Exploiting On-Demand 5G Downlink Signals for Opportunistic Navigation

Ali A. Abdallah, *Student Member, IEEE,* Joe Khalife, *Member, IEEE,*, and Zaher M. Kassas, *Senior Member, IEEE*

***Abstract*—This letter presents the first user equipment (UE)-based 5G navigation framework that exploits the "on-demand" 5G downlink signals. In this framework, the entire system bandwidth of incoming 5G signals is utilized in an opportunistic fashion. The proposed framework involves a cognitive approach to acquire the so-called ultimate reference signal (URS), which includes the "on-demand" as well as "always-on" reference signals (RSs). Experimental results are presented showing that the acquired URS: (i) spans the entire 5G downlink bandwidth, (ii) increases the carrier-to-noise ratio by 10 dB compared to state-of-the-art 5G user equipment (UE)-based opportunistic navigation receiver, and (iii) reduces significantly the carrier and code phase errors. A ranging error standard deviation of 2.75 m was achieved with proposed framework with a stationary receiver placed 290 m away from a 5G gNB in a clear line-of-sight environment, which is lower than the 5.05 m achieved when using the "always-on" 5G downlink signals.**

***Index Terms*—5G, positioning, navigation.**

I. Introduction

Fifth-generation (5G) cellular signals are envisioned to play a major role in various positioning and navigation applications, e.g., automated driving systems (ADSs), Internet of things (IoT), etc. Network-based positioning approaches have promised sub-meter-level accuracy with 5G signals [1]–[4]. These approaches require the user to be a subscriber in the network in order to utilize the downlink/uplink channels between the 5G base station (also known as gNodeB (gNB)) and the user equipment (UE). This compromises the user's privacy by revealing their accurate location and limits the user to only gNBs from the network to which they are subscribed. To compensate for this, UE-based approaches have been studied recently and showed meter-level positioning accuracy on ground and aerial vehicles utilizing sub-6 GHz infrastructure [5]–[8]. However, unlike previous cellular systems, 5G applies an ultra-lean transmission policy, which minimizes the transmission of "always-on" signals; hence, limiting UE-based opportunistic navigation to only synchronization signals. To demonstrate the impact of this limitation, consider the possible 5G downlink bandwidth $B_{\rm p}$, which ranges between 4.32 to 397.44 MHz, with synchronization signals spanning a bandwidth $B_{\rm s}$ that ranges between 3.6 to 57.6 MHz. As such, for $B_{\rm p} = 397.44$ and $B_{\rm s} = 57.6$, only 14.5% of the bandwidth is being exploited opportunistically with synchronization signals alone. Higher bandwidth signals yield more precise time-of-arrival estimates and facilitate differentiating the line-of-sight (LOS) signal from multipath components.

This letter makes the following contributions. First, the 5G downlink signals are discussed and a model for exploiting the *entire* bandwidth is presented. Second, an opportunistic navigation framework that exploits on-demand 5G downlink signals is proposed. Third, experimental results of the first signal acquisition and tracking of the so-called ultimate reference signal (URS) is presented, showing that the acquired URS: (i) spans the entire 5G downlink bandwidth, (ii) increases the carrier-to-noise (CNR) ratio by 10 dB compared to state-of-the-art 5G user equipment (UE)-based opportunistic navigation receiver, and (iii) reduces significantly the carrier and code phase errors. The proposed framework is shown to exhibit a ranging error standard deviation of 2.75 m, which is lower than the 5.05 m achieved with "always-on" 5G downlink signals.

This work was supported in part by the Office of Naval Research (ONR) under Grant N00014-19-1-2511 and in part by the U.S. Department of Transportation (USDOT) under Grant 69A3552047138 for the CARMEN University Transportation Center (UTC).

A. Abdallah and J. Khalife were with the Department of Electrical Engineering & Computer Science, University of California, Irvine, USA. Z. Kassas is with Department of Electrical & Computer Engineering, The Ohio State University, USA (email: zkassas@ieee.org). *Corresponding author: Z. Kassas*.

II. 5G Known "Always-On" Downlink Signals

This letter proposes a UE-based framework; thus, it only considers the 5G downlink signal, which employs orthogonal frequency division multiplexing (OFDM) with cyclic prefix (CP) for modulation. A 5G frame has a duration of 10 ms, which consists of 10 subframes, each with a duration of 1 ms. Each subframe breaks down into numerous slots, each of which contains 14 OFDM symbols for a normal CP length. The subcarrier spacing in 5G is flexible and is defined as $\Delta f = 2^{\mu} \times 15$ [kHz], where $\mu \in \{0, \cdots, 4\}$ is a pre-defined numerology. Each subframe is divided into numerous resource grids, each of which has multiple resource blocks with 12 subcarriers. A resource element is the smallest element of a resource grid, defined by its symbol and subcarrier number.

The 5G frame contains two synchronization signals that can be exploited for navigation: primary synchronization signal (PSS) and secondary synchronization signal (SSS), which are two orthogonal maximal length sequences of length 127. PSS has 3 possible sequences and specifies the sector ID of the gNB, and SSS has 336 possible sequences, which specifies the group identifier of the gNB. Together, they provide the frame start time and gNB physical cell ID $N_{ID}^{\rm Cell}$. The physical broadcast channel (PBCH) demodulation reference signal (DM-RS) is also transmitted in the same symbols as the synchronization signals. Altogether, they form what is called as SS/PBCH block. The length of the block is 240 subcarriers.

III. State-of-the-Art 5G Opportunistic Receivers

A. "Always-On" Approach

A carrier-aided code phase 5G receiver was developed in [5], [9] to extract navigation observables from known "always-

on" 5G downlink synchronization signals (SSs). A so-called ultimate SS (USS) was proposed, utilizing the time-domain orthogonality of downlink signals. The USS is essentially the 5G frame with a normalized SS/PBCH and zeros elsewhere. This approach is limited by the ratio of USS bandwidth versus the entire downlink bandwidth $r_{\mathrm{B,USS}}$ and the duty factor $r_{\mathrm{T,USS}}$, which limit the accuracy of the delay and carrier phase estimates, respectively [10]. For different configurations, $r_{\mathrm{B,USS}}$ and $r_{\mathrm{T,USS}}$ range between 14.5%–36% and 0.0104%–5.33%, respectively. Fig. 1 shows the USS locally-generated 5G frame in the frequency-domain, where only the yellow resource elements are known to the UE and the rest is set to zero. The depicted frame represents a 5G downlink signal with $\mu = 0$, 10 MHz bandwidth, $r_{\mathrm{B,USS}} = 36\%$, and $r_{\mathrm{T,USS}} = 1.33\%$.

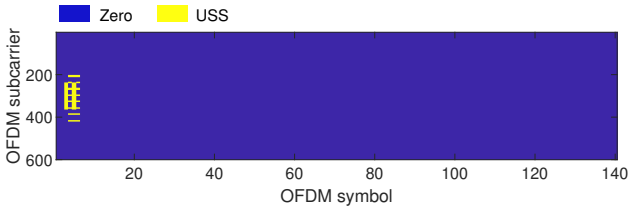

Fig. 1. The 5G OFDM locally-generated frame.

B. Cognitive Approach

The "always-on" approach requires knowing the signal structure, specifically the reference signals (RSs). To alleviate this, a cognitive opportunistic navigation (CON) framework was proposed in [11] to exploit all available RSs, including ones unknown to the UE. The CON framework successfully estimated a periodic 5G RS, which was subsequently tracked, and exploited for navigation. However, the following question arises: How much of the available resources does the cognitively-acquired RS capture compared to the "always-on" (i.e., USS)? Given that the OFDM frame start time is unknown in the CON framework, the only way to assess the acquired signal is to look at the narrowness of the normalized autocorrelation function (ACF) of both RSs, which gives an estimate of the bandwidth that is being exploited (i.e., r_{B}). The results in [11] showed $r_{\mathrm{B,CON}} = 25\%$ versus $r_{\mathrm{B,USS}} = 36\%$.

The CON framework suffers from the following limitations

- The acquisition in the CON framework is challenged by the propagation channel fading and stationarity, which limits the coherent processing interval (CPI), i.e., the time interval in which the Doppler, delay, and channel gains are considered constant. Short CPI means less resources to be captured in the cognitively-acquired signal.
- The CON framework requires the UE to be in motion to exploit multiple gNBs transmitting on the same channel. Yet, to do so, the CON framework uses Doppler subspace to differentiate between gNBs; thus, the framework acquires only the most powerful gNB among different gNBs with similar Doppler profile. This results in acquiring less gNBs than the "always-on" approach.
- The 5G frame start time remains unknown in the CON framework; hence, it is not possible to construct the frame structure of the acquired signal. As such, pre-filtering and power allocation of different RSs cannot be performed, which affects the fidelity of the acquired signal.

IV. Proposed Framework

This section presents the proposed framework in which the on-demand 5G signals are exploited. The framework aims to maximize r_{B} and r_{T} by exploiting other periodic RSs in the 5G downlink signals that are unknown to the UE, such as: channel state information RS (CSI-RS); other DM-RSs for the physical downlink control channel (PDCCH) and physical data shared channel (PDSCH); and phase tracking RS (PTRS).

A. Signal Model

The received baseband signal model can be expressed as

$$r[n] = \sum_{i=1}^{N} \left(\alpha_i c_i[\tau_n - t_{s_i}[n]] \exp\left(j\theta_i[\tau_n]\right) + d_i[\tau_n - t_{s_i}[n]] \exp\left(j\theta_i[\tau_n]\right)\right) + w[n], \quad (1)$$

where $r[n]$ is the received signal at the nth time instant; α_i is the complex channel gain between the UE and the i-th gNB; τ_n is the sample time expressed in the receiver time; N is the number of gNBs; $c_i[n]$ is the periodic RS with a period of L samples; $t_{s_i}[n]$ is the code-delay corresponding to the UE and the i-th gNB at the nth time instant; $\theta_i[\tau_n] = 2\pi f_{D_i}[n] T_s n$ is the carrier phase in radians, with $f_{D_i}[n]$ being the Doppler frequency at the nth time instant and T_s is the sampling time; $d_i[\tau_n]$ represents the samples of some data transmitted from the i-th gNB; and $w[n]$ is a zero-mean independent and identically distributed noise with $\mathbb{E}\{w[m]w^*[n]\} = \sigma_w^2 \delta[m-n]$, where $\delta[n]$ is the Kronecker delta function, and X^* denotes the complex conjugate of random variable X.

B. Proposed Approach

The structure of the proposed framework is shown in Fig. 2. This framework utilizes a so-called URS for 5G opportunistic navigation, which takes advantage of both "always-on" and "on-demand' 5G downlink RSs. Since the USS is always transmitted in the 5G downlink signal, it is used as a prior to acquire OFDM resources, which (i) extends the CPI, (ii) uses the USS subspace to exploit all available gNBs (even gNBs with similar Doppler profile), and (iii) allows preprocessing of the acquired replica to suppress noise and interference and maintain equally-distributed power among different RSs.

1) USS-Based Acquisition and Tracking: In the acquisition stage, the USS is used to determine which gNBs are in the UE's proximity and obtain a coarse estimate of their corresponding code start times $\{\hat{t}_{s_{i,0}}\}_{i=1}^{I}$ and Doppler frequencies $\left\{\hat{f}_{D_{i,0}}\right\}_{i=1}^{I}$, where I is the total number of gNBs.

In the tracking stage, the receiver refines these coarse estimates via a phase-locked loop (PLL) and a carrier-aided delay-locked loop (DLL). At first, node A in Fig. 2 is connected to 1 and the tracking loops use the USS as the local replica.

2) URS Acquisition: After the tracking loop achieves lock, acquisition of the URS is performed as

$$\mathbf{URS}_i \triangleq \frac{1}{K} \sum_{k=1}^{K} \hat{\boldsymbol{y}}_{i,k}, \quad (2)$$

where K is the total number of 5G frames used to capture the URS and $\hat{\boldsymbol{y}}_{i,k}$ is the received k-th 5G frame, defined as

$$\hat{\boldsymbol{y}}_{i,k} \triangleq \exp(-j2\pi \hat{f}_{D_{i,k}}[\boldsymbol{\tau}_k]) \odot \boldsymbol{r}_k[(n - \lfloor \hat{t}_{s_{i,k}} \cdot f_s \rceil)_L], \quad (3)$$

where $\boldsymbol{a} \odot \boldsymbol{b}$ is the element-wise product, $\lfloor \cdot \rceil$ rounds the argument to the nearest integer, $(\cdot)_L$ denotes modulo-L operation, f_s is the sampling frequency, and $\boldsymbol{r}_k$ and $\boldsymbol{\tau}_k$ are defined as

$$\boldsymbol{r}_k \triangleq [r[(k-1)L+1], r[(k-1)L+2], \cdots, r[kL]]^{\mathsf{T}},$$
$$\boldsymbol{\tau}_k \triangleq \left[\tau_{(k-1)L+1}, \tau_{(k-1)L+2}, \cdots, \tau_{kL}\right]^{\mathsf{T}}.$$

3) URS Preprocessing: A main advantage of the proposed framework is its ability to estimate the 5G OFDM frame start time. This allows converting the captured time-domain URS into 5G frame structure (i.e., frequency-domain) where the transmitted symbols are generated, which gives access to each received 5G resource element separately. This capability can be utilized to pre-filter the acquired URS and minimize interference. The preprocessing is summarized in Algorithm 1, where γ is a predefined threshold chosen empirically between 0 and 1, which depends on the fading channel between the gNB and UE. The preprocessing stage outputs a modified version of the URS signal denoted by $\mathbf{URS}_i^{'}$.

Algorithm 1 URS Preprocessing

Input: $\mathbf{URS}_i$
Output: $\mathbf{URS}_i^{'}$

Convert $\mathbf{URS}_i$ to frame structure $\mathbf{URS}_i^f$ (i.e., time-domain serial array to matrix)
Normalize by maximum magnitude of resource elements

$$\mathbf{URS}_i^f = \mathbf{URS}_i^f / \mathrm{URS_m}, \quad \mathrm{URS_m} \triangleq \max\left\{\left|\mathbf{URS}_i^f\right|\right\}$$

for $x = 0$, $x{+}{+}$, while $x <$ Number of symbols **do**
  for $y = 0$, $y{+}{+}$, while $y <$ Number of subcarriers **do**
    if $\left|\mathbf{URS}_i^f(x,y)\right| < \gamma$ **then**
      $\mathbf{URS}_i^f(x,y) \leftarrow 0$
    end if
  end for
end for
Normalize element-wise: $\mathbf{URS}_i^f = \mathbf{URS}_i^f ./ \left|\mathbf{URS}_i^f\right|$
Convert $\mathbf{URS}_i^f$ into time-domain $\mathbf{URS}_i^{'}$

4) URS Tracking: After acquiring and preprocessing the URS, node A switches to 2 and uses the URS as the local replica in standard tracking loops (e.g., as in [12]).

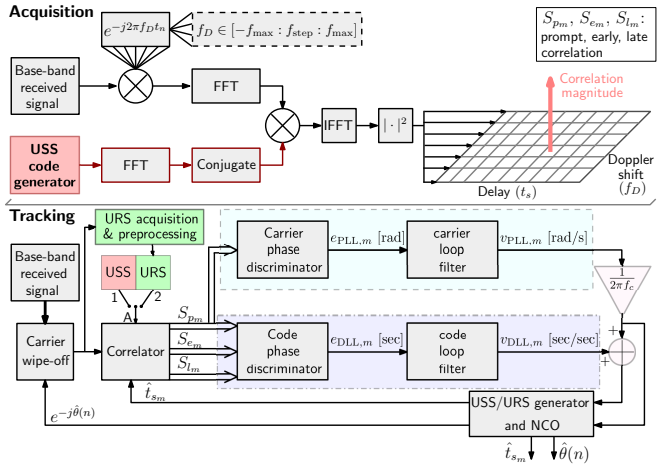

Fig. 2. Block diagram of proposed framework.

V. Experimental Results

This section presents the first UE-based carrier and code phase tracking, exploiting the entire sampled 5G downlink bandwidth. To this end, a stationary National Instrument (NI) universal software radio peripheral (USRP)-2955 was equipped with a consumer-grade omnidirectional Laird antenna to receive 5G downlink signals. The bandwidth was set to 10 MHz and the carrier frequency was set to 632.55 MHz, which corresponds to the U.S. cellular provider T-Mobile. The collected data was stored on a laptop for off-line processing. URS acquisition, preprocessing, and tracking results are presented next.

A. URS Acquisition and Preprocessing

The USRP recorded 5G signals for 300 seconds. The USS was used to detect a nearby gNB as in [5]. The gNB was mapped prior to the experiment and its location was known to the receiver. The receiver determined the gNB cell ID, Doppler, and code start time through a correlation approach detailed in [5], [9]. The cell ID was obtained from the detected synchronization sequences as summarized in Section II. A gNB with $N_{ID}^{\text{Cell}} = 394$ was detected. The processing needed to track the Doppler and code start time followed the steps outlined in Section IV-B, with $\gamma = 0.2$. Due to the limited space in letters, the reader is directed to [5], [9] for the implementation details of Doppler and code start time tracking of gNB signals.

After the tracking loops achieved lock, the proposed framework acquired the URS signal for 4 seconds. Then, the acquired signal was preprocessed as discussed in Algorithm 1. Fig. 3 shows the frame structure of acquired URS before and after preprocessing.

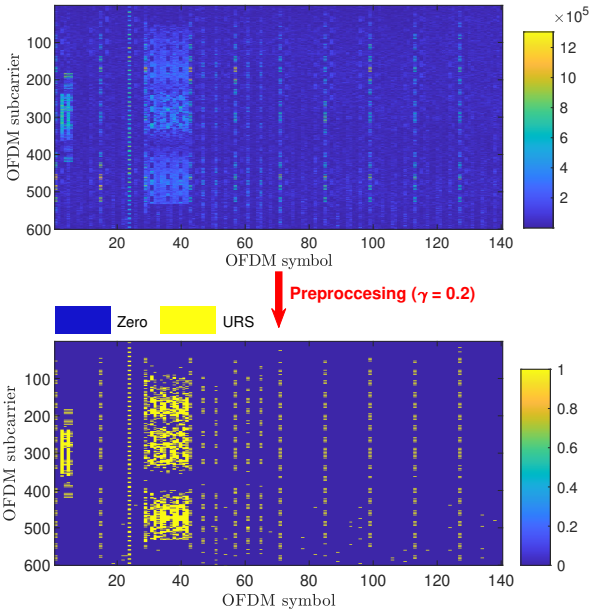

Fig. 3. Fame structure of the URS before and after preprocessing.

To study URS's spectral efficiency $r_{\text{B,URS}}$ and duty factor $r_{\text{T,URS}}$, the number of active subcarriers and symbols was obtained from the preprocessed URS as shown in Fig. 4. Assuming that a URS symbol is active if 10 or more

subcarriers are active within that symbol results in having 32 active symbols; hence, $r_{\mathrm{T,URS}} = 22.86\%$ compared to $r_{\mathrm{T,USS}} = 2.86\%$. For the bandwidth ratio, Fig. 4 shows that $r_{\mathrm{B,URS}} = 100\%$ compared to $r_{\mathrm{B,USS}} = 36\%$ and $r_{\mathrm{B,CON}} = 25\%$. The advantage of this increase in bandwidth ratio can be seen in the narrowness of the URS-ACF as shown in Fig. 5, which gives higher resolution in the time-domain to discriminate the LOS from multipath components.

B. URS Tracking Results

Next, the receiver switched to using the URS for tracking the signal parameters. Fig. 6 shows the tracking results of the proposed framework utilizing the entire sampled 5G bandwidth compared to the USS-based approach. It can be seen how the CNR significantly increased by approximately 10 dB when using the acquired URS. This is due to the fact that in typical time-of-arrival based ranging, the variance of the ranging error is a decreasing function of (i) the signal bandwidth and (ii) the signal-to-noise ratio. In the proposed approach, the bandwidth of the synchronization signal was increased by learning more synchronization sequences in higher subcarriers. Moreover, synchronization sequences were learnt in different symbols of the frame. This resulted in a 10 dB increase in CNR as shown in Fig. 6. Consequently, the standard deviation of the URS-based method is significantly decreased compared to that of the USS-based method. Also, smaller carrier and code phase errors were obtained by the proposed approach, which translates to better ranging performance. It is worth noting that the CNR increase comes with an additional complexity complexity on the order of $O(K \cdot n)$, from (2) and (3). Also, the URS cannot be used until after K time-steps. However, this delay is reasonably short, e.g., 4 seconds in the results herein.

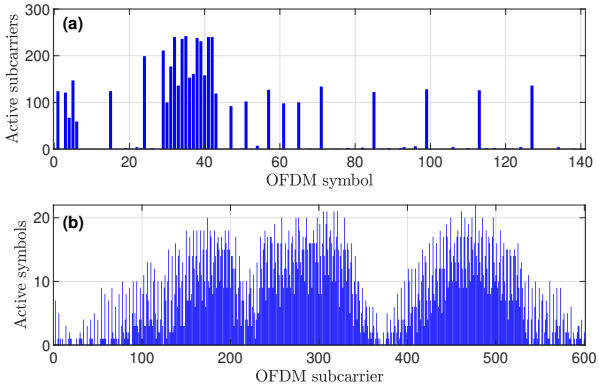

Fig. 4. (a) Number of active subcarriers for each URS symbol and (b) number of active symbols for each URS subcarrier.

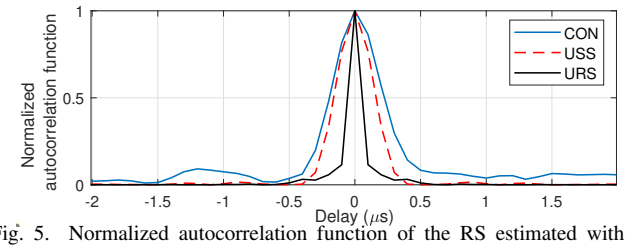

Fig. 5. Normalized autocorrelation function of the RS estimated with the CON receiver compared to the USS.

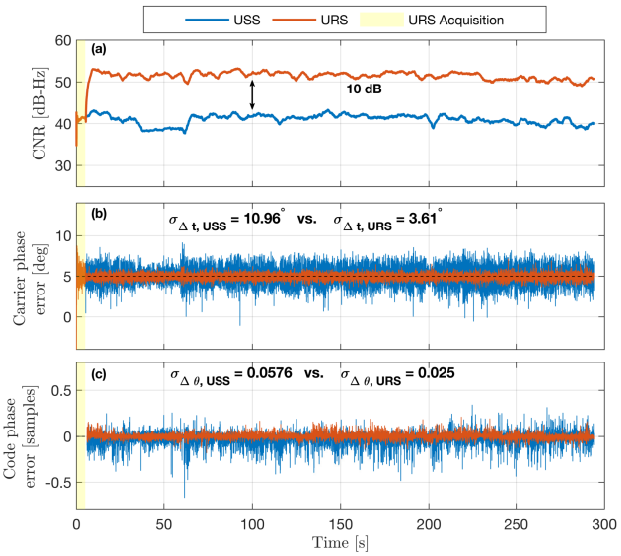

Fig. 6. Cellular 5G tracking results of the proposed URS versus USS: (a) CNR, (b) carrier phase error, and (c) code phase error,

C. Ranging Results

This subsection assesses the ranging performance of the proposed framework. In this stationary scenario, the true range is fixed (290 m); hence, removing the initial range error results in the time history of the range error as seen in Fig. 7. Note that the range error of the proposed URS-based framework drifts slower than that of the USS-based framework. The range error's standard deviation of the USS and URS frameworks were 5.05 m and 2.75 m, respectively.

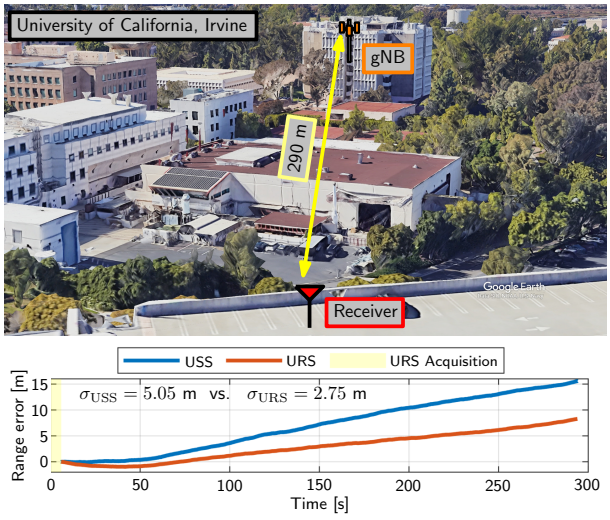

Fig. 7. Environment layout and ranging error of USS and URS frameworks.

VI. Conclusion

This letter proposed a framework to exploit the on-demand 5G downlink bandwidth for navigation. The limitations of existing state-of-the-art "always-on" and cognitive user-based frameworks were discussed. A model of the 5G received signal was formulated, and an acquisition approach to capture the on-demand RSs denoted by URS was presented. Experimental results showed that proposed approach: (i) acquired a URS that spans the entire 5G downlink bandwidth, (ii) achieved 10 dB increase in the C/N_0, and (iii) resulted in significantly more precise code and carrier phase measurements.

REFERENCES

[1] 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, 2017.

[2] 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.

[3] Qualcomm, "Demonstrating advanced 5g innovations [video]," https://www.qualcomm.com/news/onq/2021/06/27/demonstrating-advanced-5g-innovations, June 2021.

[4] M. Pan, P. Liu, S. Liu, W. Qi, Y. Huang, X. You, X. Jia, and X. Li, "Efficient joint DOA and TOA estimation for indoor positioning with 5G picocell base stations," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–19, 2022.

[5] A. Abdallah and Z. Kassas, "UAV navigation with 5G carrier phase measurements," in *Proceedings of ION GNSS Conference*, September 2021, pp. 3294–3306.

[6] I. Lapin, G. Seco-Granados, O. Renaudin, F. Zanier, and L. Ries, "Joint delay and phase discriminator based on ESPRIT for 5G NR positioning," *IEEE Access*, vol. 9, pp. 126 550–126 563, 2021.

[7] L. Chen, X. Zhou, F. Chen, L. Yang, and R. Chen, "Carrier phase ranging for indoor positioning with 5G NR signals," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10 908–10 919, July 2022.

[8] J. Del Peral-Rosado, P. Nolle, S. Razavi, G. Lindmark, D. Shrestha, F. Gunnarsson, F. Kaltenberger, N. Sirola, O. Särkkä, J. Roström, K. Vaarala, P. Miettinen, G. Pojani, L. Canzian, H. Babaroglu, E. Rastorgueva-Foi, J. Talvitie, and D. Flachs, "Design considerations of dedicated and aerial 5G networks for enhanced positioning services," in *Proceedings of Workshop on Satellite Navigation Technology*, April 2022, pp. 1–12.

[9] A. Abdallah and Z. Kassas, "Opportunistic navigation using sub-6 GHz 5G downlink signals: A case study on a ground vehicle," in *Proceedings of European Conference on Antennas and Propagation*, 2022, pp. 1–5.

[10] A. Graff, W. Blount, P. Iannucci, J. Andrews, and T. Humphreys, "Analysis of OFDM signals for ranging and communications," in *Proceedings of ION GNSS Conference*, 2021, pp. 2910–2924.

[11] M. Neinavaie, J. Khalife, and Z. Kassas, "Cognitive opportunistic navigation in private networks with 5G signals and beyond," *IEEE Journal of Selected Topics in Signal Processing*, vol. 16, no. 1, pp. 129–143, 2022.

[12] M. Braasch and A. Dempster, "Tutorial: GPS receiver architectures, front-end and baseband signal processing," *IEEE Aerospace and Electronic Systems Magazine*, vol. 34, no. 2, pp. 20–37, 2019.