Navigation with Cellular Signals of Opportunity

Zaher M. Kassas

Preprint of Chapter to Appear in J. Morton, F. van Diggelen, J. Spilker, Jr., & B. Parkinson (Eds.),
Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications, Volume 2, Wiley–IEEE, 2021

Table of Contents

1 Introduction

Among the different types of signals of opportunity, cellular signals are particularly attractive for positioning, navigation, and timing (PNT) due to their inherently attractive characteristics:

Abundance Cellular base transceiver stations (BTSs) are plentiful due to the ubiquity of cellular and smart phones and tablets. The number of BTSs is bound to increase dramatically with the introduction of small cells to support fifth generation (5G) wireless systems.

Geometric diversity The cell configuration by construction yields favorable BTS geometry, unlike certain terrestrial transmitters, which tend to be colocated (e.g., digital television). Such geometric diversity yields low geometric dilution of precision (GDOP) factors, which results in a precise PNT solution.

High carrier frequency Current cellular carrier frequency ranges between 800 MHz and 1900 MHz, which yields precise carrier phase navigation observables. Future 5G networks will tap into frequencies between 30 and 300 GHz.

Large bandwidth Cellular signals have a large bandwidth, which yields accurate time-of-arrival (TOA) estimation (e.g., the bandwidth of certain cellular long-term evolution (LTE) reference signals is up to 20 MHz).

High transmitted power Cellular signals are often available and usable in environments where global navigation satellite system (GNSS) signals are challenged (e.g., indoors and in deep urban canyons). The received carrier-to-noise ratio C/N_0 from nearby cellular BTSs is more than 20 dB-Hz than that received from GPS space vehicles (SVs).

Free to use There is no deployment cost associated with using cellular signals for PNT– the signals are practically free to use. Specifically, the user equipment (UE) could "eavesdrop" on the transmitted cellular signals without communicating with the BTS, extract necessary PNT information from received signals, and calculate the navigation solution locally. While other navigation approaches requiring two-way communication between the UE and BTS (i.e., network-based) exist, this chapter focuses on explaining how UE-based navigation could be achieved.

Regardless whether GNSS signals are available or not, cellular signals of opportunity could be used to produce or improve the navigation solution. In the absence of GNSS signals, cellular signals could be used to produce a navigation solution in a standalone fashion or to aid the inertial navigation system (INS) [1–6]. When GNSS signals are available, cellular signals could be fused with GNSS signals, yielding a superior navigation solution to a standalone GNSS solution, particularly in the vertical direction [7, 8].

Cellular signals are not intended for PNT. Therefore, to use these signals for such purpose, several challenges must be addressed. This has been the subject of extensive research over the past few years. These challenges and potential remedies are summarized next.

- Cellular signals are modulated and subsequently transmitted for non-PNT purposes. These signals are much more complicated than GNSS signals and extracting relevant PNT information from them is not straightforward. Recent research has focused on deriving

appropriate low-level models to optimally extract states and parameters of interest for PNT from received cellular signals. The effect of different propagation channels on such signals is an ongoing area of research [9–15].

- GNSS receivers are commercially available and there is a rich body of literature on GNSS receiver design. This is not the case for cellular navigation receivers. The recent literature has published specialized receiver designs for producing navigation observables from received cellular signals (e.g., code phase, carrier phase, and Doppler frequency) [16–19].

- GNSS SVs are equipped with atomic oscillators and are tightly synchronized. However, cellular towers are equipped with less stable oscillators, typically oven-controlled crystal oscillators (OCXOs), and are less tightly synchronized. This is because communication synchronization requirements are less stringent than PNT synchronization requirements. Timing errors arising due to this somewhat loose synchronization could introduce tens of meters of localization error. Researchers have been modeling such errors and synthesizing PNT estimators that compensate for them [20–25].

- GNSS SVs transmit all necessary states and parameters to the receiver in the navigation message (e.g., SV position, clock bias, ionospheric model parameters, etc.). In contrast, cellular BTSs do not transmit such information. Therefore, navigation frameworks must be developed to estimate the states and parameters of cellular BTSs (position, clock bias, clock drift, frequency stability, etc.), which are not necessarily known *a priori*. Several navigation frameworks have been proposed. One such framework is to have a dedicated station that acts as a mapper, which knows its states (from GNSS signals, for instance), is estimating the unknown states of cellular BTSs, and is sharing such estimates with navigating receivers. Another framework is to simultaneously estimate the states of the receiver and cellular BTSs in a radio simultaneous localization and mapping (radio SLAM) manner [26–29].

This chapter discusses how cellular signals could be used for PNT by presenting relevant signal models, receiver architectures, PNT sources of error and corresponding models, navigation frameworks, and experimental results. The remainder of this chapter is organized as follows. Section 2 gives a brief overview of the evolution of cellular systems. Section 3 discusses modeling the clock error dynamics to facilitate estimating the unknown BTSs' clock error states. Section 4 describes two frameworks for navigation in cellular environments. Sections 5 and 6 discuss how to navigate with cellular code-division multiple access (CDMA) and LTE signals, respectively. Section 7 discusses a timing error that arises in cellular networks: clock bias discrepancy between different sectors of a BTS cell. Section 8 highlights the achieved navigation solution improvement upon fusing cellular signals with GNSS signals. Section 9 describes how cellular signals could be used to aid an INS.

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

2 Overview of Cellular Systems

Cellular systems have evolved significantly since the first handheld mobile phone was demonstrated by John F. Mitchell and Martin Cooper of Motorola in 1973. The first commercially automated cellular network was launched in Japan by Nippon Telegraph and Telephone (NTT) in 1979. This first generation (1G) was analog and used frequency-division multiple access (FDMA). The second generation (2G) transitioned to digital and mostly used time-division multiple access (TDMA), which later evolved into 2.5G: General Packet Radio Service (GPRS) and 2.75G: Enhanced Data Rates for GSM Evolution (EDGE). The third generation (3G) upgraded 2G networks for faster internet speed and used CDMA. The fourth generation (4G), commonly referred to as LTE, was introduced to allow for even faster data rates. LTE used orthogonal frequency-division multiple access (OFDMA) and featured multiple-input multiple-output (MIMO), i.e., antenna arrays. Figure 1 summarizes the existing cellular generations and their corresponding predominant modulation schemes.

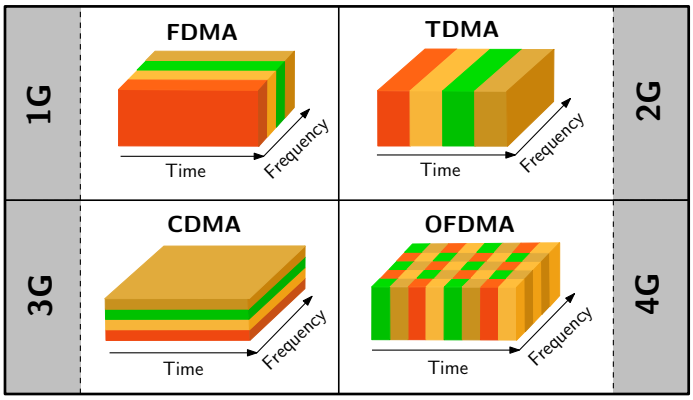


Figure 1: Cellular systems generations

This chapter focuses on using cellular CDMA and LTE signals for PNT. Table 1 compares the main characteristics of 1) GPS coarse/acquisition (C/A) code, 2) CDMA pilot signal, and 3) three LTE reference signals: primary synchronization signal (PSS), secondary synchronization signal (SSS), and cell-specific reference signal (CRS).

Table 1: GPS versus cellular CDMA and LTE comparison

Standard	Signal	Possible number of sequences	Bandwidth (MHz)	Code period (ms)	Expected ranging precision (m)*
GPS	**C/A code**	63	1.023	1	2.93
CDMA	**Pilot**	512	1.2288	26.67	2.44
LTE	**PSS**	3	0.93	10	3.22
	SSS	168	0.93	10	3.22
	CRS	504	up to 20	0.067	0.15

* 1% of chip width

In 2012, the International Telecommunication Union Radiocommunication (ITU-R) sector started a program to develop an international mobile telecommunication (IMT) system for 2020 and beyond. This program set the stage for 5G research activities. The main goals of 5G compared to 4G include: 1) higher density of mobile users; 2) supporting device-to-device, ultra reliable, and massive machine communications; 3) lower latency; and 4) lower battery consumption. To achieve these goals, millimeter wave bands were added to the current frequency bands for data transmission. Other salient features of 5G include millimeter waves, small cells, massive MIMO, beamforming, and full duplex [30, 31].

3 Clock Error Dynamics Modeling

GNSS SVs are equipped with atomic clocks, are synchronized, and their clock errors are transmitted in the navigation message along with the SVs' positions. In contrast, cellular BTSs are equipped with less stable oscillators (typically OCXOs), are roughly synchronized to GNSS, and their clock error states (bias and drift) and positions are typically unknown. As such, the cellular BTSs' clock errors and positions must be estimated. Therefore, it is important to model the clock error state dynamics. To this end, a typical model for the dynamics of the clock error states is the so-called two-state model, composed of the clock bias δt and clock drift $\dot{\delta t}$, as depicted in Figure 2.

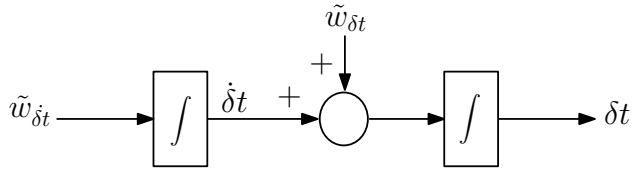


Figure 2: Clock error states dynamics model

The clock error states evolve according to

$$\dot{\boldsymbol{x}}_{\text{clk}}(t) = \mathbf{A}_{\text{clk}}\, \boldsymbol{x}_{\text{clk}}(t) + \tilde{\boldsymbol{w}}_{\text{clk}}(t),$$

$$\boldsymbol{x}_{\text{clk}} = \begin{bmatrix} \delta t \\ \dot{\delta t} \end{bmatrix}, \quad \tilde{\boldsymbol{w}}_{\text{clk}} = \begin{bmatrix} \tilde{w}_{\delta t} \\ \tilde{w}_{\dot{\delta}t} \end{bmatrix}, \quad \mathbf{A}_{\text{clk}} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \tag{1}$$

where the elements of $\tilde{\boldsymbol{w}}_{\text{clk}}$ are modeled as zero-mean, mutually independent white noise processes and the power spectral density of $\tilde{\boldsymbol{w}}_{\text{clk}}$ is given by $\tilde{\mathbf{Q}}_{\text{clk}} = \text{diag}\left[S_{\tilde{w}_{\delta t}}, S_{\tilde{w}_{\dot{\delta}t}}\right]$. The power spectra $S_{\tilde{w}_{\delta t}}$ and $S_{\tilde{w}_{\dot{\delta}t}}$ can be related to the power-law coefficients $\{h_\alpha\}_{\alpha=-2}^{2}$, which have been shown through laboratory experiments to be adequate to characterize the power spectral density of the fractional frequency deviation $y(t)$ of an oscillator from nominal frequency, which takes the form $S_y(f) = \sum_{\alpha=-2}^{2} h_\alpha f^\alpha$ [32, 33]. It is common to approximate the clock error dynamics by considering only the frequency random walk coefficient h_{-2} and the white frequency coefficient h_0, which lead to $S_{\tilde{w}_{\delta t}} \approx \frac{h_0}{2}$ and $S_{\tilde{w}_{\dot{\delta}t}} \approx 2\pi^2 h_{-2}$ [34, 35]. Typical OCXO values for h_0 and h_{-2} are given in Table 2.

Table 2: Typical h_0 and h_{-2} values for different OCXO oscillators [36]

h_0	h_{-2}
2.6×10^{-22}	4.0×10^{-26}
8.0×10^{-20}	4.0×10^{-23}
3.4×10^{-22}	1.3×10^{-24}

Discretizing the dynamics (1) at a sampling interval T yields the discrete-time-equivalent model

$$\boldsymbol{x}_{\text{clk}}\left(k+1\right) = \mathbf{F}_{\text{clk}}\, \boldsymbol{x}_{\text{clk}}(k) + \boldsymbol{w}_{\text{clk}}(k),$$

where $\boldsymbol{w}_{\text{clk}}$ is a discrete-time zero-mean white noise sequence with covariance $\mathbf{Q}_{\text{clk}}$, and

$$\mathbf{F}_{\text{clk}} = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}, \quad \mathbf{Q}_{\text{clk}} = \begin{bmatrix} S_{\tilde{w}_{\delta t}} T + S_{\tilde{w}_{\dot{\delta} t}} \frac{T^3}{3} & S_{\tilde{w}_{\dot{\delta} t}} \frac{T^2}{2} \\ S_{\tilde{w}_{\dot{\delta} t}} \frac{T^2}{2} & S_{\tilde{w}_{\dot{\delta} t}} T \end{bmatrix}. \tag{2}$$

4 Navigation Frameworks in Cellular Environments

BTS positions can be readily obtained via several methods, e.g., 1) from cellular BTS databases (if available) or 2) by deploying multiple mapping receivers with knowledge of their own states, estimating the position states of the BTSs for a sufficiently long period of time [37–39]. These estimates are physically verifiable via surveying or satellite images. Unlike BTS positions, which are static, the clock error states are stochastic and dynamic, as discussed in Section 3, and are difficult to verify.

Estimating the BTSs' states can be achieved via two frameworks:

Mapper/Navigator This framework comprises: 1) Receiver(s) with knowledge of their own states, referred to as mapper(s), making measurements on ambient BTSs (e.g., pseudorange and carrier phase). The mappers' role is to estimate the cellular BTSs' states. 2) A receiver with no knowledge of its own states, referred to as the navigator, making measurements on the same ambient BTSs to estimate its own states, while receiving estimates of the BTSs' states from the mappers.

Radio SLAM In this framework, the receiver maps the BTSs simultaneously with localizing itself in the radio environment.

To make the estimation problems associated with the above frameworks observable, certain *a priori* knowledge about the BTSs' or receiver's states must be satisfied [27, 40–42]. 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 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 $\boldsymbol{r}_r = \left[x_r, y_r\right]^{\mathsf{T}}$ is the position vector of the receiver, 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 $\boldsymbol{r}_{s_i} = \left[x_{s_i}, y_{s_i}\right]^{\mathsf{T}}$ is the position

vector of the ith BTS and δt_{s_i} is its clock bias. The pseudorange measurement to the ith BTS, ρ_i, can be expressed as

$$\rho_i = h_i(\boldsymbol{x}_r, \boldsymbol{x}_{s_i}) + v_i, \tag{3}$$

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 measurement noise, which is modeled as a zero-mean Gaussian random variable with variance σ_i^2 [27]. The following subsections outline the calculations associated with each navigation framework assuming pseudorange measurements from cellular towers. Frameworks with carrier phase measurements are discussed in [43].

4.1 Mapper/Navigator Framework

Assuming that the receiver is drawing pseudoranges from $N \geq 3$ BTSs with *known* states, the receiver's state can be estimated from (3) by solving a weighted nonlinear least-squares (WNLS) problem. However, in practice, the BTSs' states are *unknown*, in which case the mapper/navigator framework can be employed [18, 25].

Consider a mapper with knowledge of its own state vector (by having access to GNSS signals, for example) to be present in the navigator's environment as depicted in Figure 3.

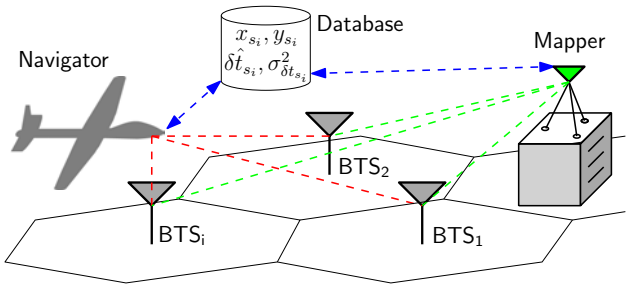


Figure 3: Mapper and navigator in a cellular environment

The mapper's objective is to estimate the BTSs' position and clock bias states and share these estimates with the navigator through a central database. For simplicity, assume the position states of the BTSs to be known and stored in a database. In the sequel, it is assumed that the mapper is producing an estimate $\delta\hat{t}_{s_i}$ and an associated estimation error variance $\sigma^2_{\delta t_{s_i}}$ for each of the ith BTSs.

Consider M mappers and N BTSs. Denote the state vector of the jth mapper by $\boldsymbol{x}_{r_j}$, the pseudorange measurement by the jth mapper 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 mappers on the ith BTS as

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

where $\mathbf{1}_M \triangleq [1,\ldots,1]^{\mathsf{T}}$ and $\boldsymbol{v}_i \triangleq -\left[v_i^{(1)},\ldots,v_i^{(M)}\right]^{\mathsf{T}}$. The clock bias δt_{s_i} is estimated by solving a weighted least-squares (WLS) problem, resulting in the estimate

$$\hat{\delta t}_{s_i} = \frac{1}{c}\left(\mathbf{1}_M^{\mathsf{T}}\mathbf{W}\mathbf{1}_M\right)^{-1}\mathbf{1}_M^{\mathsf{T}}\mathbf{W}\boldsymbol{z}, \quad \mathbf{W} = \operatorname{diag}\left[\frac{1}{{\sigma_i^{(1)}}^2},\ldots,\frac{1}{{\sigma_i^{(M)}}^2}\right]$$

and associated estimation error variance $\sigma^2_{\delta t_{s_i}} = \frac{1}{c^2}\left(\mathbf{1}_M^{\mathsf{T}}\mathbf{W}\mathbf{1}_M\right)^{-1}$, where $\mathbf{W}$ 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 $\sigma^2_{\delta t_{s_i}}$.

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 $\mathbf{C} = c^2 \cdot \operatorname{diag}\left[\sigma^2_{\delta t_{s_1}},\ldots,\sigma^2_{\delta t_{s_N}}\right]$ is the covariance matrix of $\boldsymbol{w} \triangleq [w_1,\ldots,w_N]^{\mathsf{T}}$ and $\mathbf{R} = \operatorname{diag}[\sigma_1^2,\ldots,\sigma_N^2]$ is the covariance of the measurement noise vector $\boldsymbol{v} = [v_1,\ldots,v_N]^{\mathsf{T}}$. The Jacobian matrix $\mathbf{H}$ of the nonlinear measurements $\boldsymbol{h} \triangleq [h_1(\boldsymbol{x}_r, \hat{\boldsymbol{x}}_{s_1}),\ldots,h_N(\boldsymbol{x}_r, \hat{\boldsymbol{x}}_{s_N})]^{\mathsf{T}}$ with respect to $\boldsymbol{x}_r$ is given by $\mathbf{H} = [\mathbf{G} \quad \mathbf{1}_N]$, where

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

The navigating receiver's state can now be estimated by solving a WNLS problem. The WNLS equations are given by

$$\begin{aligned} {\hat{\boldsymbol{x}}_r}^{(l+1)} &= {\hat{\boldsymbol{x}}_r}^{(l)} + \left(\mathbf{H}^{\mathsf{T}}\mathbf{R}^{-1}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathsf{T}}\mathbf{R}^{-1}\left(\boldsymbol{\rho} - \hat{\boldsymbol{\rho}}^{(l)}\right) \\ \mathbf{P}^{(l)} &= \left(\mathbf{H}^{\mathsf{T}}\mathbf{R}^{-1}\mathbf{H}\right)^{-1}, \end{aligned}$$

where l is the iteration number and $\hat{\boldsymbol{\rho}}^{(l)}$ denotes the nonlinear measurements $\boldsymbol{h}$ evaluated at the current estimate ${\hat{\boldsymbol{x}}_r}^{(l)}$.

4.2 Radio SLAM Framework

A dynamic estimator, such as an extended Kalman filter (EKF), can be used in the radio SLAM framework for standalone receiver navigation (i.e., without a mapper). Certain *a priori* knowledge about the BTSs' and/or receiver's states must be satisfied to make the radio SLAM estimation problem observable [27, 40–42].

To demonstrate a particular formulation of the radio SLAM framework, consider the simple case where the BTSs' positions are known. Also, assume the receiver's *initial* state vector to be known (e.g., from a GNSS navigation solution). Using the pseudoranges (3), the EKF will estimate the state vector composed of the receiver's position $\boldsymbol{r}_r$ and velocity $\dot{\boldsymbol{r}}_r$ as well as the difference between the receiver's clock bias and each BTS and the difference between the receiver's clock drift and each BTS, specifically

$$\boldsymbol{x} = \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}, \boldsymbol{x}_{\text{clk}_1}^{\mathsf{T}}, \ldots, \boldsymbol{x}_{\text{clk}_N}^{\mathsf{T}}\right]^{\mathsf{T}},$$

where $\boldsymbol{x}_{\text{clk}_i} \triangleq [(\delta t_r - \delta t_{s_i}), (\delta \dot{t}_r - \delta \dot{t}_{s_i})]^{\mathsf{T}}$; δt_r and δt_{s_i} are the receiver's and ith BTS clock bias, respectively; and $\delta \dot{t}_r$ and $\delta \dot{t}_{s_i}$ are the receiver's and ith BTS clock drift, respectively.

Assuming the receiver to be moving with velocity random walk dynamics, the system's dynamics after discretization at a uniform sampling period T can be modeled as

$$\boldsymbol{x}(k+1) = \mathbf{F}\,\boldsymbol{x}(k) + \boldsymbol{w}(k), \tag{4}$$

$$\begin{aligned}
\mathbf{F} &= \begin{bmatrix} \mathbf{F}_{\text{pv}} & \mathbf{0}_{4\times 2N} \\ \mathbf{0}_{2N\times 4} & \mathbf{F}_{\text{clk}} \end{bmatrix}, \qquad & \mathbf{F}_{\text{clk}_i} &= \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}, \\
\mathbf{F}_{\text{clk}} &= \text{diag}\left[\mathbf{F}_{\text{clk}_1}, \ldots, \mathbf{F}_{\text{clk}_N}\right], \qquad & \mathbf{F}_{\text{pv}} &= \begin{bmatrix} \mathbf{I}_{2\times 2} & T\,\mathbf{I}_{2\times 2} \\ \mathbf{0}_{2\times 2} & \mathbf{I}_{2\times 2} \end{bmatrix},
\end{aligned}$$

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

$$\mathbf{Q}_{\text{pv}} = \begin{bmatrix} \tilde{q}_x\frac{T^3}{3} & 0 & \tilde{q}_x\frac{T^2}{2} & 0 \\ 0 & \tilde{q}_y\frac{T^3}{3} & 0 & \tilde{q}_y\frac{T^2}{2} \\ \tilde{q}_x\frac{T^2}{2} & 0 & \tilde{q}_x T & 0 \\ 0 & \tilde{q}_y\frac{T^2}{2} & 0 & \tilde{q}_y T \end{bmatrix}, \quad \mathbf{Q}_{\text{clk}} = \begin{bmatrix} \mathbf{Q}_{\text{clk}_r} + \mathbf{Q}_{\text{clk}_{s_1}} & \mathbf{Q}_{\text{clk}_r} & \cdots & \mathbf{Q}_{\text{clk}_r} \\ \mathbf{Q}_{\text{clk}_r} & \mathbf{Q}_{\text{clk}_r} + \mathbf{Q}_{\text{clk}_{s_2}} & \cdots & \mathbf{Q}_{\text{clk}_r} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{Q}_{\text{clk}_r} & \mathbf{Q}_{\text{clk}_r} & \cdots & \mathbf{Q}_{\text{clk}_r} + \mathbf{Q}_{\text{clk}_{s_N}} \end{bmatrix},$$

where $\mathbf{Q}_{\text{clk}_r}$ and $\mathbf{Q}_{\text{clk}_{s_i}}$ correspond to the receiver's and ith BTS clock process noise covariances, respectively, specified in (2). Formulations of other more sophisticated radio SLAM scenarios are discussed in [27, 29, 41]

Note that in many practical situations, the receiver is coupled with an inertial measurement unit (IMU), which can be used instead of the statistical model to propagate the estimator's state between measurement updates from BTSs [44, 45]. This is discussed in more details in Section 9.

5 Navigation with Cellular CDMA Signals

To establish and maintain a connection between cellular CDMA BTSs and the UE, each BTS broadcasts comprehensive timing and identification information. Such information could be

utilized for PNT. The sequences transmitted on the forward link channel, i.e., from BTS to UE, are known. Therefore, by correlating the received cellular CDMA signal with a locally-generated sequence, the receiver can estimate the TOA and produce a pseudorange measurement. This technique is used in GPS. With enough pseudorange measurements and knowing the states of the BTSs, the receiver can localize itself within the cellular CDMA environment.

This section is organized as follows. Subsection 5.1 provides an overview of the modulation process of the forward link channel. Subsection 5.2 presents a receiver architecture for producing navigation observables from received cellular CDMA signals. Subsection 5.3 analyzes the precision of the cellular CDMA pseudorange observable. Subsection 5.4 shows experimental results for ground and aerial vehicles navigating with cellular CDMA signals.

5.1 Forward Link Signal Structure

Cellular CDMA networks employ orthogonal and maximal-length pseudorandom noise (PN) sequences in order to enable multiplexing over the same channel. 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 [46]. The following subsections discuss the modulation process of the forward link and give an overview of the pilot, sync, and paging channels, from which timing and positioning information can be extracted. Models of the transmitted and received signals are also given.

5.1.1 Modulation of Forward Link CDMA Signals

The data transmitted on the forward link channel in cellular CDMA systems is modulated through quadrature phase shift keying (QPSK) and then spread using direct-sequence CDMA (DS-CDMA). However, for the channels of interest from which positioning and timing information is extracted, the in-phase and quadrature components, I and Q, respectively, carry the same message $m(t)$ as shown in Figure 4. The spreading sequences c_I and c_Q, called the short code, are maximal-length 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 at a chipping rate of 1.2288 Mcps [47]. 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 is an integer multiple of 64 chips and this integer multiple, which is unique for each BTS, is known as the pilot offset. The cross-correlation of the same PN sequence with different pilot offsets can be shown to be negligible [46]. Each

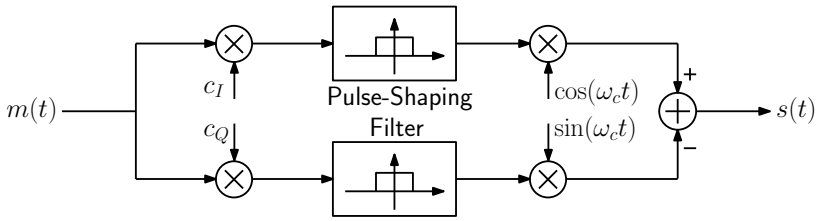


Figure 4: Forward-link modulator

individual logical channel is spread by a unique 64-chip Walsh code [48]. 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 Walsh codes enables multiple access for users over the same BTS. The CDMA signal is then 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 ω_c to produce $s(t)$.

5.1.2 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, which can be utilized by the receiver to detect the presence of a CDMA signal and then track it. The fact that the pilot signal is data-less allows for longer integration time. The receiver can differentiate between the BTSs based on their pilot offsets.

5.1.3 Sync Channel

The sync channel is used to provide time and frame synchronization to the receiver. Cellular CDMA networks typically use GPS as the reference timing source and the BTS sends the system time to the receiver over the sync channel [49]. Other information such as the pilot PN offset and the long code state are also provided on the sync channel [47]. The long code is a PN sequence and is used to spread the reverse link signal (i.e., UE 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 Figure 5.

The initial message, which is at 1.2 Ksps, is convolutionally encoded at a rate $r = (1/2)$ with generator functions $g_0 = 753$ (octal) and $g_1 = 561$ (octal) [48]. 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 [47]. 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

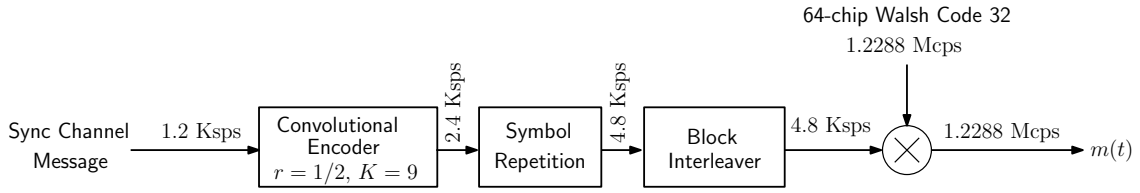


Figure 5: Forward-link sync channel encoder

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

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

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 Figure 6.

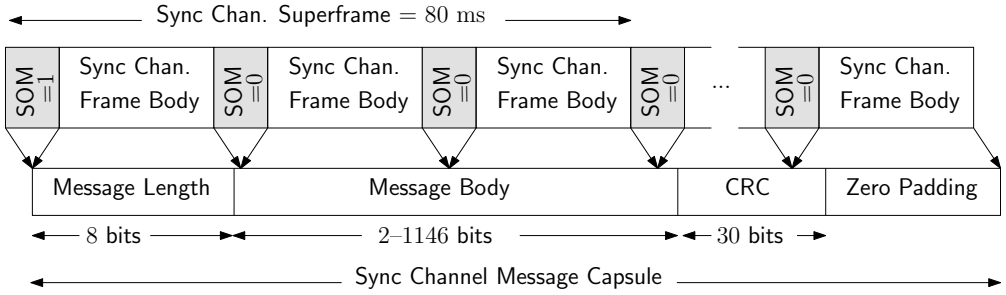


Figure 6: Sync channel message structure

5.1.4 Paging Channel

The paging channel transmits all the necessary overhead parameters for the UE to register into the network [46]. 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 latitude and longitude, but this provider does not operate anymore. The Base Station ID (BID) is also transmitted in the paging channel, which is important to decode for data association purposes. The paging channel message encoding before transmission is illustrated in Figure 7.

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

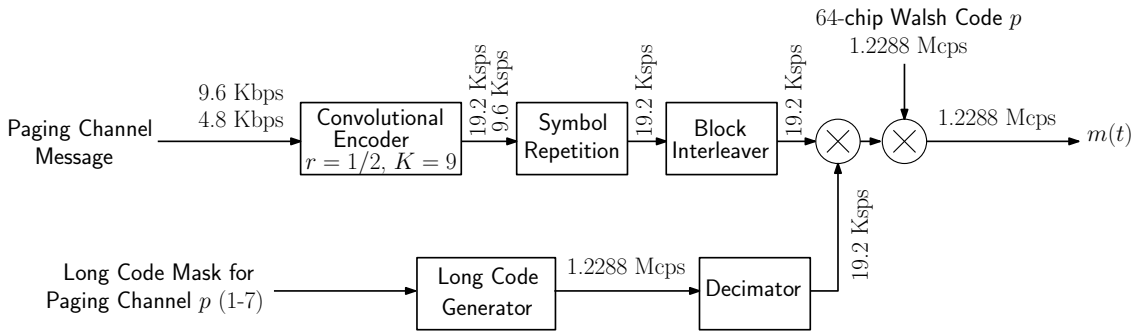


Figure 7: Forward-link paging channel encoder

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 [46]. The paging channel structure is summarized in Figure 8.

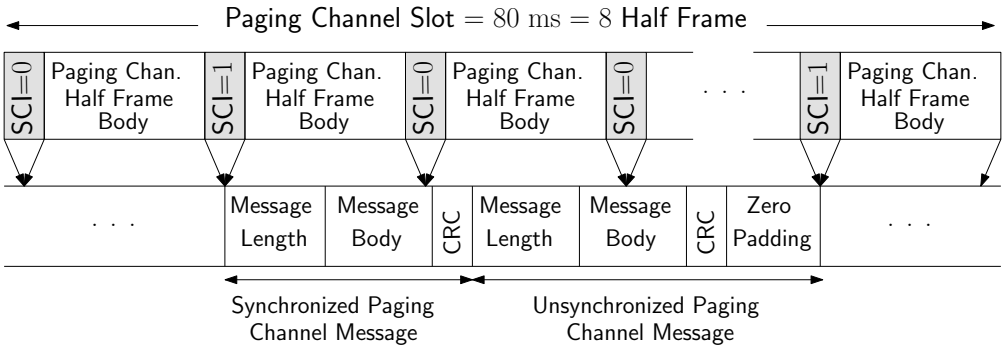


Figure 8: Paging channel message structure

5.1.5 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 Subsection 5.2. Demodulating the other channels becomes an open-loop problem, since no feedback is taken from

the sync, paging, or 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 cdma2000 specification that all the coded channels be synchronized with the pilot to within ± 50 ns [50]. Although signals from multiple BTSs could be received simultaneously, a UE can associate each individual signal with the corresponding BTS, since the offsets between the transmitted PN sequences are much larger than one chip. This is because the autocorrelation function has negligible values for delays greater than one chip. Therefore, the PN offsets, which are much larger than one chip delay guarantee that no significant interference is introduced (The autocorrelation function is discussed in Subsection 5.2.3 and is shown in Figure 13).

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

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

where $\Re\{\cdot\}$ denotes the real part; 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.

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) [51]. Note that a PN offset of 1 (i.e., 64 chips) is enough to prevent significant interference from different BTSs. This translates to more than 15 km between BTSs. Subtracting from this value 6 km due to worst case synchronization with GPS (i.e., 3 km for each BTS), then BTSs at 9 km or more from the serving BTS could cause interference (assuming all BTSs suffer from the worst case synchronizations). But, 9 km is much larger than the maximum distance for receiving cellular CDMA signals. Therefore, this synchronization 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 handoffs [47]. 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. The estimation of δt_s can be accomplished via the frameworks outlined discussed in Section 4.

5.1.6 Received Signal Model

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 signal $r[m]$ after radio frequency (RF) front-end processing: down-mixing, a quadrature approach to bandpass sampling [52], and quantization can be expressed as

$$r[m] = \frac{\sqrt{C}}{2}\left\{c'_I[t_m - t_s(t_m)] - jc'_Q[t_m - t_s(t_m)]\right\} \cdot e^{j\,\theta(t_m)} + n[m], \tag{5}$$

where $t_s(t_m) \triangleq \delta t_{\mathrm{TOF}} + \Delta(t_k - \delta t_{\mathrm{TOF}})$ 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 and identically distributed Gaussian random sequences with zero-mean and variance $\frac{N_0}{2T_s}$. The receiver presented in Subsection 5.2 will operate on the samples of $r[m]$ in (5).

5.2 CDMA Receiver Architecture

This section details the architecture of a cellular CDMA navigation receiver, which consists of three main stages: signal acquisition, tracking, and message decoding [18]. The receiver utilizes the pilot signal to detect the presence of a CDMA signal and then tracks it. Subsection 5.2.1 describes the correlation process in the receiver. Subsections 5.2.2 and 5.2.3 discuss the acquisition and tracking stages, respectively. Subsection 5.2.4 details decoding the sync and paging channel messages.

5.2.1 Correlation Function

Given samples of the baseband signal exiting the RF front-end defined in (5), 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

$$x[m] = \left[r[m] \cdot e^{-j\hat{\theta}(t_m)}\right] * h[-m], \tag{6}$$

where $\hat{\theta}$ is the beat carrier phase estimate and h 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 (FIR) given in Table 3. The samples m' of the FIR in Table 3 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

$$\begin{aligned} Z_k &= \frac{1}{N_s}\sum_{m=k}^{k+N_s-1} x[k]\left\{c_I[t_m - \hat{t}_s(t_m)] + jc_Q[t_m - \hat{t}_s(t_m)]\right\} \\ &\triangleq I_k + jQ_k, \end{aligned} \tag{7}$$

Table 3: FIR of the pulse-shaping filter used in cdma2000 [50]

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

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 the following, 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 updated 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 (5)–(6), into (7), it can be shown that

$$Z_k \;=\; \sqrt{C}\, R_c(\Delta t_k) \left[\frac{1}{N_s} \sum_{m=k}^{k+N_s-1} e^{j\Delta\theta(t_m)} \right] + n_k, \tag{8}$$

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 $n_k \triangleq n_{I_k} + j n_{Q_k}$ with n_{I_k} and n_{Q_k} being independent and identically distributed Gaussian random sequences with zero-mean and variance $\frac{N_0}{2T_s N_s} = \frac{N_0}{2T_{\text{sub}}}$.

The expression of Z_k in (8) 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, $|Z_k|$ will be halved. Figure 9 shows $|Z_k|^2$ for unsynchronized and synchronized c_I and c_Q code phases (i.e., shifted by 34 chips). The correlation peak of the synchronized codes is four-times the peak of the unsynchronized case.

The carrier wipe-off and correlation stages are illustrated in Figure 10.

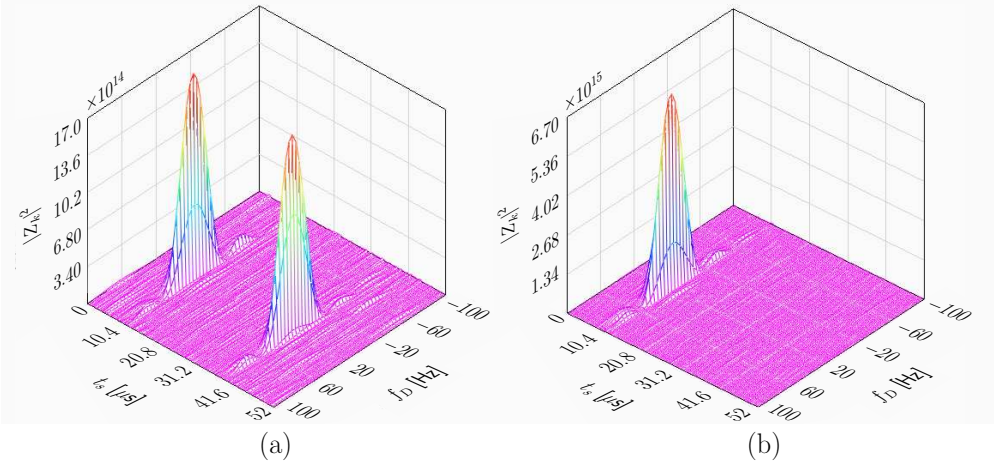


Figure 9: $|Z_k|^2$ for (a) unsynchronized and (b) synchronized c_I and c_Q codes

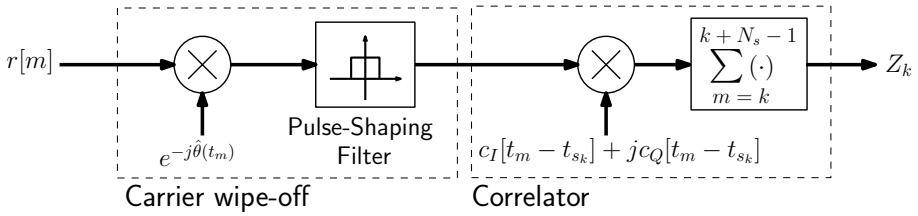


Figure 10: Carrier wipe-off and correlator. Thick lines indicate a complex-valued variable.

5.2.2 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 882.75 MHz at a mobile receiver with a receiver-to-BTS line-of-sight velocity of 150 km/h. Therefore, to account for this Doppler (at a carrier frequency of 882.75 MHz) as well as oscillator-induced Doppler, the Doppler frequency search window is chosen to be between -500 and 500 Hz. The frequency spacing Δf_D must be a fraction of $1/T_{\text{sub}}$, which implies that $\Delta f_D \ll 37.5$ Hz, if T_{sub} is assumed to be one PN code period (e.g., Δf_D can be 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 receiver presented here performs a parallel code phase search by exploiting the optimized efficiency of the fast Fourier transform (FFT) [53]. If a signal is present, a plot of $|Z_k|^2$ 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. Figure 11 depicts the acquisition stage of a cellular CDMA signal with a software-defined receiver (SDR) developed in LabVIEW, 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 [18].

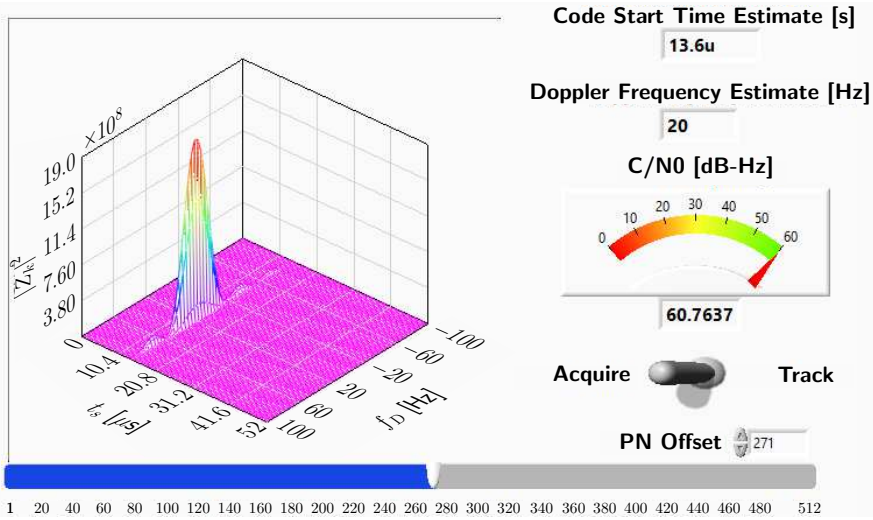


Figure 11: Cellular CDMA signal acquisition front panel showing $|Z_k|^2$ along with $\hat{t}_{s_k}$, $\hat{f}_{D_k}$, PN offset, and C/N_0 for a particular BTS

5.2.3 Tracking

After obtaining an initial coarse estimate of the code start time $\hat{t}_{s_k}$ and Doppler frequency $\hat{f}_{D_k}$, the receiver refines and maintains these estimates via tracking loops. A phase-locked loop (PLL) or a frequency-locked loop (FLL) can be employed to track the carrier phase and a carrier-aided delay-locked loop (DLL) can be used to track the code phase. FLLs are generally more robust than PLLs, are useful when transitioning from acquisition to tracking, and can track in more challenging environments [54, 55]. Figure 12 depicts a block diagram of a PLL-aided DLL tracking loop [12, 18]. The PLL and DLL are discussed in details next.

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, given by

$$e_{\text{PLL},k} = \texttt{atan2}\left(Q_{p_k}, I_{p_k}\right),$$

where $Z_{p_k} = I_{p_k} + jQ_{p_k}$ is the prompt correlation. The `atan2` discriminator remains linear over the full input error range of $\pm\pi$ and could be used without the risk of introducing

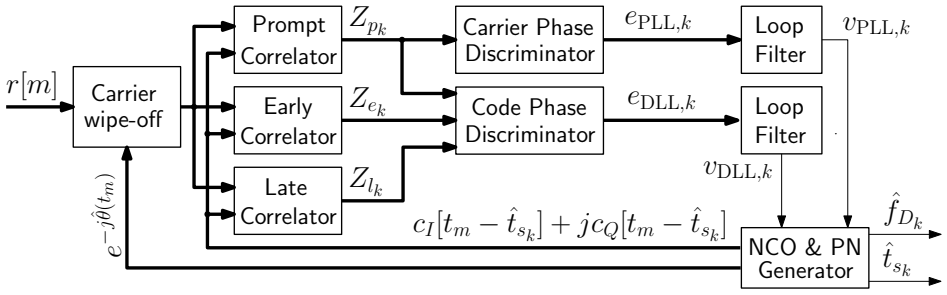


Figure 12: Tracking loops in a navigation cellular CDMA receiver. Thick lines represent complex quantities.

phase ambiguities. In contrast, a GPS receiver cannot use this discriminator unless the transmitted data bit values of the navigation message are known [54]. Furthermore, while GPS receivers require second- or higher-order PLLs due to the high dynamics of GPS 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

$$F_{\mathrm{PLL}}(s) = \frac{2\zeta\omega_n s + \omega_n^2}{s}, \tag{9}$$

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 $B_{n,\mathrm{PLL}} = \frac{\omega_n}{8\zeta}(4\zeta^2 + 1)$ [55]. The output of the loop filter $v_{\mathrm{PLL},k}$ is the rate of change of the carrier phase error, expressed in rad/s. The Doppler frequency is deduced by dividing $v_{\mathrm{PLL},k}$ by 2π. The loop filter transfer function in (9) is discretized and realized in state-space. The noise-equivalent bandwidth is chosen to range between 4 and 8 Hz.

DLL: The carrier-aided DLL employs a non-coherent dot-product discriminator, given by

$$e_{\mathrm{DLL},k} = \Lambda\left[\left(I_{e_k} - I_{l_k}\right) I_{p_k} + \left(Q_{e_k} - Q_{l_k}\right) Q_{p_k}\right],$$

where Λ is a normalization constant given by $\Lambda = T_c/2C$; C is the carrier power, which can be estimated from the prompt correlation; and $Z_{p_k} = I_{p_k} + jQ_{p_k}$, $Z_{e_k} = I_{e_k} + jQ_{e_k}$, and $Z_{l_k} = I_{l_k} + jQ_{l_k}$ are the prompt, early, and late correlations, respectively. The prompt correlation was described in Subsection 5.2.1. 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}. Figure 13 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 Figure 13 that for $t_{\mathrm{eml}} \leq 0.5$ chips, $R_c(\tau)$ in the cdma2000 standard has approximately a constant value, which is not desirable for precise tracking. A good rule of thumb is to choose $1 \leq t_{\mathrm{eml}} \leq 1.2$ chips.

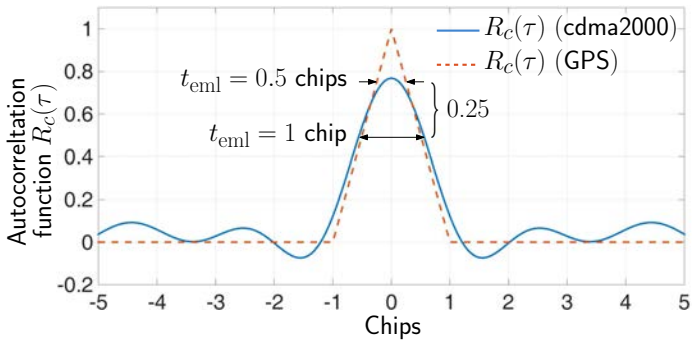


Figure 13: Autocorrelation function of GPS C/A code and cellular CDMA PN sequence according to the cdma2000 standard

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 $v_{\text{DLL},k}$ 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

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

In a GPS receiver, the pseudorange is calculated based on the time a navigation message subframe begins which eliminates ambiguities due to the relative distance between GPS SVs [55]. This necessitates decoding 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 [56].

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

$$\rho(k) = c \cdot \hat{t}_{s_k}. \tag{10}$$

Figure 14 shows the intermediate signals produced within the tracking loops of the 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.

5.2.4 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 Figure 5 and Figure 7, 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 Figure 15. Recall that the long code is also used to spread the paging

message in downlink (see Figure 7). The long code state decoded from a sync message is valid at the beginning of the corresponding paging channel message.

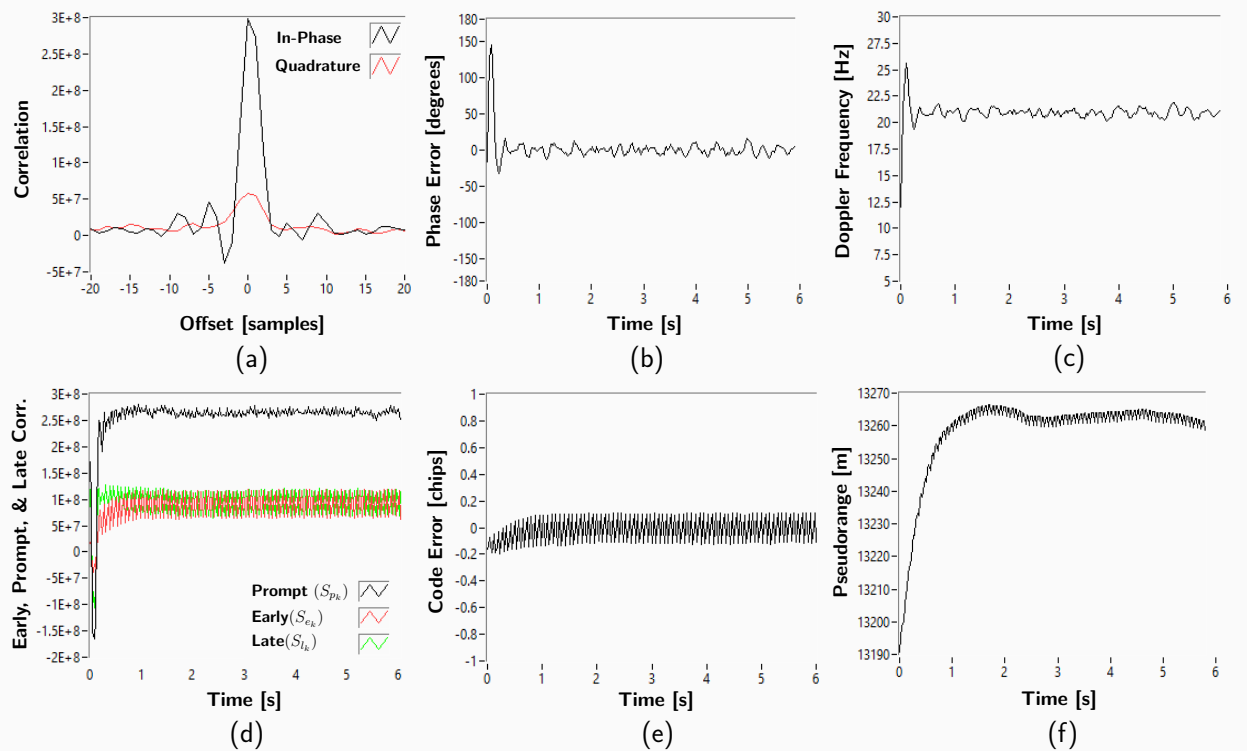


Figure 14: Cellular CDMA signal tracking: (a) code phase error (chips), (b) carrier phase error (degrees), (c) Doppler frequency estimate (Hz), (d) prompt (black), early (red), and late (green) correlation, (e) measured pseudorange (m), and (f) correlation function.

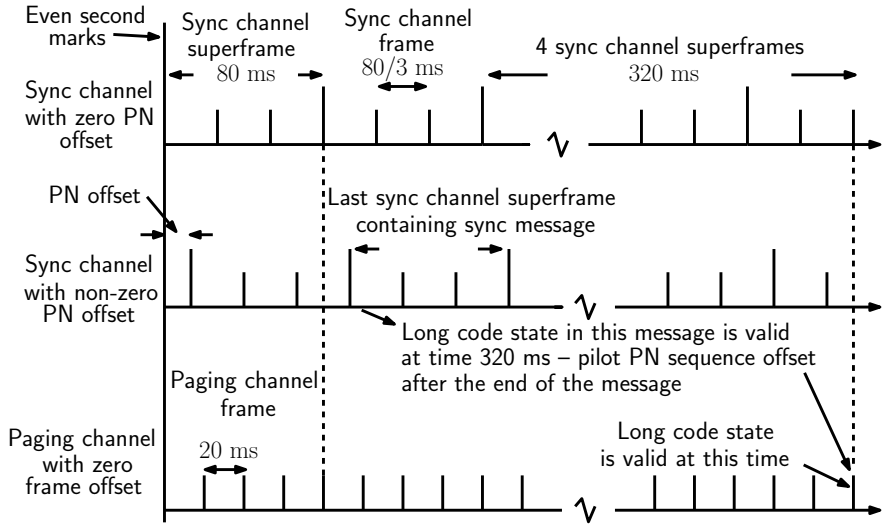


Figure 15: Sync and paging channel timing

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 the C/A code generator in GPS, the 42 long code generator registers are configured to satisfy a linear recursion given by

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

The long code mask is obtained by combining the PN offset and the paging channel number p as shown in Figure 16.

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

Figure 16: 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 [47]. Figure 17 shows the demodulated sync signal as well as the final information decoded from the sync and paging channels. Note that the shown signal corresponds to the U.S. cellular provider Verizon, which does not broadcast its BTS position information (latitude and longitude). Moreover, note that the last digit in the BTS ID corresponds to the sector number of the BTS cell. This is important for data association purposes, since different sectors of the same BTS cell are not perfectly synchronized. This is discussed in more details in Section 7.

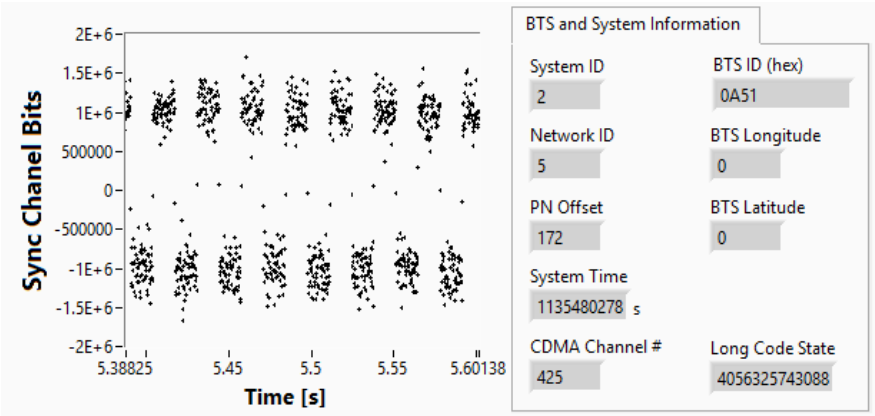


Figure 17: Message decoding: demodulated sync channel signal (left) and BTS and system information decoded from sync and paging channels (right).

5.3 Code Phase Error Analysis

Subsection 5.2 presented a recipe for designing a receiver that can extract a pseudorange estimate from cellular CDMA signals. This subsection analyzes the statistics of the error

of the code phase estimate for a coherent DLL. It is worth noting that when the receiver is closely tracking the carrier phase, the non-coherent dot-product discriminator and a coherent DLL discriminator will perform similarly. Hence, for simplicity, the analysis is carried out for 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 5.2.3, it is enough to use a first-order loop for the DLL, yielding the following closed-loop time-update error equation [57]

$$\Delta t_{k+1} = (1 - 4B_{n,\mathrm{DLL}}T_{\mathrm{sub}})\Delta t_k + Ke_{\mathrm{DLL},k}, \tag{11}$$

where $e_{\mathrm{DLL},k}$ is the output of the code phase discriminator. The discriminator statistics are discussed next.

5.3.1 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 noise channel.

Received Signal Noise Statistics: To make the analysis tractable, the continuous-time 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 continuous-time received signal after down-mixing 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 continuous-time 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

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

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 [55], the early and late correlations may be approximated with

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

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

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

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 Figure 18 for $t_{\text{eml}} = \{0.25, 0.5, 1, 1.5, 2\}$.

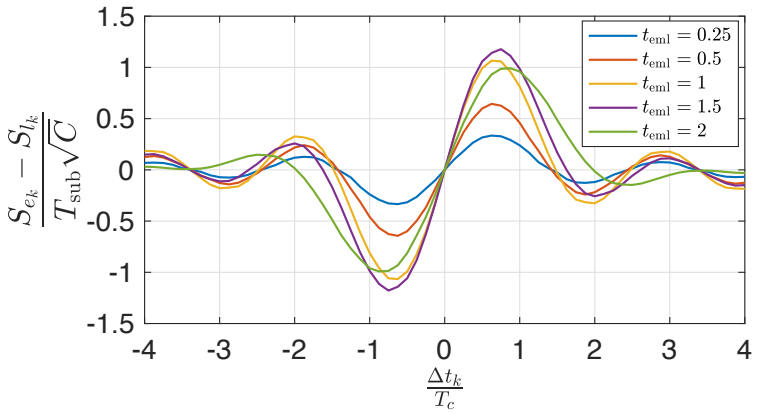


Figure 18: Output of the coherent baseband discriminator function for the CDMA short code with different correlator spacings

It can be seen from Figure 18 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 the discriminator function at $\Delta t_k = 0$ [57], which is obtained by

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

Since $R_c(\tau)$ is symmetric,

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

and the linearized discriminator output becomes

$$D_k \approx 2T_{\text{sub}}R_c'\left(\frac{t_{\text{eml}}}{2}T_c\right)\Delta t_k + \frac{(n_{e_k} - n_{l_k})}{\sqrt{C}}. \tag{12}$$

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 (12), and are given by

$$\mathbb{E}\{D_k\} = 2T_{\text{sub}}R_c'\left(\frac{t_{\text{eml}}}{2}T_c\right)\Delta t_k, \tag{13}$$

$$\begin{aligned}\text{var}\{D_k\} &= \frac{1}{C}\text{var}\{n_{e_k} - n_{l_k}\} \\ &= \frac{1}{C}\left[\text{var}\{n_{e_k}\} + \text{var}\{n_{l_k}\} - 2\mathbb{E}\{n_{e_k}n_{l_k}\}\right] \\ &= \frac{T_{\text{sub}}N_0}{C}\left[1 - R_c(t_{\text{eml}}T_c)\right].\end{aligned} \tag{14}$$

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

5.3.2 Closed-Loop Analysis

In order to achieve the desired loop noise-equivalent bandwidth, K in (11) must be normalized according to

$$K = \left.\frac{4B_{n,\text{DLL}}T_{\text{sub}}\Delta t_k}{\mathbb{E}\{D_k\}}\right|_{\Delta t_k = 0} = \frac{2B_{n,\text{DLL}}}{R_c'\left(\frac{t_{\text{eml}}}{2}T_c\right)}. \tag{15}$$

In cellular CDMA systems, for a t_{eml} of 1.2, the loop filter gain becomes $K \approx 4B_{n,\text{DLL}}$; hence, the choice of K in Subsection 5.2.3. Assuming a zero-mean tracking error, i.e., $\mathbb{E}\{\Delta t_k\} = 0$, the variance of the code start time error is given by

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

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

$$\text{var}\{\Delta t_{k+1}\} = \text{var}\{\Delta t_k\} = \text{var}\{\Delta t\}, \tag{16}$$

where Δt is the steady-state code start time error. Combining (15)–(16) yields

$$\text{var}\{\Delta t\} = \frac{B_{n,\text{DLL}}\,q(t_{\text{eml}})}{2(1 - 2B_{n,\text{DLL}}T_{\text{sub}})C/N_0}, \tag{17}$$

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

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 $\sigma^2 = c^2 \cdot \text{var}\{\Delta t\}$. Figure 19 shows a plot of the standard deviation of Δt, denoted σ, as a function of the carrier-to-noise ratio C/N_0 for $t_{\text{eml}} = 1.25$ chips.

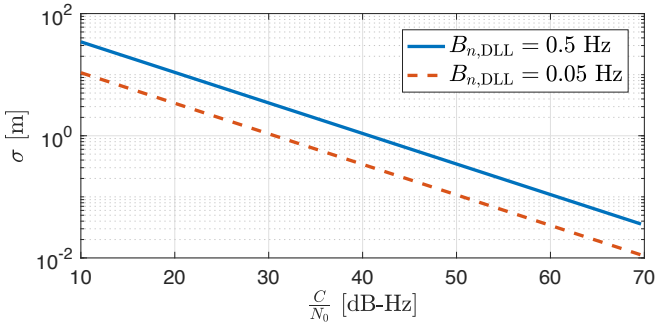


Figure 19: Plot of σ, the standard deviation of Δt, as a function of the carrier-to-noise ratio $\frac{C}{N_0}$ for $t_{\text{eml}} = 1.25$ chips and $B_{n,\text{DLL}} = \{0.5 \text{ Hz}, 0.05 \text{ Hz}\}$.

5.4 Cellular CDMA Navigation Experimental Results

This subsection presents experimental results for navigation with cellular CDMA signals. These results did not suffer from the BTS sector clock discrepancy issue (discussed in Section 7), since signals from only one sector antenna in each BTS cell were used. Experimental results exhibiting the BTS sector clock discrepancy issue and mitigation approaches are studied in [23, 25]. Subsection 5.4.1 analyzes the pseudoranage obtained by the receiver discussed in Section 5.2. Subsections 5.4.2 and 5.4.3 present navigation results with aerial and ground vehicles, respectively.

5.4.1 Pseudorange Analysis

The variation in the pseudorange obtained by the receiver discussed in Section 5.2 are compared to the variation in the true range between a mobile receiver and cellular CDMA BTSs. For this purpose, the receiver was mounted on two platforms: 1) an unmanned aerial vehicle (UAV) and 2) a ground vehicle [12, 18, 25].

UAV Results Figure 20 shows the BTS environment, the UAV trajectory, and the experimental hardware setup. Signals from two cellular BTSs corresponding to the U.S. cellular provider Verizon Wireless were tracked. The BTSs transmitted at a carrier frequency of 883.98 MHz and their positions were mapped prior to the experiment [37, 39]. The ground-truth reference for the UAV trajectory shown in Figure 20 was taken from its on-board navigation system, which uses GPS, an INS, and other sensors. The distance D between the UAV and each BTS was calculated using the navigation solution produced by the UAV's navigation system and the known BTS position. The pseudorange ρ was obtained from the

cellular CDMA receiver that was mounted on the UAV. In order to validate the resulting pseudoranges, the variation of the pseudorange $\Delta\rho \triangleq \rho - \rho(0)$ and the variation in distance $\Delta D \triangleq D - D(0)$ are plotted in Figure 21 for the two BTSs, where $\rho(0)$ is the initial value of the pseudorange and $D(0)$ is the initial distance between the UAV and the BTS. It can be seen from Figure 21 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 v_i.

Figure 20: BTS environment and experimental hardware setup for the UAV experiment. Map data: Google Earth.

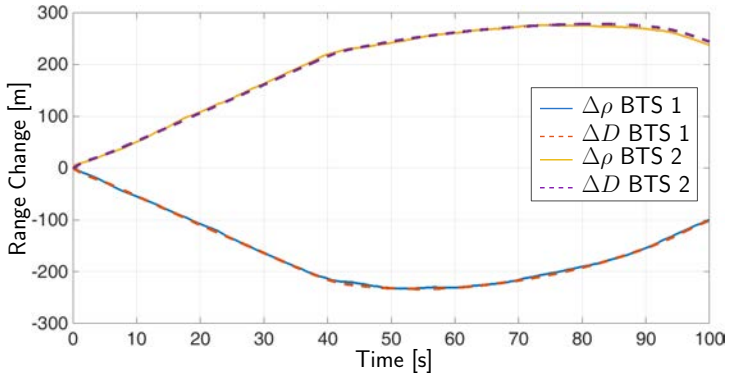


Figure 21: Variation in pseudoranges and the variation in distances between the receiver and two cellular CDMA BTSs for the UAV experiment.

Ground Vehicle Results Figure 22 shows the BTS environment, ground vehicle trajectory, and the experimental hardware setup. Signals from two cellular BTSs corresponding to the U.S. cellular provider Verizon Wireless were tracked. The BTSs transmitted at a carrier frequency of 882.75 MHz and their positions were mapped prior to the experiment [37, 39]. The ground-truth reference for the for the ground vehicle trajectory in Figure 22 was obtained from the Generalized Radionavigation Interfusion Device (GRID) GPS SDR [58]. The change in the true range and the change in pseudorange are plotted in Figure 23, similarly to the UAV experiment. It can be seen from Figure 23 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 v_i.

Figure 22: BTS environment, true trajectory, and experimental hardware setup for the ground vehicle experiment. Map data: Google Earth.

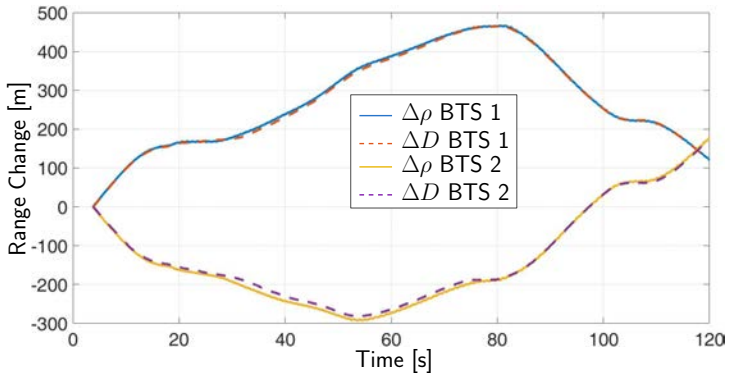


Figure 23: Variation in pseudoranges and the variation in distances between the receiver and two cellular CDMA BTSs for the ground vehicle experiment.

5.4.2 Ground Vehicle Navigation

Two cars (mapper and navigator) were equipped with the cellular CDMA navigation receiver discussed in Subsection 5.2. The receivers were tuned to the cellular carrier frequency 882.75 MHz, which is a channel allocated to the U.S. cellular provider Verizon Wireless. The mapper was stationary and was estimating the clock biases of the 3 BTSs via a WLS estimator as discussed in Subsection 4.1. The BTSs' positions were known to the mapper and the position states were expressed in a local 3–D frame whose horizontal plane passes through the 3 BTSs and is centered at the mean of the BTSs' positions. The height of the navigator was known and constant in the local 3–D frame over the trajectory driven and was passed as a constant parameter to the estimator. Hence, only the navigator's two-dimensional (2–D) position and its clock bias were estimated through the WNLS described in Subsection 4.1. The weights of the WNLS were calculated using (41) with $T_{\text{sub}} = \frac{1}{37.5}$ s. For the first pseudorange measurement, the WNLS iterations were initialized by setting the navigator's initial horizontal position states at the origin of the 3–D local frame and the initial clock bias to zero. For each subsequent pseudorange measurement, the WNLS iterations were initialized at the solution from the previous WNLS. The experimental hardware setup, the environment layout, and the true and estimated navigator trajectories are shown in Figure 24. The ground-truth trajectory was obtained from the GRID GPS SDR [58]. It can be

seen from Figure 24 that the navigation solution obtained from the cellular CDMA signals follows closely the navigation solution obtained using GPS signals.

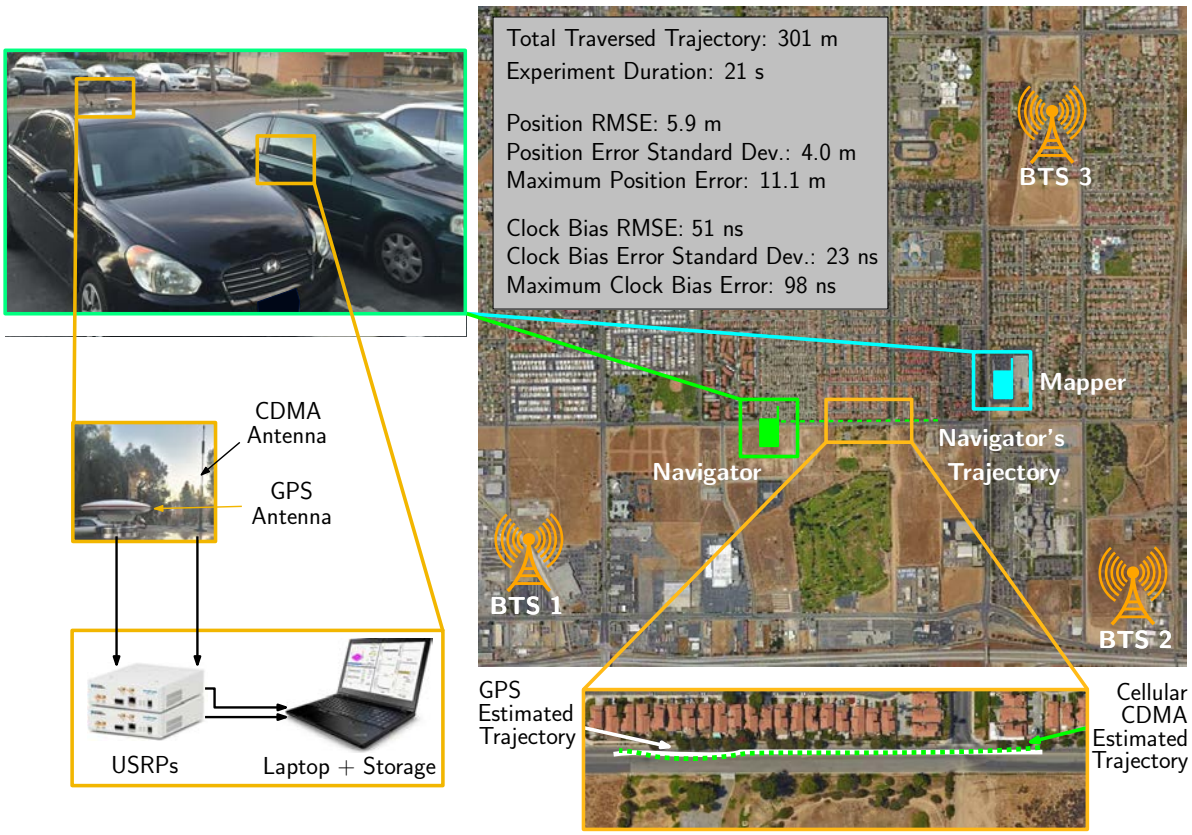


Figure 24: Experimental hardware setup, navigator trajectory, and mapper and BTS locations for ground experiment.

5.4.3 Aerial Vehicle Navigation

Two identical UAVs (mapper and navigator) were equipped with the cellular CDMA navigation receiver discussed in Subsection 5.2. Here, both the mapper and navigator were mobile. The receivers were tuned to the cellular carrier frequency 882.75 MHz used by the U.S. cellular provider Verizon Wireless. The mapper and navigator were listening to the same 4 BTSs with known positions. The mapper was estimating the BTSs' clock biases via a WLS estimator as discussed in Subsection 4.1. Similar to the ground vehicle navigation setup, the height of the navigator was a known constant in the local 3–D frame and only the navigator's 2–D position and its clock bias were estimated through the WNLS, whose weights and initialization were calculated in a similar way as the ground vehicle navigation setup. The ground-truth references for the mapper and navigator trajectories were taken from the UAVs' on-board navigation systems, which use GPS, INS, and other sensors. Figure 25 shows the BTS environment in which the mapper and navigator were present as well as the experimental hardware setup. The navigator's true trajectory and estimated trajectory from cellular CDMA pseudoranges are shown in Figure 26.

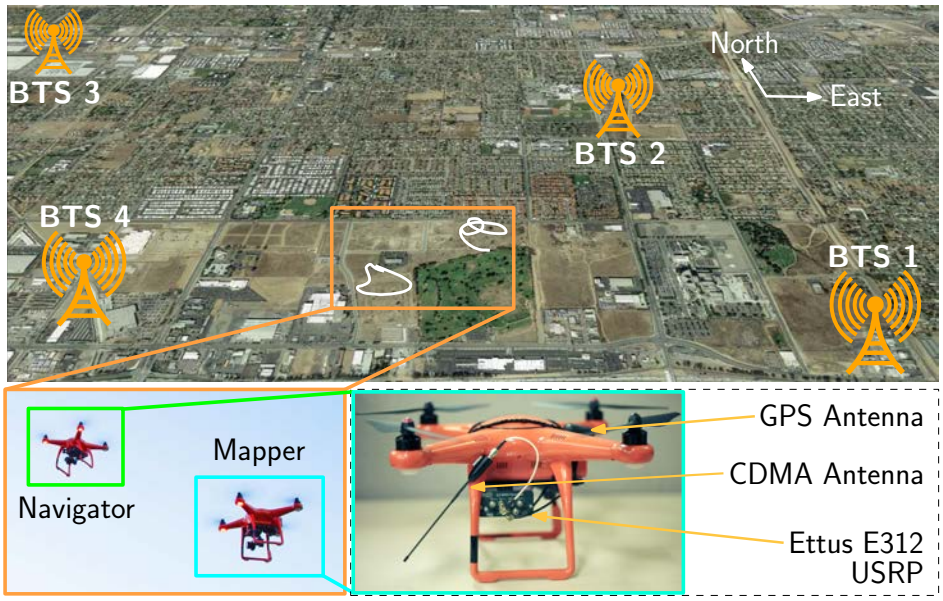


Figure 25: BTS environment and experimental hardware setup with a mobile mapper. Map data: Google Earth.

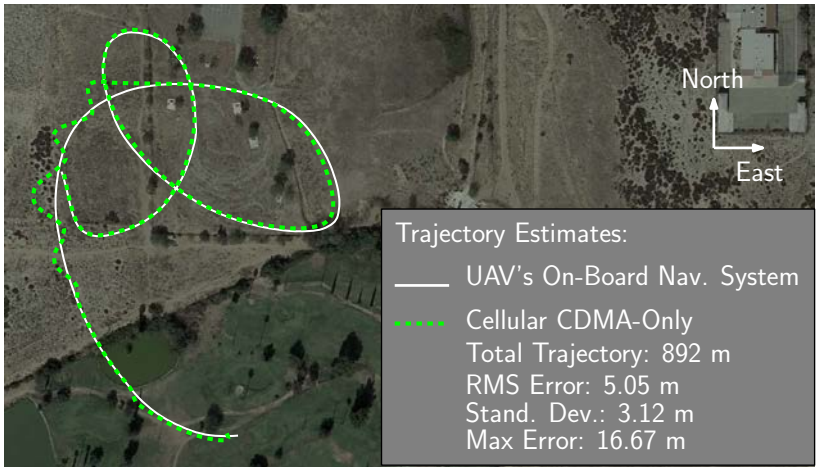


Figure 26: Navigating UAV's true and estimated trajectory. Map data: Google Earth.

6 Navigation with Cellular LTE Signals

Two different techniques can be employed to use LTE signals for PNT: network-based and UE-based. The network-based technique was enabled in LTE Release 9 by introducing a broadcast positioning reference signal (PRS). The expected positioning accuracy with PRS is on the order of 50 m [59]. Network-based positioning suffers from a number of drawbacks:

- The user's privacy is compromised, since the user's location is revealed to the network [60].
- Localization services are limited only to paying subscribers and from a particular cellular provider.

- Ambient LTE signals transmitted by other cellular providers are not exploited.
- Additional bandwidth is required to accommodate the PRS, which caused the majority of cellular providers to choose not to transmit the PRS in favor of dedicating more bandwidth for traffic channels.

To circumvent these drawbacks, UE-based PNT techniques, which exploit the existing reference signals in the transmitted LTE signals, have been developed. This section focuses on UE-based PNT techniques. When a UE enters an unknown LTE environment, the first step it performs to establish communication with the network is synchronizing with the surrounding LTE BTSs, also referred to as Evolved Node Bs (eNodeBs). This is achieved by acquiring the primary synchronization signal (PSS) and the secondary synchronization signal (SSS) transmitted by the eNodeB. The PSS and SSS can be directly exploited for navigation. Another LTE signal that can be exploited for navigation is the cell-specific reference signal (CRS); however, exploiting CRS is not as straightforward due to its scattered nature in time and frequency. Table 1 compares the salient navigation properties of PSS, SSS, and CRS.

This section is organized as follows. Subsection 6.1 discusses the LTE frame structure and reference signals that could be exploited for navigation. Section 6.2 presents a receiver architecture for producing navigation observables from received LTE signals. Section 6.3 analyzes the code phase error of SSS signals with coherent and non-coherent DLL tracking. Subsection 6.4 shows experimental results for ground and aerial vehicles navigating with cellular LTE signals.

6.1 LTE Frame and Reference Signal Structure

In LTE downlink transmission, data is encoded using orthogonal frequency division multiplexing (OFDM). OFDM is a transmission method in which the symbols are mapped onto multiple carrier frequencies called subcarriers. The serial data symbols $\{S_1, \ldots, S_{N_r}\}$ are first parallelized in groups of length N_r, where N_r represents the number of subcarriers that carry data. Then, each group is zero padded to length N_c, which is the total number of subcarriers, and an inverse FFT (IFFT) is taken. The value of N_c is set to be greater than N_r to provide a guard band in the frequency-domain. Finally, to protect the data from multipath effects, the last L_{CP} elements of the obtained symbols are repeated at the beginning of the data, called the cyclic prefix (CP). The transmitted symbols can be obtained at the receiver by executing these steps in reverse order. Since the frequency reuse factor in LTE systems is one, all the eNodeBs of the same operator use the same frequency band. To reduce the interference caused by sharing the same frequency band, each signal is coded to be orthogonal to the transmitted signals from other eNodeBs. Using different frequency bands makes it possible to allocate the same cell IDs to the eNodeBs from different operators. Figure 27 represents the block diagram of the OFDM encoding scheme for digital transmission. The following subsections discuss the LTE frame structure and reference signals, which will be exploited for navigation.

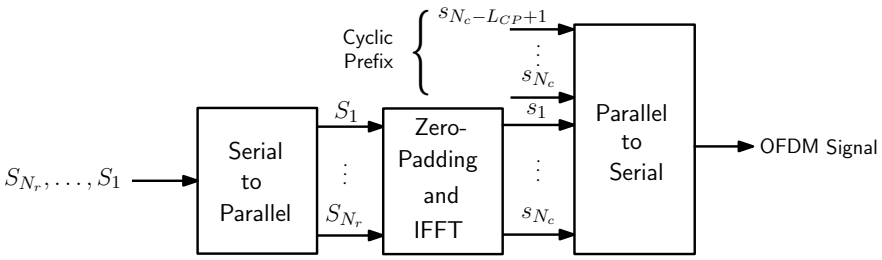


Figure 27: OFDM transmission block diagram

6.1.1 Frame Structure

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

A frame is a major component in LTE communication, which is a 2–D grid representing time and frequency. A frame is composed of 10 ms data, which is divided into either 20 slots or 10 subframes with a duration of 0.5 ms or 1 ms, respectively. A slot can be decomposed into multiple resource grids (RGs) and each RG has numerous resource blocks (RBs). Then, an RB is broken down into the smallest elements of the frame, namely resource elements (REs). The frequency and time indices of an RE are called subcarrier and symbol, respectively. The LTE frame structure is illustrated in Figure 28 and the composition of a single LTE frame with 6 RBs is depicted in Figure 29 [61].

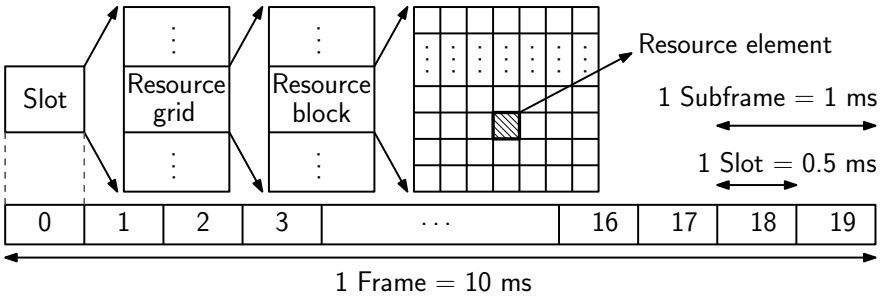


Figure 28: LTE frame structure

The number of subcarriers in an LTE frame, N_c, and the number of used subcarriers, N_r, are assigned by the network provider and can only take the values that are shown in Table 4. The subcarrier spacing is typically $\Delta f = 15$ kHz. Hence, the *occupied* bandwidth W' can be calculated using $W' = N_r \times \Delta f$. To allow for a guard band, the *allocated* bandwidth W is chosen to be slightly higher than the W' bandwidth (e.g., a $W = 1.4$ MHz is chosen for a $W' = 1.08$ MHz). Note that N_c is chosen to be a power-of-two to exploit the computational efficiency of the FFT.

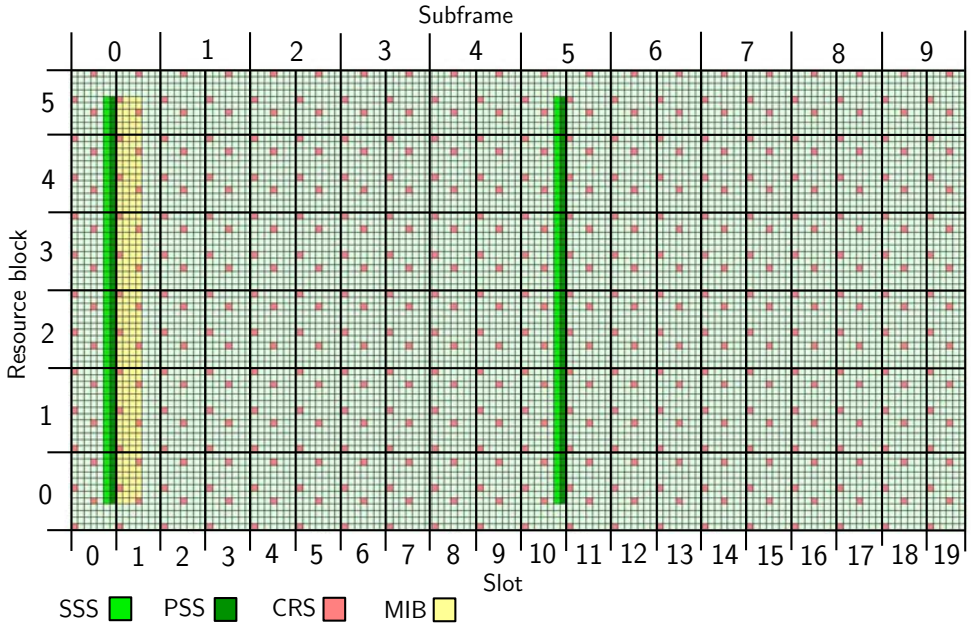


Figure 29: Composition of a single LTE frame. The slots represent time, while the RBs represent frequency.

Table 4: LTE system bandwidths and number of subcarriers

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

When a UE receives an LTE signal, it must reconstruct the LTE frame to be able to extract the information transmitted in the signal. This is achieved by first identifying the frame start time. Then, knowing the frame timing, the receiver can remove the CPs and take the FFT of each N_c symbol. The duration of the normal CP is 5.21 μs for the first symbol of each slot and 4.69 μs for the rest of the symbols [61]. To determine the frame timing, the PSS and SSS must be acquired, which will be discussed in the next subsection.

6.1.2 Timing Signals

There are three reference signals in LTE systems: PSS, SSS, and CRS, which can be exploited for positioning purposes by acquiring and tracking their subcarriers. These signals are discussed next.

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

SSS: The SSS is an orthogonal length-62 sequence which is transmitted in either slot 0 or 10, in the symbol preceding the PSS, and on the same subcarriers as the PSS. The SSS is obtained by concatenating two maximal-length sequences scrambled by a third orthogonal sequence generated based on $N_{ID}^{(2)}$. There are 168 possible sequences for the SSS that are mapped to an integer number $N_{ID}^{(1)} \in \{0, \ldots, 167\}$, called the cell group identifier. The FFT-based correlation in (21) is also exploited to detect the SSS signal. Once the PSS and SSS are detected, the UE can estimate the frame start time, $\hat{t}_s$, and the eNodeB's cell ID using $N_{ID}^{cell} = 3N_{ID}^{(1)} + N_{ID}^{(2)}$ [62]. The cell ID is used for data association purposes.

CRS: The CRS is an orthogonal pseudorandom sequence, which is uniquely defined by the eNodeB's cell ID. It is spread across the entire bandwidth (see Figure 29) and is transmitted mainly to estimate the channel frequency response. Due to the scattered nature of the CRS, it cannot be tracked with conventional DLLs [15,63]. The CRS subcarrier allocation depends on the cell ID, and it is designed to keep the interference with CRSs from other eNodeBs to a minimum. Since the CRS is transmitted throughout the bandwidth, it can accept up to 20 MHz bandwidth.

The transmitted OFDM signal from the uth eNodeB at the kth subcarrier and on the ith symbol can be expressed as

$$\boldsymbol{Y}_i^{(u)}(k) = \begin{cases} \boldsymbol{S}_i^{(u)}(k), & \text{if } k \in N_{CRS}^{(u)}, \\ \boldsymbol{D}_i^{(u)}(k), & \text{otherwise,} \end{cases} \tag{18}$$

where $\boldsymbol{S}_i^{(u)}(k)$ represents the CRS sequence; $N_{CRS}^{(u)}$ denotes the set of subcarriers containing the CRS, which is a function of the symbol number, port number, and the cell ID; and $\boldsymbol{D}_i^{(u)}(k)$ represents some other data signals.

6.1.3 Received Signal Model

Assuming that the transmitted signal propagated in an additive white Gaussian noise channel, the received signal in the ith symbol will be

$$\boldsymbol{R}_i(k) = \sum_{u=0}^{U-1} \boldsymbol{H}_i^{(u)}(k) \boldsymbol{Y}_i^{(u)}(k) + \boldsymbol{W}_i(k), \tag{19}$$

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

6.2 LTE Receiver Architecture

A cellular LTE navigation receiver consists of four main stages: signal acquisition, system information extraction, tracking, and timing information extraction [64,65]. This subsection discusses the various stages of the navigation LTE receiver, depicted in Figure 30. Subsection 6.2.1 describes the acquisition of PSS and SSS. Subsection 6.2.2 discusses the extraction of relevant system information. Subsection 6.2.3 discusses the tracking stage. Subsection 6.2.4 describes the timing information extraction.

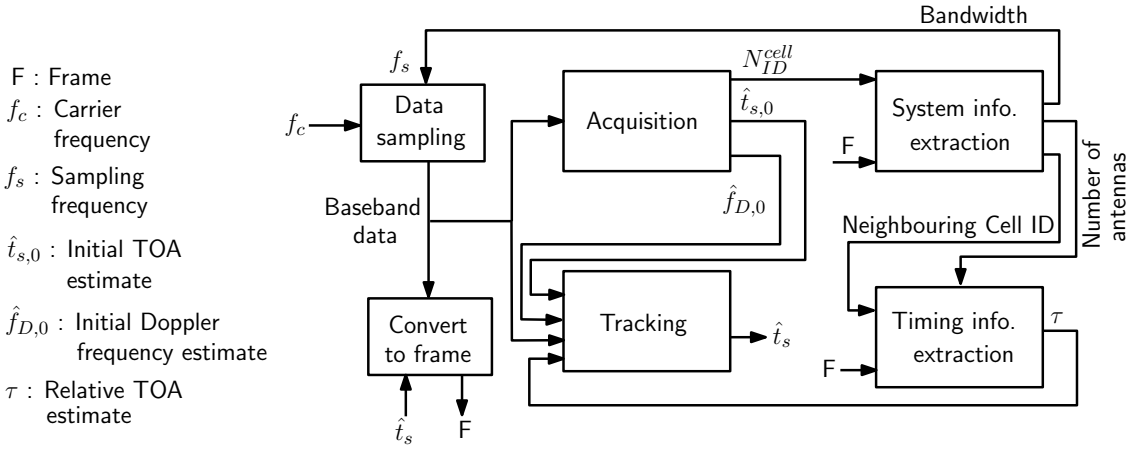


Figure 30: Block diagram of the LTE navigation receiver architecture

6.2.1 Acquisition

The first step in acquiring an LTE signal is to extract the transmitted frame timing and the eNodeB's cell ID [66–68]. These two parameters are obtained by the PSS and SSS. To detect the PSS, the UE exploits the orthogonality of the Zadoff-Chu sequences and correlates the received signal with all the possible choices of the PSS according to

$$\begin{aligned} \mathrm{Corr}(\boldsymbol{r}, \boldsymbol{s}_{PSS})_m &= \sum_{n=0}^{N-1} \boldsymbol{r}(n) \boldsymbol{s}_{PSS}^*(n+m)_N \\ &= \boldsymbol{r}(m) \circledast_N \boldsymbol{s}_{PSS}^*(-m)_N, \end{aligned} \tag{20}$$

where $\boldsymbol{r}(n)$ is the received signal, $\boldsymbol{s}_{PSS}(n)$ is the receiver-generated PSS in the time-domain, N is the frame length, $(\cdot)^*$ denotes the complex conjugate, $(\cdot)_N$ denotes the circular shift operator, and $\circledast_N$ represents the circular convolution operation. Taking the FFT and IFFT of (20) yields

$$\mathrm{Corr}(\boldsymbol{r}, \boldsymbol{s}_{PSS})_m = \mathrm{IFFT}\{\boldsymbol{R}(k) \boldsymbol{S}_{PSS}^*(k)\}, \tag{21}$$

where $\boldsymbol{R}(k) \triangleq \mathrm{FFT}\{\boldsymbol{r}(n)\}$ and $\boldsymbol{S}_{PSS}(k) \triangleq \mathrm{FFT}\{\boldsymbol{s}_{PSS}(n)\}$. The FFT-based correlation in (21) is also used to detect the SSS signal. Once the PSS and SSS are detected, the UE can estimate the frame start time.

After obtaining the frame timing, the UE estimates the frequency shift (Doppler frequency) using the CP in the received signal $r(n)$. The apparent Doppler frequency, including the carrier frequency offset due to clock drift and the Doppler shift, can be estimated by the CP as

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

where N_{CP} is the set of CP indices and T_s is the sampling interval [69]. Upon estimating the Doppler frequency, the acquisition of the LTE signal is complete. Figure 31 summarizes the LTE signal acquisition process.

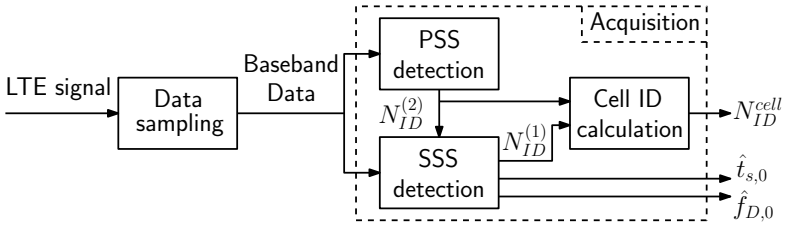


Figure 31: Signal acquisition block diagram

The normalized correlation of received LTE signals with locally-generated PSS and SSS signals are presented in Figure 32. It can be seen that since the PSS is transmitted twice per frame, the correlation has two peaks in the duration of one frame, which is 10 ms. However, the SSS correlation has only one peak, since the SSS is transmitted only once per frame. The figure also shows that the highest PSS correlation peak was at $N_{ID}^{(2)} = 0$ and the highest SSS correlation peak was at $N_{ID}^{(1)} = 77$. Therefore, the cell ID was calculated to be $N_{ID}^{Cell} = 3 \times 77 + 0 = 231$.

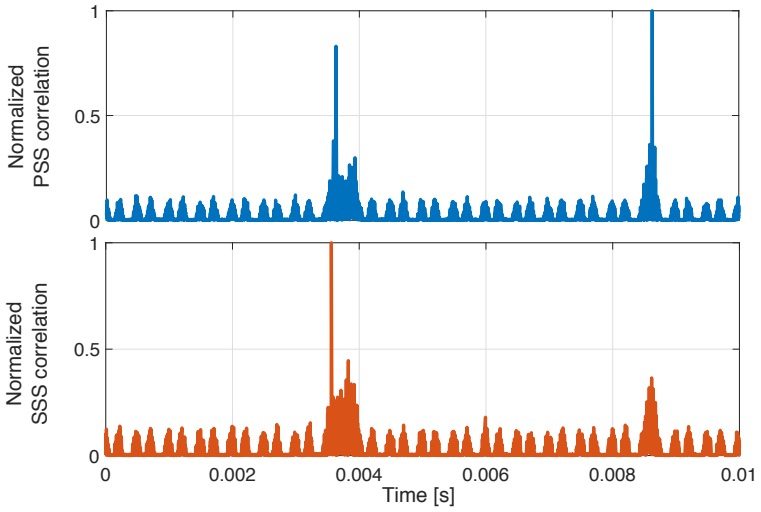


Figure 32: PSS and SSS normalized correlation results with real LTE signals

6.2.2 System Information Extraction

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

The UE starts acquiring with the lowest possible bandwidth of LTE, since the UE has no information about the actual transmission bandwidth. After acquisition, the signal is converted to the frame, and the bandwidth is obtained by decoding the MIB. Then, the UE can increase its sampling frequency to exploit the high bandwidth of the CRS. The UE can also utilize signals received from multiple eNodeB antennas to improve the TOA estimate.

Since the frequency reuse factor in LTE is one, it may not be possible to acquire the received PSS and SSS signals from eNodeBs with low C/N_0. This phenomenon is called the near-far effect. In this case, one can use the neighboring cell IDs obtained by decoding the SIB to reconstruct the CRS sequence [65]. This subsection discusses the decoding of MIB and SIB.

MIB Decoding: In order to exploit the high-bandwidth CRS signal, which improves the navigation performance in multipath environments and in the presence of interference, the UE must first reconstruct the LTE frame from the received signal. To do so, the actual transmission bandwidth and number of transmitting antennas, which are provided in the MIB, must be decoded. The MIB is transmitted on the physical broadcast channel (PBCH) and consists of 24 bits of data: 3 bits for downlink bandwidth, 3 bits for frame number, and 18 bits for other information and spare bits. The MIB is coded and transmitted on 4 consecutive symbols of a frame's second slot. However, it is not transmitted in REs reserved for the reference signals. Figure 33 shows the steps the MIB message goes through before transmission [61, 70].

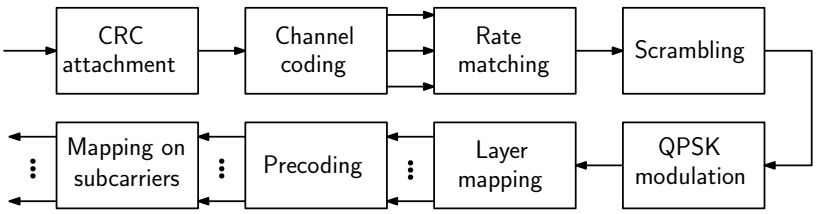


Figure 33: MIB coding process

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

possible transmitting antennas. Then, by comparing the locally-generated CRC scrambled by the CRC mask with the received CRC, the number of transmitting antennas is identified.

In the second step, channel coding is performed using a convolutional encoder with constraint length 7 and coding rate 1/3. The configuration of the encoder is shown in Figure 34. The initial value of the encoder is set to the value of the last 6 information bits in the input stream. The method illustrated in Figure 35 is used to decode the received signal [71]. In this method, the received signal is repeated one time. Then, a Viterbi decoder is executed on the resulting sequence. Finally, the middle part of the sequence is selected and circularly shifted.

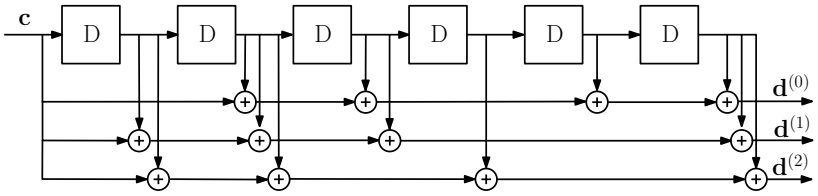


Figure 34: Tail biting convolutional encoder with constraint length 7 and coding rate 1/3

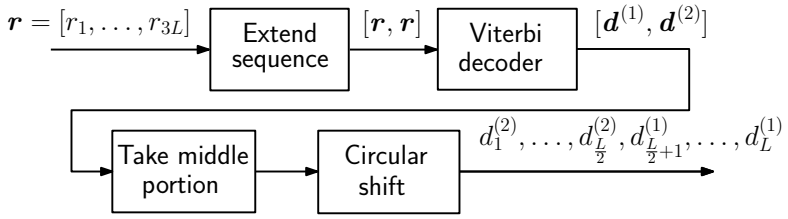


Figure 35: MIB channel decoding method

In the next step, the convolutional coded bits are rate-matched. In the rate matching step, the obtained data from channel coding is first interleaved. Then, the outcomes of interleaving each stream are repeated to obtain a 1920-bit long array [70]. Next, the output of the rate matching step is scrambled with a pseudo-random sequence, which is initialized with the cell ID, yielding unique signal detection for all eNodeBs. Subsequently, quadrature phase shift keying (QPSK) is performed on the obtained data, resulting in 960 symbols which are mapped onto different layers to provide transmission diversity. To overcome channel fading and thermal noise, space-time coding is utilized. This process is performed in the precoding step. Finally, the resulting symbols are mapped onto the predetermined subcarriers for MIB transmission [70].

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

needs to search over all possible values of the cell IDs to acquire the right ones unless the UE knows its current position, which is not a practical assumption. The other solution, which is more reliable and overcomes the aforementioned problem, is to extract the neighboring cell IDs using the information provided in the SIB transmitted by the main eNodeB. Since other operators transmit on different carrier frequencies, the same approach can be exploited to extract the cell IDs of the neighboring eNodeBs from other operators. Knowing the eNodeBs' cell IDs, the receiver only needs to know the position of the eNodeBs using a database or pre-mapping approaches [37, 39].

The SIB contains information about 1) the eNodeB to which it is connected, 2) inter- and intra-frequency neighboring cells from the same operator, 3) neighboring cells from other networks (UMTS, GSM, and cdma2000), and 4) other information. The SIB has 17 different forms called SIB1 to SIB17, which are transmitted in different schedules. SIB1, which is transmitted in subframe 5 of every even frame, carries scheduling information of the other SIBs. This information can be used to extract the schedule of SIB4, which has the intra-frequency neighboring cell IDs. To decode SIB1, the UE has to go through several steps. In each step, the UE needs to decode a physical channel to extract a parameter required to perform other steps.

In general, all the downlink physical channels are coded in a similar fashion before transmission, as shown in Figure 36. Although all the physical channels have the same general structure, each step in Figure 36 differs from one channel to another. Each step for the PBCH was discussed in the MIB decoding step. Further details are given in [61, 70]. In the following, the steps to retrieve information from SIB4 are summarized.

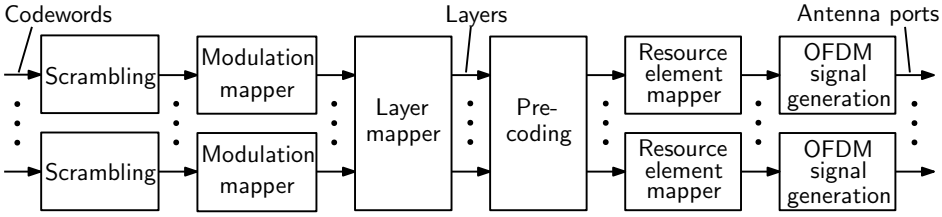


Figure 36: General structure of downlink physical channels

PCFICH Decoding: The UE first obtains the control format information (CFI) from the physical control format indicator channel (PCFICH). The CFI specifies the number of REs dedicated to the downlink control channel and can take the values 1, 2, or 3. To decode the CFI, the UE first locates the 16 REs dedicated to the PCFICH. Then, it demodulates the obtained symbols by reverting the steps in Figure 36, which results in a sequence of 32 bits. Finally, this sequence, which can be only one of three possible sequences, is mapped onto a CFI value.

PDCCH Decoding: The UE can identify the REs associated with the physical downlink control channel (PDCCH) and demodulate them by knowing the CFI. This results in a block of bits corresponding to the downlink control information (DCI) message. The DCI can be transmitted in several formats, which is not communicated with the UE. Therefore, the UE

must perform a blind search over different formats to unpack the DCI. The right format is identified by a CRC.

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

System Information Extraction and Neighboring Cells Identification: During signal acquisition, the frame timing and the eNodeB cell ID are determined. Then, the MIB is decoded and the bandwidth of the system as well as the frame number are extracted. This will allow the UE to demodulate the OFDM signal across the entire bandwidth and locate the SIB1 REs. The UE moves on to decode the SIB1 message, from which the scheduling for SIB4 is deduced and is subsequently decoded. SIB4 contains the cell ID of intra-frequency neighboring cells as well as other information pertaining to these cells. Decoding this information gives the UE the ability to simultaneously track signals from different eNodeBs and produce TOA estimates from each of these eNodeBs. Signal tracking and TOA estimation will be thoroughly discussed in the next two subsections. Figure 37 summarizes all the aforementioned system information extraction steps.

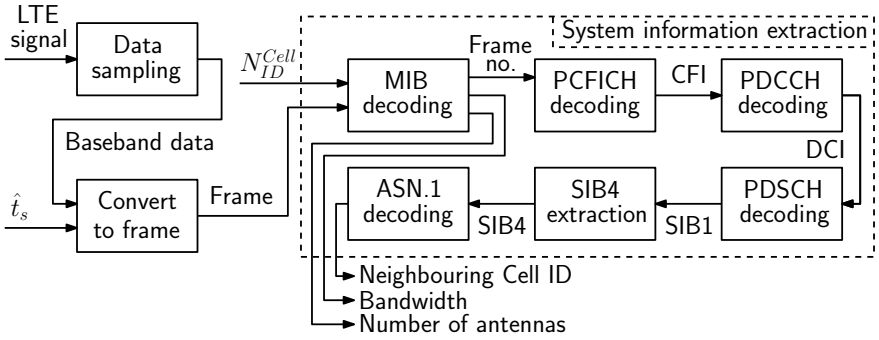


Figure 37: System information extraction block diagram

6.2.3 Tracking

After acquiring the LTE frame timing, a UE needs to keep tracking the frame timing for two reasons: 1) to produce a pseudorange measurement and 2) to continuously reconstruct the frame. The PSS and SSS are two possible sequences that a UE can exploit to track the frame timing. The PSS has only three different sequences, making it less desirable to use in tracking the frame timing because: 1) the interference from neighboring eNodeBs with the same sector IDs is high and 2) the number of eNodeBs that the UE can simultaneously track is limited. The SSS is expressible in 168 different sequences; hence, it does not suffer from the same problems as the PSS. Therefore, the SSS will be used to track the frame timing. In this subsection, the components of the tracking loops are discussed, namely an FLL-assisted PLL and a carrier-aided DLL.

FLL-Assisted PLL: The frequency reuse factor in LTE systems is set to be one, which results in high interference from neighboring cells. Under interference and dynamic stress, FLLs have better performance than PLLs. However, PLLs have significantly higher measurement accuracy compared to FLLs. An FLL-assisted PLL has both the dynamic and interference robustness of FLLs and the high accuracy of PLLs [72]. The main components of an FLL-assisted PLL are: a phase discriminator, a phase loop filter, a frequency discriminator, a frequency loop filter, and an NCO. The SSS is not modulated with other data. Therefore, an `atan2` discriminator, which remains linear over the full input error range of $\pm\pi$, could be used without the risk of introducing phase ambiguities, given by

$$e_{\mathrm{PLL},k} = \texttt{atan2}\left(Q_{p_k}, I_{p_k}\right),$$

where $S_{p_k} = I_{p_k} + jQ_{p_k}$ is the prompt correlation at time-step k. A third-order PLL can be used to track the carrier phase, with a loop filter transfer function given by

$$F_{\mathrm{PLL}}(s) = 2.4\,\omega_{n,p} + \frac{1.1\omega_{n,p}^2}{s} + \frac{\omega_{n,p}^3}{s^2}, \tag{22}$$

where $\omega_{n,p}$ is the undamped natural frequency of the phase loop, which can be related to the PLL noise-equivalent bandwidth $B_{n,\mathrm{PLL}} = 0.7845\,\omega_{n,p}$ [54]. The output of the phase loop filter is the rate of change of the carrier phase error $2\pi\hat{f}_{D,k}$, expressed in rad/s, where $\hat{f}_{D,k}$ is the Doppler frequency estimate. The phase loop filter transfer function in (22) is discretized and realized in state-space. The PLL is assisted by a second-order FLL with an `atan2` discriminator for the frequency as well. The frequency error at time-step k is expressed as

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

where $T_{\mathrm{sub}} = 10$ ms is the subaccumulation period, which is chosen to be one frame length. The transfer function of the frequency loop filter is given by

$$F_{\mathrm{FLL}}(s) = 1.414\,\omega_{n,f} + \frac{\omega_{n,f}^2}{s}, \tag{23}$$

where $\omega_{n,f}$ is the undamped natural frequency of the frequency loop, which can be related to the FLL noise-equivalent bandwidth $B_{n,\mathrm{FLL}} = 0.53\,\omega_{n,f}$ [54]. The output of the frequency loop filter is the rate of change of the angular frequency $2\pi\dot{\hat{f}}_{D,k}$, expressed in rad/s^2. It is therefore integrated and added to the output of the phase loop filter. The frequency loop filter transfer function in (23) is discretized and realized in state-space.

DLL: The carrier-aided DLL employs a non-coherent dot-product discriminator given by

$$e_{\mathrm{DLL},k} = \Gamma\left[(I_{e_k} - I_{l_k})I_{p_k} + (Q_{e_k} - Q_{l_k})Q_{p_k}\right],$$

where Γ is a normalization constant given by

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

where $S_{e_k} = I_{e_k} + jQ_{e_k}$ and $S_{l_k} = I_{l_k} + jQ_{l_k}$ are the early and late correlations, respectively, $T_c = \frac{1}{W_{SSS}}$ is the chip interval, $W_{SSS} = 63 \times 15 = 945$ kHz is the SSS bandwidth, $\mathbb{E}\{\cdot\}$ is the expectation operator, and σ^2_{IQ} is the interference-plus-noise variance. The calculation of the overall noise level including interference and channel noise is discussed in [65].

The DLL loop filter is chosen to be similar to (23), with a noise-equivalent bandwidth $B_{n,\mathrm{DLL}}$ (in Hz). The output of the DLL loop filter v_{DLL} (in s/s) is the rate of change of the SSS code phase. Assuming low-side mixing, the code start time is updated according to

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

The SSS code start time estimate is used to reconstruct the transmitted frame. Figure 38 shows the block diagram of the tracking loops, where $\omega_c = 2\pi f_c$ and f_c is the carrier frequency (in Hz). Finally, the pseudorange estimate ρ can be deduced by multiplying the code start time by the speed of light c (cf. (10)).

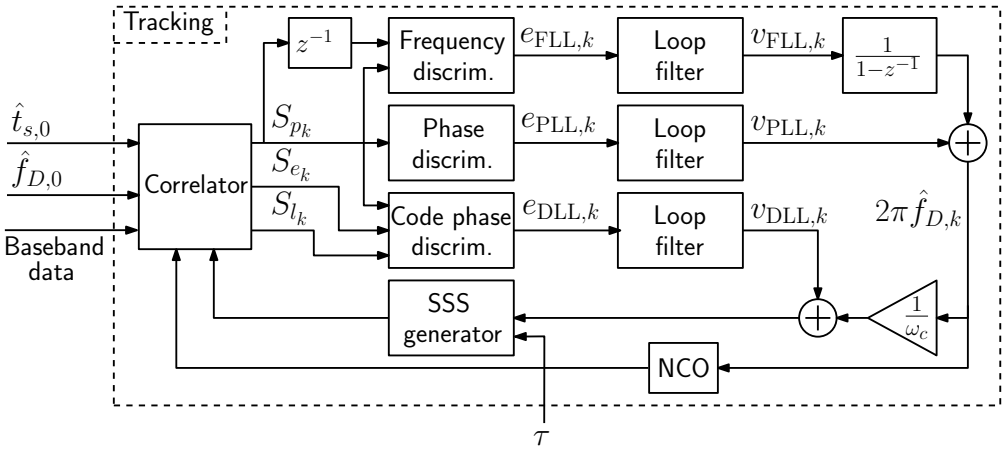


Figure 38: LTE SSS signal tracking block diagram

Figure 39 shows tracking results with real LTE signals. Here, the PLL, FLL, and DLL noise-equivalent bandwidths were set to 4, 0.2, and 0.001 Hz, respectively. To calculate the interference-plus-noise variance, the received signal was correlated with an orthogonal sequence that is not transmitted by any of the eNodeBs in the environment. Then, the average of the squared-magnitude of the correlation was assumed to be the interference-plus-noise variance. Since the receiver was stationary and its clock was driven by a GPS-disciplined oscillator (GPSDO), the Doppler frequency was stable around zero. Note that the aiding term τ is computed in the Timing Information Extraction block to improve SSS tracking. The term τ gets added to $\hat{t}_{s,k+1}$ in the SSS generator block. The calculation of τ is discussed next.

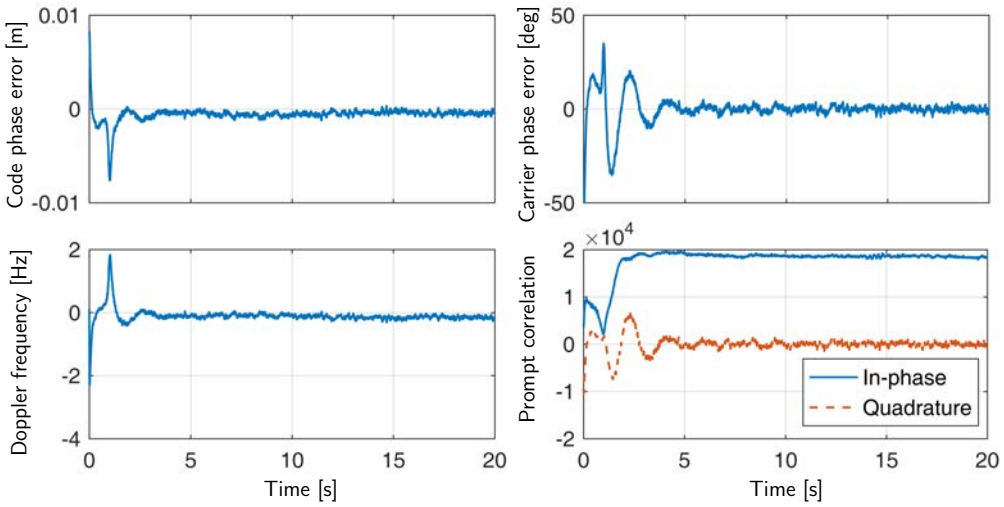


Figure 39: LTE SSS tracking results with a stationary receiver

6.2.4 Timing Information Extraction

In LTE systems, the PSS and SSS are transmitted with the lowest possible bandwidth. The ranging precision and accuracy of the SSS is analyzed in [73, 74], which shows that the SSS can provide very precise ranging resolution using conventional DLLs in an environment without multipath. However, because of its relatively low bandwidth, the SSS is extremely susceptible to multipath. To achieve more precise localization using LTE signals, the CRS can be exploited. The ranging precision of SSS and CRS in a semi-urban environment with multipath was studied experimentally in [63], which showed that CRS is more robust to multipath.

In the timing information extraction stage of the receiver, the TOA can be estimated by detecting the first peak of the channel impulse response (CIR). The CIR can be computed from the received signal model in the ith symbol, given in (19). The subscript i will be dropped in the sequel for simplicity of notation. The estimated CFR of the uth eNodeB is given by

$$\hat{\boldsymbol{H}}^{(u)}(k) = \boldsymbol{S}^{(u)^*}(k)\boldsymbol{R}(k) = \boldsymbol{H}^{(u)}(k) + \boldsymbol{V}^{(u)}(k), \quad k \in N_{CRS}^{(u)}, \tag{24}$$

where $\boldsymbol{V}^{(u)}(k) \triangleq \boldsymbol{S}^{(u)^*}(k)\boldsymbol{W}(k)$. Equation (24) is obtained using the fact that $\left|\boldsymbol{S}^{(u)}(k)\right|^2 = 1$. The CIR estimate $\hat{\boldsymbol{h}}$ is obtained by taking the IFFT of the estimated CFR, yielding

$$\hat{\boldsymbol{h}}^{(u)}(n) = \text{IFFT}\left\{\hat{\boldsymbol{H}}^{(u)}(k)\right\} = \boldsymbol{h}^{(u)}(n) + \boldsymbol{v}^{(u)}(n), \tag{25}$$

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

The TOA estimate τ is then fed back to the tracking loops. A low pass filter (e.g., a moving average filter) can be used to remove outliers in the estimated τ. Figure 40 shows the block diagram of the timing information extraction stage.

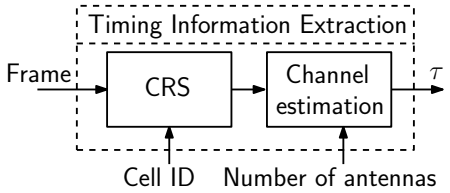


Figure 40: Timing information extraction block diagram

The first peak detection approach was implemented in [17, 64]. While this method is computationally inexpensive, the first peak of the channel impulse response cannot be detected when the multipath has a short range. An adaptive threshold approach was developed in [65] that yielded more robust performance in urban environments experiencing severe multipath. In contrast to peak detection algorithms, super resolution algorithms (SRA) can be used [5, 11], which are computationally involved. A computationally efficient receiver that deals with the shortcomings of the SRA-based and first peak detection-based approaches was proposed in [15, 19].

6.3 Code Phase Error Analysis

Subsection 6.2 presented a recipe for designing an FLL-assisted PLL with a rate-aided DLL receiver that can extract a pseudorange estimate from cellular LTE signals. This subsection analyzes the statistics of the error of the SSS code phase estimate. Recall from Subsection 6.1 that the SSS is zero padded to length N_c and an IFT is taken according to

$$s_{\text{SSS}}(t) = \begin{cases} \text{IFT}\{S_{\text{SSS}}(f)\}, & \text{for } t \in (0, T_{\text{symb}}), \\ 0, & \text{for } t \in (T_{\text{symb}}, T_{\text{sub}}), \end{cases}$$

where $S_{\text{SSS}}(f)$ is the SSS sequence in the frequency-domain, $T_{\text{symb}} = 1/\Delta f$ is the duration of one symbol, and Δf is the subcarrier spacing.

The received signal is processed in blocks, each of which spans the duration of a frame, which can be modeled as

$$r(t) = \sqrt{C} e^{j(2\pi \Delta f_D t + \Delta\phi)} \left[s_{\text{code}}(t - t_{s_k} - kT_{\text{sub}}) + d(t - t_{s_k} - kT_{\text{sub}}) \right] + n(t), \quad k = 0, 1, 2, \ldots,$$

for $kT_{\text{sub}} \leq t \leq (k+1)T_{\text{sub}}$, where $s_{\text{code}}(t) \triangleq \sqrt{\frac{T_{\text{sub}}}{W_{\text{SSS}}}} s_{\text{SSS}}(t)$; $W_{\text{SSS}} = 930$ kHz is the SSS bandwidth; C is the received signal power including antenna gains and implementation loss; t_{s_k} is the true TOA of the SSS signal; $\Delta\phi$ and Δf_D are the residual carrier phase and Doppler frequency, respectively; $n(t)$ is an additive white noise with a constant power spectral density $\frac{N_0}{2}$ Watts/Hz; and $d(t)$ is some data transmitted by the eNodeB other than the SSS, where

$$d(t) = 0 \quad \text{for } t \notin (t_{s_k}, t_{s_k} + T_{\text{symb}}).$$

Instead of the non-coherent DLL discriminator used in the design in Subsection 6.2, a coherent DLL discriminator can also be used [57, 75]. Coherent discriminators are used when

carrier phase tracking is ideal and the receiver's residual carrier phase and Doppler frequency are negligible ($\Delta\phi \approx 0$ and $\Delta f_D \approx 0$), while non-coherent discriminators are independent of carrier phase tracking. Subsections 6.3.1 and 6.3.2 analyze the statistics of the code phase error statistics with coherent and non-coherent DLL tracking, respectively.

6.3.1 Coherent DLL Tracking

Assume that the residual carrier phase and Doppler frequency are negligible, i.e., $\Delta\phi \approx 0$ and $\Delta f_D \approx 0$. Therefore, a coherent baseband discriminator may be used in the DLL. Figure 41 represents the structure of a coherent DLL that is used for tracking the code phase [55]. In what follows, the ranging precision of the DLL shown in Figure 41 is evaluated.

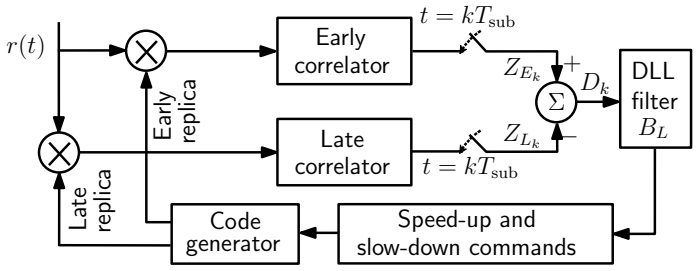


Figure 41: Structure of a DLL employing a coherent baseband discriminator to track the code phase.

In the DLL, the received signal is first correlated with the early and late locally-generated replicas of the SSS. The resulting early and late correlations are given respectively by

$$\begin{aligned} Z_{E_k} &= \frac{1}{T_{\text{sub}}} \int_{kT_{\text{sub}}}^{(k+1)T_{\text{sub}}} r(t) s_{\text{code}}(t - \hat{t}_{s_k} + \frac{t_{\text{eml}}}{2} T_c - kT_{\text{sub}}) dt \\ &\triangleq S_{E_k} + N_{E_k} \end{aligned}$$

$$\begin{aligned} Z_{L_k} &= \frac{1}{T_{\text{sub}}} \int_{kT_{\text{sub}}}^{(k+1)T_{\text{sub}}} r(t) s_{\text{code}}(t - \hat{t}_{s_k} - \frac{t_{\text{eml}}}{2} T_c - kT_{\text{sub}}) dt \\ &\triangleq S_{L_k} + N_{L_k}, \end{aligned}$$

where T_c is the chip interval, t_{eml} is the correlator spacing (early-minus-late), and $\hat{t}_{s_k}$ is the estimated TOA. The signal components of the early and late correlations, S_{E_k} and S_{L_k}, respectively, are given by

$$S_{E_k} = \sqrt{C} R\left(\Delta\tau_k - \frac{t_{\text{eml}}}{2} T_c\right), \quad S_{L_k} = \sqrt{C} R\left(\Delta\tau_k + \frac{t_{\text{eml}}}{2} T_c\right),$$

where $\Delta\tau_k \triangleq \hat{t}_{s_k} - t_{s_k}$ is the propagation time estimation error and $R(\cdot)$ is the autocorrelation

function of $s_{\text{code}}(t)$, given by

$$\begin{aligned} R(\Delta\tau) &= \frac{1}{T_{\text{sub}}} \int_0^{T_{\text{sub}}} s_{\text{code}}(t) s_{\text{code}}(t+\Delta\tau) dt \\ &= \text{sinc}(W_{SSS}\Delta\tau) - \frac{\Delta f}{W_{SSS}} \text{sinc}(\Delta f \Delta\tau) \\ &\approx \text{sinc}(W_{SSS}\Delta\tau). \end{aligned}$$

It can be shown that the noise components of the early and late correlations, N_{E_k} and N_{L_k}, respectively, are zero-mean with the following statistics

$$\begin{aligned} \text{var}\{N_{E_k}\} &= \text{var}\{N_{L_k}\} = \frac{N_0}{2T_{\text{sub}}}, & \forall k \\ \mathbb{E}\{N_{E_k} N_{L_k}\} &= \frac{N_0 R(t_{\text{eml}} T_c)}{2T_{\text{sub}}}, & \forall k \\ \mathbb{E}\{N_{E_k} N_{E_j}\} &= \mathbb{E}\{N_{L_k} N_{L_j}\} = 0, & \forall k \neq j. \end{aligned}$$

Open-Loop Analysis: The coherent baseband discriminator function is defined as

$$\begin{aligned} D_k &\triangleq Z_{E_k} - Z_{L_k} \\ &= (S_{E_k} - S_{L_k}) + (N_{E_k} - N_{L_k}). \end{aligned}$$

The signal component of the normalized discriminator function $\frac{S_{E_k} - S_{L_k}}{\sqrt{C}}$ is shown in Figure 42 for $t_{\text{eml}} = \{0.25, 0.5, 1, 1.5, 2\}$.

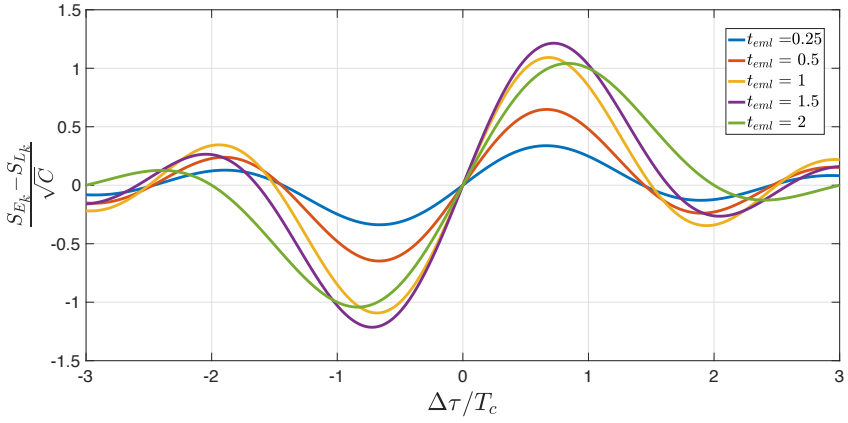


Figure 42: Output of the coherent baseband discriminator function for the SSS with different correlator spacing

It can be seen from Figure 42 that the discriminator function can be approximated by a linear function for small values of $\Delta\tau_k$, given by

$$D_k = k_{SSS}\Delta\tau_k + N_{E_k} - N_{L_k}, \tag{26}$$

where k_{SSS} is the slope of the discriminator function at $\Delta\tau_k = 0$, which is obtained by

$$\begin{aligned} k_{SSS} &= \left.\frac{\partial D_k}{\partial \Delta\tau_k}\right|_{\Delta\tau_k=0} \\ &= 4\sqrt{C}W_{SSS}\left(2\,\frac{\sin(\pi t_{\text{eml}}/2)}{\pi t_{\text{eml}}^2} - \frac{\cos(\pi t_{\text{eml}}/2)}{t_{\text{eml}}}\right). \end{aligned}$$

The mean and variance of D_k can be obtained from (26) as

$$\mathbb{E}\{D_k\} = k_{SSS}\Delta\tau_k, \tag{27}$$

$$\text{var}\{D_k\} = \frac{N_0}{T_{\text{sub}}}\big[1 - R(t_{\text{eml}}T_c)\big]. \tag{28}$$

Closed-Loop Analysis: In a rate-aided DLL, the pseudorange rate estimated by the FLL-assisted PLL is added to the output of the DLL discriminator. In general, it is enough to use a first-order loop for the DLL loop filter since the FLL-assisted PLL's pseudorange rate estimate is accurate. The closed-loop error time-update for a first-order loop is shown to be [57]

$$\Delta\tau_{k+1} = (1 - 4B_{n,\text{DLL}}T_{\text{sub}})\Delta\tau_k + K_L D_k,$$

where $B_{n,\text{DLL}}$ is the DLL noise-equivalent bandwidth and K_L is the loop gain. To achieve the desired loop noise-equivalent bandwidth, K_L must be normalized according to

$$K_L = \left.\frac{4B_{n,\text{DLL}}T_{\text{sub}}\Delta\tau_k}{\mathbb{E}\{D_k\}}\right|_{\Delta\tau_k=0}.$$

Using (27), the loop noise gain for a coherent baseband discriminator becomes $K_L = \frac{4B_{n,\text{DLL}}T_{\text{sub}}}{k_{SSS}}$.

Assuming zero-mean tracking error, i.e., $\mathbb{E}\{\Delta\tau_k\} = 0$, the variance time-update is given by

$$\text{var}\{\Delta\tau_{k+1}\} \triangleq (1 - 4B_{n,\text{DLL}}T_{\text{sub}})^2\text{var}\{\Delta\tau_k\} + K_L^2\text{var}\{D_k\}. \tag{29}$$

At steady state, $\text{var}\{\Delta\tau\} = \text{var}\{\Delta\tau_{k+1}\} = \text{var}\{\Delta\tau_k\}$; hence,

$$\begin{aligned} \text{var}\{\Delta\tau\} &= \frac{B_{n,\text{DLL}}\, g(t_{\text{eml}})}{8(1 - 2B_{n,\text{DLL}}T_{\text{sub}})W_{SSS}^2 C/N_0} \\ g(t_{\text{eml}}) &\triangleq \frac{[1 - \text{sinc}(t_{\text{eml}})]}{\left[2\frac{\sin(\pi t_{\text{eml}}/2)}{\pi t_{\text{eml}}^2} - \frac{\cos(\pi t_{\text{eml}}/2)}{t_{\text{eml}}}\right]^2}. \end{aligned} \tag{30}$$

From (30), it can be seen that the standard deviation of the ranging error is related to the correlator spacing through $g(t_{\text{eml}})$. Figure 43 shows $g(t_{\text{eml}})$ for $0 \le t_{\text{eml}} \le 2$. It can be seen that $g(t_{\text{eml}})$ is not a linear function, and it increases significantly faster when $t_{\text{eml}} > 1$. Therefore, to achieve a relatively high ranging precision, t_{eml} must be set to be less than 1. It is worth mentioning that for the GPS C/A code with an infinite bandwidth, $g(t_{\text{eml}}) = t_{\text{eml}}$.

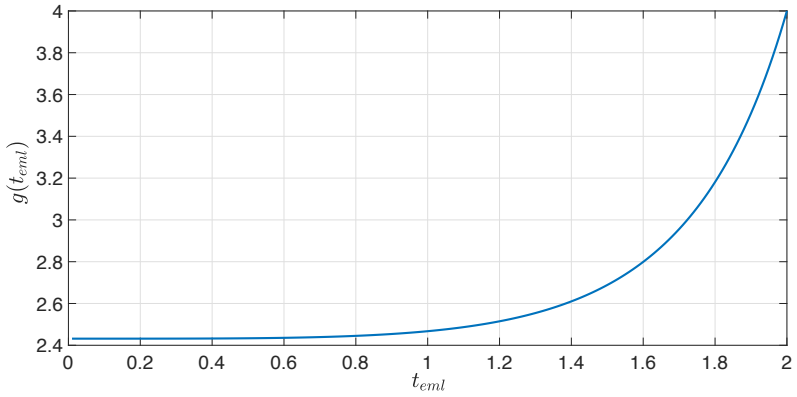


Figure 43: The standard deviation of the ranging error $\Delta\tau$ is related to the correlator spacing through $g(t_{\text{eml}})$, which is shown as a function of t_{eml}.

Figure 44 shows the pseudorange error of a coherent DLL as a function of the C/N_0, with $B_{n,\text{DLL}} = \{0.005, 0.05\}$ Hz and $t_{\text{eml}} = \{0.25, 0.5, 1, 1.5, 2\}$. It is worth mentioning that in Figure 44, the bandwidth is chosen as such to enable the reader to compare the results with the standard GPS results provided in [55].

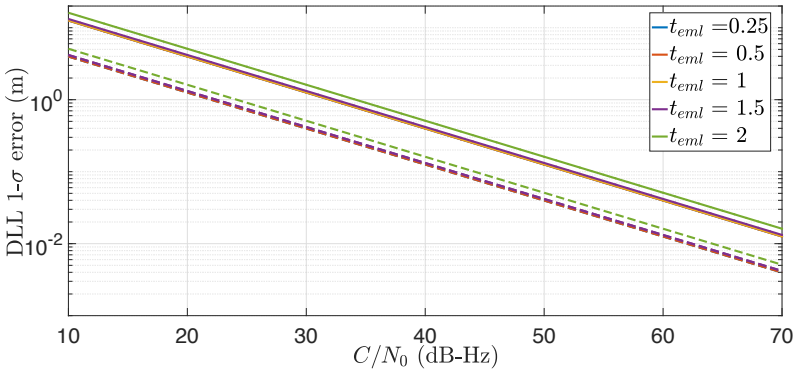


Figure 44: Coherent baseband discriminator noise performance as a function of C/N_0 for different t_{eml} values. Solid and dashed lines represent the results for $B_{n,\text{DLL}} = 0.05$ Hz and $B_{n,\text{DLL}} = 0.005$ Hz, respectively.

6.3.2 Non-Coherent DLL Tracking

In a typical DLL, the correlation of the received signal with the early, prompt, and late locally-generated signals at time $t = kT_{\text{sub}}$ are calculated according to

$$Z_{x_k} = I_{x_k} + jQ_{x_k},$$

where x can be either e, p, or l representing early, prompt, or late correlations, respectively. Figure 45 represents the general structure of the DLL. This subsection studies the code phase error with two non-coherent discriminators: dot-product and early-power-minus-late-power.

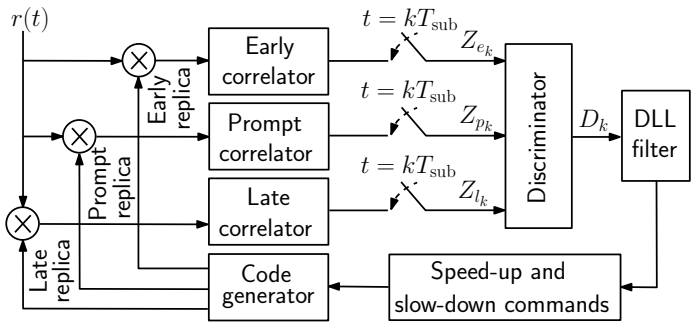


Figure 45: General structure of the DLL to track the code phase

Assuming the receiver's signal acquisition stage to provide a reasonably accurate estimate of f_D, the in-phase and quadrature components of the early, prompt, and late correlations can be written as

$$I_{x_k} = \sqrt{C}R\left(\Delta\tau_k + \kappa\frac{t_{\text{eml}}}{2}T_c\right)\cos(\Delta\phi_k) + \eta_{I,x_k},$$
$$Q_{x_k} = \sqrt{C}R\left(\Delta\tau_k + \kappa\frac{t_{\text{eml}}}{2}T_c\right)\sin(\Delta\phi_k) + \eta_{Q,x_k},$$

where x is e, p, or l and κ is -1, 0, or 1 for early, prompt, and late correlations, respectively; t_{eml} is the correlator spacing (early-minus-late); $\Delta\tau_k \triangleq \hat{t}_{s_k} - t_{s_k}$ is the propagation time estimation error; $\hat{t}_{s_k}$ and t_{s_k} are the estimated and the true TOA, respectively; and $R(\Delta\tau) \approx \text{sinc}(W_{\text{SSS}}\Delta\tau)$ is the autocorrelation function of $s_{\text{code}}(t)$.

It can be shown that the noise components η_{I,x_k} and η_{Q,x_k} of the correlations have: 1) uncorrelated in-phase and quadrature samples, 2) uncorrelated samples at different time, 3) zero-mean, and 4) the following statistics

$$\text{var}\{\eta_{I,x_k}\} = \text{var}\{\eta_{Q,x_k}\} = \frac{N_0}{4T_{\text{sub}}} \tag{31}$$
$$\mathbb{E}\{\eta_{I,e_k}\eta_{I,l_k}\} = \mathbb{E}\{\eta_{Q,e_k}\eta_{Q,l_k}\} = \frac{N_0 R(t_{\text{eml}}T_c)}{4T_{\text{sub}}}$$
$$\mathbb{E}\{\eta_{I,x'_k}\eta_{I,p_k}\} = \mathbb{E}\{\eta_{Q,x'_k}\eta_{Q,p_k}\} = \frac{N_0 R(\frac{t_{\text{eml}}}{2}T_c)}{4T_{\text{sub}}}, \tag{32}$$

where x' is e or l.

Open-Loop Analysis: The open-loop statistics of the code phase error using dot-product and early-power-minus-late-power discriminators are analyzed next.

Dot-Product Discriminator The dot-product discriminator function is defined as

$$\begin{aligned} D_k &\triangleq (I_{e_k} - I_{l_k})I_{p_k} + (Q_{e_k} - Q_{l_k})Q_{p_k} \\ &\triangleq S_k + N_k, \end{aligned}$$

where S_k is the signal component of the dot-product discriminator given by

$$S_k = CR(\Delta\tau)\left[R\left(\Delta\tau - \frac{t_{\text{eml}}}{2}T_c\right) - R\left(\Delta\tau + \frac{t_{\text{eml}}}{2}T_c\right)\right],$$

and N_k is the noise component of the discriminator function, which has zero-mean. Figure 46(a) shows the normalized S_k/C for $t_{\text{eml}} = \{0.25, 0.5, 1, 1.5, 2\}$. It can be seen that the signal component of the discriminator function is non-zero for $\Delta\tau/T_c > (1 + t_{\text{eml}}/2)$, which is in contrast to being zero for GPS C/A code with infinite bandwidth. This is due to the sinc autocorrelation function of the SSS versus the triangular autocorrelation function of the GPS C/A code.

For small values of $\Delta\tau_k$, the discriminator function can be approximated by a linear function according to

$$D_k \approx k_{\text{SSS}}\Delta\tau_k + N_k, \tag{33}$$

where $k_{\text{SSS}} \triangleq \frac{\partial D_k}{\partial \Delta\tau_k}\Big|_{\Delta\tau_k=0}$ and is given by

$$k_{\text{SSS}} = 4CW_{\text{SSS}}\left[\frac{\text{sinc}\left(\frac{t_{\text{eml}}}{2}\right) - \cos\left(\frac{\pi t_{\text{eml}}}{2}\right)}{t_{\text{eml}}}\right]. \tag{34}$$

The mean and variance of D_k are calculated to be

$$\mathbb{E}\{D_k\} = k_{\text{SSS}}\Delta\tau_k, \tag{35}$$

$$\begin{aligned}\text{var}\{D_k\} &= \text{var}\{N_k\}\big|_{\Delta\tau_k=0} \\ &= \left(\frac{N_0^2}{4T_{\text{sub}}^2} + \frac{CN_0}{2T_{\text{sub}}}\right)\big[\,1 - R(t_{\text{eml}}T_c)\,\big].\end{aligned} \tag{36}$$

Early-Power-Minus-Late-Power Discriminator The early-power-minus-late-power discriminator function is defined as

$$\begin{aligned}D_k &\triangleq I_{e_k}^2 + Q_{e_k}^2 - I_{l_k}^2 - Q_{l_k}^2 \\ &\triangleq S_k + N_k,\end{aligned}$$

where S_k can be shown to be

$$S_k = C\left[R^2\left(\Delta\tau - \frac{t_{\text{eml}}}{2}T_c\right) - R^2\left(\Delta\tau + \frac{t_{\text{eml}}}{2}T_c\right)\right],$$

and N_k is the noise component of the discriminator function, which has zero-mean. Figure 46(b) shows the normalized S_k/C of the early-power-minus-late-power discriminator function for $t_{\text{eml}} = \{0.25, 0.5, 1, 1.5, 2\}$.

The discriminator function can be approximated by a linear function for small values of $\Delta\tau_k$ (cf. (33)) with

$$k_{\mathrm{SSS}} = 8CW_{\mathrm{SSS}}R\left(\frac{t_{\mathrm{eml}}}{2}T_c\right)\left[\frac{\mathrm{sinc}\left(\frac{t_{\mathrm{eml}}}{2}\right)-\cos\left(\frac{\pi t_{\mathrm{eml}}}{2}\right)}{t_{\mathrm{eml}}}\right]. \tag{37}$$

The mean and variance of D_k are calculated to be

$$\mathbb{E}\{D_k\} = k_{\mathrm{SSS}}\Delta\tau_k, \tag{38}$$

$$\mathrm{var}\{D_k\} = \frac{N_0^2}{2T_{\mathrm{sub}}^2}\left[1-R^2\left(t_{\mathrm{eml}}T_c\right)\right]+\frac{2CN_0}{T_{\mathrm{sub}}}R^2\left(\frac{t_{\mathrm{eml}}}{2}T_c\right)\left[1-R\left(t_{\mathrm{eml}}T_c\right)\right]. \tag{39}$$

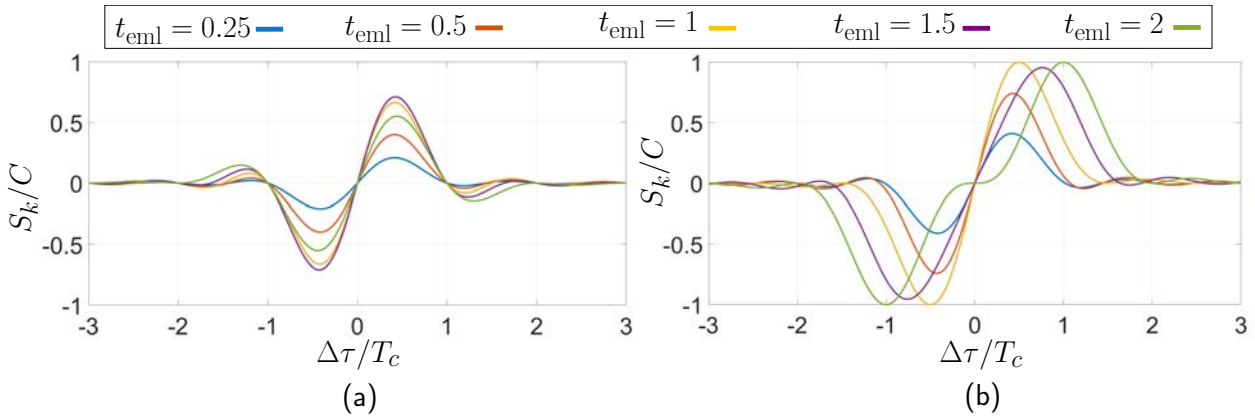


Figure 46: Normalized signal component of non-coherent discriminator functions: (a) dot-product and (b) early-power-minus-late-power for different correlator spacings

Closed-Loop Analysis: An FLL-assisted PLL produces reasonably accurate pseudorange rate estimate, making first-order DLLs sufficient. At steady-state, $\mathrm{var}\{\Delta\tau\} = \mathrm{var}\{\Delta\tau_{k+1}\} = \mathrm{var}\{\Delta\tau_k\}$ and using (29) yields

$$\mathrm{var}\{\Delta\tau\} = \frac{K_L^2}{8B_{n,\mathrm{DLL}}T_{\mathrm{sub}}(1-2B_{n,\mathrm{DLL}}T_{\mathrm{sub}})}\mathrm{var}\{D_k\}. \tag{40}$$

In the following, the closed-loop statistics of the code phase error are derived for a dot-product and an early-power-minus-late-power discriminator functions.

Dot-Product Discriminator The closed-loop code phase error in a dot-product discriminator can be obtained by substituting (34) and (36) into (40), yielding

$$\mathrm{var}\{\Delta\tau\} = \frac{B_{n,\mathrm{DLL}}\,g_\alpha(t_{\mathrm{eml}})\left(1+\frac{1}{2T_{\mathrm{sub}}C/N_0}\right)}{16(1-2B_{n,\mathrm{DLL}}T_{\mathrm{sub}})W_{\mathrm{SSS}}^2C/N_0} \tag{41}$$

$$g_\alpha(t_{\mathrm{eml}}) \triangleq \frac{t_{\mathrm{eml}}^2\left[1-R(t_{\mathrm{eml}}T_c)\right]}{\left[\mathrm{sinc}\left(t_{\mathrm{eml}}/2\right)-\cos\left(\pi t_{\mathrm{eml}}/2\right)\right]^2}. \tag{42}$$

Figure 47(a) shows $g_\alpha(t_{\text{eml}})$ for $0 \leq t_{\text{eml}} \leq 2$. It can be seen that $g_\alpha(t_{\text{eml}})$ is a nonlinear function and increases significantly faster for $t_{\text{eml}} > 1$. Figure 48 shows the standard deviation of the pseudorange error for a dot-product DLL as a function of C/N_0 with $t_{\text{eml}} = 1$ and $B_{n,\text{DLL}} = \{0.005, 0.05\}$ Hz, chosen as such in order to enable comparison with the GPS pseudorange error standard deviation provided in [55, 73].

Early-Power-Minus-Late-Power Discriminator The variance of the ranging error in an early-power-minus-late-power discriminator can be obtained by substituting (37) and (39) into (40), yielding

$$\text{var}\{\Delta\tau\} = \frac{B_{n,\text{DLL}}\left[\frac{g_\beta(t_{\text{eml}})}{(C/N_0)} + 4T_{\text{sub}}g_\alpha(t_{\text{eml}})\right]}{64(1-2B_{n,\text{DLL}}T_{\text{sub}})T_{\text{sub}}W_{\text{SSS}}^2 C/N_0} \tag{43}$$

$$g_\beta(t_{\text{eml}}) \triangleq \frac{1+R\left(t_{\text{eml}}T_c\right)}{R^2\left(\frac{t_{\text{eml}}}{2}T_c\right)}g_\alpha(t_{\text{eml}}). \tag{44}$$

Figure 47(b) shows $g_\beta(t_{\text{eml}})$ for $0 \leq t_{\text{eml}} \leq 2$. It can be seen that $g_\beta(t_{\text{eml}})$ is significantly larger than $g_\alpha(t_{\text{eml}})$. To reduce the ranging error due to $g_\beta(t_{\text{eml}})$, t_{eml} must be chosen to be less than 1.5.

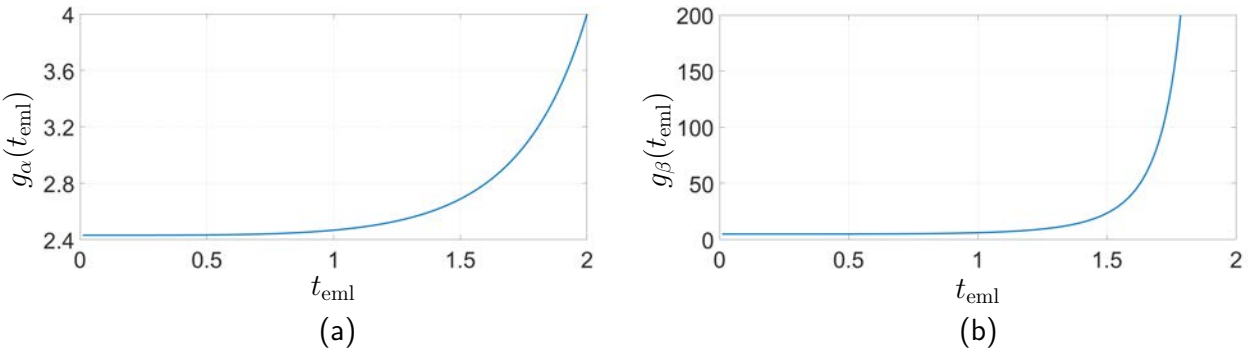


Figure 47: The variance of the ranging error in a dot-product discriminator is related to the correlator spacing through $g_\alpha(t_{\text{eml}})$ shown in (a), while for an early-power-minus-late-power discriminator it is related through $g_\alpha(t_{\text{eml}})$ and $g_\beta(t_{\text{eml}})$ shown in (b).

Figure 48 shows the standard deviation of the pseudorange error for an early-power-minus-late-power discriminator DLL as a function of C/N_0 with $B_{n,\text{DLL}} = \{0.05, 0.005\}$ Hz and $t_{\text{eml}} = 1$. It can be seen that decreasing the loop bandwidth decreases the standard deviation of the pseudorange error. However, very small values of $B_{n,\text{DLL}}$ may cause the DLL to lose lock in a highly dynamic scenario.

6.3.3 Code Phase Error Analysis in Multipath Environments

Subsections 6.3.1 and 6.3.2 evaluated the ranging accuracy with coherent and non-coherent baseband discriminators in the presence of additive white Gaussian noise. However, multipath is another significant source of error, particularly for ground receivers. Multipath analysis and mitigation for navigation with LTE signals is an ongoing area of research [3, 11, 15, 19, 63, 73, 74, 76–79].

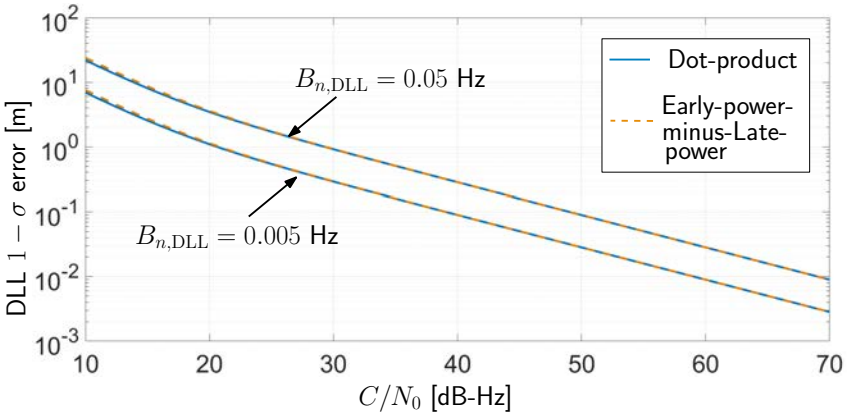


Figure 48: DLL performance as a function of C/N_0 for non-coherent discriminators: dot-product discriminator (solid line) and early-power-minus-late-power discriminator (dashed line), $B_{n,\mathrm{DLL}} = \{0.05, 0.005\}$ Hz, and $t_{\mathrm{eml}} = 1$.

6.4 Cellular LTE Navigation Experimental Results

This subsection presents experimental results for navigation with cellular LTE signals. Subsection 6.4.1 analyzes the pseudorange obtained with the SSS and CRS signals produced by the receiver discussed in Section 6.2. Subsections 6.4.2 and 6.4.3 present navigation results with aerial and ground vehicles, respectively.

6.4.1 Pseudorange Analysis

This subsection evaluates the pseudorange obtained by the receiver discussed in Subsection 6.2. To this end, the pseudorange variation from GPS is compared with the pseudorange variation due to 1) only tracking the SSS and 2) aiding the SSS tracking loops with the CRS. The receiver was mounted on a ground vehicle and was tuned to the carrier frequencies of 1955 and 2145 MHz, which are allocated to the U.S. LTE providers AT&T and T-Mobile, respectively [63]. The transmission bandwidth was measured to be 20 MHz. The vehicle-mounted receiver traversed a total trajectory of 2 km while listening to the 2 eNodeBs simultaneously as illustrated in Figure 49. The position states of the eNodeBs were mapped beforehand. Figures 50 and 51 show (a) the change in the pseudoranges between the receiver and the 2 eNodeBs, (b) the error between the GPS pseudorange and the LTE pseudoranges, and (c) the distance error cumulative distribution function (CDF) of the LTE pseudoranges.

The error in the pseudorange obtained by tracking the SSS is mainly due to multipath. The estimated CIR at $t = 13.04$ s for eNodeB 1 and $t = 8.89$ s and $t = 40.5$ s for eNodeB 2 show several peaks due to multipath, which are dominating the line-of-sight (LOS) peak. These peaks contributed a pseudorange error of around 330 m at $t = 13.04$ s for eNodeB 1 and around 130 m at $t = 8.89$ s for eNodeB 2. These results highlight the importance of utilizing the CRS signals to correct for multipath-induced errors.

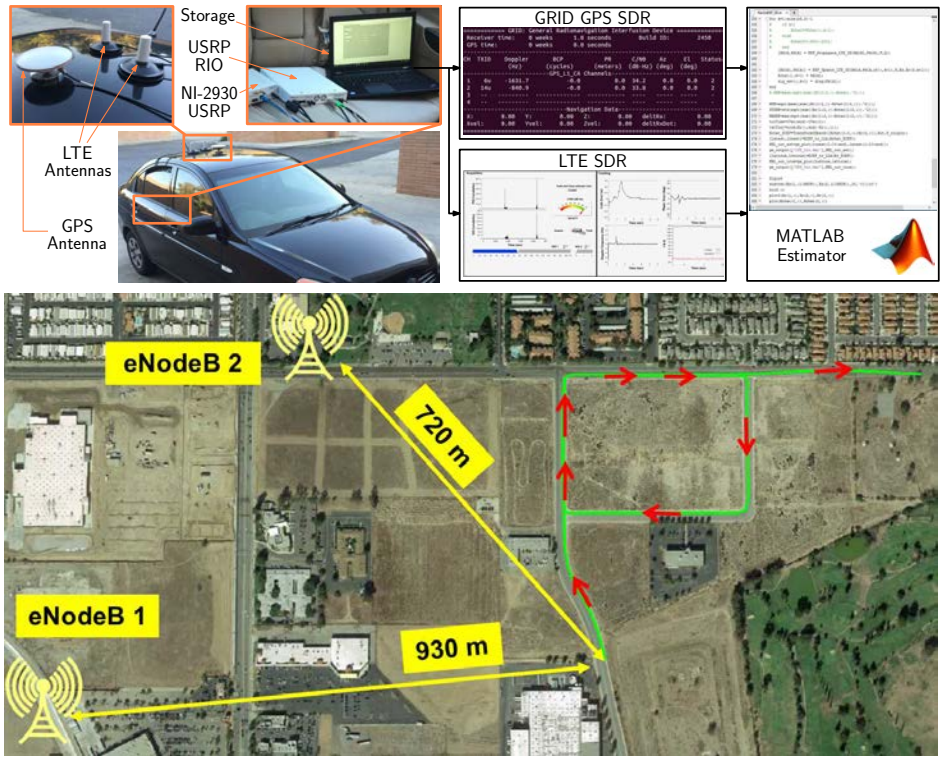


Figure 49: LTE environment layout and experimental hardware setup

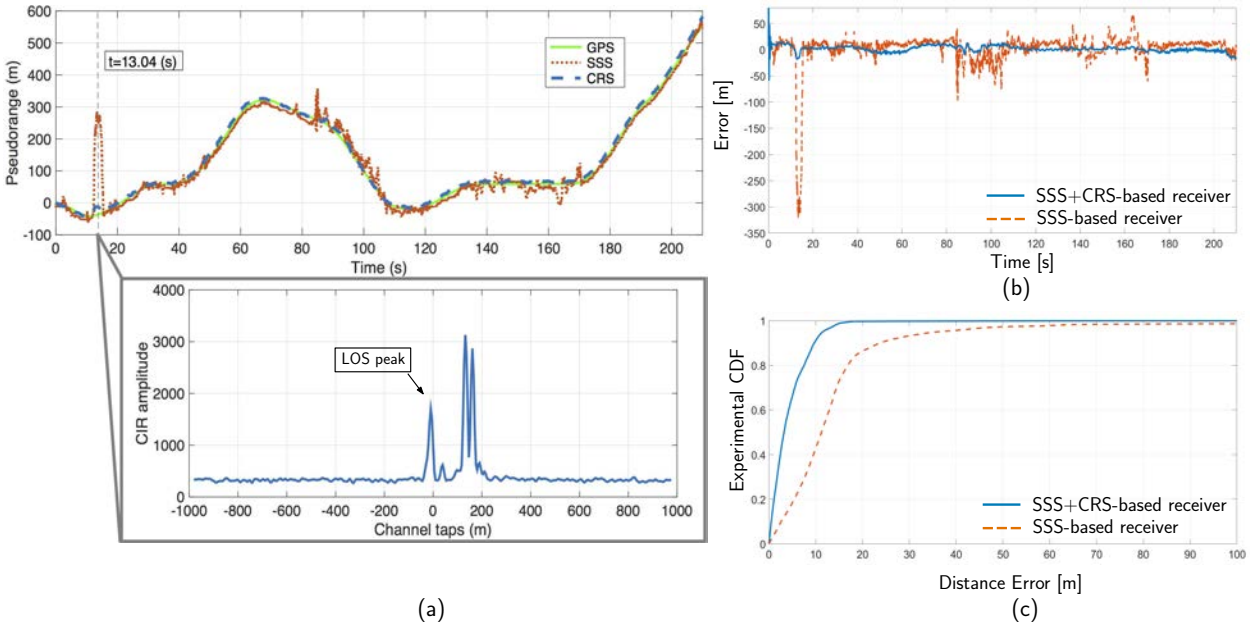


Figure 50: (a) Estimated change in pseudorange and estimated CIR at $t = 13.04$ s for eNodeB 1. The change in the pseudorange was calculated using: 1) SSS pseudoranges, 2) SSS+CRS pseudoranges, and 3) true ranges obtained using GPS. (b) Pseudorange error between 1) GPS and SSS and 2) GPS and SSS+CRS. (c) CDF of the error in (b).

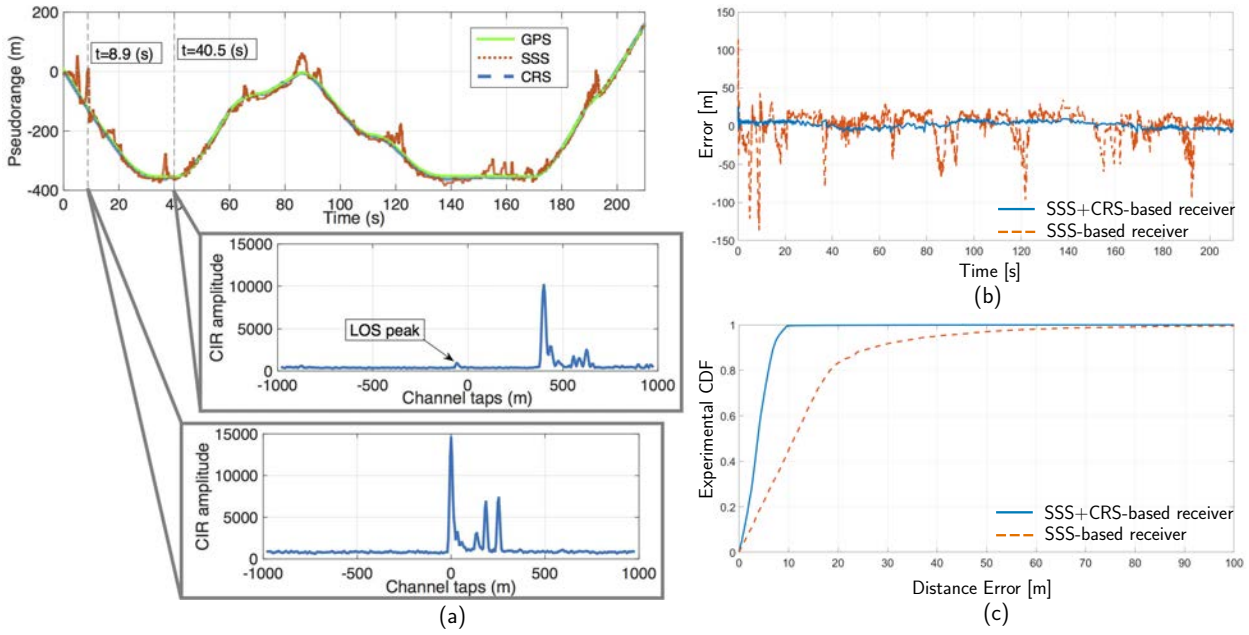


Figure 51: (a) Estimated change in pseudorange and estimated CIR at $t = 8.89$ s and $t = 40.5$ s for eNodeB 2. The change in the pseudorange was calculated using: 1) SSS pseudoranges, 2) CRS pseudoranges, and 3) true ranges obtained using GPS. (b) Pseudorange error between 1) GPS and SSS and 2) GPS and SSS+CRS. (c) CDF of the error in (b).

6.4.2 Ground Vehicle Navigation

A car was equipped with the cellular LTE navigation receiver discussed in Subsection 6.2. The receiver was tuned to the cellular carrier frequencies 739 MHz and 1955 MHz, which are used by the U.S. cellular provider AT&T. The PLL, FLL, and DLL noise equivalent-bandwidths were set to 4, 0.2, and 0.001 Hz, respectively. The adaptive threshold approach proposed in [65] was adopted to mitigate multipath.

All measurements and trajectories were projected onto a 2–D plane. It was assumed that the receiver had access to GPS, and GPS was cut off at the start time of the experiment. Therefore, the EKF's states were initialized with the values obtained from the GPS navigation solution. The standard deviation of the initial uncertainty of position and velocity were set to be 5 m and 0.01 m/s, respectively [55]. The standard deviation of the initial uncertainty of the clock bias and drift were set to be 0.1 m and 0.01 m/s, which were obtained empirically. The clock oscillators were modeled as oven-controlled crystal oscillators (OCXOs) with $S_{\tilde{w}_{\delta t_s}} \approx h_0/2$ and $S_{\tilde{w}_{\dot{\delta} t_s}} \approx 2\pi^2 h_{-2}$, where $h_0 = 2.6 \times 10^{-22}$ and $h_{-2} = 4 \times 10^{-26}$. The power spectral densities $\tilde{q}_x$ and $\tilde{q}_y$ were set to 0.2 $\mathrm{m}^2/\mathrm{s}^3$ and measurement noise covariance was set to be 10 m^2, which were obtained empirically. The vehicle was listening to 6 eNodeBs whose position states were mapped beforehand. The cell IDs of the eNodeBs were 216, 489, 457, 288, 232, 152, respectively. The first 3 eNodeBs had a 20 MHz transmission bandwidth and the rest of the eNodeBs had a 10 MHz transmission bandwidth. The C/N_0 for all received eNodeB signals was between 50 and 68 dB-Hz. The experimental hardware

setup, the environment layout, and the true and estimated navigator trajectories are shown in Figure 52. The ground-truth trajectory was obtained from the GRID GPS SDR [58].

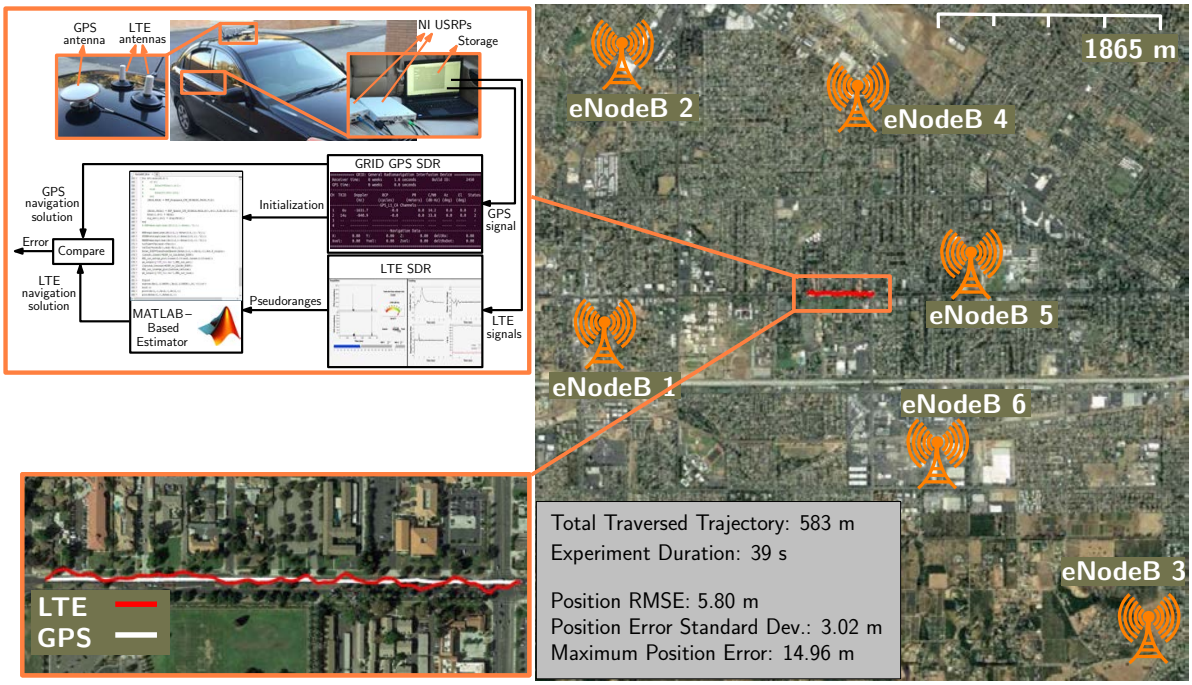


Figure 52: (a) Experimental hardware and software setup and environment layout in downtown Riverside, California showing eNodeBs' locations and the traversed trajectory as estimated by GPS and LTE signals. Image: Google Earth.

6.4.3 Aerial Vehicle Navigation

A UAV was equipped with the cellular LTE navigation receiver discussed in Subsection 6.2. When a UAV flies high enough, the received signal to the UAV does not experience multipath from the surrounding environment, except from the UAV's body. Here, the multipath effect from the UAV's body is negligible; therefore, only tracking the SSS yields good results and the CRS was not used. This significantly decreases the computational burden in the receiver. It also reduces the need for high sampling rate, which results in lower hardware cost and size. The receiver was tuned to the cellular carrier frequency of 1955 MHz, which is used by the U.S. cellular provider AT&T.

Over the course of the experiment, the UAV was flying at an altitude of 40 m. The receiver was listening to 3 eNodeBs, each of which had 2 transmitting antennas with 20 MHz transmission bandwidth. The positions of the eNodeBs were mapped prior to the experiment with approximately 2 m accuracy. All measurements and trajectories were projected onto a 2–D plane. Subsequently, only the horizontal position of the receiver was estimated. It was assumed that the receiver had access to GPS, and GPS was cut off at the start time of the experiment. Therefore, the EKF's states were initialized with the values obtained from the GPS navigation solution. The EKF process noise and measurement noise covariances

were set in a similar manner to the ground vehicle navigation experiment. The environment layout as well as the true and estimated receiver trajectories are shown in Figure 53. It can be seen from Figure 53 that the navigation solution obtained from LTE signals follows closely the GPS navigation solution. The ground-truth trajectory was obtained from the GRID GPS SDR [58].

Figure 53: Experimental hardware setup and environment layout in Riverside, California showing eNodeBs' locations and the traversed trajectory as estimated by GPS and LTE signals. Image: Google Earth.

In an urban environment, the pseudoranges received by a ground vehicle will suffer from more multipath-induced error compared to pseudoranges received by a UAV with LOS conditions. However, this comparison can be made as long as the ground vehicle and UAV are navigating in the same environment, using the same eNodeBs, and following the same trajectories, except for one being on the ground while the other being airborne. In the results presented in Figures 52 and 53, the ground vehicle was equipped with a better USRP than the one on the UAV, due to payload limitations. Consequently, the LTE receiver on-board the ground vehicle was able to listen to more eNodeBs than the receiver on-board the UAV, providing the former with more measurements at a better geometric diversity than the latter. Moreover, the UAV did not use the CRS signals, which were used by the ground vehicle to aid its SSS tracking loops. These aforementioned factors resulted in the position root mean squared error (RMSE) of the ground vehicle being less than the position RMSE of the UAV.

7 BTS Sector Clock Bias Mismatch

A typical 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 and 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, 22]. In the following subsections, a stochastic dynamic model for the observed clock bias mismatch for different sectors of the same BTS cell is derived.

7.1 Sector Clock Bias Mismatch Detection

In order to demonstrate the presence of the discrepancy between sectors' clock biases, a cellular CDMA receiver was placed at the border of two sectors of an ith BTS cell corresponding to the U.S. cellular provider Verizon Wireless 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 Figure 54.

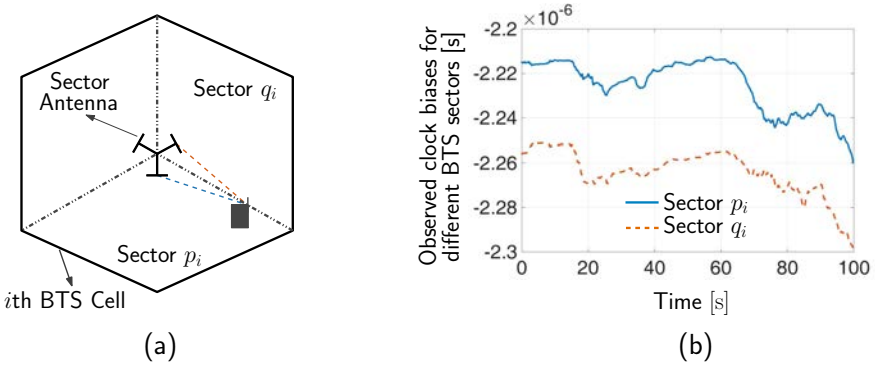


Figure 54: (a) A cellular CDMA receiver placed at the border of two sectors of a BTS cell, making pseudorange observations on both sector antennas simultaneously. The receiver has knowledge of its own states and has knowledge of the BTS position states. (b) Observed BTS clock bias corresponding to two different sectors from a real BTS.

Figure 54 suggests that the clock biases $\delta t_{s_i}^{(p_i)}$ and $\delta t_{s_i}^{(q_i)}$ can be related through

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

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

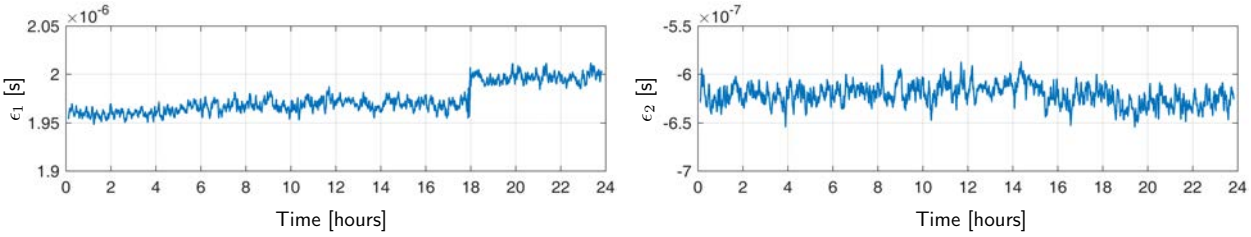
$$1_{q_i}(p_i) = \begin{cases} 1, & \text{if } p_i = q_i, \\ 0, & \text{otherwise,} \end{cases}$$

is the indicator function.

Note that 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 [80]. 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 $-10\mu\text{s} \leq \delta t_{s_i}^{(p_i)}(k) \leq 10\mu\text{s}$ and $-10\mu\text{s} \leq \delta t_{s_i}^{(q_i)}(k) \leq 10\mu\text{s}$. Therefore, ϵ_i will be within 20μs 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 Figure 55(a)–(b) for two different BTSs. Both BTSs pertained 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 Figure 55 that $|\epsilon_i|$ is bounded by approximately 2.02μs and 0.65μs, respectively, which is well below 20 μs. In the following subsection, a stochastic dynamic model for ϵ_i is identified.



(a) (b)

Figure 55: 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 pertained 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.

7.2 Sector Clock Bias Discrepancy Model Identification

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 of order n, which can be expressed as [81]

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

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 $0 < \beta_i << 1$ (on the order of 8×10^{-5} to 3×10^{-4}). This implies that ϵ_i is exponentially correlated with the continuous-time dynamics given by

$$\dot{\epsilon}_i(t) = -\alpha_i \epsilon_i(t) + \tilde{\zeta}_i(t), \tag{45}$$

where $\alpha_i \triangleq \frac{1}{\tau_i}$, τ_i is the time constant of the discrepancy dynamic model, and $\tilde{\zeta}_i$ is a continuous-time white process with variance $\sigma_{\tilde{\zeta}_i}^2$. Discretizing (45) at a sampling period

T yields the discrete-time model

$$\epsilon_i(k+1) = \phi_i\, \epsilon_i(k) + \zeta_i(k), \tag{46}$$

where $\phi_i = e^{-\alpha_i T}$. The variance of ζ_i is given by $\sigma^2_{\zeta_i} = \frac{\sigma^2_{\zeta_i}}{2\alpha_i}\left(1 - e^{-2\alpha_i T}\right)$. Figure 56 shows an experimental realization of ϵ_i and the corresponding residual ζ_i.

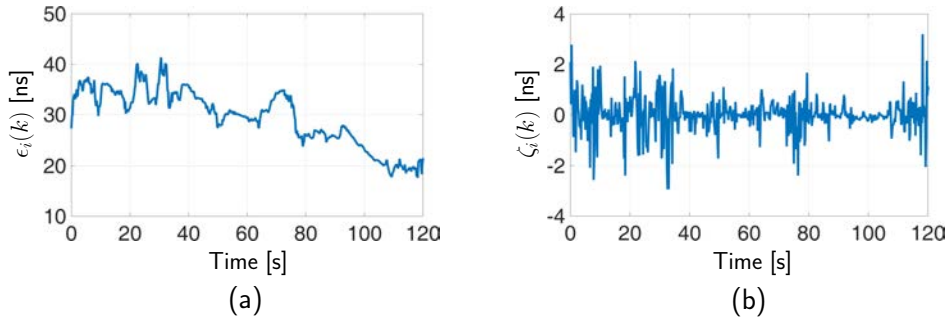


Figure 56: (a) A realization of the discrepancy ϵ_i between the observed clock biases of two BTS sectors and (b) the corresponding residual ζ_i.

Residual analysis is used to validate the model (46). 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 (46), i.e., $e_i \triangleq \epsilon_i' - \epsilon_i$, were computed [81]. Figure 57 shows the acf and psd of e_i computed from a different realization of ϵ_i. The psd was computed using Welch's method [82]. It can be seen from Figure 57 that the residual error e_i is nearly white; hence, the identified model is capable of describing the true system.

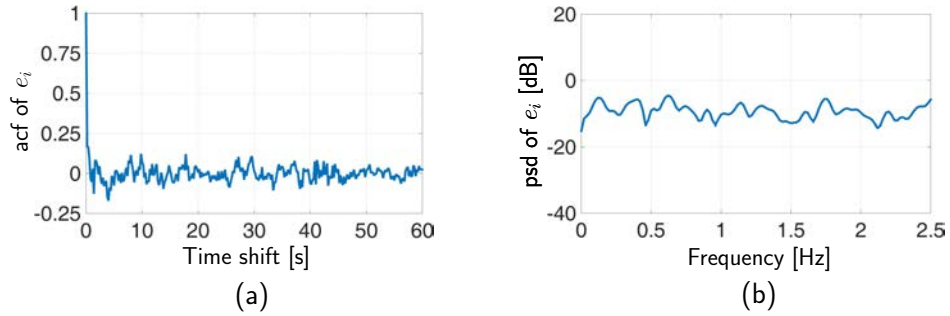


Figure 57: The (a) acf and (b) psd of e_i with a sampling frequency of 5 Hz.

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

$$p(\zeta_i) = \frac{1}{2\lambda_i} \exp\left(-\frac{|\zeta_i - \mu_i|}{\lambda_i}\right), \tag{47}$$

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 $p(\zeta_i)$ [83]. Figure 58 shows the actual distribution of the data along with the estimated pdf. For comparison purposes, a Gaussian and Logistic pdf fits obtained via an MLE are also plotted.

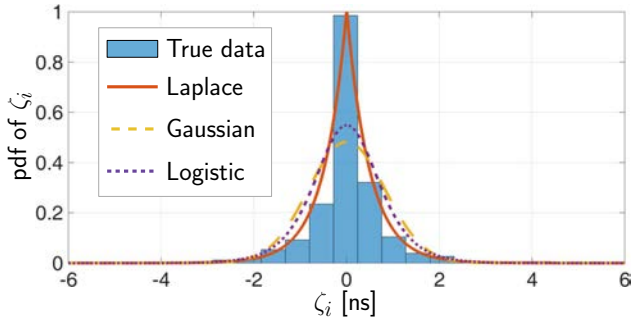


Figure 58: Distribution of ζ_i from experimental data and the estimated Laplace pdf via MLE. For comparison, a Gaussian (dashed) and Logistic (dotted) pdf fits are also plotted.

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 $2\lambda_i^2$.

The identified model was consistent at different locations, at different times, and for different cellular providers. To demonstrate this, tests were performed twice at 3 different locations. There is a six-day period between each test at each of the 3 locations. A total of 3 carrier frequencies were considered, two of them pertaining to Verizon Wireless and one to Sprint. The test scenarios are summarized in Table 5 and Figure 59. The date field in Table 5 shows the date in which the test was conducted in MM/DD/YYYY format.

Table 5: 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

Figure 60 shows six realizations, 5 minutes each, of the discrepancy corresponding to Tests (a)–(f) in Table 5. It can be seen from Figure 60 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. The process noise driving the discrepancy was calculated from (45) with $\phi_i = e^{-\alpha_i T}$ 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 Figure 60 exhibited very quick de-correlation, validating that ζ_i is approximately a white sequence [12]. Also, a histogram of each realization of ζ_i along with the estimated pdf $p(\zeta_i)$ demonstrated that that the Laplace pdf consistently matched the experimental data [12].

Figure 59: Locations of the cellular CDMA BTSs: Colton, California; Riverside, California; and the University of California, Riverside (UCR). Map data: Google Earth.

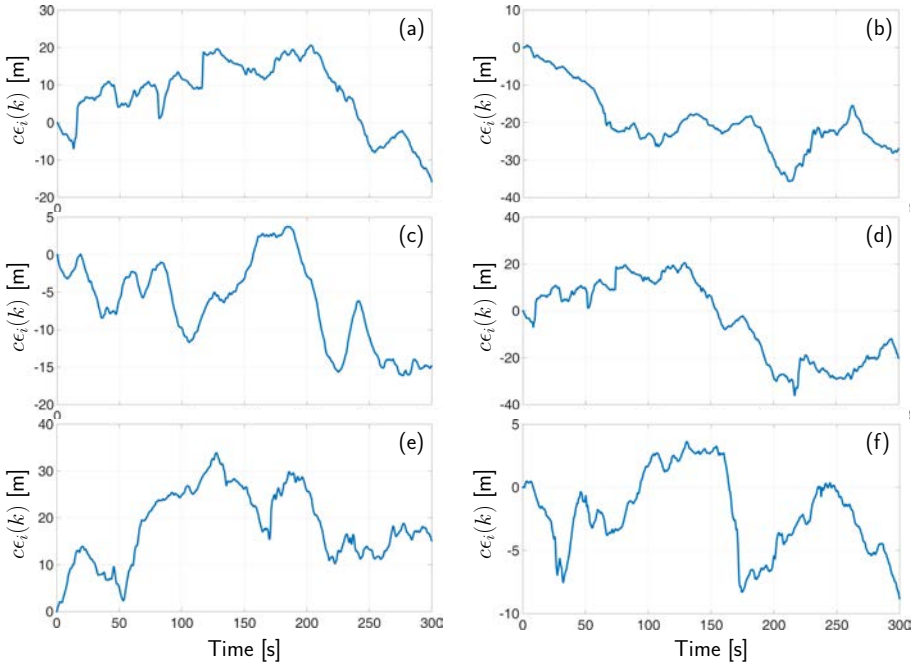


Figure 60: Six realizations, five minutes each, of the sector clock bias discrepancy for the tests in Table 5.

7.3 PNT Estimation Performance in the Presence of Clock Bias Discrepancy

The clock bias discrepancy will degrade the navigation solution in two scenarios: 1) whenever the receiver is receiving signals from both sector antennas within a BTS cell and 2) whenever the receiver is exchanging pseudorange measurements with another receiver in a different sector (e.g., in a mapper/navigator framework or a collaborative navigation framework). A practical upper bound on the introduced error in the navigation solution due to this discrepancy as well as theoretical lower bounds on the estimation error covariance for static and batch estimators are derived in [25].

8 Multi-Signal Navigation: GNSS and Cellular

The quality of the GNSS navigation solution is determined by both the pseudorange measurement noise statistics and the spatial geometry of GNSS SVs. GNSS position solutions suffer from a relatively high vertical estimation uncertainty due to the lack of GNSS SV angle diversity (SVs are usually above the receiver). To address this, an external sensor (e.g., a barometer) is typically fused with a GNSS receiver. Cellular towers are abundant and available at varying geometric configurations unattainable by GNSS SVs. For example, BTSs could be below an aerial vehicle-mounted receiver. Therefore, fusing cellular signals with GNSS signals would yield a more accurate navigation solution, particularly in the vertical direction. This section highlights the benefits of fusing cellular signals with GNSS signals.

This section is organized as follows. Subsection 8.1 studies the dilution of precision (DOP) reduction due to fusing cellular signals with GNSS signals. Subsection 8.2 shows experimental results with ground and aerial vehicles.

8.1 Dilution of Precision Reduction

To study the DOP reduction due to fusing cellular signals with GNSS signals, consider an environment comprising a receiver making pseudorange measurements on M GNSS SVs and N terrestrial cellular BTSs. The pseudorange measurements are fused through a weighted nonlinear least-squares (WNLS) estimator to estimate the states of the receiver $\boldsymbol{x}_r = \left[\boldsymbol{r}^\mathsf{T}, c\delta t_r\right]^\mathsf{T}$, where $\boldsymbol{x}_r$ and δt_r are the 3–D position and clock bias of the receiver, respectively, and c is the speed of light. To simplify the discussion, assume that the measurement noise is independent and identically distributed across all channels with variance σ^2. If the measurement noise was not independent and identically distributed, the weighted DOP factors must be considered [84]. The estimator produces an estimate $\hat{\boldsymbol{x}}_r$ and an associated estimation error covariance matrix $\mathbf{P} = \sigma^2 \left(\mathbf{H}^\mathsf{T}\mathbf{H}\right)^{-1}$, where $\mathbf{H}$ is the measurement Jacobian matrix. Without loss of generality, assume an East, North, UP (ENU) coordinate frame to be centered at $\hat{\boldsymbol{x}}_r$. Then, the Jacobian in this ENU frame can be expressed as

$$\mathbf{H} = \left[\mathbf{H}_{\text{sv}}^\mathsf{T}, \mathbf{H}_{\text{s}}^\mathsf{T}\right]^\mathsf{T},$$

$$\mathbf{H}_{\text{sv}} = \begin{bmatrix} \mathsf{c}(el_{\text{sv}_1})\,\mathsf{s}(az_{\text{sv}_1}) & \mathsf{c}(el_{\text{sv}_1})\,\mathsf{c}(az_{\text{sv}_1}) & \mathsf{s}(el_{\text{sv}_1}) & 1 \\ \vdots & \vdots & \vdots & \vdots \\ \mathsf{c}(el_{\text{sv}_M})\,\mathsf{s}(az_{\text{sv}_M}) & \mathsf{c}(el_{\text{sv}_M})\,\mathsf{c}(az_{\text{sv}_M}) & \mathsf{s}(el_{\text{sv}_M}) & 1 \end{bmatrix}$$

$$\mathbf{H}_{\text{s}} = \begin{bmatrix} \mathsf{c}(el_{\text{s}_1})\,\mathsf{s}(az_{\text{s}_1}) & \mathsf{c}(el_{\text{s}_1})\,\mathsf{c}(az_{\text{s}_1}) & \mathsf{s}(el_{\text{s}_1}) & 1 \\ \vdots & \vdots & \vdots & \vdots \\ \mathsf{c}(el_{\text{s}_N})\,\mathsf{s}(az_{\text{s}_N}) & \mathsf{c}(el_{\text{s}_N})\,\mathsf{c}(az_{\text{s}_N}) & \mathsf{s}(el_{\text{s}_N}) & 1 \end{bmatrix},$$

where $\mathsf{c}(\cdot)$ and $\mathsf{s}(\cdot)$ are the cosine and sine functions, respectively; el_{sv_m} and az_{sv_m} are the elevation and azimuth angles, respectively, of the mth GNSS SV; and el_{s_n} and az_{s_n} are the elevation and azimuth angles, respectively, of the nth cellular tower as observed from the receiver. Therefore, $\mathbf{G} \triangleq \left(\mathbf{H}^{\mathsf{T}}\mathbf{H}\right)^{-1}$ is completely determined by the receiver-to-SV and receiver-to-tower geometry. The diagonal elements of $\mathbf{G}$, denoted g_{ii}, are the DOP factors: geometric DOP (GDOP), horizontal DOP (HDOP), and vertical DOP (VDOP)

$$\text{GDOP} \triangleq \sqrt{\text{tr}\,[\mathbf{G}]}, \quad \text{HDOP} \triangleq \sqrt{g_{11}+g_{22}}, \quad \text{VDOP} \triangleq \sqrt{g_{33}}.$$

With the exception of GNSS receivers mounted on high-flying aerial and space vehicles, all GNSS SVs are typically above the receiver [85], i.e., the elevation angles in $\mathbf{H}_{\text{sv}}$ are theoretically limited between 0° and 90°. Moreover, GNSS receivers typically ignore signals arriving from GNSS SVs below a certain elevation mask (typically 0° to 20°), since such signals are heavily degraded due to the ionosphere, troposphere, and multipath. When using GNSS together with cellular signals for navigation, the elevation angle span may effectively double to be between −90° and 90°. For ground vehicles, useful measurements can be made on cellular towers at elevation angles of $el_{\text{s}_n} \approx 0°$. For aerial vehicles, cellular BTSs can reside at elevation angle as low as $el_{\text{s}_n} = -90°$, e.g., if the vehicle is flying directly above the BTS.

To compare the DOP of a GNSS-only navigation solution with a GNSS + cellular navigation solution, a receiver position expressed in an Earth-Centered-Earth-Fixed (ECEF) coordinate frame was set to $\boldsymbol{r}_r \equiv 10^6 \cdot [-2.431171, -4.696750, 3.553778]^{\mathsf{T}}$. The elevation and azimuth angles of the GPS SV constellation above the receiver over a twenty-four hour period was computed using GPS SV ephemeris files from the Garner GPS Archive [86]. The elevation mask was set to $el_{\mathsf{sv,min}} \equiv 20°$. The azimuth and elevation angles of 3 towers, which were calculated from surveyed terrestrial cellular CDMA tower positions in the receiver's vicinity, were $\boldsymbol{az}_{\text{s}} \equiv [42.4°, 113.4°, 230.3°]^{\mathsf{T}}$ and $\boldsymbol{el}_{\text{s}} \equiv [3.53°, 1.98°, 0.95°]^{\mathsf{T}}$. The resulting VDOP, HDOP, GDOP, and associated number of available GPS SVs for a twenty-four hour period starting from midnight, September 1$^{\mathsf{st}}$, 2015, are plotted in Figure 61. These results were consistent for different receiver locations and corresponding GPS SV configurations. The following can be concluded from these plots for using $N \geq 1$ cellular towers. First, the resulting VDOP using GPS + N cellular towers is always less than the resulting VDOP using GPS alone. Second, using GPS + N cellular towers prevents large spikes in VDOP when the number of GPS SVs drops. Third, using GPS + N cellular towers also reduces both HDOP and GDOP. Additional analysis is given in [7, 8].

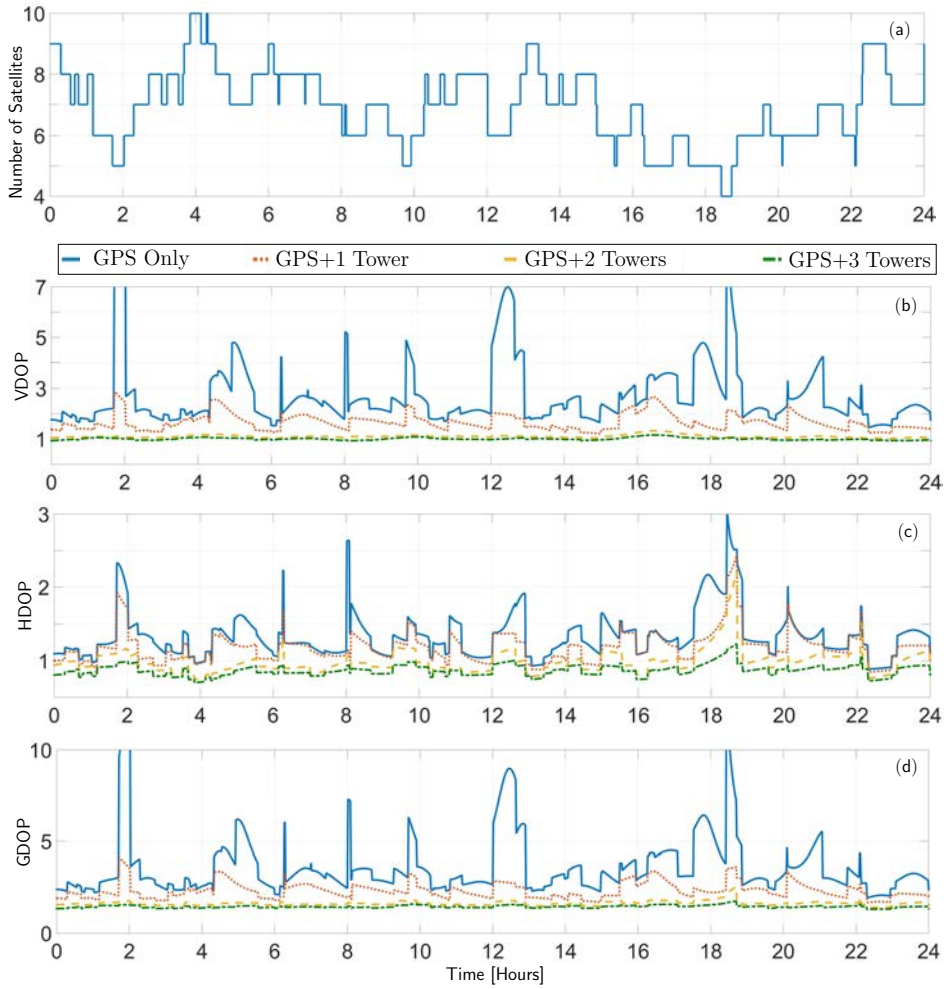


Figure 61: Figure (a) represents the number of GPS SVs with an elevation angle $> 20°$ as a function of time. Figures (b)–(d) correspond to the resulting VDOP, HDOP, and GDOP, respectively, of the navigation solution using GPS only, GPS + 1 cellular tower, GPS + 2 towers, and GPS + 3 towers.

8.2 GPS and Cellular Experimental Results

8.2.1 Ground Vehicle Navigation

A ground vehicle-mounted receiver was placed in an environment comprising N cellular CDMA towers. The states of the towers $\{\boldsymbol{x}_{\mathrm{s}_n}\}_{n=1}^{N}$, where $\boldsymbol{x}_{\mathrm{s}_n} = \left[\boldsymbol{r}_{\mathrm{s}_n}^{\mathsf{T}}, c\delta t_{\mathrm{s}_n}\right]^{\mathsf{T}}$, were collaboratively estimated by mapping receivers in the navigating receiver's vicinity. The mapping receivers had knowledge of their own states from GPS. The pseudoranges made by the receiver on the N cellular towers along with the estimates $\{\hat{\boldsymbol{x}}_{\mathrm{s}_n}\}_{n=1}^{N}$ produced by the mapping receivers were fed to a least-squares estimator to produce an estimate $\hat{\boldsymbol{x}}_r$ of the receiver's states and an associated estimation error covariance matrix $\mathbf{P}$, from which the VDOP, HDOP, and GDOP were calculated and are tabulated in Table 6 for M GPS SVs and N cellular towers. A sky plot of the GPS SVs is shown in Figure 62(a). The tower locations, receiver location, and a comparison of the resulting 95^{th}-percentile estimation uncertainty ellipsoids

of $\hat{\boldsymbol{x}}_r$ for $\{M, N\} = \{5, 0\}$ and $\{5, 3\}$ are illustrated in Figure 62(b). The corresponding vertical error was 1.82 m and 0.65 m, respectively. Hence, adding 3 cellular towers to the navigation solution that used 5 GPS SVs reduced the vertical error by 64.3%.

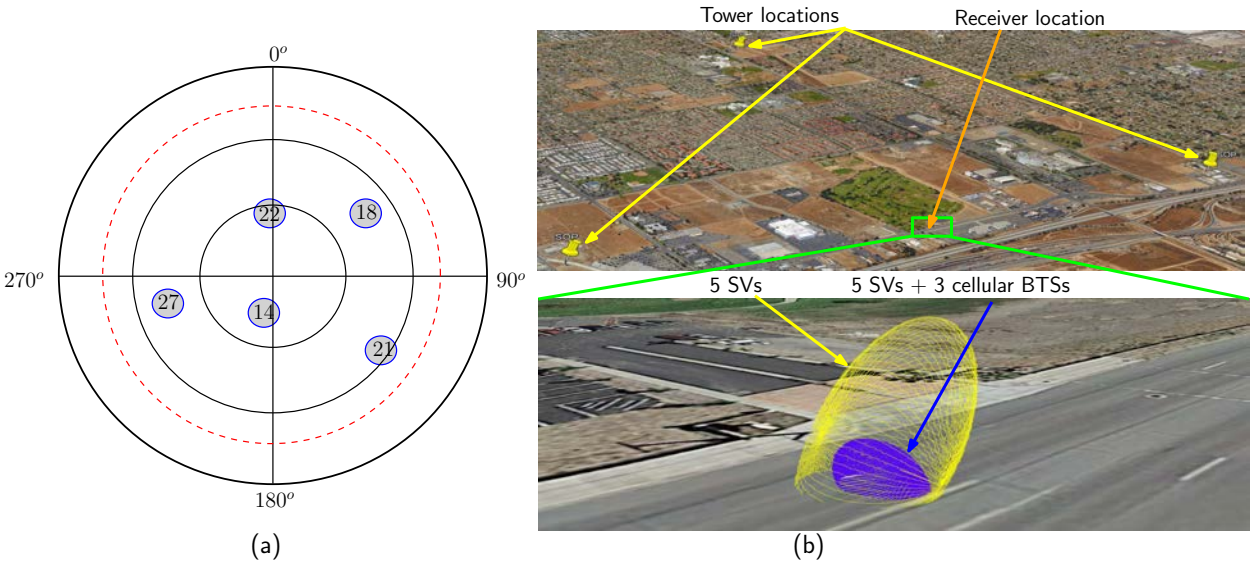


Figure 62: (a) Sky plot of GPS SVs: 14, 18, 21, 22, and 27 used for the 5 SV scenarios. For the 4 SV scenario, SVs 14, 21, 22, and 27 were used. The elevation mask, $el_{\text{sv,min}}$, was set to 20° (dashed red circle). (b) Top: Cellular CDMA tower locations and receiver location. Bottom: uncertainty ellipsoid (yellow) of navigation solution from using pseudoranges from 5 GPS SVs and uncertainty ellipsoid (blue) of navigation solution from using pseudoranges from 5 GPS SVs and 3 cellular CDMA towers.

Table 6: DOP values for M GPS SVs + N cellular towers

(M) **SVs,** (N) **Towers:** $\{M, N\}$	**{4, 0}**	**{4, 1}**	**{4, 2}**	**{4, 3}**	**{5, 0}**	**{5, 1}**	**{5, 2}**	**{5, 3}**
VDOP	3.773	1.561	1.261	1.080	3.330	1.495	1.241	1.013
HDOP	2.246	1.823	1.120	1.073	1.702	1.381	1.135	1.007
GDOP	5.393	2.696	1.933	1.654	4.565	2.294	1.880	1.566

8.2.2 Aerial Vehicle Navigation

A UAV was flown in a cellular environment comprising 3 cellular CDMA BTSs and 2 LTE eNodeBs, whose states were estimated by mapping receivers in their environment [6]. The UAV was equipped with the cellular CDMA and LTE navigation receivers discussed in Sections 5 and 6, respectively, which produced pseudorange measurements to all 5 towers. The UAV was also equipped with the GRID SDR that produced pseudorange measurements to 7 GPS SVs. The towers' state estimates and GPS and cellular tower pseudoranges were used to estimate the UAV's 3–D position and clock bias through a nonlinear least-squares estimator. Figure 63 illustrates the environment and the resulting 95$^{\text{th}}$-percentile uncertainty ellipsoids associated with the position estimate using (i) 7 GPS SVs and (ii) 7 GPS SVs along

with 3 cellular CDMA BTSs and 2 LTE eNodeBs. Note that the volume of the GPS-only navigation solution uncertainty ellipsoid V_{GPS} was reduced upon upon fusing the 5 cellular pseudoranges to $0.16(V_{\mathsf{GPS}})$.

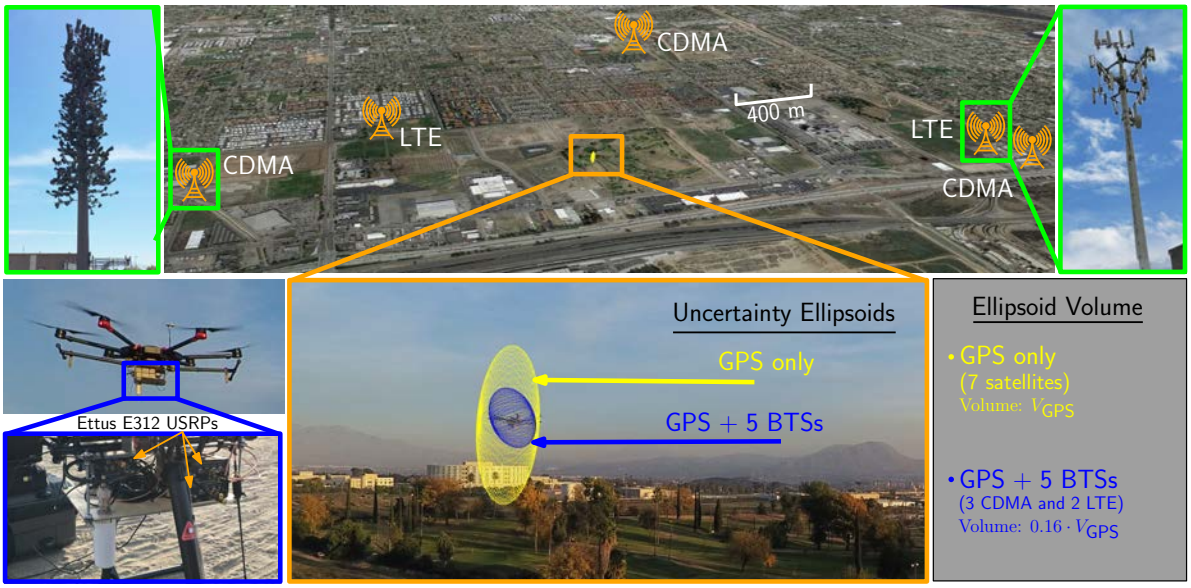


Figure 63: Experimental results comparing the navigation solution uncertainty ellipsoids produced by (i) GPS alone and (ii) GPS and cellular CDMA and LTE.

9 Cellular-Aided Inertial Navigation System

Traditional integrated navigation systems, particularly onboard vehicles, integrate GNSS receivers with an INS. When these systems are integrated, the long-term stability of a GNSS navigation solution complements the short-term accuracy of an INS. GNSS–INS fusion architectures with loosely-coupled, tightly-coupled, and deeply-coupled estimators, are well-studied [87]. Regardless of the coupling type, the errors of a GNSS-aided INS will diverge in the absence of GNSS signals, and the rate of divergence depends on the quality of the IMU. Cellular signals could be used in place of GNSS signals to aid an INS [44]. This section outlines how cellular signals could be used to aid an INS in the absence of GNSS signals. Additional details can be found in [4, 45, 88, 89].

This section is organized as follows. Subsection 9.1 discusses how to aid the INS with cellular signals in a radio SLAM fashion. Subsections 9.2 and 9.3 present simulation and experimental results, respectively, of a UAV navigating in a radio SLAM fashion, while aiding its INS with ambient cellular signals.

9.1 Radio SLAM with Cellular Signals

To correct INS errors using cellular pseudoranges, an EKF framework similar to a traditional tightly coupled GNSS-aided INS integration strategy can be adopted, with the added

complexity that the cellular towers' states (position and clock error states) are simultaneously estimated alongside the navigating vehicle's states (position, velocity, attitude, IMU measurement error states, and receiver clock error states). This framework is composed of two modes:

Mapping Mode The EKF produces estimates and associated estimation error covariances of both the navigating vehicle and the cellular towers' states (augmented in $\boldsymbol{x}$) using both GNSS SV and cellular pseudoranges. Between aiding corrections, the EKF produces the state prediction $\hat{\boldsymbol{x}}^-$ and prediction error covariance $\mathbf{P}^-$ using the INS and receiver and cellular transmitter clocks models. When an aiding source is available, either GNSS SV or cellular pseudoranges, the EKF produces a state estimate update $\hat{\boldsymbol{x}}^+$ and associated estimation error covariance $\mathbf{P}^+$.

Radio SLAM Mode The cellular-aided INS framework enters a radio SLAM mode when GNSS pseudoranges become unavailable. In this mode, INS errors are corrected using cellular pseudoranges and the cellular transmitters' state estimates that were last computed in the mapping mode. As the vehicle navigates, it continues to refine the cellular transmitters' state estimates simultaneously with estimating the vehicle's own states.

Figure 64 illustrates a high-level diagram of the cellular-aided INS framework.

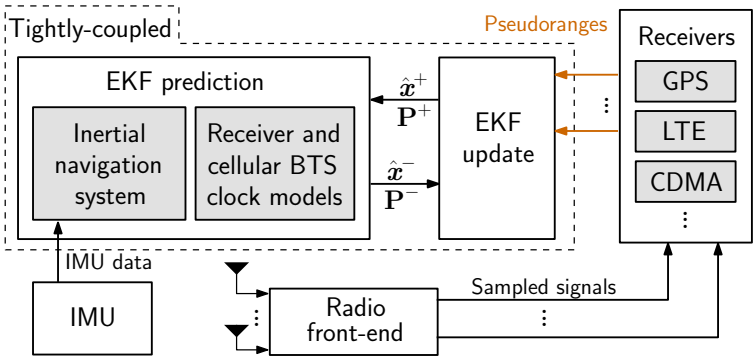


Figure 64: Tightly coupled cellular-aided INS framework

9.2 Simulation Results

To demonstrate the performance of the cellular-aided INS framework, simulations were conducted of a UAV equipped with cellular navigation receivers, navigating in downtown Los Angeles, California, while listening to ambient cellular signals. Two navigation systems were employed to estimate the trajectory of the UAV: 1) a traditional tightly-coupled GPS-aided INS with a tactical-grade IMU and 2) the cellular-aided INS discussed in Subsection 9.1 with a consumer-grade IMU. A simulator generated the true trajectory of the UAV and clock error states of the UAV-mounted receiver, the cellular transmitter' clock error states, noise-corrupted IMU measurements of specific force and angular rates, and noise-corrupted pseudoranges to multiple cellular towers and GPS SVs. The IMU signal generator used a triad gyroscope and a triad accelerometer model, each with time-evolving biases that provided sampled data at 100 Hz. GPS L1 C/A pseudoranges were generated at 1 Hz using SV

orbits produced from receiver independent exchange files downloaded on October 22, 2016, from a continuously operating reference station server [90]. The GPS L1 C/A pseudoranges were set to be available for only the first 100 seconds of the 200-second simulation. Cellular pseudoranges were generated at 5 Hz to 4 cellular towers, which were surveyed from real tower positions in downtown Los Angeles. The UAV's true trajectory included a straight segment followed by two banked orbits in the vicinity of the 4 cellular towers, shown in Figure 65(a). The resulting EKF estimation errors and corresponding 3 standard deviation bounds for the north and east position of the UAV are plotted in Figure 65(b). The navigation solutions from using 1) the cellular-aided INS and 2) only an INS during the 100 seconds GPS pseudoranges were unavailable appear in Figure 65(c). The final tower estimated position and corresponding 95$^{\text{th}}$-percentile estimation uncertainty ellipse is shown in Figure 65(d). One can see that when GPS pseudoranges became unavailable at 100 seconds, the estimation errors associated with the traditional GPS-aided INS integration strategy began to diverge, as expected, whereas the errors associated with the cellular-aided INS were bounded within this 100-second duration of GPS unavailability. Second, when GPS was still available during the first 100 seconds, the cellular-aided INS with a consumer-grade IMU almost always produced lower estimation error uncertainties when compared to the traditional GPS-aided INS integration strategy with a tactical-grade IMU.

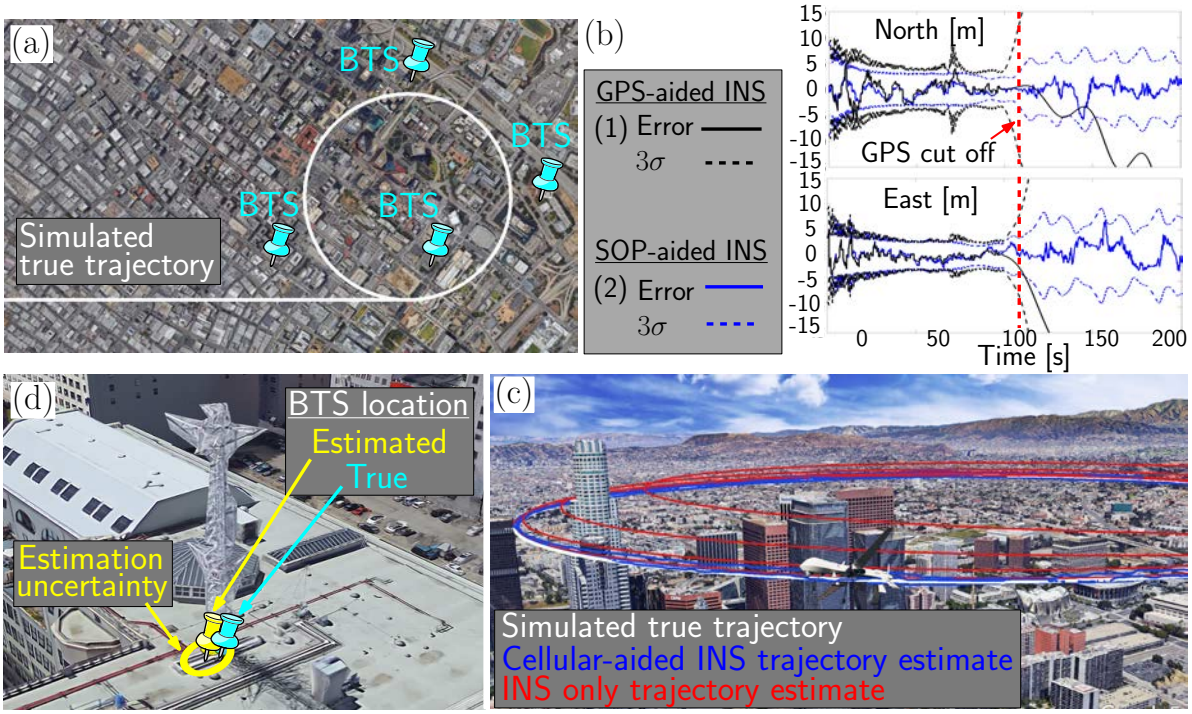


Figure 65: Illustration of simulation results for a UAV flying over downtown Los Angeles, California. (a) Simulated true trajectory (white curve) and cellular tower locations (blue pins). (b) EKF estimation errors and corresponding 3 standard deviation bounds (3σ) of the North and East position states of the UAV. (c) Unaided INS navigation solution (red curve), and cellular-aided INS navigation solution (blue curve) during the GPS outage. (d) True and estimated tower location and estimation uncertainty ellipse.

9.3 Experimental Results

To demonstrate the performance of the cellular-aided INS, a UAV was flown in an environment comprising 3 cellular CDMA BTSs and 2 LTE eNodeBs, whose locations were pre-surveyed and are illustrated in Figure 66(a) [6]. The UAV was equipped with a consumer-grade IMU, a GPS receiver, and cellular CDMA and LTE navigation receivers discussed in Sections 5 and 6. Experimental results are presented for two scenarios: 1) the cellular-aided INS described in Subsection 9.1 and 2) for comparative analysis, a traditional GPS-aided INS using the UAV's IMU. The true trajectory traversed by the UAV is plotted in Figure 66(b)–(c), which consists of GPS unavailability for 50 seconds, starting at a location marked by the red arrow. The north-east RMSE of the GPS-aided INS's navigation solution after GPS became unavailable was more than 100 meters. The UAV also estimated its trajectory using the cellular-aided INS framework using signals from the 3 CDMA BTSs and 2 eNodeBs to aid its onboard INSs. Table 7 summarizes the UAV's 2–D and 3–D RMSEs and final errors.

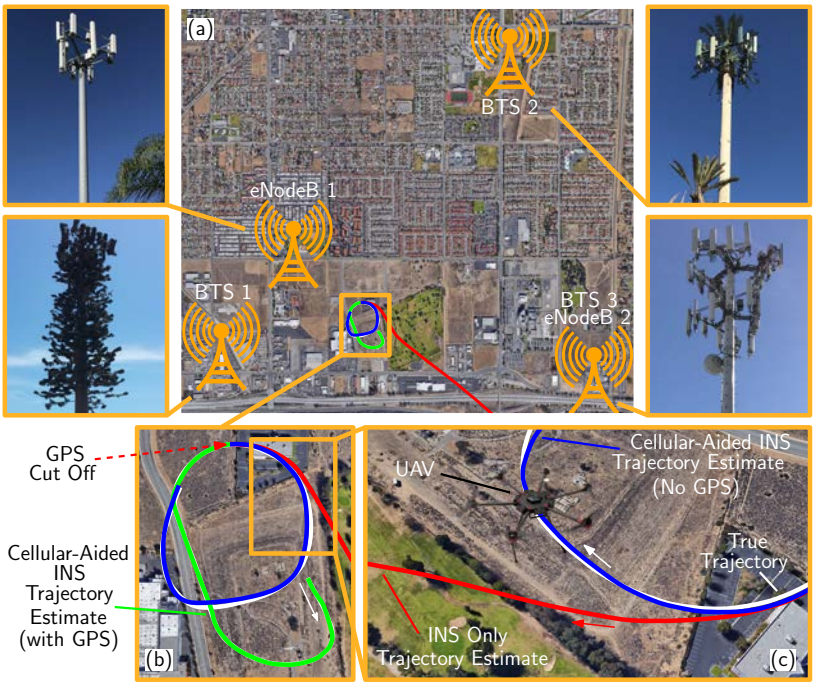


Figure 66: Experimental results of a UAV aiding its INS with cellular signals in the absence of GPS signals. (a) Cellular environment comprising 3 CDMA BTSs and 2 LTE eNodeBs. (b) UAV's estimated trajectories: white: true trajectory, green: cellular-aided INS with GPS (before GPS cutoff), red: INS only (after GPS cutoff), and blue: cellular-aided INS (after GPS cutoff). (c) Zoom on the UAV's diverging INS trajectory after GPS cutoff.

Table 7: UAV's RMSEs and final errors after 50 seconds of GPS cutoff

	2–D RMSE (m)	3–D RMSE (m)	Final 3–D error (m)
INS only	> 100	> 100	> 100
Cellular-aided INS	4.68	7.76	4.92

References

[1] M. Bshara, U. Orguner, F. Gustafsson, and L. Van Biesen, "Robust tracking in cellular networks using HMM filters and cell-ID measurements," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 3, pp. 1016–1024, March 2011.

[2] 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.

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

[4] Z. Kassas, J. Morales, K. Shamaei, and J. Khalife, "LTE steers UAV," *GPS World Magazine*, vol. 28, no. 4, pp. 18–25, April 2017.

[5] M. Driusso, C. Marshall, M. Sabathy, F. Knutti, H. Mathis, and F. Babich, "Vehicular position tracking using LTE signals," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3376–3391, April 2017.

[6] Z. Kassas, J. Khalife, K. Shamaei, and J. Morales, "I hear, therefore I know where I am: Compensating for GNSS limitations with cellular signals," *IEEE Signal Processing Magazine*, pp. 111–124, September 2017.

[7] J. Morales, J. Khalife, and Z. Kassas, "GNSS vertical dilution of precision reduction using terrestrial signals of opportunity," in *Proceedings of ION International Technical Meeting Conference*, January 2016, pp. 664–669.

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

[9] M. Huang and W. Xu, "Enhanced LTE TOA/OTDOA estimation with first arriving path detection," in *Proceedings of IEEE Wireless Communications and Networking Conference*, April 2013, pp. 3992–3997.

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

[11] M. Driusso, F. Babich, F. Knutti, M. Sabathy, and C. Marshall, "Estimation and tracking of LTE signals time of arrival in a mobile multipath environment," in *Proceedings of International Symposium on Image and Signal Processing and Analysis*, September 2015, pp. 276–281.

[12] J. Khalife, K. Shamaei, and Z. Kassas, "Navigation with cellular CDMA signals – part I: Signal modeling and software-defined receiver design," *IEEE Transactions on Signal Processing*, vol. 66, no. 8, pp. 2191–2203, April 2018.

[13] W. Xu, M. Huang, C. Zhu, and A. Dammann, "Maximum likelihood TOA and OTDOA estimation with first arriving path detection for 3GPP LTE system," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 3, pp. 339–356, 2016.

[14] P. Muller, J. del Peral-Rosado, R. Piche, and G. Seco-Granados, "Statistical trilateration with skew-t distributed errors in LTE networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 7114–7127, October 2016.

[15] K. Shamaei and Z. Kassas, "LTE receiver design and multipath analysis for navigation in urban environments," *NAVIGATION, Journal of the Institute of Navigation*, vol. 65, no. 4, pp. 655–675, December 2018.

[16] C. Yang, T. Nguyen, E. Blasch, and D. Qiu, "Assessing terrestrial wireless communications and broadcast signals as signals of opportunity for positioning and navigation," in *Proceedings of ION GNSS Conference*, September 2012, pp. 3814–3824.

[17] J. del Peral-Rosado, J. Lopez-Salcedo, G. Seco-Granados, F. Zanier, P. Crosta, R. Ioannides, and M. Crisci, "Software-defined radio LTE positioning receiver towards future hybrid localization systems," in *Proceedings of International Communication Satellite Systems Conference*, October 2013, pp. 14–17.

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

[19] K. Shamaei, J. Khalife, S. Bhattacharya, and Z. Kassas, "Computationally efficient receiver design for mitigating multipath for positioning with LTE signals," in *Proceedings of ION GNSS Conference*, September 2017, pp. 3751–3760.

[20] S. Kim, H. Choi, J. Park, and Y. Park, "Timing error suppression scheme for CDMA network based positioning system," in *Proceedings of IEEE/ION Position, Location and Navigation Symposium*, May 2008, pp. 364–368.

[21] J. del Peral-Rosado, J. Lopez-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, "Achievable localization accuracy of the positioning reference signal of 3GPP LTE," in *Proceedings of International Conference on Localization and GNSS*, June 2012, pp. 1–6.

[22] J. Khalife and Z. Kassas, "Characterization of sector clock biases in cellular CDMA systems," in *Proceedings of ION GNSS Conference*, September 2016, pp. 2281–2285.

[23] J. Khalife and Z. Kassas, "Modeling and analysis of sector clock bias mismatch for navigation with cellular signals," in *Proceedings of American Control Conference*, May 2017, pp. 3573–3578.

[24] J. Khalife and Z. Kassas, "Evaluation of relative clock stability in cellular networks," in *Proceedings of ION GNSS Conference*, September 2017, pp. 2554–2559.

[25] J. Khalife and Z. Kassas, "Navigation with cellular CDMA signals – part II: Performance analysis and experimental results," *IEEE Transactions on Signal Processing*, vol. 66, no. 8, pp. 2204–2218, April 2018.

[26] 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.

[27] Z. Kassas and T. Humphreys, "Observability analysis of collaborative opportunistic navigation with pseudorange measurements," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 260–273, February 2014.

[28] C. Yang and A. Soloviev, "Simultaneous localization and mapping of emitting radio sources-SLAMERS," in *Proceedings of ION GNSS Conference*, September 2015, pp. 2343–2354.

[29] J. Morales and Z. Kassas, "Information fusion strategies for collaborative radio SLAM," in *Proceedings of IEEE/ION Position Location and Navigation Symposium*, April 2018, pp. 1445–1454.

[30] F. Boccardi, R. Heath, A. Lozano, T. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 74–80, February 2014.

[31] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1617–1655, February 2016.

[32] J. Barnes, A. Chi, R. Andrew, L. Cutler, D. Healey, D. Leeson, T. McGunigal, J. Mullen, W. Smith, R. Sydnor, R. Vessot, and G. Winkler, "Characterization of frequency stability," *IEEE Transactions on Instrumentation and Measurement*, vol. 20, no. 2, pp. 105–120, May 1971.

[33] A. Thompson, J. Moran, and G. Swenson, *Interferometry and Synthesis in Radio Astronomy*, 2nd ed. John Wiley & Sons, 2001.

[34] Y. Bar-Shalom, X. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation*. New York, NY: John Wiley & Sons, 2002.

[35] R. Brown and P. Hwang, *Introduction to Random Signals and Applied Kalman Filtering*, 3rd ed. John Wiley & Sons, 2002.

[36] J. Curran, G. Lachapelle, and C. Murphy, "Digital GNSS PLL design conditioned on thermal and oscillator phase noise," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 48, no. 1, pp. 180–196, Jan. 2012.

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

[38] 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.

[39] J. Morales and Z. Kassas, "Optimal collaborative mapping of terrestrial transmitters: receiver placement and performance characterization," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 2, pp. 992–1007, April 2018.

[40] 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.

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

[42] J. Morales and Z. Kassas, "Stochastic observability and uncertainty characterization in simultaneous receiver and transmitter localization," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 2, pp. 1021–1031, April 2019.

[43] J. Khalife and Z. Kassas, "Precise UAV navigation with cellular carrier phase measurements," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2018, pp. 978–989.

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

[45] J. Morales, J. Khalife, and Z. Kassas, "Collaborative autonomous vehicles with signals of opportunity aided inertial navigation systems," in *Proceedings of ION International Technical Meeting Conference*, January 2017, 805–818.

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

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

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

[49] 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.

[50] 3GPP2, "Physical layer standard for cdma2000 spread spectrum systems (C.S0002-E)," 3rd Generation Partnership Project 2 (3GPP2), TS C.S0002-E, June 2011.

[51] 3GPP2, "Recommended minimum performance standards for cdma2000 spread spectrum base stations," December 1999.

[52] 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.

[53] 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.

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

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

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

[57] A. van Dierendonck, P. Fenton, and T. Ford, "Theory and performance of narrow correlator spacing in a GPS receiver," *NAVIGATION, Journal of the Institute of Navigation*, vol. 39, no. 3, pp. 265–283, September 1992.

[58] 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.

[59] S. Fischer, "Observed time difference of arrival (OTDOA) positioning in 3GPP LTE," Qualcomm Technologies, Inc., Tech. Rep., June 2014.

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

[61] 3GPP, "Evolved universal terrestrial radio access (E-UTRA); physical channels and modulation," 3rd Generation Partnership Project (3GPP), TS 36.211, January 2011. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36211.htm

[62] S. Sesia, I. Toufik, and M. Baker, *LTE, The UMTS Long Term Evolution: From Theory to Practice*. Wiley Publishing, 2009.

[63] K. Shamaei, J. Khalife, and Z. Kassas, "Comparative results for positioning with secondary synchronization signal versus cell specific reference signal in LTE systems," in *Proceedings of ION International Technical Meeting Conference*, January 2017, pp. 1256–1268.

[64] K. Shamaei, J. Khalife, and Z. Kassas, "Performance characterization of positioning in LTE systems," in *Proceedings of ION GNSS Conference*, September 2016, pp. 2262–2270.

[65] K. Shamaei, J. Khalife, and Z. Kassas, "Exploiting LTE signals for navigation: Theory to implementation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2173–2189, April 2018.

[66] I. Kim, Y. Han, and H. Chung, "An efficient synchronization signal structure for OFDM-based cellular systems," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 99–105, January 2010.

[67] F. Benedetto, G. Giunta, and E. Guzzon, "Initial code acquisition in lte systems," *Recent Patents on Computer Science*, vol. 6, pp. 2–13, April 2013.

[68] M. Morelli and M. Moretti, "A robust maximum likelihood scheme for PSS detection and integer frequency offset recovery in LTE systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1353–1363, February 2016.

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

[70] 3GPP, "Evolved universal terrestrial radio access (E-UTRA); multiplexing and channel coding," 3rd Generation Partnership Project (3GPP), TS 36.212, January 2010. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36212.htm

[71] Y. Wang and R. Ramesh, "To bite or not to bite-a study of tail bits versus tail-biting," in *Proceedings of Personal, Indoor and Mobile Radio Communications*, vol. 2, October 1996, pp. 317–321.

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

[73] K. Shamaei, J. Khalife, and Z. Kassas, "Ranging precision analysis of LTE signals," in *Proceedings of European Signal Processing Conference*, August 2017, pp. 2788–2792.

[74] K. Shamaei, J. Khalife, and Z. Kassas, "Pseudorange and multipath analysis of positioning with LTE secondary synchronization signals," in *Proceedings of Wireless Communications and Networking Conference*, 2018, pp. 286–291.

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

[76] J. del Peral-Rosado, J. Lopez-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, "Evaluation of the LTE positioning capabilities under typical multipath channels," in *Proceedings of Advanced Satellite Multimedia Systems Conference and Signal Processing for Space Communications Workshop*, September 2012, pp. 139–146.

[77] J. del Peral-Rosado, J. Lopez-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, "Joint maximum likelihood time-delay estimation for LTE positioning in multipath

channels," in *Proceedings of EURASIP Journal on Advances in Signal Processing, special issue on Signal Processing Techniques for Anywhere, Anytime Positioning*, September 2014, pp. 1–13.

[78] C. Gentner, B. Ma, M. Ulmschneider, T. Jost, and A. Dammann, "Simultaneous localization and mapping in multipath environments," in *Proceedings of IEEE/ION Position Location and Navigation Symposium*, April 2016, pp. 807–815.

[79] C. Gentner, T. Jost, W. Wang, S. Zhang, A. Dammann, and U. Fiebig, "Multipath assisted positioning with simultaneous localization and mapping," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 6104–6117, September 2016.

[80] 3GPP2, "Recommended minimum performance standards for cdma2000 spread spectrum base stations," 3rd Generation Partnership Project 2 (3GPP2), TS C.S0010-E, March 2014. [Online]. Available: http://www.arib.or.jp/english/html/overview/doc/STD-T64v7_00/Specification/ARIB_STD-T64-C.S0010-Ev2.0.pdf

[81] L. Ljung, *System identification: Theory for the user*, 2nd ed. Prentice Hall PTR, 1999.

[82] J. Proakis and D. Manolakis, *Digital signal processing.* Prentice-Hall, Upper Saddle River, NJ, 1996.

[83] R. Norton, "The double exponential distribution: Using calculus to find a maximum likelihood estimator," *The American Statistician*, vol. 38, no. 2, pp. 135–136, May 1984.

[84] D. H. Won, J. Ahn, S. Lee, J. Lee, S. Sung, H. Park, J. Park, and Y. J. Lee, "Weighted DOP with consideration on elevation-dependent range errors of GNSS satellites," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 12, pp. 3241–3250, December 2012.

[85] J. Spilker, Jr., *Global Positioning System: Theory and Applications.* Washington, D.C.: American Institute of Aeronautics and Astronautics, 1996, ch. 5: Satellite Constellation and Geometric Dilution of Precision, pp. 177–208.

[86] University of California, San Diego, "Garner GPS archive," http://garner.ucsd.edu/, accessed November 23, 2015.

[87] D. Gebre-Egziabher, "What is the difference between 'loose', 'tight', 'ultra-tight' and 'deep' integration strategies for INS and GNSS," *Inside GNSS*, pp. 28–33, January 2007.

[88] J. Morales and Z. Kassas, "Distributed signals of opportunity aided inertial navigation with intermittent communication," in *Proceedings of ION GNSS Conference*, September 2017, pp. 2519–2530.

[89] J. Morales and Z. Kassas, "A low communication rate distributed inertial navigation architecture with cellular signal aiding," in *Proceedings of IEEE Vehicular Technology Conference*, 2018, pp. 1–6.

[90] R. Snay and M. Soler, "Continuously operating reference station (CORS): history, applications, and future enhancements," *Journal of Surveying Engineering*, vol. 134, no. 4, pp. 95–104, November 2008.