

# Assessing Real 5G Signals for Opportunistic Navigation

Ali A. Abdallah, Kimia Shamaei, and Zaher M. Kassas  
*University of California, Irvine, USA*

## BIOGRAPHIES

Ali A. Abdallah is a Ph.D student in the Department of Electrical Engineering and Computer Science at the University of California, Irvine and a member of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He received a B.E. in Electrical Engineering from the Lebanese American University (LAU). His current research interests include opportunistic navigation, software-defined radio, long-term evolution (LTE), 5G, and indoor localization.

Kimia Shamaei received a Ph.D. in Electrical Engineering from the University of California, Irvine and a B.S. and M.S. in Electrical Engineering from the University of Tehran. She was a member of the ASPIN Laboratory. She is a recipient of the 2018 Institute of Navigation (ION) Samuel Burka Award and 2020 ION Bradford Parkinson Award.

Zaher (Zak) M. Kassas is an associate professor at the University of California, Irvine and director of the ASPIN Laboratory. He received a B.E. in Electrical Engineering from the Lebanese American University, an M.S. in Electrical and Computer Engineering from The Ohio State University, and an M.S.E. in Aerospace Engineering and a Ph.D. in Electrical and Computer Engineering from The University of Texas at Austin. In 2018, he received the National Science Foundation (NSF) Faculty Early Career Development Program (CAREER) award, and in 2019, he received the Office of Naval Research (ONR) Young Investigator Program (YIP) award. He is a recipient of 2018 IEEE Walter Fried Award, 2018 ION Samuel Burka Award, and 2019 ION Col. Thomas Thurlow Award. He is an Associate Editor for the IEEE Transactions on Aerospace and Electronic Systems and the IEEE Transactions on Intelligent Transportation Systems. His research interests include cyber-physical systems, estimation theory, navigation systems, autonomous vehicles, and intelligent transportation systems.

## ABSTRACT

Cellular fifth-generation (5G) signals are assessed for opportunistic navigation. A carrier-aided code-based software-defined receiver (SDR) is presented, which produces navigation observables from received downlink 5G signals. These observables are analyzed to assess the performance of 5G signals for opportunistic navigation. Experimental results are presented of a ground vehicle navigating with the 5G SDR while receiving signals from two 5G base stations (known as gNBs). It is shown that over a trajectory of 1.02 km traversed in 100 seconds, the position root mean-squared error (RMSE) was 14.9 m.

## I. INTRODUCTION

Over the past few years, the third-generation partnership project (3GPP) has been developing the fifth-generation (5G) (also known as new radio (NR)) as the next wireless communication system [1, 2]. 5G provides faster data transfer speeds, lower latency, higher capacity, lower transmission power, and network slicing over the previous fourth-generation cellular system, also known as long-term evolution (LTE). These features allow 5G to play a major role in autonomous technologies. For example, autonomous vehicles involve enormous quantity of data collection, processing, and communication. This data includes navigation trajectory, traffic information, and surrounding vehicles and obstacles. 5G could revolutionize autonomous vehicle's capabilities, from data sharing to navigation and situational awareness. This paper focuses on assessing the potential of 5G signals for opportunistic navigation.

Recent research has considered the use of signals of opportunity (SOPs) as complementary and alternative navigation sources in global navigation satellite systems (GNSS)-challenged environments. SOPs are signals not intended for navigation purposes; however, can be exploited for navigation, such as AM/FM [3–5], Wi-Fi [6–8], digital television [9–11], low earth orbit (LEO) [12–14], and cellular [15–17]. Cellular signals, namely code-division multiple access

(CDMA) and LTE, have shown high ranging and localization accuracy using specialized software-defined receivers (SDRs) [18–22]. The performance of these SDRs have been evaluated with different navigation frameworks, both indoors [23–25] and outdoors [26–28], where experimental results demonstrated meter-level accuracy positioning accuracy on ground-mounted receivers with LTE and CDMA signals [29–31] and sub-meter-level positioning accuracy on aerial vehicle-mounted receivers with real LTE and CDMA signals [32, 33].

The cellular 5G system will be the first system to coexist with the previous system, LTE. The 5G system deploys a structure that is similar to the one deployed for LTE, where both systems use orthogonal frequency division multiplexing (OFDM) for downlink transmission. The 5G system is very attractive by design for navigation purposes due to its following qualities:

- High carrier frequencies: 5G is designed to transmit at two main frequency ranges (FRs): (i) FR1, which spans frequencies from 450 MHz to 6 GHz and (ii) FR2, which spans frequencies from 24.25 to 52.6 GHz [34]. High carrier frequencies yield precise carrier phase navigation observables and reduce multipath effect due to high path signal loss, especially for FR2.
- Abundance: the 5G design tackles the problem of high signal path loss of millimeter waves (mmWaves) by using beamforming techniques and small cells, which makes the 5G base stations (also known as gNodeBs (gNB)) ubiquitous.
- Geometric diversity: cellular towers have favorable geometry by construction of the cells to provide better coverage.
- Large bandwidth: While a single LTE signal has a bandwidth up to 20 MHz, a single 5G signal has a bandwidth up to 100 MHz and 400 MHz bandwidth for FR1 and FR2, respectively. This makes it less susceptible to multipath errors, i.e., it can differentiate multipath components with shorter delays from the line-of-sight (LOS) signal.
- High received power: the received carrier-to-noise-ratio  $C/N_0$  of cellular signals from nearby cellular towers is more than 20 dB-Hz higher than global position system (GPS) signals.

The positioning capabilities of 5G has been studied over the past few years. Different approaches have been proposed, in which direction-of-arrival (DOA), direction-of-departure (DOD), time-of-arrival (TOA), or a combination thereof were used to achieve accurate positioning from 5G signals. In [35], the authors investigated the positioning performance of six different 5G impulse radio waveforms, where 5G had no generally accepted waveform at the time. The performance analysis showed the capability of mmWaves in achieving sub-meter level accuracy, where the best performance was achieved when using Guassian raised-cosine, Guassian pulse, and Sinc-RCP impulse radio waveforms. The capability of massive multiple-input-multiple-output (mMIMO) systems in providing very accurate localization when relying on DOA was studied in [36]. The paper addressed the limitation of DOA in mMIMO systems in the presence of multipath by proposing a compressed sensing navigation framework and relied on the channel properties to distinguish LOS from multipath components. The proposed algorithm showed sub-meter accuracy in simulation. Another approach to reduce 5G small cell interference and multipath effect in angular localization methods by combining near-field and far-field effects was proposed in [37]. Simulation results showed that the proposed approach improved the angular resolution by orders of magnitude. In [38], a GNSS/5G integrated positioning framework based on a particle filter was proposed, in which device-to-device (D2D) range and angle measurements were utilized between mobile terminals (MTs). An experiment was performed assuming real GNSS data and emulated 5G D2D data, where the integrated system reduced the GNSS position root mean-squared error (RMSE) from around 5 m to 2-3 m, assuming 10 MTs. In [39], a network-based positioning framework using joint TOA and DOA was proposed using cascaded extended Kalman filters (EKF). The proposed framework considered the clock biases between the user equipment (UE) and the gNBs, and among the gNBs themselves. The framework was evaluated by simulating a real 5G scenario using three-dimensional (3-D) ray tracing, where sub-meter-level positioning accuracy was demonstrated.

All the aforementioned were limited to theoretical analyses, simulations, or laboratory-emulated 5G signals. This is due to:

- The structure of 5G signals has been recently finalized.
- 5G has been implemented only in a few major cities.
- The hardware limitation for both reception and transmission 5G systems, where mmWaves systems are still in development.
- The proposed navigation approaches require a network-based approach, in which the user's privacy is revealed

for the network. This also limits the UE to a single serving cellular provider, which limits the number of gNBs in sight.

This paper tackles the aforementioned challenges by

- Studying opportunistic navigation of 5G signals and presenting potential signals to be exploited for navigation purposes.
- Presenting an SDR to extract navigation observables from 5G signals
- Implementing a navigation framework using an EKF to estimate the receiver's position, along with the clock biases of the receiver and gNBs from extracted 5G navigation observables.
- Performing the first experimental demonstration of navigation with real cellular 5G signals.

The remainder of the paper is organized as follows. Section II discusses the 5G received signal structure and the potential reference signals for opportunistic navigation. Section III presents the carrier-aided code-based 5G receiver-design. Section IV proposes a 5G navigation framework. Section V validates the performance of the proposed navigation framework in a suburban environment over a 1.02 km trajectory traversed in 100 seconds. The achieved two-dimensional (2-D) RMSE is shown to be 14.93 m, while listening to two gNBs. Concluding remarks are given in Section VI.

## II. 5G SIGNAL STRUCTURE

OFDM with cyclic prefix (CP) is used as a modulation technique for 5G downlink signals, which is the same waveform LTE has adopted for its downlink signal. This paper discusses an opportunistic UE-based navigation approach; thus, only 5G downlink signal structure is discussed. In OFDM, a multi-carrier transmission scheme is used, where transmitted data symbols are mapped into multiple narrowband subcarriers in the frequency-domain, which reduces frequency selective fading effect caused by multipath. The serial data symbols  $\{S_1, \dots, S_{N_r}\}$  are parallelized in group symbols, each of length  $N_r$ , where  $N_r$  is the number of subcarriers carrying the data. Then, a guard band in the frequency-domain is applied by zero-padding both sides of the signal and extending the  $N_r$  subcarriers into  $N_c$  subcarriers. At this step, an inverse fast Fourier transform (IFFT) is taken, and the last  $L_{CP}$  elements are repeated in the beginning, which serves as a guard band in the time-domain to protect the OFDM signals from inter-symbol interference (ISI).

At the receiver, the transmitted symbols are demodulated by executing the aforementioned steps in reverse order. The obtained OFDM signals are arranged in a 2-D frame. The structure of this frame depends on the transmission type of the 5G signal, which can be either time division duplexing (TDD) or frequency division duplexing (FDD). This paper will use 5G signals from FR1, where most cellular providers are using FDD due to its superior performance in providing better coverage and less latency.

Compared to LTE numerology (i.e., subcarrier spacing (SCS) and symbol length), which supports only one type of subcarrier spacing,  $\Delta f = 15$  kHz, 5G supports different types of subcarrier spacing. Fig. 1 shows the different types, where  $\mu$  denotes the numerology.

The duration of the FDD 5G frame is

$$T_f = \frac{\Delta f_{\max} N_f}{100} \cdot T_c = 10 \text{ ms},$$

where,  $\Delta f_{\max} = 480$  kHz,  $N_f = 4096$ , and  $T_c = \frac{1}{\Delta f_{\max} N_f} = 0.509$  ns is the basic time unit for 5G. Each 5G frame consists of ten subframes, with duration 1 ms each. The number of OFDM symbols per subframe is  $N_{\text{subframe}, \mu}^{\text{subframe}, \mu} = N_{\text{slot}}^{\text{slot}} N_{\text{subframe}, \mu}^{\text{subframe}, \mu}$ . The frame is divided into two equally-sized half-frames consisting of five subframes each and denoted by: (i) half-frame 0 consisting of subframes 0-4 and (ii) half-frame 1 consisting of subframes 5-9.

For a predefined  $\mu$ , the number of slots is denoted by  $n_s^\mu \in \{0, 1, \dots, N_{\text{slot}}^{\text{subframe}, \mu}\}$  or  $n_s^\mu \in \{0, 1, \dots, N_{\text{slot}}^{\text{frame}, \mu}\}$  in an increasing order within a subframe or a frame, respectively. The number of symbols per slot  $N_{\text{symbol}}^{\text{slot}}$  depends on the type of cyclic prefix and the specified numerology. Table I shows for different numerologies: the number of OFDM symbols per slot, number of slots per frame, number of slots per subframe, and CP duration.

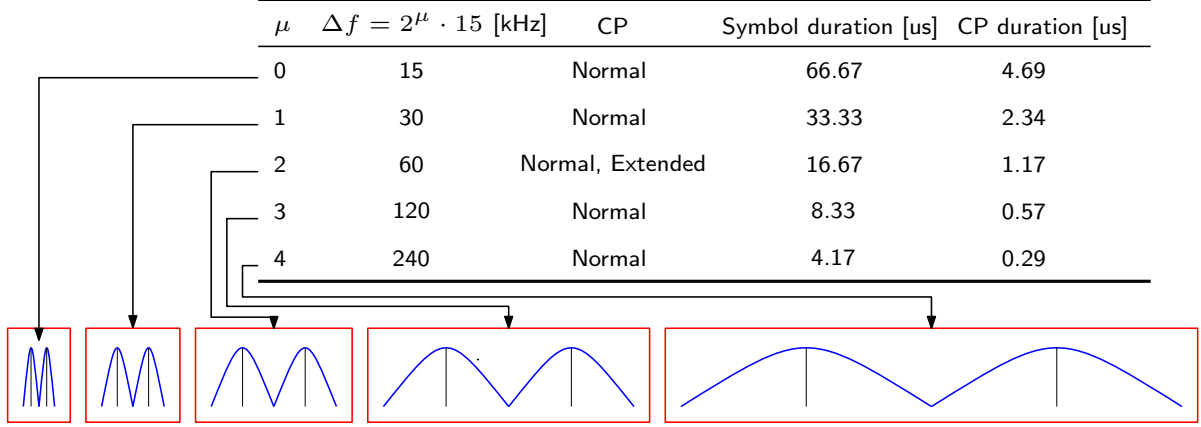


Fig. 1. Different numerologies of 5G and the corresponding: subcarrier spacing, CP type, OFDM symbol duration, CP duration, and two-subcarriers representation.

TABLE I  
NUMBER OF OFDM SYMBOLS PER SLOT, SLOTS PER FRAME, AND SLOTS PER SUBFRAME

$\mu$	Cyclic prefix	$N_{\text{slot}}^{\text{slot}}$	$N_{\text{slot}}^{\text{frame}, \mu}$	$N_{\text{slot}}^{\text{subframe}, \mu}$
0	Normal	14	10	1
1	Normal	14	20	2
2	Normal	14	40	4
2	Extended	12	40	4
3	Normal	14	80	8
4	Normal	14	160	16

A resource block (RB) is defined as  $N_{\text{sc}}^{\text{RB}} = 12$  subcarriers in the frequency-domain and has the time length of a resource grid  $N_{\text{symb}}^{\text{subframe}, \mu}$ . A resource block consists of resource elements. The minimum and maximum number of resource blocks along with the corresponding bandwidth for different numerologies are summarized in Table II. Each element in the 5G frame is uniquely identified for a specific antenna port  $p$  and subcarrier configuration  $\mu$  by  $(k, l)_{p, \mu}$ , where  $k$  is the index in frequency domain  $l$  is the symbol position in the time domain relative to some reference point. In the 5G protocol, “Point A” serves as a common reference point and can be obtained as reported in [40].

TABLE II  
THE MINIMUM AND MAXIMUM NUMBER OF RESOURCE BLOCKS AND THE CORRESPONDING BANDWIDTHS FOR DIFFERENT NUMEROLOGIES.

$\mu$	$N_{\text{RB}}^{\text{min}}$	$N_{\text{RB}}^{\text{max}}$	Minimum bandwidth [Mhz]	Maximum bandwidth [Mhz]
0	24	275	4.32	49.5
1	24	275	8.64	99
2	24	275	17.28	198
3	24	275	34.56	396
4	24	138	69.12	397.44

At the receiver side, the received 5G signal must be converted to frame structure before extracting signals of interest. To do so, the frame start time should be known. For the purpose of providing the frame start time, the gNB broadcasts synchronization signals (SS) with a pre-specified symbol mapping in the 5G frame. The SS includes two reference signals: primary synchronization signal (PSS) and secondary synchronization signal (SSS), which provide symbol and frame timing, respectively. Once the frame start time is known, the CPs can be removed and a fast Fourier transform (FFT) is taken to construct the OFDM symbols in the frame. The SS, the physical broadcast channel (PBCH), and its associated demodulation reference signal (DM-RS) are transmitted in the same 4 symbols block called the SS/PBCH block. The SS/PBCH block consists of 240 contiguous subcarrier (20 RBs) and four consecutive OFDM symbols. Within the SS/PBCH, the subcarriers are numbered in an ascending order from 0 to

239. Fig. 2 shows the SS/PBCH block structure and the corresponding OFDM symbols and subcarriers mapping of the different signals within the block. Note that the position of PBCH-DM-RS varies with  $v$ , and the value  $v$  changes depending on the physical cell ID  $N_{ID}^{Cell}$ . The SS/PBCH block is transmitted every two frames and is transmitted numerous times, where each set of these transmitted block is called an SS/PBCH burst. The SS/PBCH burst has to be confined within a half-frame window (5 ms). Each block in the SS/PBCH burst is beamformed in a different direction. The frequency location of the SS/PBCH within the 5G frame depends on the 5G high-level signaling. The time location of the SS/PBCH block and the size of the SS/PBCH burst in the frame depends on the transmission frequency  $f_c$  and the numerology  $\mu$  as shown in Table III, where index 0 corresponds to the first OFDM symbol of the first slot in a half-frame.

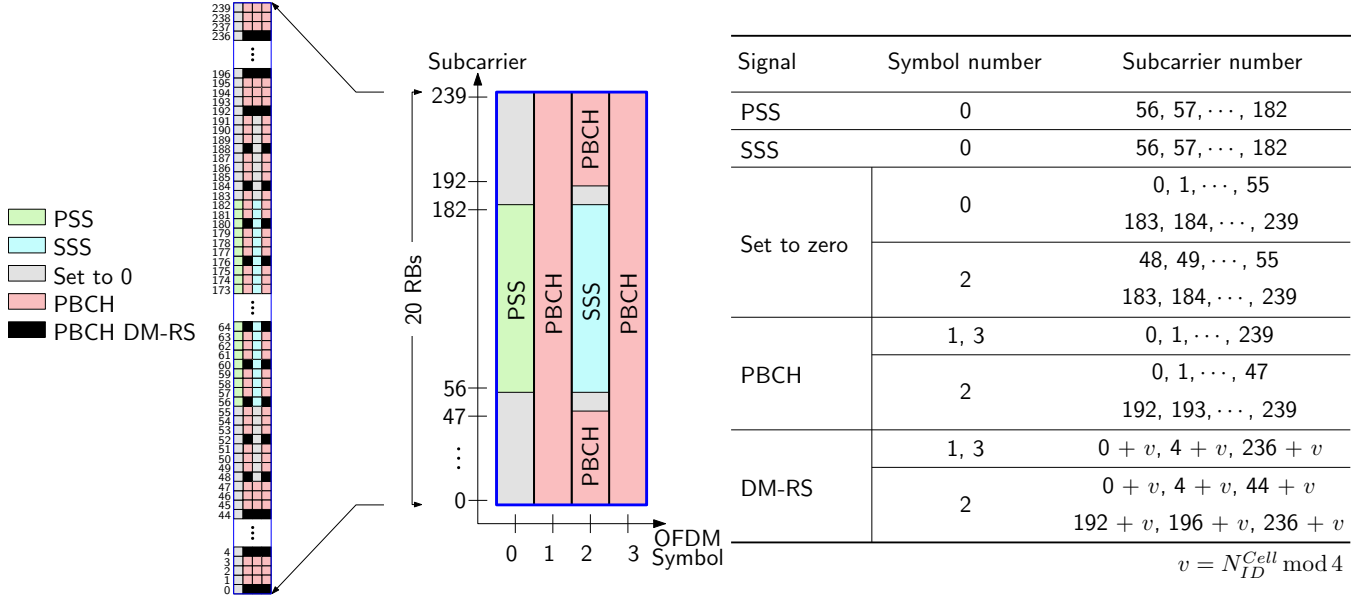


Fig. 2. SS/PBCH block structure and the corresponding OFDM symbols and subcarriers mapping of the different signals within the block.

TABLE III  
SYMBOL NUMBERS CONTAINING SS/PBCH BLOCK FOR DIFFERENT NUMEROLOGIES AND FREQUENCY BANDS

subcarrier spacing (kHz)	Carrier frequency	Symbol number	Slot number $n$
Case A: 15	$f_c \leq 3$ GHz	$\{2, 8\} + 14n$	$\{0, 1\}$
	$3 < f_c \leq 6$ GHz		$\{0, \dots, 3\}$
Case B: 30	$f_c \leq 3$ GHz	$\{4, 8, 16, 20\} + 28n$	$\{0\}$
	$3 < f_c \leq 6$ GHz		$\{0, 1\}$
Case C: 30	$f_c \leq 3$ GHz	$\{2, 8\} + 14n$	$\{0, 1\}$
	$3 < f_c \leq 6$ GHz		$\{0, \dots, 3\}$
Case D: 120	$f_c > 6$ GHz	$\{4, 8, 16, 20\} + 28n$	$\{0, \dots, 3, 5, \dots, 8, 10, \dots, 13, 15, \dots, 18\}$
Case E: 240	$f_c > 6$ GHz	$\{8, 12, 16, 20, 32, 36, 40, 44\} + 56n$	$\{0, \dots, 8\}$

The PSS and SS are two orthogonal maximum-length sequences (m-sequences) of length 127 and are transmitted on contiguous subcarriers. The PSS has three possible sequences  $N_{ID}^{(2)} \in \{0, 1, 2\}$ , each of which maps to an integer representing the sector ID of the gNB. The SSS has 336 possible sequences  $N_{ID}^{(1)} \in \{0, \dots, 335\}$ , each of which maps

to an integer representing the group identifier of the gNB. See Section 7.4.2 of [40]. Both  $N_{ID}^{(1)}$  and  $N_{ID}^{(2)}$  define the physical cell identity of the gNB according to

$$N_{ID}^{Cell} = 3N_{ID}^{(1)} + N_{ID}^{(2)}.$$

PBCH is a physical channel that is used to transmit the system information required to establish the connection between the gNB and the UE. The decoding of the PBCH parameters is explained in details in [41]. The DM-RS signal associated with the PBCH is used for decoding purposes and estimate the channel frequency response. The PBCH DM-RS sequence is generated as explained in Section 7.4.1.4 of [40].

### III. 5G RECEIVER STRUCTURE

This section presents a carrier-aided code SDR to opportunistically extract TOA measurements from 5G signals. The receiver is a modified version from the receiver developed in [41], and it has three main stages: (i) 5G carrier frequency extraction, (ii) acquisition, and (iii) tracking. The rest of this section overviews each of these stages.

#### A. 5G Carrier Frequency Extraction

This stage is required if the carrier frequency of the transmitted 5G signal is unknown to the UE. Otherwise, if this information is known, this stage can be skipped, and the UE can start at the acquisition stage. At this stage, a blind search is performed over all candidate 5G frequency bands in order to find the carrier frequency of the transmitted 5G signals. To do so, the UE searches for available SS/PBCH block, which is carried by the synchronization raster. The synchronization raster indicates the frequency positions of the synchronization block that can be used by the UE for system acquisition when explicit signaling of the synchronization block position is not present. The center frequency of the synchronization raster is the center subcarrier of the SS/PBCH block, i.e., the 121-th subcarrier denoted by  $SS_{REF}$ . The frequency position of  $SS_{REF}$  is defined with corresponding to global synchronization channel number (GSCN) [34]. The parameters defining the  $SS_{REF}$  and GSCN for all frequency ranges are presented in Table IV. More details can be found in Section 5.4.3 in [34].

TABLE IV  
GSCN PARAMETERS FOR THE GLOBAL FREQUENCY RASTER

Frequency range [MHz]	$SS_{REF}$ frequency position	GSCN	Range of GSCN
0 – 3,000	$N \cdot 1,200 \text{ kHz} + M \cdot 50 \text{ kHz}$ $N = 1 : 1 : 2,499, M \in \{1, 3, 5\}^*$	$3N + (M - 3)/2$	2 – 7,498
3,000 – 24,250	$3,000 \text{ MHz} + N \cdot 1.44 \text{ MHz}$ $N = 1 : 1 : 14,756$	$7,499 + N$	7,499 – 22,255
24,250 – 100,000	$24,250.08 \text{ MHz} + N \cdot 17.28 \text{ MHz}$ $N = 1 : 1 : 4,383$	$22,256 + N$	22,256 – 26,639

\* The default value for operating bands with SCS spaced channel raster is  $M = 3$ .

#### B. Acquisition

Knowing the frequency position of  $SS_{REF}$ , the UE starts sampling the 5G signals with at least a sufficient sampling rate to capture the entire SS/PBCH bandwidth. Then, the received signal is converted to the baseband domain by wiping out the carrier frequency. At this level, a coarse estimate of the frame start time and  $N_{ID}^{(2)}$  are obtained by acquiring the PSS signal. The frame start time is used to control the FFT window timing. The CP elements are removed and an FFT is taken to convert the signal into the 5G frame structure. Then, the SS/PBCH block is extracted, and the received SSS signal is correlated with the possible locally generated sequences to determine  $N_{ID}^{(1)}$ , and calculate  $N_{ID}^{Cell}$  of the gNB. Note that the frequency reuse of 5G is 1, i.e., the received signal may have a 5G signal from multiple gNBs with different  $N_{ID}^{Cell}$ . In this case, multiple PSS and SSS peaks can be observed corresponding to more than one gNB. Once the UE determines the  $N_{ID}^{Cell}$  of the acquired signal, it maps the DM-RS

subcarriers and extract it from the SS/PBCH block. The extracted DM-RS is correlated with all possible sequences, and the one with the highest peak is used to estimate the channel frequency response (CFR). Knowing the CFR, the estimated channel distortion is reversed using a channel equalizer. Then, the PBCH message is decoded and the second and fourth symbols of the SS/PBCH block are used to refine the frame start time estimate using estimation of signal parameters via rotational invariance techniques (ESPRIT) algorithm, where in this paper, the frame start time represents the TOA of the received 5G signal. A coarse estimate of Doppler frequency  $\hat{f}_D$  is obtained by looking at the phase difference between the CFR estimated from two distinct symbols in the SS/PBCH block.

### C. Tracking

In this stage, a phase-locked loop (PLL)-aided delay-locked loop (DLL) is used to track the TOA of the received signal. At each tracking loop iteration, the phase effect is wiped off from the received signal, which is assumed constant over a duration of two frames and calculated by integrating  $\hat{f}_D$  over time. Then, the TOA is normalized by the sampling time  $T_s$ , where the integer part of samples  $\text{Int}\{\cdot\}$  is used to control the FFT window timing and the fractional part of samples  $0 \leq \text{Frac}\{\cdot\} < 1$  is removed from the signal using a phase rotation in the frequency-domain. The remaining code and carrier phase errors are estimated using a DLL and PLL, respectively.

The carrier phase discriminator can be defined as the phase of the integrated CFRs over the entire subcarrier as shown in [42]. Then, a second-order loop filter at the output of the discriminator can be used to estimate the rate of change of the carrier phase error  $2\pi\hat{f}_D$ , expressed in rad/s. For code tracking, an early-power-minus-late-power discriminator is used to derive the normalized timing error  $\hat{e}_\tau$  [43]. Assuming that the symbol timing error has linear variations, a second-order loop is used to achieve zero steady-state error. Finally, the TOA estimate  $\hat{e}_\tau$  is updated according to

$$\hat{e}_\tau \leftarrow \hat{e}_\tau + \frac{T_f}{T_s} (v_{DLL} - v_{PLL}),$$

where  $T_f = 20$  ms and  $v_{DLL}$  and  $v_{PLL}$  are the outputs of the DLL and PLL filters, respectively.

## IV. 5G NAVIGATION FRAMEWORK

An EKF is used to estimate the state vector from the 5G pseudorange measurements  $\mathbf{z} \triangleq c\hat{\mathbf{e}}_\tau \triangleq c[\hat{e}_\tau^{(1)}, \dots, \hat{e}_\tau^{(U)}] = [\rho^{(1)}, \dots, \rho^{(U)}]$ , where  $c$  and  $U$  are the speed of light and the number of gNBs, respectively. The pseudorange between the receiver and the  $u$ -th gNB at the  $i$ -th time-step can be expressed as

$$\rho^{(u)}(i) = \|\mathbf{r}_r(i) - \mathbf{r}_{s,u}\|_2 + c \cdot [\delta t_r(i) - \delta t_{s,u}(i)] + \nu_u(i), \quad i = 1, 2, \dots$$

where  $\mathbf{r}_r = [x_r, y_r, z_r]^\top$  is the receiver's 3-D position vector,  $\mathbf{r}_{s,u} = [x_{s,u}, y_{s,u}, z_{s,u}]^\top$  is the gNB's 3-D position vector,  $c$  is the speed of light,  $\delta t_r$  is the receiver's clock bias,  $\delta t_{s,u}$  is the gNB's clock bias, and  $\nu_u$  is the measurement noise, which is modeled as a zero-mean, white Gaussian random sequence with variance  $\sigma_u^2$ . The gNBs positions  $\{\mathbf{r}_{s,u}\}_{u=1}^U$  are assumed to be known, e.g., from radio mapping or cloud-hosted databases. The EKF estimates the state vector defined as

$$\mathbf{x} \triangleq [\mathbf{x}_r^\top, \mathbf{x}_{\text{clk}}^\top]^\top,$$

where  $\mathbf{x}_r = [\mathbf{r}_r^\top, \dot{\mathbf{r}}_r^\top]^\top$  and  $\mathbf{x}_{\text{clk}}$  is the clock state vector  $\mathbf{x}_{\text{clk}}$  defined as  $\mathbf{x}_{\text{clk}} \triangleq [c\Delta\delta t_1, c\Delta\dot{\delta t}_1, \dots, c\Delta\delta t_U, c\Delta\dot{\delta t}_U]^\top$ , where  $\{\Delta\delta t_u \triangleq \delta t_r - \delta t_{s,u}\}_{u=1}^U$  and  $\{\Delta\dot{\delta t}_u \triangleq \dot{\delta t}_r - \dot{\delta t}_{s,u}\}_{u=1}^U$  are the relative clock bias and drift between the receiver and the  $u$ -th gNB. The clock error dynamics are assumed to evolve according to the following discrete-time dynamics

$$\mathbf{x}_{\text{clk}_j}(i+1) = \mathbf{F}_{\text{clk}}\mathbf{x}_{\text{clk}_j}(i) + \mathbf{w}_{\text{clk}_j}(i),$$

where

$$\mathbf{x}_{\text{clk}_j} \triangleq \begin{bmatrix} c\delta t_i \\ c\dot{\delta t}_i \end{bmatrix}, \quad \mathbf{F}_{\text{clk}} = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}, \quad \mathbf{w}_{\text{clk}_j} = \begin{bmatrix} w_{\delta t_i} \\ w_{\dot{\delta t}_i} \end{bmatrix}, \quad \text{for } j \in \{r, s_u\},$$

where  $T \equiv T_f$  is the measurement's sampling time and  $\mathbf{w}_{\text{clk}_j}$  is the process noise, which is modeled as a discrete-time zero-mean white sequence with covariance  $\mathbf{Q}_{\text{clk}_j}$  with

$$\mathbf{Q}_{\text{clk}_j} \triangleq c^2 \cdot \begin{bmatrix} S_{\tilde{w}_{\delta t_j}} T + S_{\tilde{w}_{\delta t_j}} \frac{T^3}{3} & S_{\tilde{w}_{\delta t_j}} \frac{T^2}{2} \\ S_{\tilde{w}_{\delta t_j}} \frac{T^2}{2} & S_{\tilde{w}_{\delta t_j}} T \end{bmatrix},$$

where  $S_{\tilde{w}_{\delta t,i}}$  and  $S_{\tilde{w}_{\delta t,i}}$  are the clock bias and drift process noise power spectra, respectively. The values of  $S_{\tilde{w}_{\delta t,i}}$  and  $S_{\tilde{w}_{\delta t,i}}$  depend on the clock's quality [44].

The receiver is assumed to move in a 2-D plane with a constant known height  $z_r \equiv z_0$ . The receiver's motion is assumed to evolve according to a nearly constant velocity dynamics, i.e.,

$$\ddot{\mathbf{r}}(t) = \tilde{\mathbf{w}},$$

where  $\tilde{\mathbf{w}}$  is a process noise vector, which is modeled as zero-mean white random process with power spectral density  $\tilde{\mathbf{Q}}_{\text{ped}} = \text{diag}[\tilde{q}_x, \tilde{q}_y]$ , where  $\tilde{q}_x$  and  $\tilde{q}_y$  are the power spectral densities of the acceleration in the  $x$ - and  $y$ - directions, respectively [45]. The receiver's discrete-time dynamics are hence given by

$$\mathbf{x}_r(i+1) = \mathbf{F}_r \mathbf{x}_r(i) + \mathbf{w}_r(i),$$

where

$$\mathbf{x} \triangleq \begin{bmatrix} x_r \\ y_r \\ \dot{x}_r \\ \dot{y}_r \end{bmatrix}, \quad \mathbf{F}_r = \begin{bmatrix} 1 & 0 & T & 0 \\ 0 & 1 & 0 & T \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

and  $\mathbf{w}_r$ , the process noise, which is modeled as a discrete-time zero-mean white sequence with covariance  $\mathbf{Q}_r$ , where

$$\mathbf{Q}_r = \begin{bmatrix} \tilde{q}_x \frac{T^3}{3} & 0 & \tilde{q}_x \frac{T^2}{2} & 0 \\ 0 & \tilde{q}_y \frac{T^3}{3} & 0 & \tilde{q}_y \frac{T^2}{2} \\ \tilde{q}_x \frac{T^2}{2} & 0 & \tilde{q}_x T & 0 \\ 0 & \tilde{q}_y \frac{T^2}{2} & 0 & \tilde{q}_y T \end{bmatrix}.$$

## V. EXPERIMENTAL RESULTS

This section validates the proposed 5G opportunistic navigation framework experimentally in a suburban environment using ambient 5G signals. To the best of the author's knowledge, this is the first navigation solution produced using 5G signals from serving gNBs.

### A. Experimental Setup and Environmental Layout

The experiment was performed on the Fairview road in Costa Mesa, California, USA. In this experiment, a quad-channel National Instrument (NI) universal software radio peripheral (USRP)-2955 was mounted on a vehicle, where only two channels were used to sample 5G signals with a sampling ratio of 10 MSps. The receiver was equipped with two consumer-grade cellular omnidirectional Laird antennas. The USRP was tuned to listen to two carrier frequencies corresponding to two U.S. cellular providers whose characteristics are summarized in Table V. The USRP was driven by a GPS-disciplined oscillator (GPSDO) and the sampled data were stored for post-processing. The vehicle was equipped with a Septentrio AsteRx-i V integrated GNSS-IMU whose  $x$ -axis pointed toward the front of the vehicle,  $y$ -axis pointed to the right side of the vehicle, and  $z$ -axis pointed upward. AsteRx-i V is equipped with a dual-antenna multi-frequency GNSS receiver and a VectorNav VN-100 micro-electromechanical system (MEMS) IMU. The loosely-coupled GNSS-IMU with satellite-based augmentation system (SBAS) navigation solution produced by AsteRx-i V was used as ground truth in this experiment. Fig. 3 shows the experimental hardware and software setup.



TABLE V  
GNBs's CHARACTERISTICS

gNB	Carrier frequency [MHz]	$N_{ID}^{Cell}$	Cellular provider
1	632.55	398	T-Mobile
2	872	608	AT&T

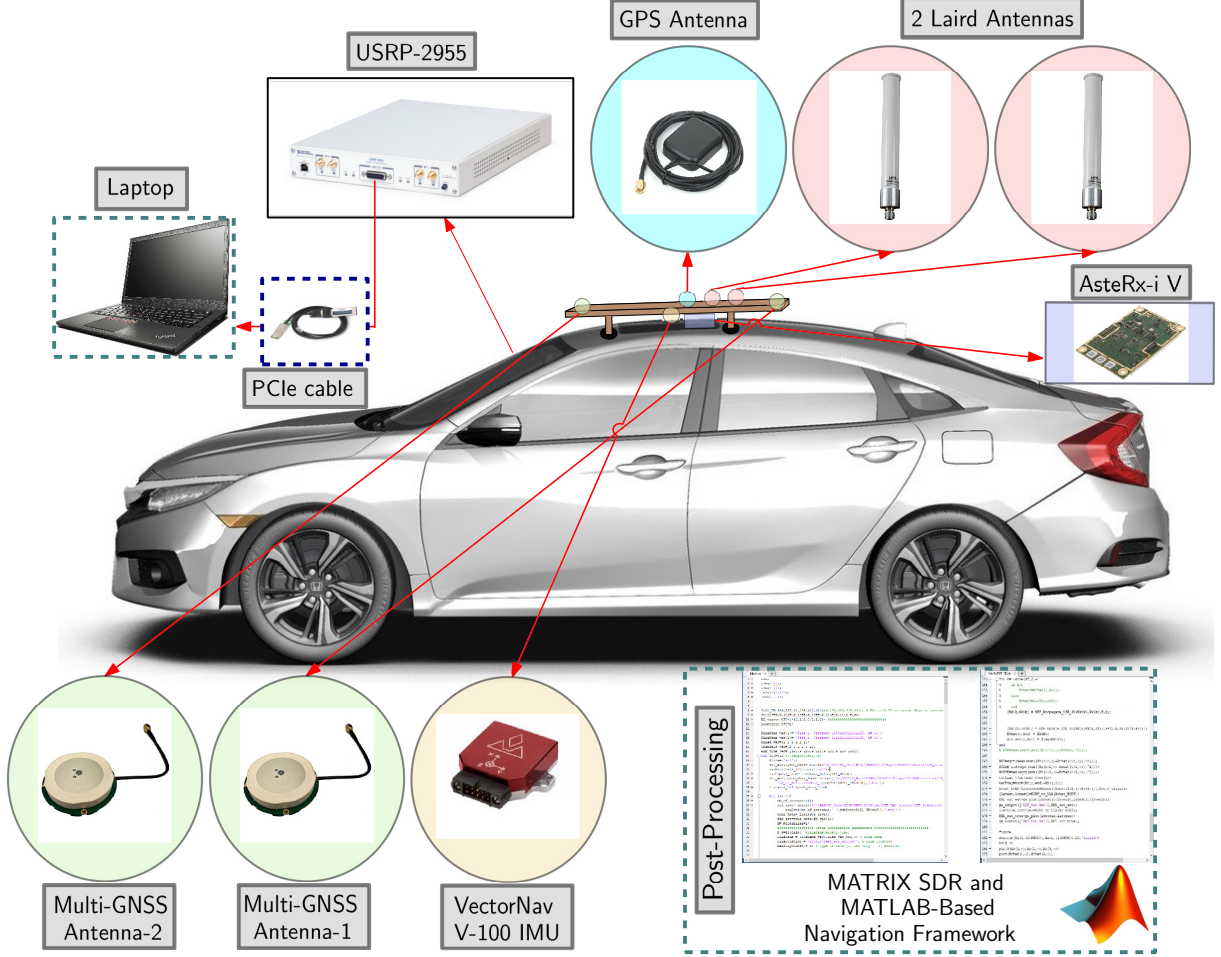


Fig. 3. Experimental hardware and software setup.

## B. Navigation Solution

The vehicle traversed a distance of 1.02 km in 100 seconds. The tracking results of the PSS and the SSS of the received 5G signals produced by Multichannel Adaptive Transceiver Information eXtractor (MATRIX) SDR from both gNBs are shown in Figs. 4. The SDR's DLL bandwidth was tuned to 0.05 Hz, while the PLL bandwidth was tuned to 4 Hz. The true range and Doppler measurements were obtained using the ground truth positions throughout the experiment and the surveyed location of the gNBs. The receiver's position and velocity state vectors and their corresponding covariances were initialized using the output of the GNSS-IMU system. The initial relative clock biases were eliminated, i.e., the EKF's relative clock biases were initialized to zero. The first two 5G measurements were dropped, where the first two position from the GNSS-IMU system were used to initialize the relative clock drifts. The receiver's and gNBs' clocks were modeled as oven-controlled crystal (OCXO) with  $S_{\tilde{w}_{\delta t_j}} = 1.3 \times 10^{-22}$  and  $S_{\tilde{w}_{\delta t_j}} = 7.9 \times 10^{-25}$  [44]. The process noise power spectral densities  $\tilde{q}_x$  and  $\tilde{q}_y$  were set to 0.1 ( $\text{m}^2/\text{s}^3$ ). The measurement noise standard deviations were set to 3 m and 6 m for gNBs 1 and 2, respectively, which were obtained empirically.

Fig. 5 shows the environmental layout, the location of the gNBs, the navigation solution of the proposed 5G framework, and the receiver's ground truth. The performance of the opportunistic navigation framework with two gNBs is summarized in Table VI.

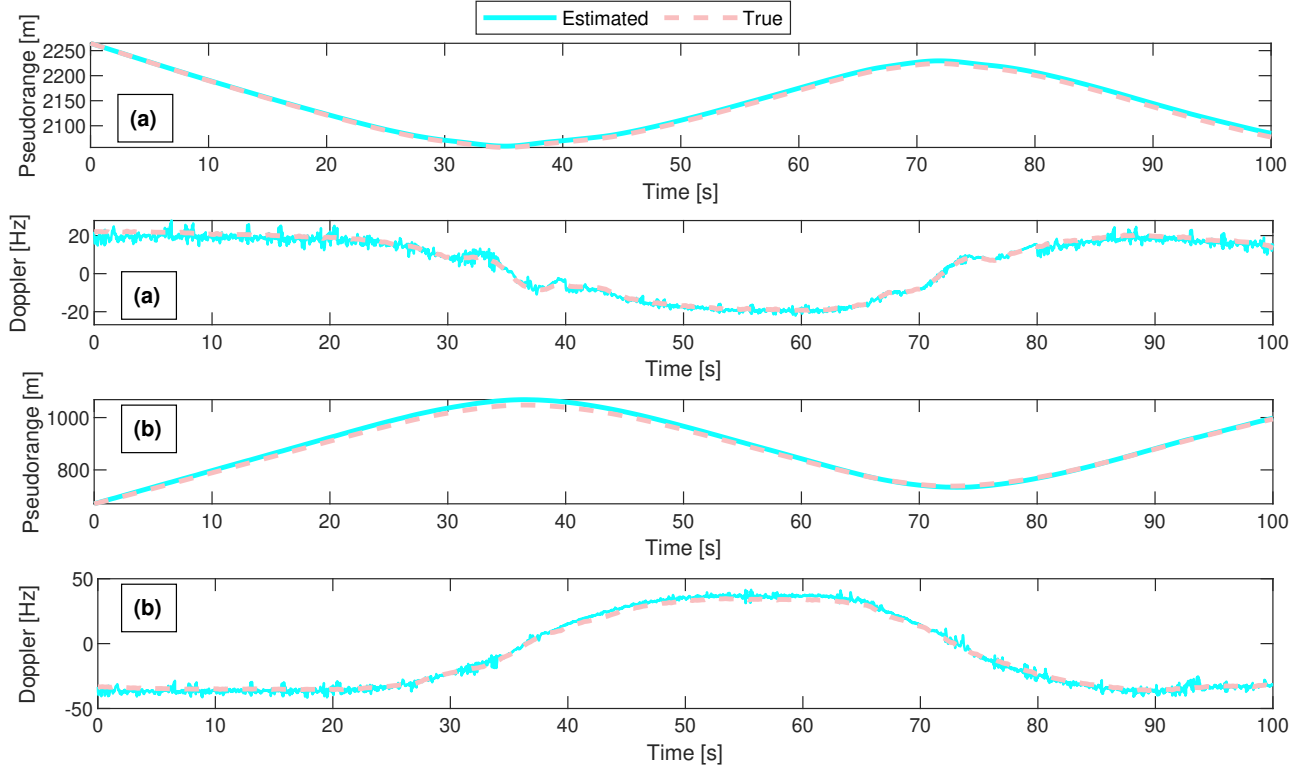


Fig. 4. The estimated pseudorange and Doppler versus true range and Doppler measurements for (a) the T-Mobile gNB with  $N_{ID}^{Cell} = 398$  (b) the AT&T gNB with  $N_{ID}^{Cell} = 608$ .

TABLE VI  
EXPERIMENTAL RESULTS

Metric	Value
Trajectory length	1.02 km
Trip time	100 seconds
Position RMSE	14.93 m
Standard deviation	8.28 m
Maximum error	25.87 m

## VI. CONCLUSION

This paper presented a navigation framework in which 5G signals are exploited for navigation purposes in an opportunistic fashion. The framework includes: (i) a carrier-aided code-based SDR that produces navigation observables from 5G signals and (ii) a navigation filter in which the observables are processed to estimate the UE's position and velocity. An experiment was conducted on a mobile ground vehicle to assess the navigation performance of 5G signals. In the experiment, the vehicle-mounted receiver navigated using 5G signals from two gNBs for 1.02 km in 100 seconds. The proposed 5G navigation framework demonstrated a position RMSE of 14.93 m, while listening to signals from two gNBs only.

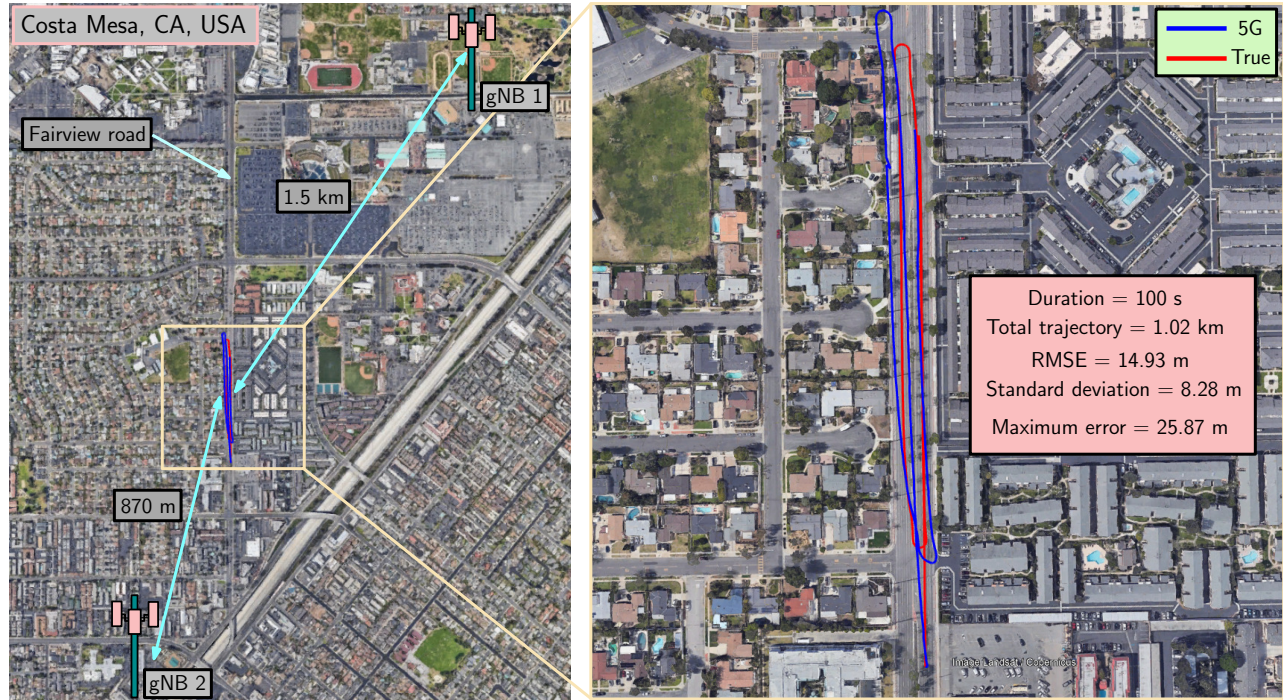


Fig. 5. Environmental layout, gNBs' locations, and the traversed trajectory. The 5G navigation solution exhibited a position RMSE of 14.93 m versus to the GNSS-IMU with SBAS navigation solution produced by AsterX-i V. Image: Google Earth.

## ACKNOWLEDGMENT

The authors would like to thank Joe Khalife for his help in data collection. This work was supported in part by the Office of Naval Research (ONR) under Grant N00014-19-1-2511; in part under the financial assistance award 70NANB17H192 from U.S. Department of Commerce, National Institute of Standards and Technology (NIST); and in part by the U.S. Department of Transportation (USDOT) under University Transportation Center (UTC) Program Grant 69A3552047138.

## References

- [1] 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.
- [2] 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.
- [3] A. Popteev, "Indoor positioning using FM radio signals," Ph.D. dissertation, University of Trento, Italy, 2011.
- [4] V. Moghtadaiee and A. Dempster, "Indoor location fingerprinting using FM radio signals," *IEEE Transactions on Broadcasting*, vol. 60, no. 2, pp. 336–346, June 2014.
- [5] M. Psiaki and B. Slosman, "Tracking of digital FM OFDM signals for the determination of navigation observables," in *Proceedings of ION GNSS Conference*, September 2019, pp. 2325–2348.
- [6] Y. Bai, S. Wu, G. Retscher, A. Kealy, L. Holden, M. Tomko, A. Borriak, B. Hu, H. Wu, and K. Zhang, "A new method for improving Wi-Fi-based indoor positioning accuracy," *Journal of Location Based Services*, vol. 8, no. 3, pp. 135–147, July 2014.
- [7] R. Faragher and R. Harle, "Towards an efficient, intelligent, opportunistic smartphone indoor positioning system," *NAVIGATION, Journal of the Institute of Navigation*, vol. 62, no. 1, pp. 55–72, 2015.
- [8] H. Zou, M. Jin, H. Jiang, L. Xie, and C. Spanos, "WinIPS: Wi-Fi-based non-intrusive indoor positioning system with online radio map construction and adaptation," *IEEE Transactions on Wireless Communications*, vol. 16, no. 12, pp. 8118–8130, 2017.
- [9] P. Thevenon, S. Damien, O. Julien, C. Macabiau, M. Bousquet, L. Ries, and S. Corazza, "Positioning using mobile TV based on the DVB-SH standard," *NAVIGATION, Journal of the Institute of Navigation*, vol. 58, no. 2, pp. 71–90, 2011.
- [10] J. Yang, X. Wang, M. Rahman, S. Park, H. Kim, and Y. Wu, "A new positioning system using DVB-T2 transmitter signature waveforms in single frequency networks," *IEEE Transactions on Broadcasting*, vol. 58, no. 3, pp. 347–359, September 2012.
- [11] L. Chen, O. Julien, P. Thevenon, D. Serant, A. Pena, and H. Kuusniemi, "TOA estimation for positioning with DVB-T signals in outdoor static tests," *IEEE Transactions on Broadcasting*, vol. 61, no. 4, pp. 625–638, 2015.
- [12] R. Landry, A. Nguyen, H. Rasae, A. Amrhar, X. Fang, and H. Benzerrouk, "Iridium Next LEO satellites as an alternative PNT in GNSS denied environments-part 1," *Inside GNSS Magazine*, pp. 56–64, May 2019.
- [13] Z. Kassas, J. Morales, and J. Khalife, "New-age satellite-based navigation – STAN: simultaneous tracking and navigation with LEO satellite signals," *Inside GNSS Magazine*, vol. 14, no. 4, pp. 56–65, 2019.

- [14] Z. Kassas, J. Khalife, M. Neinavaie, and T. Mortlock, "Opportunity comes knocking: overcoming GPS vulnerabilities with other satellites' signals," *Inside Unmanned Systems Magazine*, pp. 30–35, June/July 2020.
- [15] 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.
- [16] 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.
- [17] J. del Peral-Rosado, R. Raulefs, J. López-Salcedo, and G. Seco-Granados, "Survey of cellular mobile radio localization methods: From 1G to 5G," *IEEE Communications Surveys Tutorials*, vol. 20, no. 2, pp. 1124–1148, 2018.
- [18] 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.
- [19] 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.
- [20] M. Driusso, C. Marshall, M. Sabathy, F. Knutti, H. Mathis, and F. Babich, "Indoor positioning using LTE signals," in *Proceedings of International Conference on Indoor Positioning and Indoor Navigation*, October 2016, pp. 1–8.
- [21] 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.
- [22] 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.
- [23] C. Gentner, E. Munoz, M. Khider, E. Staudinger, S. Sand, and A. Dammann, "Particle filter based positioning with 3GPP-LTE in indoor environments," in *Proceedings of IEEE/ION Position, Location and Navigation Symposium*, April 2012, pp. 301–308.
- [24] 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.
- [25] A. Abdallah, K. Shamaei, and Z. Kassas, "Performance characterization of an indoor localization system with LTE code and carrier phase measurements and an IMU," in *Proceedings of International Conference on Indoor Positioning and Indoor Navigation*, September 2019, pp. 1–8.
- [26] 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.
- [27] Z. Kassas, M. Maaref, J. Morales, J. Khalife, and K. Shamaei, "Robust vehicular localization and map matching in urban environments through IMU, GNSS, and cellular signals," *IEEE Intelligent Transportation Systems Magazine*, vol. 12, no. 3, pp. 36–52, June 2020.
- [28] A. Abdallah and Z. Kassas, "Deep learning-aided spatial discrimination for multipath mitigation," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2020, pp. 1324–1335.
- [29] C. Yang and T. Nguyen, "Tracking and relative positioning with mixed signals of opportunity," *NAVIGATION, Journal of the Institute of Navigation*, vol. 62, no. 4, pp. 291–311, December 2015.
- [30] 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.
- [31] K. Shamaei, J. Morales, and Z. Kassas, "A framework for navigation with LTE time-correlated pseudorange errors in multipath environments," in *Proceedings of IEEE Vehicular Technology Conference*, April 2019, pp. 1–6.
- [32] J. Khalife, K. Shamaei, S. Bhattacharya, and Z. Kassas, "Centimeter-accurate UAV navigation with cellular signals," in *Proceedings of ION GNSS Conference*, September 2018, pp. 2321–2331.
- [33] K. Shamaei and Z. Kassas, "Sub-meter accurate UAV navigation and cycle slip detection with LTE carrier phase," in *Proceedings of ION GNSS Conference*, September 2019, pp. 2469–2479.
- [34] 3GPP, "Base station (BS) radio transmission and reception," 3rd Generation Partnership Project (3GPP), TS 38.104, July 2018. [Online]. Available: <https://www.etsi.org/deliver/etsi-ts/138100-138199/138104/15.02.00-60/ts-138104v150200p.pdf>
- [35] X. Cui, T. Gulliver, J. Li, and H. Zhang, "Vehicle positioning using 5G millimeter-wave systems," *IEEE Access*, vol. 4, pp. 6964–6973, 2016.
- [36] N. Garcia, H. Wymeersch, E. Larsson, A. Haimovich, and M. Coulon, "Direct localization for massive MIMO," *IEEE Transactions on Signal Processing*, vol. 65, no. 10, pp. 2475–2487, May 2017.
- [37] K. Han, Y. Liu, Z. Deng, L. Yin, and L. Shi, "Direct positioning method of mixed far-field and near-field based on 5G massive MIMO system," *IEEE Access*, vol. 7, pp. 72 170–72 181, 2019.
- [38] L. Yin, Q. Ni, and Z. Deng, "A GNSS/5G integrated positioning methodology in D2D communication networks," *IEEE Transactions on Signal Processing*, vol. 36, no. 2, pp. 351–362, February 2018.
- [39] M. Koivisto, M. Costa, J. Werner, K. Heiska, J. Talvitie, K. Leppanen, V. Koivunen, and M. Valkama, "Joint device positioning and clock synchronization in 5G ultra-dense networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 2866–2881, May 2017.
- [40] 3GPP, "Physical channels and modulation," <https://www.etsi.org/deliver/etsi-ts/138200-138299/138211/15.02.00-60/ts-138211v150200p.pdf>, 5G; NR; 3rd Generation Partnership Project (3GPP), TS 38.211, July 2018.
- [41] K. Shamaei and Z. Kassas, "Opportunistic navigation with 5G signals," *IEEE Transactions on Wireless Communications*, 2020, submitted.
- [42] 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.
- [43] B. Yang, K. Letaief, R. Cheng, and Z. Cao, "Timing recovery for OFDM transmission," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 11, pp. 2278–2291, November 2000.
- [44] Z. Kassas, V. Ghadiok, and T. Humphreys, "Adaptive estimation of signals of opportunity," in *Proceedings of ION GNSS Conference*, September 2014, pp. 1679–1689.
- [45] 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.