purposes, (2) the absence of published receiver architectures capable of producing navigation observables, and (3) the lack of sources of error identification and error models for SOP-based navigation. To the authors' knowledge, while previous work demonstrated experimental results for navigation via cellular CDMA signals, none of these three challenges has been fully addressed. This paper, the first in a series of two, addresses these three challenges for cellular CDMA signals. Cellular CDMA signals are particularly attractive SOPs due to their abundance, high carrier frequency, large bandwidth, high received power, and CDMA modulation structure, which is similar to the well-studied GPS signals.

Unlike GNSS signals, cellular CDMA signals are not intended for navigation [32]. As such, to exploit these signals for

Manuscript received June 28, 2017; revised December 6, 2017; accepted January 17, 2018. Date of publication January 30, 2018; date of current version March 12, 2018. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Pengfei Xia. This work was supported in part by the Office of Naval Research under Grant N00014-16-1-2305. *(Corresponding author: Zaher M. Kassas.)*

The authors are with the Department of Electrical and Computer Engineering, The University of California, Riverside, Riverside, CA 92521 USA (e-mail: joe.khalife@email.ucr.edu; kimia.shamaei@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/TSP.2018.2799167

navigation purposes, the received signals must be parameterized in terms of relevant navigation observables. Subsequently, an appropriate specialized receiver capable of extracting this relevant positioning and timing information from the received signals must be designed. The navigation observables produced by these receivers can be used to either (1) map the states of the transmitting base transceiver station (BTS) tower (i.e., estimate the BTS's position, clock bias, and clock drift) or (2) navigate via the received BTS signals.

Cellular CDMA communication receivers are routinely implemented in hardware in mobile phones; however, hardware implementations limit the ability to extract or modify information within the receiver. As such, a software-defined receiver (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 [33]. 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 [34]. An SDR for navigation with cellular CDMA signals based on the IS-95 standard was presented in [18].

Sources of error and the so-called error budget for GNSS-based navigation have been thoroughly studied [35], [36]. In contrast, navigation sources of error for SOPs are not yet fully characterized. It is important to note that while some of these errors are not harmful for communication purposes, they severely degrade the navigation performance if they are not modeled and accounted for appropriately. In [18], a new navigation error source corresponding to cellular CDMA signals was revealed, namely bias mismatch for different sectors within the same BTS cell. A rudimentary random walk (RW) model for the dynamics of this error was identified in [37]. This bias discrepancy across different sectors can be particularly harmful for navigation purposes in two scenarios. In the first scenario, a receiver that has no knowledge of its own states, nor has access to GNSS, is present in a cellular CDMA environment and is making pseudorange measurements to BTSs nearby. The receiver has access to estimates of the BTSs' states through a central database. These estimates could be produced through a stationary mapping receiver or crowdsourced from mobile receivers in the environment. In some cases, while estimates of the BTS sector in which the navigating receiver is located may not be available, estimates of a different sector of the same BTS cell may be available in the database. If the navigating receiver uses such estimates without accounting for the fact that they are produced by a mapping receiver in a different sector, the discrepancy between the sector clock biases will introduce errors on the order of tens of meters in the receiver's position estimate and tens of nanoseconds in the receiver's clock bias estimate. A second scenario where this discrepancy must be accounted for is when the receiver is navigating in a simultaneous localization and mapping (SLAM) framework. In the SLAM approach, the receiver does not need access to the BTS state estimates from an external source; however, it must account for the aforementioned discrepancy when transitioning from one sector of the BTS to another sector.

This paper makes four contributions. First, it extends the work in [18] by presenting precise, low-level signal models for optimal extraction of relevant navigation and timing information from received cellular CDMA signals compatible with the latest cdma2000 standard. Second, the statistics of the pseudorange error in an additive white Gaussian channel are derived. Third, the paper presents experimental results validating this SDR by comparing the variation in the pseudoranges obtained by the proposed SDR and the true ranges to two BTSs. Fourth, the paper identifies an elaborate exponentially correlated dynamical model for the discrepancy in the clock biases in different sectors of a BTS cell and discusses when this model could be appropriately approximated by a RW model. The derived model is validated experimentally in different locations, at different times, and for different cellular providers.

The remainder of the paper is organized as follows. Section II provides an overview of the cellular CDMA forward link pilot signal structure. Section III presents a complete implementation of the acquisition and tracking stages of a navigation cellular CDMA SDR. Section IV analyzes the statistics of the pseudorange error of the CDMA SDR in an additive white Gaussian channel. Section V models the discrepancy between the clock biases of different sectors of the same BTS. Section VI validates the proposed navigation SDR and analyzes the consistency of the obtained clock bias discrepancy model experimentally. Concluding remarks are given in Section VII.

II. Cellular CDMA Forward Link Signal Structure

In a cellular CDMA communication system, several logical channels are multiplexed on the forward link channel, including: a pilot channel, a sync channel, and 7 paging channels [38]. The following subsection presents an overview of the modulation process of the forward link pilot channel and provides models of the transmitted and received signals from which timing and positioning information can be extracted.

A. Modulation of Forward Link CDMA Pilot Signals

The data transmitted on the forward link channel in cellular CDMA systems (i.e., BTS to mobile receiver) is modulated through quadrature phase shift keying (QPSK) and then spread using direct-sequence CDMA (DS-CDMA). The in-phase and quadrature components, I and Q, respectively, of the pilot channel carry the same message $m(t)$. The spreading sequences c_I and c_Q, called the short code, are 2^{15}-chip long pseudorandom noise (PN) codes that are generated using linear feedback shift registers (LFSRs). 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 PN offset, is unique for each BTS and is an integer multiple of 64 chips, hence a total of 512 PN offsets can be realized. It can be shown that the cross-correlation of the same PN sequence with different pilot offsets

is negligible [32], [39]. The transmitted pilot signal is nothing but the short code; however, other channels, such as the sync and paging channels, carry data and are furthermore spread by Walsh codes. The CDMA signal is subsequently filtered using a digital pulse shaping filter that limits the bandwidth of the transmitted CDMA signal according to the cdma2000 standard. The signal is finally modulated by the carrier frequency to produce $s(t)$.

B. Transmitted Signal Model

The transmitted pilot signal $s(t)$ by a particular BTS can be expressed as

$$\begin{aligned} s(t) &= \sqrt{C}\left\{c_I'[t-\Delta(t)]\cos(\omega_c t) - c_Q'[t-\Delta(t)]\sin(\omega_c t)\right\} \\ &= \frac{\sqrt{C}}{2}\left\{c_I'[t-\Delta(t)] + jc_Q'[t-\Delta(t)]\right\}\cdot e^{j\omega_c t} \\ &\quad + \frac{\sqrt{C}}{2}\left\{c_I'[t-\Delta(t)] - jc_Q'[t-\Delta(t)]\right\}\cdot e^{-j\omega_c t}, \end{aligned}$$

where C is the total power of the transmitted signal; $c_I'(t) = c_I(t) * h(t)$ 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, $T_c = \frac{1\times 10^{-6}}{1.2288}$ 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. While the clock bias of the BTS can be neglected for communication purposes, it cannot be ignored for navigation purposes and must be estimated in some fashion. The sequel to this paper presents a framework for estimating this clock bias that is based on mapping and navigating receivers.

C. Received Signal Model After Front-End Processing

Assuming the transmitted signal to have propagated through an additive white Gaussian noise channel with a power spectral density of $\frac{N_0}{2}$, a model of the received discrete-time (DT) signal $r[m]$ after RF front-end processing: downmixing, a quadrature approach to bandpass sampling [40], and quantization can be expressed as

$$\begin{aligned} r[m] &= \frac{\sqrt{C}}{2}\left\{c_I'[t_m - t_s(t_m)] - jc_Q'[t_m - t_s(t_m)]\right\} \\ &\quad \cdot\, e^{j\theta(t_m)} + n[m], \end{aligned} \tag{1}$$

where $t_s(t_m) \triangleq \delta t_{TOF} + \Delta(t_k - \delta t_{TOF})$ is the PN code phase of the BTS, $t_m = mT_s$ 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, θ is the beat carrier phase of the received signal, and $n[m] = n_I[m] + jn_Q[m]$ with n_I and n_Q being independent, identically-distributed (i.i.d.) Gaussian random sequences with zero-mean and variance $\frac{N_0}{2T_s}$. The receiver developed in Section III will operate on the samples of $r[m]$ in (1).

TABLE I
FIR OF THE PULSE-SHAPING FILTER USED IN CDMA2000 [38]

m'	$h[m']$	m'	$h[m']$	m'	$h[m']$
0, 47	-0.02528832	8, 39	0.03707116	16, 31	-0.01283966
1, 46	-0.03416793	9, 38	-0.02199807	17, 30	-0.14347703
2, 45	-0.03575232	10, 37	-0.06071628	18, 29	-0.21182909
3, 44	-0.01673370	11, 36	-0.05117866	19, 28	-0.14051313
4, 43	0.02160251	12, 35	0.00787453	20, 27	0.09460192
5, 42	0.06493849	13, 34	0.08436873	21, 26	0.44138714
6, 41	0.09100214	14, 33	0.12686931	22, 25	0.78587564
7, 40	0.08189497	15, 32	0.09452834	23, 24	1.0

III. CELLULAR CDMA NAVIGATION RECEIVER ARCHITECTURE

The cellular CDMA navigation receiver consists of three main stages: signal acquisition, tracking, and decoding. 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 this section. The next subsection gives a brief description of the correlation process in the cellular CDMA navigation receiver. The following subsections present a software implementation in LabVIEW of the acquisition and tracking stages. Details on decoding the sync and paging channel messages are provided in [18], [41], [42].

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

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

where $\hat{\theta}$ is the beat carrier phase estimate and h is a pulse shaping filter, which is a DT version of the one used to shape the spectrum of the transmitted signal, with a finite-impulse response (FIR) given in Table I. The samples m' of the FIR in Table I are spaced by $\frac{T_c}{4}$.

Next, $x[m]$ is correlated with a local replica of the spreading PN sequence. In a digital receiver, the correlation operation is expressed as

$$Z_k = \frac{1}{N_s}\sum_{m=k}^{k+N_s-1} x[k]\left\{c_I[t_m - \hat{t}_s(t_m)] + jc_Q[t_m - \hat{t}_s(t_m)]\right\}, \tag{3}$$

where Z_k is the kth subaccumulation, N_s is the number of samples per subaccumulation, and $\hat{t}_s(t_m)$ is the code start time estimate over the kth subaccumulation. The code phase can be assumed to be approximately constant over a short subaccumulation interval $T_{\text{sub}} = N_s T_s$; hence, $\hat{t}_s(t_m) \approx \hat{t}_{s_k}$. It is worth mentioning that theoretically, T_{sub} can be made arbitrarily large since no data is transmitted on the pilot channel. Practically,

T_{sub} is mainly limited by the stability of the BTS and receiver oscillators. In this paper, T_{sub} is set to one PN code period. The carrier phase estimate is modeled as $\hat{\theta}(t_m) = 2\pi \hat{f}_{D_k} t_m + \theta_0$, where $\hat{f}_{D_k}$ 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 $r[m]$ and $x[m]$, defined in (1) and (2), into (3), it can be shown that

$$Z_k = \sqrt{C}\, R_c(\Delta t_k) \left[\frac{1}{N_s} \sum_{m=k}^{k+N_s-1} e^{j\Delta\theta(t_m)} \right] + n_k, \quad (4)$$

where R_c is the autocorrelation function of the PN sequences c'_I and c'_Q, $\Delta t_k \triangleq \hat{t}_{s_k} - t_{s_k}$ is the code phase error, $\Delta\theta(t_m) \triangleq \theta(t_m) - \hat{\theta}(t_m)$ is the carrier phase error, and $n_k \triangleq n_{I_k} + jn_{Q_k}$ with n_{I_k} and n_{Q_k} being i.i.d. Gaussian random sequences with zero-mean and variance $\frac{N_0}{2T_s N_s} = \frac{N_0}{2T_{\text{sub}}}$.

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. A search over the code start time and Doppler frequency is performed to detect the presence of a signal. Based on experimental data, the Doppler frequency search window is chosen to be between -500 and 500 Hz at a carrier frequency in the 800/850 MHz cellular band, with a frequency spacing Δf_D between 8 and 12 Hz if T_{sub} is only one PN code period. The code start time search window is naturally chosen to be one PN code interval with a delay spacing of one sample. The proposed receiver performs a parallel code phase search by exploiting the optimized efficiency of the fast Fourier transform (FFT) [43]. A hypothesis test on $|Z_k|^2$ could be performed to decide whether the peak corresponds to a transmitted signal or to noise. Since there is only one PN sequence, the search needs to be performed once. Fig. 3(a) illustrates the front panel of the acquisition stage of the LabVIEW cellular CDMA SDR showing $|Z_k|^2$ along with $\hat{t}_{s_k}$, $\hat{f}_{D_k}$, PN offset, and carrier-to-noise ratio 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. 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

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

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's noise-equivalent bandwidth $B_{n,\text{PLL}}$ by $B_{n,\text{PLL}} = \frac{\omega_n}{8\zeta}(4\zeta^2 + 1)$ [36]. 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 at a sampling period T_{sub} and realized in state-space. The noise-equivalent bandwidth is chosen to range between 4 and 8 Hz.

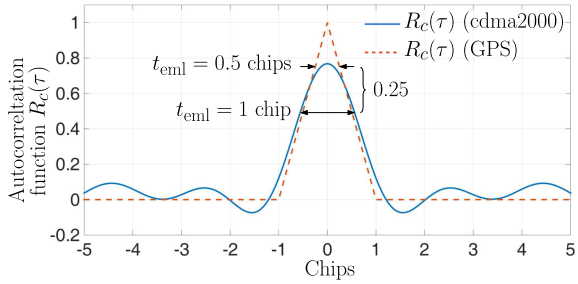

Fig. 1. Autocorrelation function of GPS C/A code and cellular CDMA PN sequence according to the cdma2000 standard.

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 Z_{p_k}, Z_{e_k}, and Z_{l_k}, 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 Z_{e_k} and Z_{l_k} 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 Z_{p_k}, Z_{e_k}, and Z_{l_k}. Fig. 1 shows the autocorrelation function of the cellular CDMA PN code as specified by the cdma2000 standard and that of the C/A code in GPS. It can be seen from Fig. 1 that for $t_{\text{eml}} \leq 0.5$ chips, $R_c(\tau)$ in the cdma2000 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.

The DLL loop filter is a simple gain K, with a noise-equivalent bandwidth $B_{n,\text{DLL}} = \frac{K}{4} \equiv 0.5$ 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

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

The pseudorange estimate ρ can therefore be deduced by multiplying the code start time by the speed-of-light c, i.e.,

$$\rho(k) = c \cdot \hat{t}_{s_k}. \quad (6)$$

Fig. 2 depicts a diagram of the tracking loops.

Fig. 3(b)–(e) shows the intermediate signals produced within the tracking loops of the LabVIEW cellular CDMA naviga-

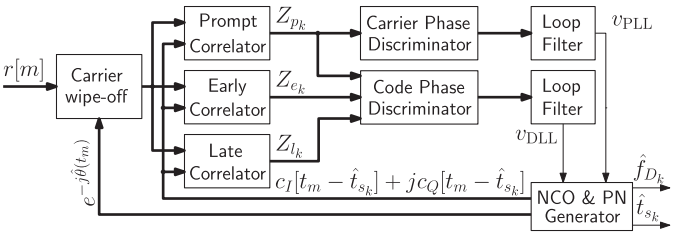

Fig. 2. Tracking loops in the navigation cellular CDMA receiver. Thick lines represent complex quantities.

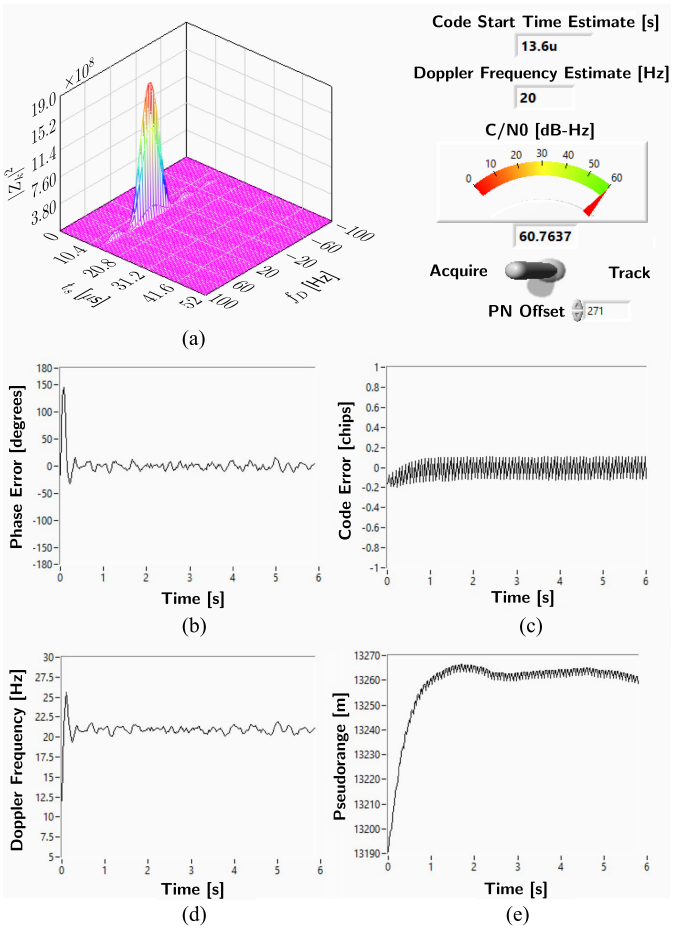

Fig. 3. (a) Cellular CDMA signal acquisition front panel showing $|Z_k|^2$ along with $\hat{t}_{s_k}$, $\hat{f}_{D_k}$, PN offset, and C/N_0 for a particular BTS. (b)–(e) Cellular CDMA signal tracking: (b) Carrier phase error (degrees), (c) code phase error (chips), (d) Doppler frequency estimate (Hz), and (e) measured pseudorange (m).

tion receiver: phase error, code error, Doppler frequency, and pseudorange.

In the next section, the tracking performance of the DLL is studied and the closed-loop statistics of the code start time estimate are derived.

IV. Pseudorange Error Analysis in an Additive White Gaussian Noise Channel

Section III presented a recipe for designing a receiver that can extract a pseudorange estimate from cellular CDMA signals. This section analyzes the statistics of the error of the pseudorange estimate for a coherent DLL. It is worth noting that when the receiver is closely tracking the carrier phase, the dot-product discriminator and a coherent DLL discriminator will perform similarly. Hence, the analysis is carried for a coherent discriminator. Moreover, this subsection studies the statistics of the pseudorange error in a coherent baseband discriminator. To this end, it is assumed that t_s is constant. Therefore, the carrier aiding term will be negligible and the code start time error Δt_k will be affected only by the channel noise. As mentioned in Subsection III-C, it is enough to use a first-order loop for the DLL yielding the following closed-loop time-update error equation [44]

$$\Delta t_{k+1} = (1 - 4B_{n,\mathrm{DLL}} T_{\mathrm{sub}})\Delta t_k + KD_k, \tag{7}$$

where D_k is the output of the code discriminator. The discriminator statistics are discussed next.

A. Discriminator Statistics

In order to study the discriminator statistics, the received signal noise statistics must first be determined. In what follows, the received signal noise is characterized for an additive white Gaussian channel.

1) Received Signal Noise Statistics: In order to make the analysis more tractable, the continuous-time (CT) received signal and correlation are considered. The transmitted signal is assumed to propagate in an additive white Gaussian noise channel with a power spectral density $\frac{N_0}{2}$. The CT received signal after downmixing and bandpass sampling is given by

$$r(t) = \frac{\sqrt{C}}{2}\left[c_I'(t - t_s) - jc_Q'(t - t_s)\right] e^{j\theta(t)} + n(t),$$

and the CT matched-filtered baseband signal $x(t)$ is given by

$$x(t) = \left[r(t) \cdot e^{-j\hat{\theta}(t)}\right] * h(-t).$$

The resulting early and late correlations in the DLL are given by

$$Z_{e_k} = \int_0^{T_{\mathrm{sub}}} x(t)\left[c_I(t - \tau_{e_k}) + jc_Q(t - \tau_{e_k})\right] dt,$$

$$Z_{l_k} = \int_0^{T_{\mathrm{sub}}} x(t)\left[c_I(t - \tau_{l_k}) + jc_Q(t - \tau_{l_k})\right] dt,$$

where $\tau_{e_k} \triangleq \hat{t}_{s_k} - \frac{t_{\mathrm{eml}}}{2}T_c$ and $\tau_{l_k} \triangleq \hat{t}_{s_k} + \frac{t_{\mathrm{eml}}}{2}T_c$. Assuming the receiver is closely tracking the carrier phase [36], the early and late correlations may be approximated with

$$Z_{e_k} \approx T_{\mathrm{sub}}\sqrt{C}R_c\left(\Delta t_k - \frac{t_{\mathrm{eml}}}{2}T_c\right) + n_{e_k} \triangleq S_{e_k} + n_{e_k},$$

$$Z_{l_k} \approx T_{\mathrm{sub}}\sqrt{C}R_c\left(\Delta t_k + \frac{t_{\mathrm{eml}}}{2}T_c\right) + n_{l_k} \triangleq S_{l_k} + n_{l_k},$$

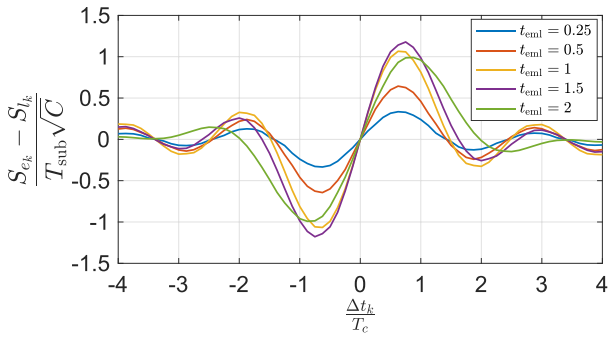

Fig. 4. Output of the coherent baseband discriminator function for the CDMA shortcode with different correlator spacings.

where n_{e_k} and n_{l_k} are zero-mean Gaussian random variables with the following variances and covariances

$$\begin{aligned}
\text{var}\{n_{e_k}^2\} &= \text{var}\{n_{l_k}^2\} = \frac{T_{\text{sub}} N_0}{2} \quad \forall k, \\
\mathbb{E}\{n_{e_k} n_{l_k}\} &= \frac{T_{\text{sub}} N_0 R_c(t_{\text{eml}} T_c)}{2}, \quad \forall k, \\
\mathbb{E}\{n_{e_k} n_{e_j}\} &= \mathbb{E}\{n_{l_k} n_{l_j}\} = \mathbb{E}\{n_{e_k} n_{l_j}\} = 0, \quad \forall k \neq j.
\end{aligned}$$

2) Coherent Discriminator Statistics: The coherent baseband discriminator function is defined as

$$D_k \triangleq \frac{Z_{e_k} - Z_{l_k}}{\sqrt{C}} = \frac{(S_{e_k} - S_{l_k})}{\sqrt{C}} + \frac{(n_{e_k} - n_{l_k})}{\sqrt{C}}.$$

The normalized signal component of the discriminator function $\frac{(S_{e_k} - S_{l_k})}{T_{\text{sub}}\sqrt{C}}$ is shown in Fig. 4 for $t_{\text{eml}} = \{0.25, 0.5, 1, 1.5, 2\}$.

It can be seen from Fig. 4 that for small values of $\frac{\Delta t_k}{T_c}$, the discriminator function can be approximated by a linear function given by

$$D_k \approx \alpha \Delta t_k + \frac{(n_{e_k} - n_{l_k})}{\sqrt{C}},$$

where α is the slope of the discriminator function at $\Delta t_k = 0$ [44], which is obtained by

$$\alpha = \left.\frac{\partial D_k}{\partial \Delta t_k}\right|_{\Delta t_k = 0} = T_{\text{sub}} \left[\frac{d}{d\tau} R_c(-\tau) - \frac{d}{d\tau} R_c(\tau)\right]\Bigg|_{\tau = \frac{t_{\text{eml}}}{2} T_c}.$$

Since $R_c(\tau)$ is symmetric,

$$\left.\frac{d}{d\tau} R_c(\tau)\right|_{\tau = -\frac{t_{\text{eml}}}{2} T_c} = -\left.\frac{d}{d\tau} R_c(\tau)\right|_{\tau = \frac{t_{\text{eml}}}{2} T_c} \triangleq R_c'\left(\frac{t_{\text{eml}}}{2} T_c\right),$$

and the linearized discriminator output becomes

$$D_k \approx 2 T_{\text{sub}} R_c'\left(\frac{t_{\text{eml}}}{2} T_c\right) \Delta t_k + \frac{(n_{e_k} - n_{l_k})}{\sqrt{C}}. \tag{8}$$

It is worth noting that $R_c(\tau)$ and $R_c'(\tau)$ are obtained by numerically computing the autocorrelation function of the pulse-shaped short code. Since the FIR of the pulse-shaping filter $h[k]$ is defined over only 48 values of k, the autocorrelation function $R_c(\tau)$ will be defined over 95 values of τ. However, interpolation may be used to evaluate $R_c(\tau)$ and $R_c'(\tau)$ at any τ. The mean and variance of D_k can be obtained from (8), and are given by

$$\mathbb{E}\{D_k\} = 2 T_{\text{sub}} R_c'\left(\frac{t_{\text{eml}}}{2} T_c\right) \Delta t_k, \tag{9}$$

$$\begin{aligned}
\text{var}\{D_k\} &= \frac{1}{C} \text{var}\{n_{e_k} - n_{l_k}\} \\
&= \frac{1}{C} \left[\text{var}\{n_{e_k}\} + \text{var}\{n_{l_k}\} - 2\mathbb{E}\{n_{e_k} n_{l_k}\}\right] \\
&= \frac{T_{\text{sub}} N_0}{C} \left[1 - R_c(t_{\text{eml}} T_c)\right].
\end{aligned} \tag{10}$$

Now that the discriminator statistics are known, the closed-loop pseudorange error is characterized.

B. Closed-Loop Analysis

In order to achieve the desired loop noise-equivalent bandwidth, K in (7) must be normalized according to

$$K = \left.\frac{4 B_{n,\text{DLL}} T_{\text{sub}} \Delta t_k}{\mathbb{E}\{D_k\}}\right|_{\Delta t_k = 0} = \frac{2 B_{n,\text{DLL}}}{R_c'\left(\frac{t_{\text{eml}}}{2} T_c\right)}. \tag{11}$$

In cellular CDMA systems, for a t_{eml} of 1.2, the loop filter gain becomes $K \approx 4 B_{n,\text{DLL}}$, hence the choice of K in Subsection III-C. Assuming a zero-mean tracking error, i.e., $\mathbb{E}\{\Delta t_k\} = 0$, then the variance of the code start time error is given by

$$\begin{aligned}
\text{var}\{\Delta t_{k+1}\} = &\ (1 - 4 B_{n,\text{DLL}} T_{\text{sub}})^2 \text{var}\{\Delta t_k\} \\
&+ K^2 \text{var}\{D_k\}.
\end{aligned} \tag{12}$$

At steady-state, $\text{var}\{\Delta t_{k+1}\}$ becomes

$$\text{var}\{\Delta t_{k+1}\} = \text{var}\{\Delta t_k\} = \text{var}\{\Delta t\}, \tag{13}$$

where Δt is the steady-state code start time error. Combining (11)–(13) yields

$$\text{var}\{\Delta t\} = \frac{B_{n,\text{DLL}}\, q(t_{\text{eml}})}{2(1 - 2 B_{n,\text{DLL}} T_{\text{sub}}) C/N_0}, \tag{14}$$

where

$$q(t_{\text{eml}}) \triangleq \frac{1 - R_c(t_{\text{eml}} T_c)}{\left[R_c'\left(\frac{t_{\text{eml}}}{2} T_c\right)\right]^2}.$$

The pseudorange can hence be expressed as

$$\rho(k) = c \cdot t_{s_k} + c \cdot \Delta t_k \triangleq c \cdot t_{s_k} + v(k),$$

where $v(k)$ is a zero-mean random variable with variance $\sigma^2 = c^2 \cdot \text{var}\{\Delta t\}$. Fig. 5 shows a plot of σ as a function of the carrier-to-noise ratio C/N_0 for $t_{\text{eml}} = 1.25$ chips.

V. Clock Bias Discrepancy Model Between Different Sectors of a BTS Cell

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

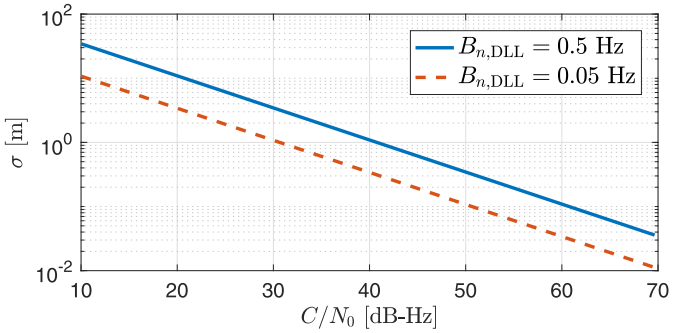

Fig. 5. Plot of σ as a function of the carrier-to-noise ratio $\frac{C}{N_0}$ for $t_{\mathrm{eml}} = 1.25$ chips and $B_{n,\mathrm{DLL}} = \{0.5\text{ Hz}, 0.05\text{ Hz}\}$.

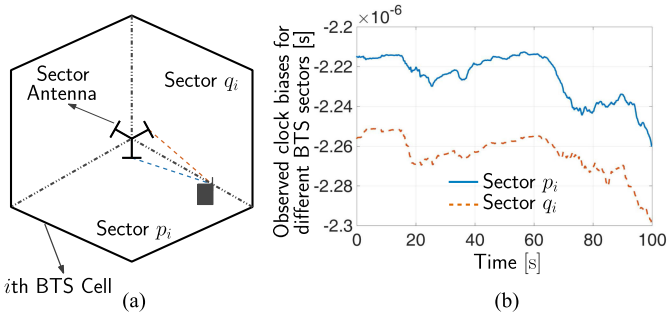

Fig. 6. (a) A cellular CDMA receiver placed at the border of two sectors of a BTS cell, making pseudorange observations on both sector antennas simultaneously. The receiver has knowledge of its own states and has knowledge of the BTS position states. (b) Observed BTS clock bias corresponding to two different sectors from a real BTS (Verizon Wireless).

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 in different locations, at different times, and for different cellular providers [18], [45]. In this section, the model for the pseudorange produced by the cellular CDMA navigation receiver developed in Section III is given. Subsequently, a stochastic dynamic model for the observed clock bias mismatch for different sectors of the same BTS cell is identified and experimentally validated.

A. Pseudorange Measurement Model

The pseudorange can be obtained from the proposed cellular CDMA navigation SDR by multiplying the code phase estimate by the speed-of-light. A model for this produced pseudorange can be parameterized as a function of the receiver and BTS position and clock bias states. For simplicity, a planar environment will be assumed, with the receiver and BTS three-dimensional (3-D) position states appropriately projected onto such planar environment. The subsequent discussion can be straightforwardly generalized to 3-D. 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 $\boldsymbol{r}_r = [x_r, y_r]^{\mathsf{T}}$ is the position vector of the navigator, δt_r is the navigator'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 $\boldsymbol{r}_{s_i} = [x_{s_i}, y_{s_i}]^{\mathsf{T}}$ is the position vector of the ith BTS and δt_{s_i} is the clock bias. After mild approximations discussed in [26], the pseudorange measurement to the ith BTS at time k, $\rho_i(k)$, can be expressed as

$$\rho_i(k) = \|\boldsymbol{r}_r(k) - \boldsymbol{r}_{s_i}\| + c \cdot [\delta t_r(k) - \delta t_{s_i}(k)] + v_i(k), \tag{15}$$

where v_i is the observation noise, which is modeled as a zero-mean white Gaussian random sequence with variance σ_i^2.

B. Sector Clock Bias Discrepancy Detection

In order to detect the discrepancy between sectors' clock biases, the proposed cellular CDMA receiver was placed at the border of two sectors of a BTS cell and was drawing pseudorange measurements from both sector antennas. The receiver had full knowledge of its state and of the BTS's position. Subsequently, the receiver solved for the BTS clock biases $\delta t_{s_i}^{(p_i)}$ and $\delta t_{s_i}^{(q_i)}$ observed in sectors p_i and q_i, respectively. A realization of $\delta t_{s_i}^{(p_i)}$ and $\delta t_{s_i}^{(q_i)}$ is depicted in Fig. 6.

Fig. 6 suggests that the clock biases $\delta t_{s_i}^{(p_i)}$ and $\delta t_{s_i}^{(q_i)}$ can be related through

$$\delta t_{s_i}^{(q_i)}(k) = \delta t_{s_i}^{(p_i)}(k) + \left[1 - 1_{q_i}(p_i)\right] \epsilon_i(k),$$

where ϵ_i is a random sequence that models the discrepancy between the sectors' clock biases and

$$1_{q_i}(p_i) = \begin{cases} 1, & \text{if } p_i = q_i, \\ 0, & \text{otherwise,} \end{cases}$$

is the indicator function.

Remark: The cdma2000 protocol requires all PN offsets to be synchronized to within 10 μs from GPS time; however, synchronization to within 3 μs is recommended [46]. Since each sector of a BTS uses a different PN offset, then the clock biases $\delta t_{s_i}^{(p_i)}$ and $\delta t_{s_i}^{(q_i)}$ will be bounded according to -10 μs $\leq \delta t_{s_i}^{(p_i)}(k) \leq 10$ μs and -10 μs $\leq \delta t_{s_i}^{(q_i)}(k) \leq 10\mu$ s. Therefore, ϵ_i will be within 20 μs from GPS time, namely

$$-20\ \mu\text{s} \leq \epsilon_i \leq 20\ \mu\text{s}.$$

The discrepancy $\{\epsilon_i\}_{i=1}^2$ between the clock biases observed in two different sectors of some BTS cell over a 24-hour period is shown in Figs. 7(a) and (b) for two different BTSs. Both cellular towers pertain to the U.S. cellular provider Verizon Wireless and are located near the University of California, Riverside campus. The cellular signals were recorded between September 23 and 24, 2016. It can be seen from Fig. 7 that $|\epsilon_i|$ is bounded by approximately 2.02 μs and 0.65 μs, respectively, which is well below 20 μs.

In what follows, a stochastic dynamic model for ϵ_i is identified.

C. Model Identification

It is hypothesized that the discrepancy $\epsilon_i(k) = \delta t_{s_i}^{(q_i)}(k) - \delta t_{s_i}^{(p_i)}(k)$ for $p_i \neq q_i$ adheres to an autoregressive (AR) model

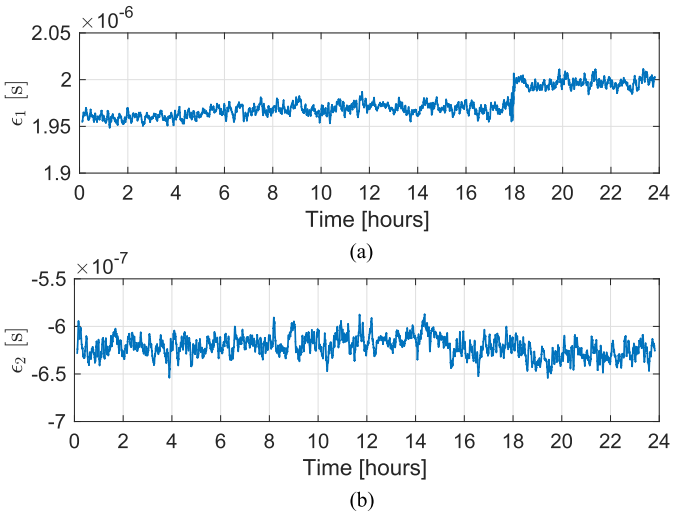

Fig. 7. The discrepancies ϵ_1 and ϵ_2 between the clock biases observed in two different sectors of some BTS cell over a 24-hour period. (a) and (b) correspond to ϵ_1 and ϵ_2 for BTSs 1 and BTS 2, respectively. Both BTSs pertain to the U.S. cellular provider Verizon Wireless and are located near the University of California, Riverside campus. The cellular signals were recorded between September 23 and 24, 2016. It can be seen that $|\epsilon_i|$ is well below 20 μs.

of order n [47], which can be expressed as

$$\epsilon_i(k) + \sum_{j=1}^{n} a_{i,j}\epsilon_i(k-j) = \zeta_i(k),$$

where ζ_i is a white sequence. The objective is to find the order n and the coefficients $\{a_{i,j}\}_{j=1}^{n}$ that will minimize the sum of the squared residuals $\sum_{l=0}^{k}\zeta_i^2(l)$. To find the order n, several AR models were identified and for a fixed order, a least-squares estimator was used to solve for $\{a_{i,j}\}_{j=1}^{n}$. It was noted that the sum of the squared residuals corresponding to each $n \in \{1,\ldots,10\}$ were comparable, suggesting that the minimal realization of the AR model is of first-order. For $n=1$, it was found that $a_{i,1} = -(1-\beta_i)$, where $0 < \beta_i \ll 1$ (on the order of 8×10^{-5} to 3×10^{-4}). This implies that ϵ_i is an exponentially correlated random variable (ECRV) with the continuous-time (CT) dynamics given by

$$\dot{\epsilon}_i(t) = -\alpha_i\epsilon_i(t) + \tilde{\zeta}_i(t), \tag{16}$$

where $\alpha_i \triangleq \frac{1}{\tau_i}$, τ_i is the time constant of the discrepancy dynamical model, and $\tilde{\zeta}_i$ is a CT white process with variance $\sigma^2_{\tilde{\zeta}_i}$. Discretizing (16) at a sampling period T yields the DT model

$$\epsilon_i(k+1) = \phi_i\,\epsilon_i(k) + \zeta_i(k), \tag{17}$$

where $\phi_i = e^{-\alpha_i T}$. The variance of ζ_i is given by $\sigma^2_{\zeta_i} = \frac{\sigma^2_{\tilde{\zeta}_i}}{2\alpha_i}(1 - e^{-2\alpha_i T})$. Fig. 8 shows an experimental realization of ϵ_i and the corresponding residual ζ_i.

D. Model Validation

The identified model in (17) was validated through residual analysis [47]. To this end, the autocorrelation function (acf) and power spectral density (psd) of the residual error e_i defined as the difference between the measured data ϵ_i' and predicted value from the identified model ϵ_i in (17), i.e., $e_i \triangleq \epsilon_i' - \epsilon_i$, were computed. Fig. 9 shows the acf and psd of e_i computed from a different realization of ϵ_i. The psd was computed using Welch's method [48]. It can be seen from Fig. 9 that the residual error e_i is nearly white; hence, the identified model is capable of describing the true system.

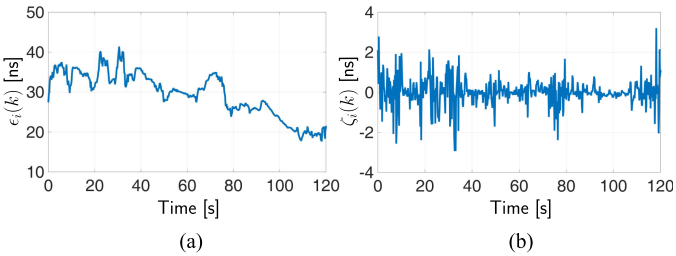

Fig. 8. (a) A realization of the discrepancy ϵ_i between the observed clock biases of two BTS sectors and (b) the corresponding residual ζ_i.

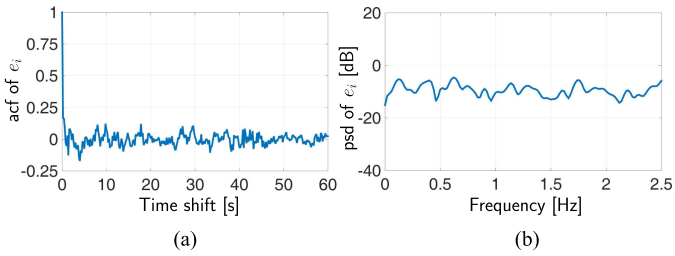

Fig. 9. The (a) acf and (b) psd of e_i with a sampling frequency of 5 Hz.

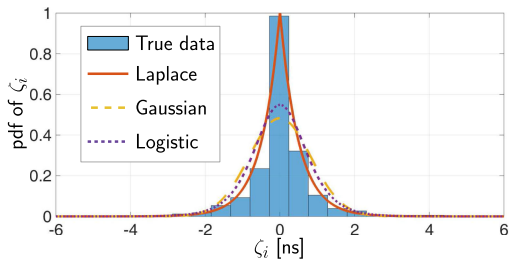

Fig. 10. Distribution of ζ_i from experimental data and the estimated Laplace pdf via MLE. For comparison purposes, a Gaussian (dashed) and Logistic (dotted) pdf fits are plotted as well.

E. Residual Statistics Characterization

Next, the probability density function (pdf) of ζ_i will be characterized, assuming that ζ_i is an ergodic process. It was found that the Laplace distribution best matches the actual distribution of ζ_i obtained from experimental data, i.e., the pdf of ζ_i is given by

$$p(\zeta_i) = \frac{1}{2\lambda_i}\exp\left(-\frac{|\zeta_i - \mu_i|}{\lambda_i}\right), \tag{18}$$

where μ_i is the mean of ζ_i and λ_i is the parameter of the Laplace distribution, which can be related to the variance by $\sigma^2_{\zeta_i} = 2\lambda_i^2$. A maximum likelihood estimator (MLE) was adopted to calculate the parameters μ_i and λ_i of $p(\zeta_i)$ [49]. Fig. 10 shows the actual distribution of the data along with the estimated pdf. For

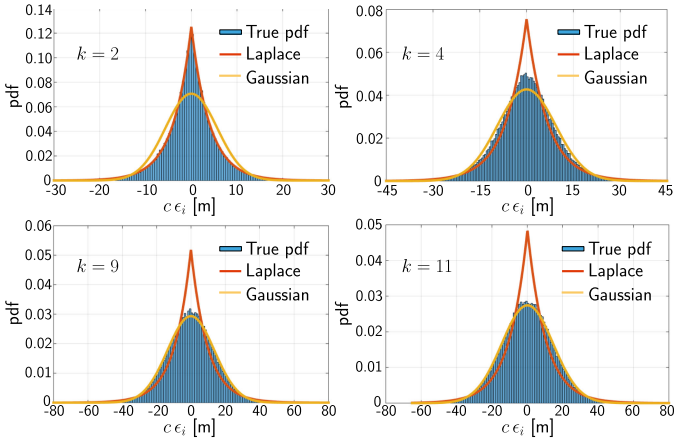

Fig. 11. Simulation of the distribution of $c\epsilon_i$ (expressed in meters) for $\phi_i = 0.95$, $\mu_i = 0$, and $\lambda_i = 13$ ns. The true distribution is fitted to a Gaussian distribution (yellow) and a Laplace distribution (red).

comparison purposes, a Gaussian and Logistic pdf fits obtained via an MLE are plotted as well.

It was noted that $\mu_i \approx 0$ from several batches of collected experimental data; therefore, ζ_i is appropriately modeled as a zero-mean white Laplace-distributed random sequence with variance $2\lambda_i^2$.

F. Statistics of the Discrepancy Between Sector Clock Biases

The solution to the dynamic model (17) can be expressed as

$$\epsilon_i(k) = \phi_i^k \epsilon_i(0) + \sum_{l=0}^{k-1} \phi_i^{k-1-l} \zeta_i(l),$$

where $\epsilon_i(0)$ is the known initial discrepancy. Without loss of generality, $\epsilon_i(0)$ is assumed to be zero. Therefore, $\epsilon_i(k)$ has mean $\mathbb{E}[\epsilon_i(k)] = 0$ and variance $\text{var}[\epsilon_i(k)] = \frac{\sigma_{\zeta_i}^2}{2\alpha_i}\left(1 - e^{-2\alpha_i kT}\right)$. Note that the discrepancy ϵ_i is the weighted sum of uncorrelated Laplace-distributed random variables. The central limit theorem asserts that the pdf of ϵ_i converges to a Gaussian pdf. It was noted that the convergence happens for $k \geq 9$ for $\phi_i \geq 0.95$, as depicted in Fig. 11.

G. Approximation With a Random Walk

When $\alpha_i \to 0$, the dynamics of $\epsilon_i(k)$ converge to that of a random walk. Since the values of α_i obtained experimentally are very small, studying the RW model as an approximation becomes relevant. The mean of the RW process is also zero and the variance is given by $\sigma_{\zeta_i}^2 kT$. It can be readily shown that $\sigma_{\zeta_i}^2 kT > \frac{\sigma_{\zeta_i}^2}{2\alpha_i}\left(1 - e^{-2\alpha_i kT}\right), \forall\, \alpha_i > 0, k > 0$, and $T > 0$. Denote the relative error between the variances of the ECRV and RW models by γ, then the following can be established

$$\frac{1}{2\alpha_i kT}\left(1 - e^{-2\alpha_i kT}\right) \geq 1 - \gamma. \tag{19}$$

Note that (19) may also be expressed as

$$f(x, \gamma) \geq 0,$$

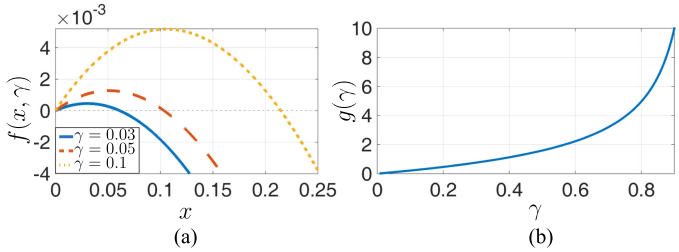

Fig. 12. (a) Plot of $f(x, \gamma)$ for $\gamma = \{0.03, 0.05, 0.1\}$. (b) Plot of $g(\gamma)$.

where

$$x \triangleq 2\alpha_i kT \quad \text{and} \quad f(x, \gamma) \triangleq 1 - (1 - \gamma)x - e^{-x}.$$

Fig. 12(a) shows $f(x, \gamma)$ as a function of x for different values of γ. Let $x^\star = g(\gamma)$ denote the solution to $f(x, \gamma) = 0$ for a given γ. According to Fig. 12(a), for a given γ, $f(x, \gamma) \geq 0$ is satisfied $\forall\, x \in (0, g(\gamma)]$. Fig. 12(b) depicts the solution $x^\star = g(\gamma)$ as a function of γ. Note that $g(\gamma)$ does not have a closed form but can be calculated using iterative methods, e.g., Newton's method.

Subsequently, for a desired γ and a known α_i, one can solve for k that guarantees the relative error between the RW and ECRV variances to be less than γ using $2\alpha_i kT \leq g(\gamma)$. For example, given that $\gamma = 0.01$ and $\alpha_i = 3 \times 10^{-4}$ Hz, then for $kT \leq \frac{g(0.01)}{2\times 3\times 10^{-4}} = 33.55$ s, the relative error between the RW and ECRV variances will remain less than 1%.

VI. Experimental Results

In this section, experimental results on an aerial and ground vehicle, validating the proposed cellular CDMA navigation SDR are presented. Next, the consistency of the clock bias discrepancy model derived in Section V is analyzed experimentally.

A. Cellular CDMA Navigation SDR Experimental Results

In order to test the proposed cellular CDMA SDR, the variation in the pseudorange obtained by the receiver was compared to the variation in true range between the moving receiver and cellular CDMA BTSs. For this purpose, two experiments were conducted where the proposed receiver was mounted on (1) an unmanned aerial vehicle (UAV) and (2) a ground vehicle.

1) UAV Results: In the first experiment, a DJI Matrice 600 UAV was equipped with the proposed SDR, a consumer-grade 800/1900 MHz cellular antenna, and a small consumer-grade GPS antenna to discipline the on-board oscillator. The cellular signals were down-mixed and sampled via a single-channel universal software radio peripheral (USRP) driven by a GPS-disciplined oscillator (GPSDO). The cellular receiver was tuned to a carrier frequency of 883.98 MHz, which is a channel allocated for the U.S. cellular provider Verizon Wireless. Samples of the received signals were stored for off-line post-processing. The cellular CDMA signals were processed by the proposed LabVIEW-based SDR. The ground-truth reference for the UAV trajectory was taken from its on-board navigation system, which uses GPS, an inertial navigation system, and other sensors. Fig. 13 shows the SOP BTS environment in which the UAV was present as well as the experimental hardware setup.

Fig. 13. SOP BTS environment and experimental hardware setup for the UAV experiment. Map data: Google Earth.

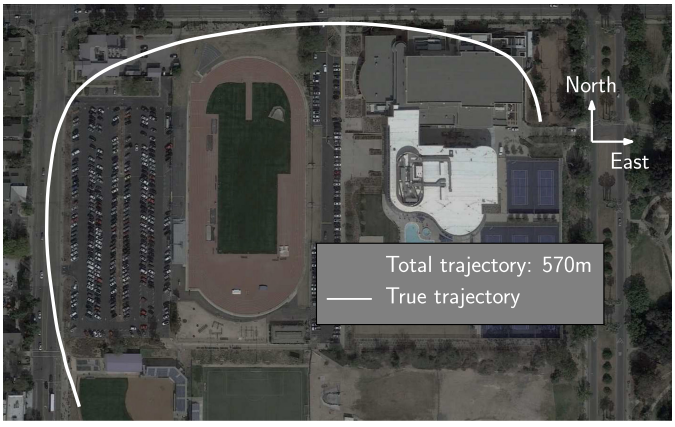

Fig. 14. Trajectory taken by the UAV over the course of the experiment. Map data: Google Earth.

Over the course of the experiment, the receiver was listening to two BTSs, whose position states were mapped prior to the experiment according to the framework discussed in [31]. The distance D between the UAV and the BTS was calculated using the navigation solution produced by the UAV's navigation system and the known BTS position, and the pseudorange ρ was obtained from the proposed cellular CDMA SDR mounted on the UAV over the trajectory shown in Fig. 14.

In order to validate the resulting pseudoranges, the variation of the pseudorange $\Delta\rho \triangleq \rho - \rho(0)$, where $\rho(0)$ is the initial value of the pseudorange, and the variation in distance $\Delta D \triangleq D - D(0)$, where $D(0)$ is the initial distance between the UAV and the BTS are plotted in Fig. 15 for the two BTSs.

It can be seen from Fig. 15 that the variations in the pseudoranges follow closely the variations in distances. The difference between ΔD and $\Delta\rho$ for a particular BTS is due to the variation in the clock bias difference $c\,(\delta t_r - \delta t_{s_i})$ and the noise terms v_i.

2) Ground Vehicle Results: In the second experiment, a car was equipped with the proposed SDR, a consumer-grade 800/1900 MHz cellular antenna, and a surveyor-grade GPS antenna to collect GPS L1 signal and to discipline the on-board oscillator. The cellular and GPS signals were down-mixed and synchronously sampled via a dual-channel USRP driven by a GPSDO. The cellular receiver was tuned to a carrier frequency of 882.75 MHz, which is also a channel allocated for the U.S. cellular provider Verizon Wireless. Samples of the received signals

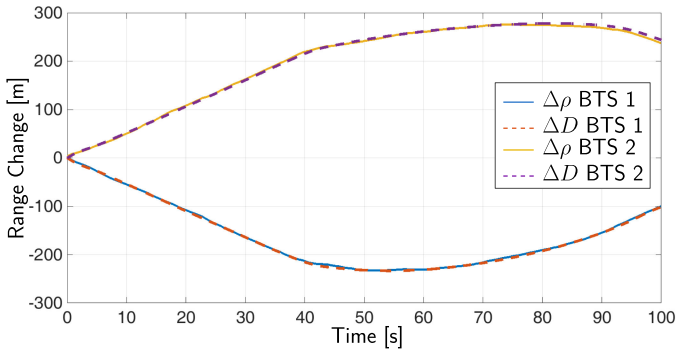

Fig. 15. Variation in pseudoranges and the variation in distances between the receiver and two cellular CDMA BTSs for the UAV experiment.

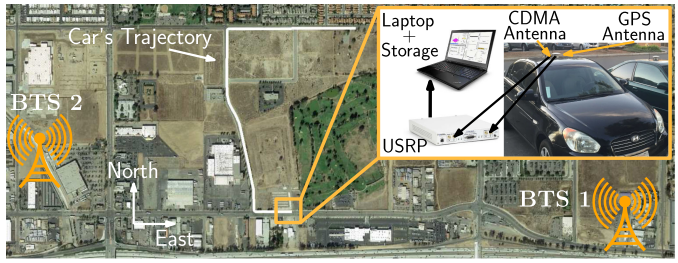

Fig. 16. SOP BTS environment, true trajectory, and experimental hardware setup for the ground vehicle experiment. Map data: Google Earth.

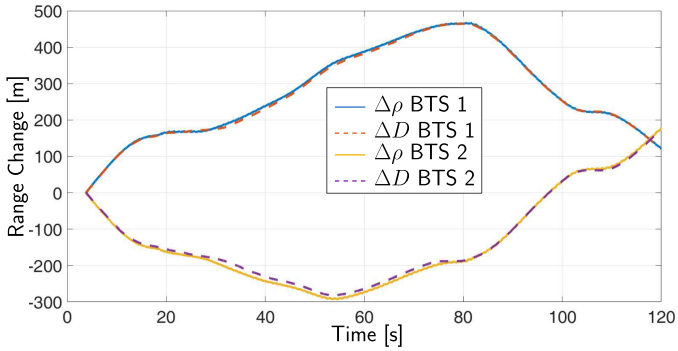

Fig. 17. Variation in pseudoranges and the variation in distances between the receiver and two cellular CDMA BTSs for the ground vehicle experiment.

were stored for off-line post-processing. The cellular CDMA signals were processed by the proposed LabVIEW-based SDR. The GPS signal was processed by the Generalized Radionavigation Interfusion Device (GRID) SDR [50] and the resulting GPS solution was assumed to be the ground-truth reference for the car trajectory. Fig. 16 shows the SOP BTS environment, car trajectory, and the experimental hardware setup.

Over the course of the experiment, the receiver was listening to two BTSs, whose position states were mapped prior to the experiment according to the framework discussed in [31]. The change in the true range and the change in pseudorange are plotted in Fig. 17, similarly to the UAV experiment.

It can be seen from Fig. 17 that the variations in the pseudoranges follow closely the variations in distances. The difference between ΔD and $\Delta\rho$ for a particular BTS is due to the variation in the clock bias difference $c\,(\delta t_r - \delta t_{s_i})$ and the noise terms

TABLE II
TEST DATES, LOCATIONS, AND CARRIER FREQUENCIES

Test	Date	Location	Frequency	Provider
(a)	01/14/2016	1	882.75 MHz	Verizon
(b)	01/20/2016	1	882.75 MHz	Verizon
(c)	08/28/2016	2	883.98 MHz	Verizon
(d)	09/02/2016	2	883.98 MHz	Verizon
(e)	08/28/2016	3	1940.0 MHz	Sprint
(f)	09/02/2016	3	1940.0 MHz	Sprint

Fig. 18. Locations of the cellular CDMA BTSs: Colton, CA; Riverside, CA; and the University of California, Riverside (UCR). Map data: Google Earth.

v_i. The sequel paper will study the navigation performance and estimation of the clock bias in further detail.

B. Clock Bias Discrepancy Model Consistency Analysis

The consistency of the clock bias discrepancy model was analyzed experimentally in different locations, at different times, and for different cellular providers. The results are presented in this section.

1) Cellular CDMA SOP Test Scenarios and Hardware Setup: The tests were performed twice at three different locations. There is a six-day period between each test at each of the three locations. A total of three carrier frequencies were considered, two of them pertaining to Verizon Wireless and one to Sprint. The test scenarios are summarized in Table II and Fig. 18. The date field in Table II shows the date in which the test was conducted in MM/DD/YYYY format.

For the purpose of collecting data, a receiver that was placed close to the border of two sectors for each BTS was equipped with two antennas to acquire and track: (1) GPS signals and (2) signals from the cellular CDMA BTS sector antennas. The CDMA antenna used for the experiments in location 1 was a consumer-grade 800/1900 MHz cellular antenna and a high-gain tri-band cellular antenna for locations 2 and 3. Both GPS antennas were surveyor-grade Leica antennas. The GPS and cellular signals were simultaneously down-mixed and synchronously sampled at 2.5 MS/s via a dual channel USRP driven by a GPSDO. Samples of the received signals were stored for off-line post-processing. The GPS signal was processed by GRID and the cellular CDMA signals were processed by the proposed

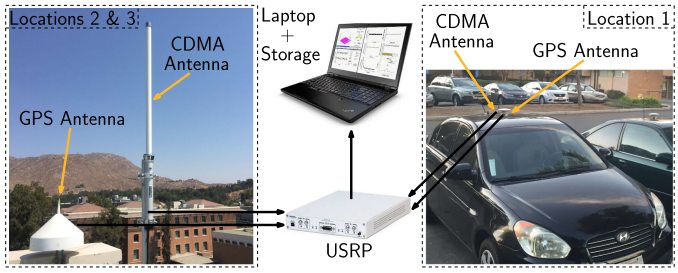

Fig. 19. Experimental hardware setup for each location. Left: hardware setup for locations 2 and 3. Center: data collection equipment. Right: hardware setup for location 1.

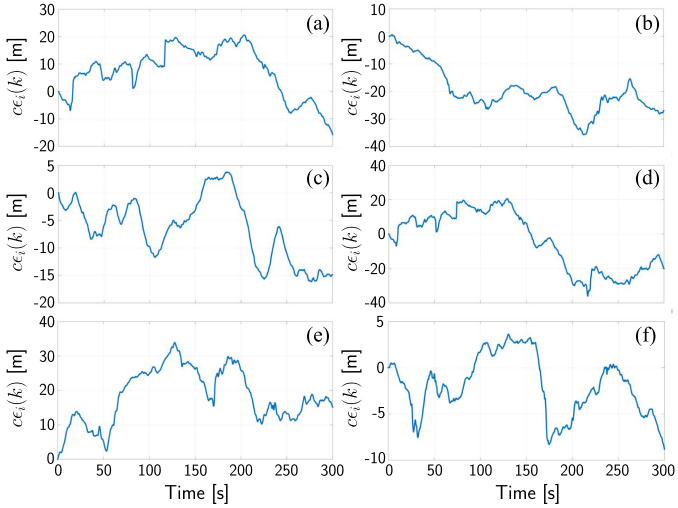

Fig. 20. Six realizations, five minutes each, of the sector clock bias discrepancy for the tests in Table II.

LabVIEW-based SDR. The receiver's clock bias obtained from the GPS solution was used to solve for the BTS sector clock bias. Fig. 19 shows the experimental hardware setup.

2) Analysis of Sector Clock Bias Discrepancy Realizations: Fig. 20 shows six realizations, five minutes each, of the discrepancy corresponding to Tests (a)–(f) in Table II. It can be seen from Fig. 20 that the behavior of the discrepancy is consistent across the tests. The initial discrepancy is subtracted out so that all realizations start at the origin. The inverse of the time constant for each realization was found to be $\{\alpha_i\}_{i=1}^{6} = \{2.08, 1.66, 1.77, 1.70, 1.39, 2.53\} \times 10^{-4}$ Hz.

Next, the process noise driving the discrepancy is characterized. The process noise was calculated according to

$$\zeta_i(k) = \epsilon_i(k+1) - \phi_i \epsilon_i(k),$$

where $\phi_i = e^{-\alpha_i T}$ and $T = 0.2$ s. The acf of each of the six realizations of ζ_i corresponding to the six realizations of ϵ_i from Fig. 20 are shown in Fig. 21. Similarly to Fig. 9(a), the shape of the acfs in Fig. 21 exhibits very quick de-correlation, validating that ζ_i is approximately a white sequence.

Fig. 22 shows a histogram of each realization of ζ_i along with the estimated pdf $p(\zeta_i)$. The pdfs were obtained by estimating the μ_i and λ_i parameters associated with the Laplace pdf (18). It can be seen that the Laplace pdf consistently matched the experimental data.

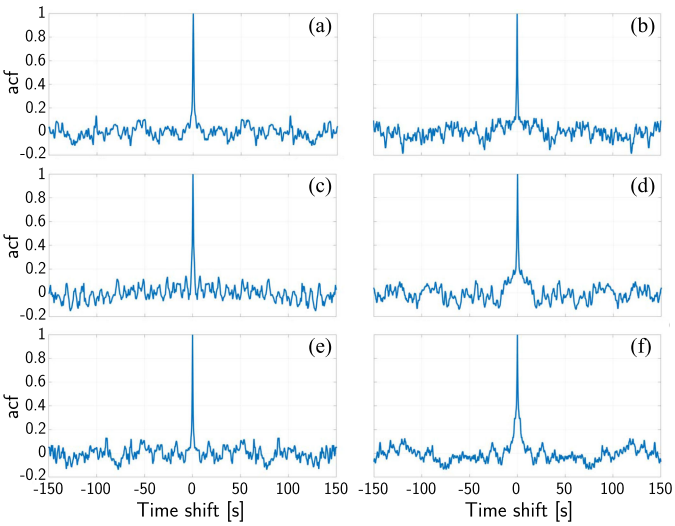

Fig. 21. The acf of the six realizations of the process noise ζ_i corresponding to the discrepancies in Fig. 20.

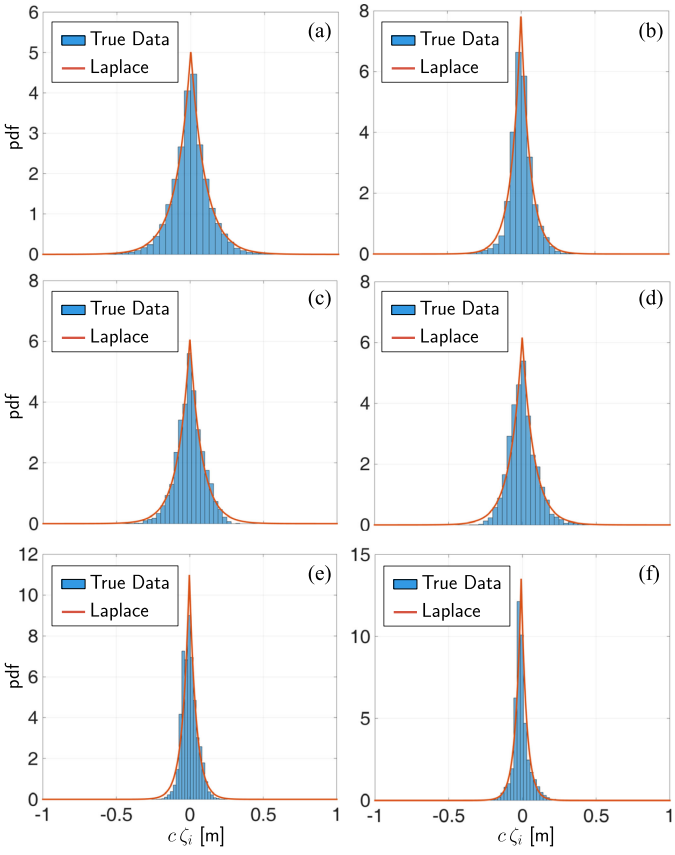

Fig. 22. A histogram of each realization of the process noise along with the estimated Laplace distribution.

VII. 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 description of the acquisition and tracking stages of a LabVIEW-based SDR was presented. The statistics of the pseudorange error of the proposed SDR in an additive white Gaussian channel were derived. Furthermore, the discrepancy between the clock biases observed by a receiver in two different sectors of the BTS cell was analyzed and modeled as a stochastic dynamic sequence. The consistency of the obtained model was experimentally analyzed in different locations, at different times, and for different cellular providers. Finally, experimental results validating the pseudoranges produced by the proposed SDR were presented, in which the SDR's pseudoranges followed closely the true range between mobile UAV-mounted and car-mounted receivers and two cellular BTSs.

Acknowledgment

The authors would like to thank S. Ragothaman and L. Yang for their help in data collection.

References

[1] S. Saab and Z. Kassas, "Power matching approach for GPS coverage extension," *IEEE Trans. Intell. Transp. Syst.*, vol. 7, no. 2, pp. 156–166, Jun. 2006.
[2] F. Caron, M. Davy, E. Duflos, and P. Vanheeghe, "Particle filtering for multisensor data fusion with switching observation models: Application to land vehicle positioning," *IEEE Trans. Signal Process.*, vol. 55, no. 6, pp. 2703–2719, Jun. 2007.
[3] G. Seco-Granados, J. Lopez-Salcedo, D. Jimenez-Banos, and G. Lopez-Risueno, "Challenges in indoor global navigation satellite systems: Unveiling its core features in signal processing," *IEEE Signal Process. Mag.*, vol. 29, no. 2, pp. 108–131, Mar. 2012.
[4] Y. Wu, J. Wang, and D. Hu, "A new technique for INS/GNSS attitude and parameter estimation using online optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 10, pp. 2642–2655, May 2014.
[5] J. Raquet and R. Martin, "Non-GNSS radio frequency navigation," in *Proc. IEEE Acoust., Speech, Signal Process. Conf.*, Mar. 2008, pp. 5308–5311.
[6] L. Merry, R. Faragher, and S. Schedin, "Comparison of opportunistic signals for localisation," in *Proc. IFAC Symp. Intell. Auton. Veh.*, Sep. 2010, pp. 109–114.
[7] Z. Kassas, "Collaborative opportunistic navigation," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 28, no. 1, pp. 38–41, Jun. 2013.
[8] Z. Kassas, "Analysis and synthesis of collaborative opportunistic navigation systems," Ph.D. dissertation, Univ. Texas at Austin, Austin, TX, USA, 2014.
[9] J. McEllroy, "Navigation using signals of opportunity in the AM transmission band," Master's thesis, Air Force Inst. Technol., Wright-Patterson Air Force Base, OH, USA, 2006.
[10] 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 Trans. Broadcast.*, vol. 55, no. 3, pp. 577–588, Sep. 2009.
[11] M. Joerger, L. Gratton, B. Pervan, and C. Cohen, "Analysis of iridium-augmented GPS for floating carrier phase positioning," *Navigation*, vol. 57, pp. 137–160, 2010.
[12] K. Pesyna, Z. Kassas, and T. Humphreys, "Constructing a continuous phase time history from TDMA signals for opportunistic navigation," in *Proc. IEEE/ION Position Location Navig. Symp.*, Apr. 2012, pp. 1209–1220.
[13] M. Rabinowitz and J. Spilker Jr., "A new positioning system using television synchronization signals," *IEEE Trans. Broadcast.*, vol. 51, no. 1, pp. 51–61, Mar. 2005.
[14] P. Thevenon *et al.*, "Positioning using mobile TV based on the DVB-SH standard," *Navigation*, vol. 58, pp. 71–90, 2011.
[15] R. Martin, C. Yan, H. Fan, and C. Rondeau, "Algorithms and bounds for distributed TDOA-based positioning using OFDM signals," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1255–1268, Mar. 2011.
[16] I. Bilik, K. Adhikari, and J. R. Buck, "Shannon capacity bound on mobile station localization accuracy in urban environments," *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 6206–6216, 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] J. Khalife, K. Shamaei, and Z. Kassas, "A software-defined receiver architecture for cellular CDMA-based navigation," in *Proc. IEEE/ION Position, Location, Navig. Symp.*, Apr. 2016, pp. 816–826.
[19] K. Shamaei, J. Khalife, and Z. Kassas, "Performance characterization of positioning in LTE systems," in *Proc. Int. Tech. Meeting Satell. Division Inst. Navig. Conf.*, Sep. 2016, pp. 2262–2270.
[20] R. Faragher, C. Sarno, and M. Newman, "Opportunistic radio SLAM for indoor navigation using smartphone sensors," in *Proc. IEEE/ION Position, Location, Navig. Symp.*, Apr. 2012, pp. 120–128.
[21] J. Prieto, S. Mazuelas, A. Bahillo, P. Fernandez, R. Lorenzo, and E. Abril, "Adaptive data fusion for wireless localization in harsh environments," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1585–1596, Apr. 2012.
[22] 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 *Proc. Int. Tech. Meeting Satell. Division Inst. Navig. Conf.*, Sep. 2015, pp. 2291–2300.
[23] K. Pesyna, Z. Kassas, J. Bhatti, and T. Humphreys, "Tightly-coupled opportunistic navigation for deep urban and indoor positioning," in *Proc. Int. Tech. Meeting Satell. Division Inst. Navig. Conf.*, Sep. 2011, pp. 3605–3617.
[24] 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 *Proc. IEEE Global Telecommun. Conf. Workshops*, Dec. 2011, pp. 242–247.
[25] Z. Kassas and T. Humphreys, "Observability and estimability of collaborative opportunistic navigation with pseudorange measurements," in *Proc. Int. Tech. Meeting Satell. Division Inst. Navig. Conf.*, Sep. 2012, pp. 621–630.
[26] Z. Kassas and T. Humphreys, "Observability analysis of collaborative opportunistic navigation with pseudorange measurements," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 260–273, Feb. 2014.
[27] Z. Kassas and T. Humphreys, "Motion planning for optimal information gathering in opportunistic navigation systems," in *Proc. AIAA Guid., Navig., Control Conf.*, Aug. 2013, pp. 551–4565.
[28] Z. Kassas and T. Humphreys, "Receding horizon trajectory optimization in opportunistic navigation environments," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 51, no. 2, pp. 866–877, Apr. 2015.
[29] Z. Kassas, A. Arapostathis, and T. 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.
[30] Z. Kassas and T. Humphreys, "The price of anarchy in active signal landscape map building," in *Proc. IEEE Global Conf. Signal Inf. Process.*, Dec. 2013, pp. 165–168.
[31] J. Morales and Z. Kassas, "Optimal collaborative mapping of terrestrial transmitters: Receiver placement and performance characterization," *IEEE Trans. Aerosp. Electron. Syst.*, to be published.
[32] W. Lee, "Overview of cellular CDMA," *IEEE Trans. Veh. Technol.*, vol. 40, no. 2, pp. 291–302, May 1991.
[33] T. Humphreys, M. Psiaki, P. Kintner, and B. Ledvina, "GNSS receiver implementation on a DSP: Status, challenges, and prospects," in *Proc. Int. Tech. Meeting Satell. Division Inst. Navig. Conf.*, Sep. 2006, pp. 1567–1575.
[34] Z. Kassas, J. Bhatti, and T. Humphreys, "A graphical approach to GPS software-defined receiver implementation," in *Proc. IEEE Global Conf. Signal Inf. Process.*, Dec. 2013, pp. 1226–1229.
[35] E. Kaplan and C. Hegarty, *Understanding GPS: Principles and Applications*, 2nd ed. Norwood, MA, USA: Artech House, 2005.
[36] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed. Lincoln, MA, USA: Ganga-Jamuna Press, 2010.
[37] J. Khalife and Z. Kassas, "Modeling and analysis of sector clock bias mismatch for navigation with cellular signals," in *Proc. Amer. Control Conf.*, May 2017, pp. 3573–3578.
[38] 3GPP2, "Physical layer standard for CDMA2000 spread spectrum systems (C.S0002-E)," 3rd Generation Partnership Project 2 (3GPP2), TS C.S0002-E, Jun. 2011.
[39] J. Lee and L. Miller, *CDMA Systems Engineering Handbook*, 1st ed. Norwood, MA, USA: Artech House, 1998.
[40] R. Vaughn, N. Scott, and D. White, "The theory of bandpass sampling," *IEEE Trans. Signal Process.*, vol. 39, no. 9, pp. 1973–1984, Sep. 1991.
[41] 3GPP2, "Upper layer (layer 3) signaling standard for cdma2000 spread spectrum systems," 3rd Generation Partnership Project 2 (3GPP2), TS C.S0005-F v2.0, May 2014.
[42] 3GPP2, "Medium access control (MAC) standard for cdma2000 spread spectrum systems," 3rd Generation Partnership Project 2 (3GPP2), TS C.S0003-F v2.0, May 2014.
[43] D. van Nee and A. Coenen, "New fast GPS code-acquisition technique using FFT," *Electron. Lett.*, vol. 27, pp. 158–160, Jan. 1991.
[44] A. van Dierendonck, P. Fenton, and T. Ford, "Theory and performance of narrow correlator spacing in a GPS receiver," *Navigation*, vol. 39, pp. 265–283, Sep. 1992.
[45] J. Khalife and Z. Kassas, "Characterization of sector clock biases in cellular CDMA systems," in *Proc. Int. Tech. Meeting Satell. Division Inst. Navig. Conf.*, Sep. 2016, pp. 2281–2285.
[46] 3GPP2, "Recommended minimum performance standards for cdma2000 spread spectrum base stations," 3rd Generation Partnership Project 2 (3GPP2), TS C.S0010-E, Mar. 2014. [Online]. Available: http://www.arib.or.jp/english/html/overview/doc/STD-T64v7_00/Specification/ARIB_STD-T64-C.S0010-Ev2.0.pdf
[47] L. Ljung, *System identification: Theory for the user*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 1999.
[48] J. Proakis and D. Manolakis, *Digital signal processing*. Upper Saddle River, NJ, USA: Prentice-Hall, 1996.
[49] R. Norton, "The double exponential distribution: Using calculus to find a maximum likelihood estimator," *Amer. Statistician*, vol. 38, pp. 135–136, May 1984.
[50] T. Humphreys, J. Bhatti, T. Pany, B. Ledvina, and B. O'Hanlon, "Exploiting multicore technology in software-defined GNSS receivers," in *Proc. Int. Tech. Meeting Satell. Division Inst. Navig. Conf.*, Sep. 2009, pp. 326–338.

Joe Khalife (S'15) received the B.S. (with Distinction) degree in electrical engineering and the M.S. degree in computer engineering from the Lebanese American University, Byblos, Lebanon. He is currently working toward the Ph.D. degree in electrical and computer engineering at The University of California, Riverside, Riverside, CA, USA. He is a member of the Autonomous Systems Perception, Intelligence, and Navigation Laboratory. His research interests include estimation, navigation, software-defined receiver design, autonomous vehicles, and intelligent transportation systems.

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.

Zaher M. Kassas (S'98–M'08–SM'11) is an assistant professor at the University of California, Riverside and director of the ASPIN Laboratory. He received a B.E. with Honors in Electrical Engineering from the Lebanese American University, an M.S. in Electrical and Computer Engineering from The Ohio State University, and an M.S.E. in Aerospace Engineering and a Ph.D. in Electrical and Computer Engineering from The University of Texas at Austin. From 2004 through 2010 he was a research and development engineer with the LabVIEW Control Design and Dynamical Systems Simulation Group at National Instruments Corp. His research interests include cyber-physical systems, estimation theory, navigation systems, autonomous vehicles, and intelligent transportation systems.