UAV Navigation With 5G Carrier Phase Measurements

Ali A. Abdallah and Zaher M. Kassas
University of California, Irvine

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.

Zaher (Zak) M. Kassas is an associate professor at the University of California, Irvine and director of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He is also director of the U.S. Department of Transportation Center: CARMEN (Center for Automated Vehicle Research with Multimodal AssurEd Navigation), focusing on navigation resiliency and security of highly automated transportation systems. 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. He is a recipient of the 2018 National Science Foundation (NSF) Faculty Early Career Development Program (CAREER) award, 2019 Office of Naval Research (ONR) Young Investigator Program (YIP) award, 2018 IEEE Walter Fried Award, 2018 Institute of Navigation (ION) Samuel Burka Award, and 2019 ION Col. Thomas Thurlow Award. His research interests include cyber-physical systems, estimation theory, navigation systems, autonomous vehicles, and intelligent transportation systems.

ABSTRACT

A framework for unmanned aerial vehicle (UAV) navigation using downlink cellular fifth-generation (5G) signals is presented. In the proposed framework, a software-defined receiver (SDR) is developed to extract carrier phase measurements from received 5G signals. The SDR utilizes the time-domain orthogonality of the orthogonal frequency division multiplexing (OFDM)-based 5G signals. A so-called ultimate synchronization signal (USS) to combine all available resources is proposed. The proposed 5G SDR includes two stages: (i) acquisition stage, in which only unique USS resources are utilized to detect the hearable gNBs and (ii) tracking stage, in which the entire USS is utilized to produce 5G carrier phase measurements. These measurements are processed in an extended Kalman filter (EKF) to assess the navigation performance of the proposed 5G opportunistic SDR. Experimental results are presented of an UAV navigating with the proposed 5G SDR, while receiving signals from four 5G base stations (known as gNBs). It is shown that over a trajectory of 500 m traversed in 145 seconds, the position root mean-squared error (RMSE) was 3.35 m.

I. INTRODUCTION

The dramatic growth in the unmanned aerial vehicle (UAV) industry and their public adoption is propelling researchers and designers to develop integrated navigation systems that ensure continuous, trusted operation. Towards this end, one could diversify the navigation sources, either by introducing (a) complementary sensors (e.g., inertial measurement units (IMUs) [1, 2], cameras [3, 4], lidar [5, 6], etc.) and/or (b) complementary signal-based navigation signals (e.g., WiFi [7, 8], UWB [9, 10], cellular [11–15], low Earth orbit (LEO) satellites [16, 17], etc.). The focus of this paper is to develop a navigation system that exploit 5G cellular signals.

Recent research has considered the use of cellular signals as complementary and alternative navigation system GNSS signals. Code-division multiple access (CDMA) and long-term evolution (LTE), have shown high ranging and localization accuracy using specialized software-defined receivers (SDR) [18–20]. The performance of these SDRs

Preprint of the 2021 ION GNSS+ Conference St. Louis, Missouri, September 20–24, 2021

have been evaluated in different navigation frameworks (standalone, differential, and integrated with other sensors), both indoors and outdoors, where experimental results demonstrated meter-level accuracy positioning accuracy on ground-based receivers [21–24] and sub-meter-level positioning accuracy on aerial vehicle-based receivers [25, 26].

Unconventionally, 5G will be the first cellular system to coexist with the previous system (namely, LTE). Similar to LTE, 5G deploys a structure that uses orthogonal frequency division multiplexing (OFDM) for downlink transmission. The 5G system is very attractive by design for navigation purposes due to:

- High carrier frequencies: High carrier frequencies yield precise carrier phase navigation observables and reduce multipath effects due to high path signal loss.
- Abundance: 5G 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 400 MHz for mmWave band, which 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 GPS signals [27].

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 combination of them is used to achieve accurate positioning from 5G signals. In [28], 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 Gaussian raised-cosine, Gaussian 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 [29]. The paper addressed the limitation of DOA in mMIMO systems in the presence of multipath by proposing a compressed sensing navigation framework which 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 [30]. Simulation results showed that the proposed approach improved the angular resolution by orders of magnitude. In [31], a GNSS/5G integrated positioning framework was developed, in which device-to-device (D2D) range and angle measurements are assumed between mobile terminals (MTs). An experiment was performed with real GNSS data and emulated 5G D2D data, in which the integrated system reduced the GNSS position root mean-squared error (RMSE) from around 5 m to 3 m assuming 10 MTs. A similar study was conducted in [32], where the performance of different hybrid navigation filters exploiting GPS, Galileo and 5G TOA measurements in multipath environment was assessed. The hybrid GNSS/5G was studied for different type of filters with a specific design of the assumed Gaussian errors. Simulation results showed an accuracy of less than 2 m for the hybrid GNSS/5G assuming an urban environment. In [33], a network-based positioning framework using joint TOA and DOA was proposed using cascaded extended Kalman filters (EKFs). 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. In [34], the positioning capabilities of 5G on edge devices was studied. A preliminary simulation study was conducted, in which an integrated 5G/IMU navigation solution exhibited a positioning horizontal absolute error ranging around 2.5 m.

On one hand, all the aforementioned studies are limited to simulations and laboratory emulated 5G signals as well as outdated or restrictive assumptions. In particular the proposed approaches require the user to be in the network so that network-based localization approaches (i.e., utilizing downlink and uplink channels from the gNB to the user and back). This compromises the user privacy by revealing their accuracte location and limits the user to only the gNBs of the network they are subscribed to.

In contrast to existing literature, the authors studied real downlink 5G signals for opportunistic exploitation (i.e., without communicating back with the 5G gNB nor subscribing to the network). In [35], a comprehensive approach for opportunistic navigation with 5G that exploits the downlink channel was developed. The proposed approach extracted navigation observables from the "always-on" transmitted synchronization signals. The proposed SDR was

validated experimentally, where the ranging performance with real 5G signals was evaluated. After removing the effect of the clock bias and drift from the estimated pseudorange, the ranging error standard deviation was shown to be 1.19 m. In [36], the proposed SDR in [35] was modified to extract navigation observables from different synchronization signals. These observables were analyzed and fused in an EKF to estimate the 2-D position and velocity of the receiver, along with the relative clock bias and drift between the receiver and each gNB. Experimental results were presented of a ground vehicle navigating with the 5G SDR in a suburban environment: Costa Mesa, California, USA, while receiving signals from two gNBs. It was shown that over a trajectory of 1.02 km traversed in 100 seconds, the position RMSE and standard deviation were 14.93 m and 8.28 m, respectively. In [37], a more challenging environment compared to [36] was considered for experimental demonstration, where the ground vehicle navigated in an urban environment: Santa Ana, California, USA, while receiving signals from five gNBs intermittently over the entire trajectory. It was shown that over a trajectory of 773 m traversed in 110 seconds, the position RMSE and standard deviation were 4.1 m and 2 m, respectively.

This paper considers UAVs as the navigation platform and develops a more precis navigation approach than the previous work. This paper makes the following contributions:

- First, it develops a carrier phase-based 5G SDR to opportunistically extract 5G carrier phase measurements. The proposed receiver exploits the orthogonality property of OFDM signals in both frequency and time-domains, where all available synchronization signals are combined into one ultimate signal.
- Second, it implements a navigation framework to obtain an accurate navigation on a UAV platform.
- Third, it assesses the proposed system experimentally on a UAV using exiting sub-6 GHz 5G cellular signals.

The remainder of the paper is organized as follows. Section II discusses 5G signal model, frame structure, and potential reference signals for opportunistic navigation. Also, it proposes a 5G ultimate synchronization signal (USS). Section III proposes a USS-based carrier-aided code-based 5G opportunistic navigation receiver. Section IV presents a navigation framework, in which an EKF is used to estimate the UAV's position using 5G carrier phase measurements. Section V demonstrates the experimental results. Section VI gives concluding remarks.

II. 5G SIGNAL STRUCTURE

A. Frame Structure and System Information

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 $\{S_1, \cdots, S_{N_r}\}$ 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.

The duration of the FDD 5G frame is

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

where, $\Delta f_{\max} = 480\,\text{kHz}$, $N_f = 4096$, 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 $N_{\text{symb}}^{\text{subframe},\mu} = N_{\text{symb}}^{\text{slot}} N_{\text{slot}}^{\text{subframe},\mu}$. 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 μ, the number of slots is denoted by $n_s^\mu \in \{0, 1, \cdots, N_{\text{slot}}^{\text{subframe},\mu}\}$ or $n_s^\mu \in \{0, 1, \cdots, N_{\text{slot}}^{\text{frame},\mu}\}$ in an increasing order within a subframe or a frame, respectively. The number of symbols per slot $N_{\text{symb}}^{\text{slot}}$ depends on the type of cyclic prefix and the specified numerology. For different numerologies: the subcarrier spacing, CP type, number of OFDM symbols per slot, number of slots per frame, number of slots per subframe, symbol duration, and CP duration.

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 I. Each element in the 5G frame is uniquely identified for a specific antenna port p and subcarrier configuration μ 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 [38].

TABLE I

The minimum and maximum number of resource blocks and the corresponding bandwidths for different numerologies.

μ	$N_{\text{RB}}^{\min}$	$N_{\text{RB}}^{\max}$	**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. 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 and has an identifier denoted as $\bar{i}_{\text{ssb}}$. The $\bar{i}_{\text{ssb}}$ is a time-dependent part of the DM-RS scrambling initialization specified as an integer from 0 to 7, which is derived in the SS burst configuration from the least significant bits (LSBs) of the SS/PBCH block index and the half-frame number. 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 μ as shown in Table II, where index 0 corresponds to the first OFDM symbol of the first slot in a half-frame.

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 $N_{ID}^{(1)} \in \{0, \cdots, 335\}$, each of which maps to an integer representing the group identifier of the gNB. See Section 7.4.2 of [38]. Both $N_{ID}^{(1)}$ and $N_{ID}^{(2)}$ define the physical cell identity of the gNB according to

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

TABLE II

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 $3 < f_c \leq 6$ GHz	$\{2, 8\} + 14n$	$\{0, 1\}$ $\{0, \cdots, 3\}$
Case B: 30	$f_c \leq 3$ GHz $3 < f_c \leq 6$ GHz	$\{4, 8, 16, 20\} + 28n$	$\{0\}$ $\{0, 1\}$
Case C: 30	$f_c \leq 3$ GHz $3 < f_c \leq 6$ GHz	$\{2, 8\} + 14n$	$\{0, 1\}$ $\{0, \cdots, 3\}$
Case D: 120	$f_c > 6$ GHz	$\{4, 8, 16, 20\} + 28n$	$\{0, \cdots, 3,$ $5, \cdots, 8,$ $10, \cdots, 13,$ $15, \cdots, 18\}$
Case E: 240	$f_c > 6$ GHz	$\{8, 12, 16, 20, 32,$ $36, 40, 44\} + 56n$	$\{0, \cdots, 8\}$

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 [35]. 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 [38].

B. 5G Ultimate Synchronization Signal

In previous 5G-based opportunistic navigation approaches, the proposed navigation receivers considered the orthogonality of the synchronization and channel-estimation signals in frequency-domain, i.e., the transmitted OFDM frame is always re-constructed from the received time-domain data by executing the transmission steps discussed in Subsection II-A in a reverse order, then navigation are estimated by utilization the reference signal with the highest bandwidth. This conventional approach is necessary for communication applications, in which the UE has to extract various system information to initiate two-ways communication with the gNB; however, for UE-based navigation applications, the goal is to produce navigation observables by utilizing the entire frequency and time-domain resources in the signal. For this purpose, this paper presents a navigation receiver that exploits the orthogonality property of OFDM signals in both frequency and time-domains. In this receiver, all available synchronization signals are combined into one signal denoted by the USS. The USS consists of the PSS, SSS, and PBCH DM-RS as shown Fig. 1. Then the time-domain-based sequence is obtained by zero-padding both sides of the signals in the frequency domain. Then, the IFFT is taken, and the L_{CP} elements are added. This procedure is exactly the procedure happening at the gNB, except for having zeros instead of having data outside the SS/PBCH block.

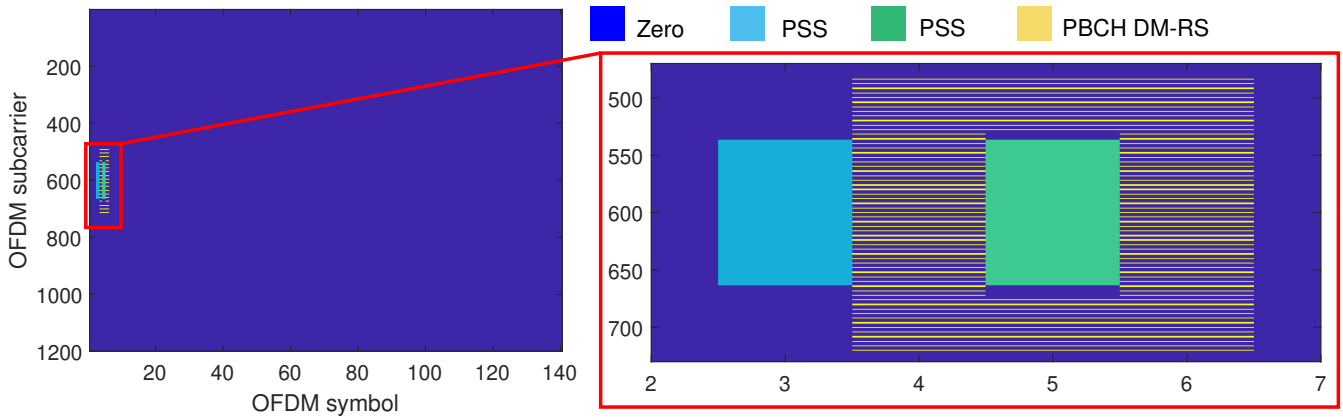

Fig. 1. The 5G OFDM locally-generated frame (i.e., the so-called ultimate synchronization signal (USS).

III. 5G SDR STRUCTURE

In this section, a carrier-aided code phase-based SDR to opportunistically extract TOA measurements from 5G signals is developed. The proposed receiver exploits the USS as a one ultimate sequence. The receiver has three main stages: (i) 5G carrier frequency extraction, (ii) acquisition, and (iii) tracking. The first stage was discussed in the authors' previous work and does not change in the proposed SDR [35, 36]. The rest of this section discusses the other stages.

A. Acquisition

The objective of this stage is to determine which gNBs are in the receiver's proximity and to obtain a coarse estimate of their corresponding code start times and Doppler frequencies. For this purpose, and after extracting the carrier frequency of the surrounding gNBs, the UE starts sampling the 5G signals with at least a sufficient sampling rate to capture the entire SS/PBCH (i.e., USS) bandwidth and convert the signals to the baseband domain by wiping out the carrier frequency. The received discrete-time signal is denoted by $x[n]$, where n is a discrete-time instance. Then, a search over the code start time and Doppler frequency is performed to detect the presence of a signal in $x[n]$ at $n = 0$. For 5G, there are 1008 possible USS sequences resulting from the possible sequences of PSS and SSS and denoted by

$$\mathrm{USS}_{N_{ID}^{Cell}}, \quad \text{for} \quad N_{ID}^{Cell} \in \{0, 1, \cdots, 1007\}. \tag{1}$$

It is worth mentioning that the USS is not transmitted every frame and has a periodicity of 5 ms, 10 ms, 20 ms, 40 ms, 80 ms, or 160 ms. However, a UE can assume a default periodicity of 20 ms during initial cell search or idle mode mobility. In this case, while the USS has a frame duration of 10 ms, it is zero-padded in the time-domain to obtain a 20 ms sequence.

The PSS sequence is not unique for every USS and is common for N_{ID}^{Cell} (mod 3). If the proposed USS is used, as is, to detect the existing N_{ID}^{Cell} in the received 5G signals, signals with same PSS will be also detected as long as the PSS received power is enough to pass the detection threshold. This will cause faulty detection of 5G gNBs. To circumvent this, a USS$^{'}$ is used in the acquisition stage, in which only SSS and PBCH DM-RS are utilized. After detecting the available gNBs, another acquisition is performed using the USS in which PSS is also utilized to obtain more accurate initial estimates of the Doppler frequency $\hat{f}_{D_0}$ and the code start time $\hat{t}_{s_0}$, which are then fed to the tracking loops.

B. Tracking

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

The PLL consists of a phase discriminator, a loop filter, and a numerically-controlled oscillator (NCO). Since USS is a data-less pilot channel, an atan2 discriminator, which remains linear over the full input error range of $\pm\pi$, could be used without the risk of having phase ambiguities. Given the limited dynamics of small UAVs, it was found that a second-order PLL is sufficient to maintain track of the carrier phase. The loop filter transfer function is given by

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

where $\zeta \equiv \frac{1}{\sqrt{2}}$ is the damping ratio and w_n is the undamped natural frequency, which can be related to the PLL's noise-equivalent bandwidth $B_{n,\mathrm{PLL}}$ by $B_{n,\mathrm{PLL}} = \frac{w_n}{8\zeta}\left(4\zeta^2 + 1\right)$ [39]. The output of the loop filter at the m-th subaccumulation $v_{\mathrm{PLL,m}}$ is the rate of change of the carrier phase error, expressed in rad/s. Then, the Doppler frequency estimate is obtained as $\hat{f}_{D_m} = \frac{v_{\mathrm{PLL,m}}}{2\pi}$. The carrier phase estimate is modeled as

$$\hat{\theta}(t_n) = 2\pi \hat{f}_{D_m} t_n + \theta_0, \tag{3}$$

where $t_n = nT_s$ is the sample time expressed in receiver time, T_s is the sampling time, and θ_0 is the initial beat carrier phase of the received signal.

The carrier-aided DLL employs the non-coherent dot product discriminator, in which the prompt, early, and late correlations, denoted by S_{p_m}, S_{e_m}, and S_{l_m}, respectively. The DLL loop filter is a simple gain K, with a noise-equivalent bandwidth $B_{n,\mathrm{DLL}} = \frac{K}{4} \equiv 0.05$ Hz. The output of the DLL loop filter $v_{\mathrm{DLL,m}}$ is the rate of change of the code phase, expresses in s/s. Assuming low-side mixing, the code start time is updated according to

$$\hat{t}_{s_{m+1}} = \hat{t}_{s_m} - (v_{\mathrm{DLL,m}} + \hat{f}_{D_m}/f_c) \cdot N_s T_s, \tag{4}$$

where f_c is the carrier frequency of the received signal and N_s is the number of samples per subaccumulation.

IV. NAVIGATION FRAMEWORK

This section presents a navigation framework, in which an EKF is deployed to estimate the UAV's position using 5G carrier phase measurements.

A. 5G Carrier Phase Measurements

As discussed in Subsection III-B, the carrier phase estimate is obtained as shown in (3). Then the pseudorange estimate corresponding to the u-th gNB $\rho^{(u)}$ can therefore be deduced by multiplying the carrier phase estimate by the wavelength $\lambda^{(u)} = \frac{c}{f_c^{(u)}}$, where c is the speed of light. The pseudorange between the receiver and the u-th gNB at the n-th time-step can be modeled as

$$\rho^{(u)}(n) = \|\boldsymbol{r}_r(n) - \boldsymbol{r}_{s,u}\|_2 + c \cdot [\delta t_r(n) - \delta t_{s,u}(n)] + \nu_u(n), \quad n = 1, 2, \cdots, \tag{5}$$

where in the model above,the term $\lambda^{(u)}\theta_0$ is lumped in the initial relative clock bias, $\boldsymbol{r}_r = [x_r, y_r, z_r]^{\mathsf{T}}$ is the receiver's 3-D position vector, $\boldsymbol{r}_{s,u} = [x_{s,u}, y_{s,u}, z_{s,u}]^{\mathsf{T}}$ is the u-th gNB's 3-D position vector, δt_r is the receiver's clock bias, $\delta t_{s,u}$ is the gNB's clock bias, and ν_u is the measurement noise, which is modeled as a zero-mean, white Gaussian random sequence with variance σ_2^u. The gNBs positions $\{\boldsymbol{r}_{s,u}\}_{u=1}^{U}$ are assumed to be known, e.g., from radio mapping or cloud-hosted databases.

B. EKF Implementation

The EKF state vector consists of the receiver's position and velocity, and the relative clock bias and drift between the receiver and each gNB, given by

$$\boldsymbol{x} \triangleq \left[\boldsymbol{x}_r^{\mathsf{T}}, \boldsymbol{x}_{\mathrm{clk}}^{\mathsf{T}}\right]^{\mathsf{T}},$$

where $\boldsymbol{x}_r = \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}\right]$ and $\boldsymbol{x}_{\mathrm{clk}}$ is the clock state vector $\boldsymbol{x}_{\mathrm{clk}}$ defined as $\boldsymbol{x}_{\mathrm{clk}} \triangleq \left[c\Delta\delta t_1, c\Delta\dot{\delta} t_1, \cdots, c\Delta\delta t_U, c\Delta\dot{\delta} t_U\right]^{\mathsf{T}}$, 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

$$\boldsymbol{x}_{\mathrm{clk}_j}(n+1) = \mathbf{F}_{\mathrm{clk}} \boldsymbol{x}_{\mathrm{clk}_j}(n) + \boldsymbol{w}_{\mathrm{clk}_j}(n),$$

where

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

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

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

where $S_{\tilde{w}_{\delta t,j}}$ and $S_{\tilde{w}_{\dot{\delta} t,j}}$ are the clock bias and drift process noise power spectra, respectively. The values of $S_{\tilde{w}_{\delta t,j}}$ and $S_{\tilde{w}_{\dot{\delta} t,j}}$ depend on the clock's quality [20].

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.,

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

where $\tilde{\boldsymbol{w}}$ 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 [40]. The receiver's discrete-time dynamics are hence given by

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

where

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

and $\boldsymbol{w}_r$, 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 cellular 5G opportunistic navigation receiver and the navigation framework experimentally on a UAV in an urban environment using ambient 5G signals.

A. Experimental Setup and Environmental Layout

An experiment was conducted in Santa Ana, California, USA. In the experiment, the navigator was an Autel Robotics X-Star Premium UAV equipped with a single-channel Ettus 312 USRP connected to a consumer-grade 800/1900 MHz cellular antenna and a small consumer-grade GPS antenna to discipline the on-board oscillator. The cellular receivers were tuned to the cellular carrier frequency 632.55 MHz, which is a 5G frequency allocated to the U.S. cellular provider T-Mobile. The Samples of the received signals were stored for off-line postprocessing with a sampling ratio of 10 MSps. The ground-truth reference trajectory was taken from the on-board Ettus 312 universal software radio peripheral (USRP) GPS solution. The UAV traversed a trajectory of 500 m in 145 seconds. Figures 2 and 3 show the experimental setup and the environment layout, respectively.

Fig. 2. Experimental setup.

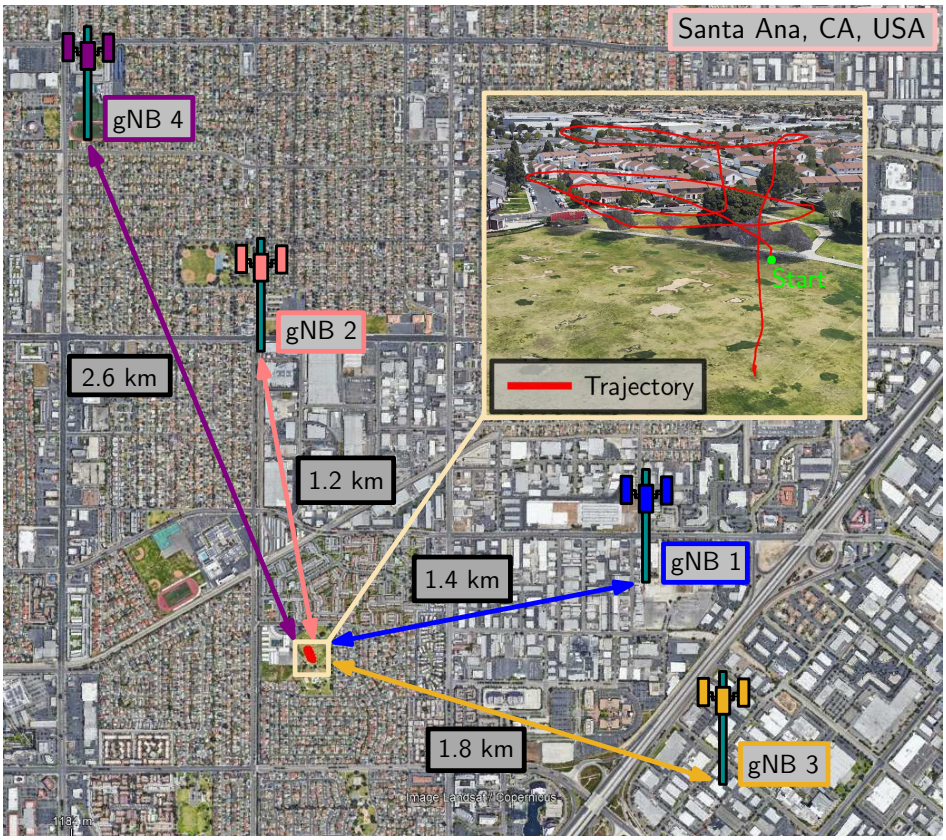

Fig. 3. Environment layout and UAV trajectory.

B. Receiver Output

Next, the signal acquisition stage was applied to detect the ambient 5G signals. Based on experimental data, the Doppler frequency search window was chosen to be between -25 and 25 Hz. The code start time search window was chosen to be one code interval with a delay spacing of one sample. Four gNBs were detected, three of which were hearable starting at $t_n = 0$ seconds, and a fourth gNB was hearable at $t_n = 25$ seconds. The gNBs' positions were mapped prior to the experiment.

In the tracking stage, the noise-equivalent bandwidths $B_{n,\text{PLL}}$ and $B_{n,\text{DLL}}$ were chosen to be 6 Hz and 0.05 Hz, respectively. Fig. 4 shows cellular 5G signal tracking results of the four gNBs including: (i) carrier-to-noise ratio (CNR), (ii) Doppler frequency estimate in solid lines versus expected Doppler obtained using the UAV's ground-truth reference in dashed lines, (iii) Pseudorange estimate in solid lines versus expected range in dashed lines after removing the initial bias, and (iv) range error estimate in solid lines versus measured error in dashed lines.

C. Navigation Solution

The UAV traversed a distance of 500 m in 145 seconds. The receiver's position and velocity state vectors and their corresponding covariances were initialized using the output of the Ettus 312 USRP GPS solution. 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 Ettus 312 GPS solution were used to initialize the relative clock drifts. Table III presents the EKF settings.

Fig. 5 shows the navigation solution of the USS-based 5G receiver versus the Ettus 312 GPS solution. The proposed receiver yielded a UAV position RMSE of 3.35 m.

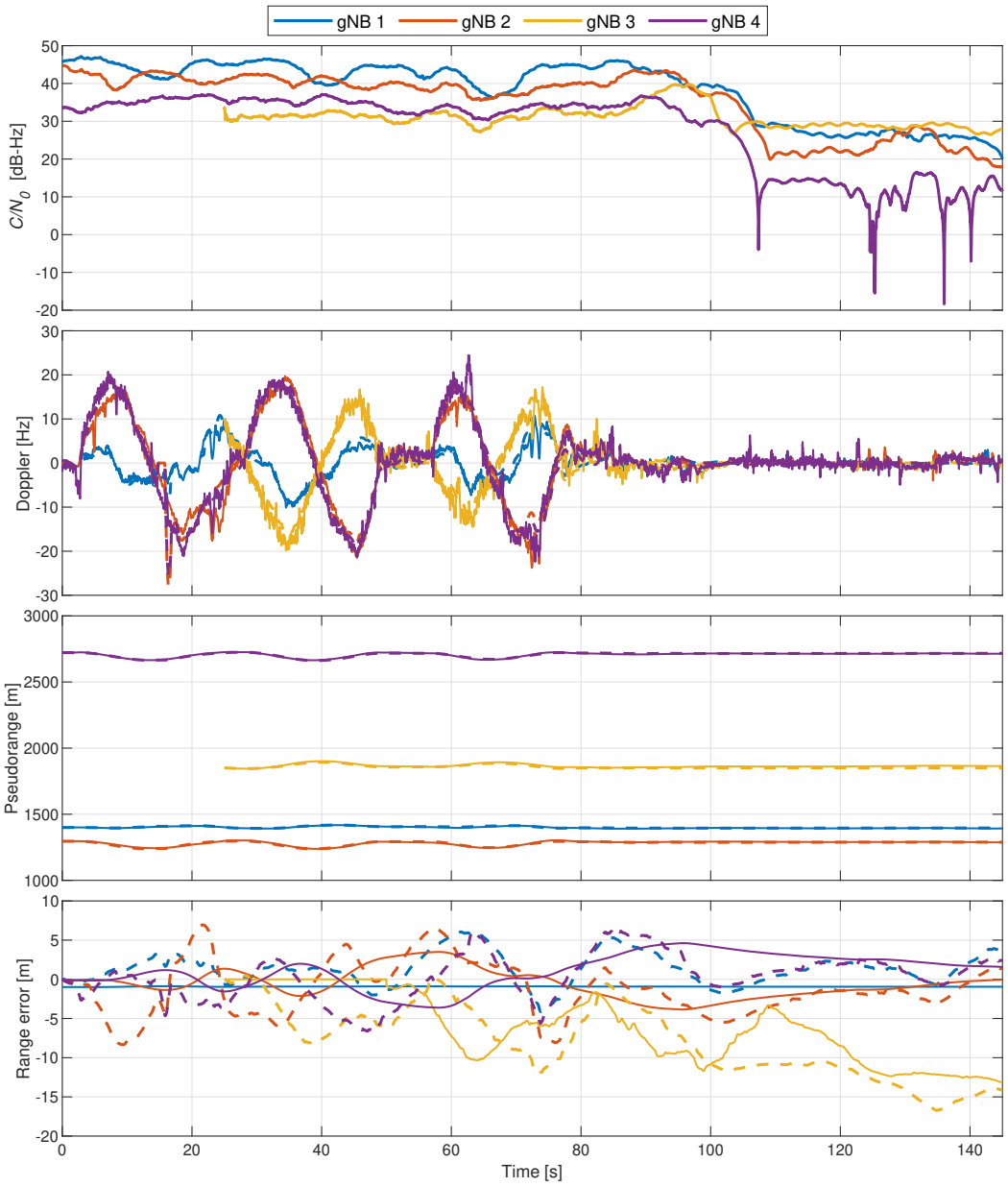

Fig. 4. Cellular 5G signal tracking results of the four gNBs showing: (i) carrier-to-noise ratio (CNR), (ii) Doppler frequency estimate in solid lines versus expected Doppler obtained using the UAV's ground-truth reference in dashed lines, (iii) Pseudorange estimate in solid lines versus expected range in dashed lines after removing the initial bias, and (iv) range error estimate in solid lines versus measured error in dashed lines.

VI. CONCLUSION

This paper presented a 5G opportunistic navigation framework using 5G carrier phase. A 5G SDR was presented, in which the 5G time-domain orthogonality is utilized to combine all available resources in the received 5G signal into one ultimate signal, denoted by USS. The proposed 5G SDR includes two stages: (i) the acquisition stage in which only unique 5G resources (i.e., SSS and PBCH DM-RS) are utilized to detect the hearable gNBs and (ii) the tracking stage in which the entire USS is utilized to produce 5G navigation observable. An EKF was implemented to process the observables and estimate the UE's position and velocity, along with the relative clock bias and drift between the receiver and each gNB. An experiment was conducted on a UAV to assess the navigation performance of the proposed framework. In the experiment, the UAV-mounted receiver navigated using 5G signals from four gNBs

TABLE III
EKF Settings.

Component	Parameter(s)
UAV's motion	$\{\tilde{q}_x, \tilde{q}_y\} \equiv \{1, 1\}\,(\mathrm{m}^2/\mathrm{s}^3)$
UAV's clock	$\left\{S_{\tilde{w}_{\delta t_j}}, S_{\tilde{w}_{\dot{\delta} t_j}}\right\} \equiv \left\{1.3 \times 10^{-22}, 7.9 \times 10^{-25}\right\}$
gNB 1	$\left\{S_{\tilde{w}_{\delta t_j}}, S_{\tilde{w}_{\dot{\delta} t_j}}\right\} \equiv \left\{1.3 \times 10^{-22}, 7.9 \times 10^{-25}\right\}$
gNBs 2,3, and 4	$\left\{S_{\tilde{w}_{\delta t_j}}, S_{\tilde{w}_{\dot{\delta} t_j}}\right\} \equiv \left\{4 \times 10^{-20}, 7.9 \times 10^{-22}\right\}$

Fig. 5. The 5G navigation solution exhibited a position RMSE of 3.35 m versus the ground-truth reference navigation solution. Image: Google Earth.

for 500 m in 145 seconds. The proposed framework exhibited a position RMSE of 3.35 m, while listening to signals from one cellular provider.

ACKNOWLEDGMENT

The authors would like to thank Moahamad Orabi 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 and Grant N00014-19-1-2613, in part by the U.S. Department of Transportation (USDOT) under Grant 69A3552047138 for the CARMEN University Transportation Center (UTC), and in part under the financial assistance award 70NANB17H192 from U.S. Department of Commerce, National Institute of Standards and Technology (NIST).

References

[1] L. Carrillo, A. López, R. Lozano, and C. Pégard, "Combining stereo vision and inertial navigation system for a quad-rotor UAV," *Journal of Intelligent & Robotic Systems*, vol. 65, no. 1, pp. 373–387, 2012.

[2] J. Gross, Y. Gu, and M. Rhudy, "Robust uav relative navigation with DGPS, INS, and peer-to-peer radio ranging," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 12, no. 3, pp. 935–944, July 2015.

[3] B. Schnaufer, P. Hwang, J. Nadke, G. McGraw, and D. Venable, "Collaborative image navigation simulation and analysis for UAVs in GPS challenged conditions," in *Proceedings of IEEE/ION Position Location and Navigation Symposium*, April 2012, pp. 719–729.

[4] N. Mandel, F. Alvarez, M. Milford, and F. Gonzalez, "Towards simulating semantic onboard UAV navigation," in *Proceedings of the IEEE Aerospace Conference*, 2020, pp. 1–15.

[5] J. Kim, I. Bae, C. Quan, S. Lee, W. Son, J. Rhee, S. Kim, and J. Seo, "Collaborative navigation of UAV and UGV using vision and LIDAR sensors," in *Proceedings of ION Pacific PNT Meeting*, April 2013, pp. 762–768.

[6] T. Gee, J. James, W. V. D. Mark, P. Delmas, and G. Gimel'farb, "Lidar guided stereo simultaneous localization and mapping (SLAM) for UAV outdoor 3-D scene reconstruction," in *International Conference on Image and Vision Computing*, November 2016, pp. 1–6.

[7] Y. Zhuang, Y. Li, H. Lan, Z. Syed, and N. El-Sheimy, "Wireless access point localization using nonlinear least squares and multi-level quality control," *IEEE Wireless Communications Letters*, vol. 4, no. 6, pp. 693–696, 2015.

[8] T. Kazaz, G. Janssen, J. Romme, and A. Van der Veen, "Delay estimation for ranging and localization using multiband channel state information," *IEEE Transactions on Wireless Communications*, pp. 1–16, September 2021.

[9] Y. Xu, Y. Shmaliy, Y. Li, and X. Chen, "UWB-based indoor human localization with time-delayed data using EFIR filtering," *IEEE Access*, vol. 5, pp. 16 676–16 683, 2017.

[10] Z. Koppanyi, C. Toth, and D. Grejner Brzezinska, "Scalable ad-hoc UWB network adjustment," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2018, pp. 1502–1508.

[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] 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.

[13] 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.

[14] 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.

[15] J. del Peral-Rosado, O. Renaudin, C. Gentner, R. Raulefs, E. Dominguez-Tijero, A. Fernandez-Cabezas, F. Blazquez-Luengo, G. Cueto-Felgueroso, A. Chassaigne, D. Bartlett, F. Grec, L. Ries, R. Prieto-Cerdeira, J. Lopez-Salcedo, and G. Seco-Granados, "Physical-layer abstraction for hybrid GNSS and 5G positioning evaluations," in *Proceedings of IEEE Vehicular Technology Conference*, September 2019, pp. 1–6.

[16] H. Benzerrouk, Q. Nguyen, F. Xiaoxing, A. Amrhar, A. Nebylov, and R. Landry, "Alternative PNT based on Iridium Next LEO satellites Doppler/INS integrated navigation system," in *Proceedings of Saint Petersburg International Conference on Integrated Navigation Systems*, May 2019, pp. 1–10.

[17] 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.

[18] 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.

[19] 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.

[20] Z. Kassas, "Position, navigation, and timing technologies in the 21st century," J. Morton, F. van Diggelen, J. Spilker, Jr., and B. Parkinson, Eds. Wiley-IEEE, 2021, vol. 2, ch. 37: Navigation with Cellular Signals of Opportunity, pp. 1171–1223.

[21] 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.

[22] M. Maaref and Z. Kassas, "Ground vehicle navigation in GNSS-challenged environments using signals of opportunity and a closed-loop map-matching approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 7, pp. 2723–2723, July 2020.

[23] 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.

[24] C. Yang and A. Soloviev, "Mobile positioning with signals of opportunity in urban and urban canyon environments," in *IEEE/ION Position, Location, and Navigation Symposium*, April 2020, pp. 1043–1059.

[25] 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.

[26] 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.

[27] A. Abdallah, J. Khalife, and Z. Kassas, "Experimental characterization of received 5G signals carrier-to-noise ratio in indoor and urban environments," in *Proceedings of IEEE Vehicular Technology Conference*, April 2021, pp. 1–5.

[28] X. Cui, T. Gulliver, J. Li, and H. Zhang, "Vehicle positioning using 5G millimeter-wave systems," *IEEE Access*, vol. 4, pp. 6964–6973, 2016.

[29] 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.

[30] 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.

[31] 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.

[32] A. Tobie, A. Garcia-Pena, P. Thevenon, J. Vezinet, and M. Aubault, "Hybrid navigation filters performances between GPS, Galileo and 5G TOA measurements in multipath environment," in *Proceedings of ION GNSS Conference*, 2020, pp. 2107–2140.

[33] 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.
[34] C. Guo, J. Yu, W. Guo, Y. Deng, and J. Liu, "Intelligent and ubiquitous positioning framework in 5G edge computing scenarios," *IEEE Access*, vol. 8, pp. 83 276–83 289, 2020.
[35] K. Shamaei and Z. Kassas, "Receiver design and time of arrival estimation for opportunistic localization with 5G signals," *IEEE Transactions on Wireless Communications*, vol. 20, no. 7, pp. 4716–4731, 2021.
[36] A. Abdallah, K. Shamaei, and Z. Kassas, "Assessing real 5G signals for opportunistic navigation," in *Proceedings of ION GNSS Conference*, 2020, pp. 2548–2559.
[37] Z. Kassas, A. Abdallah, and M. Orabi, "Carpe signum: seize the signal – opportunistic navigation with 5G," *Inside GNSS Magazine*, vol. 16, no. 1, pp. 52–57, 2021.
[38] 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.
[39] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed. Ganga-Jamuna Press, 2010.
[40] X. Li and V. Jilkov, "Survey of maneuvering target tracking. Part I: Dynamic models," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 39, no. 4, pp. 1333–1364, 2003.