Receiver Design and Time of Arrival Estimation for Opportunistic Localization With 5G Signals

Kimia Shamaei* and Zaher M. Kassas®, Senior Member, IEEE

Abstract—A comprehensive approach for opportunistic navigation with fifth-generation (5G) cellular signals that exploits the downlink channel is developed. The structure of possible 5G reference signals that can be exploited is presented. Then, a software-defined receiver (SDR) to extract navigation observables from cellular 5G signals is proposed. The statistics of the code phase error in a multipath-free environment and in the presence of multipath are derived, which are subsequently used to analyze the statistics of the position estimation error with different simulated channel models. Finally, experimental results are conducted to evaluate the ranging performance of the proposed SDR with real 5G signals. After removing the effect of the clock bias and drift from the estimated pseudorange, the ranging error standard deviation is shown to be 1.19 m.

Index Terms—5G, signals of opportunity, navigation, positioning, localization.

I. INTRODUCTION

AUTONOMOUS ground vehicles (AGVs), also known as self-driving cars, already navigate the streets today in several cities around the world. Companies such as Waymo, GM Cruise, and Apple have reported more than 1.5 million miles with their self-driving cars in 2018 [1]. AGVs promise higher quality of life by reducing the number accidents and reducing countless hours of wasted time. However, this is only achievable with reliable autonomy. One important factor to evaluate the reliability of an AGV is called disengagement rate, which is defined based on the California Department of Motor Vehicles (DMV) as the number of times the AGV’s test driver has to disengage the autonomous mode and to take immediate manual control of the vehicle [2]. Although Waymo’s, GM Cruise’s, and Apple’s AGVs are among the top tier performing AGVs, they have reported disengagement rates of 0.09, 0.19, and 0.5 per 1,000 miles, respectively, in 2018. At this point, AGVs are a long way from reliable, full autonomy.

Situational awareness is key to achieving reliable, full autonomy. One of the key enablers is vehicle-to-everything (V2X) communication, which includes vehicle’s communication with other vehicles, pedestrians, infrastructure, and network. In 2009, the United States assigned an IEEE 802.11p-based dedicated short range communication (DSRC) technology to vehicle-to-vehicle (V2V) communication over a pre-specified transmission band to ensure low interference. Although DSRC has been tested over large-scale trials over the past years for V2V transmissions, it has failed to answer the demands for vehicle-to-network (V2N) and vehicle-to-infrastructure (V2I) due to its low transmission bandwidth and lack of proper roadside units. To overcome the limitations of DSRC, a new study group called the IEEE 802.11 Next Generation V2X was formed to work on the IEEE 802.11bd amendment [3]. Besides, the third generation partnership project (3GPP) has developed a cellular-based V2X communication in Release 15 and 16 for the 5th generation (5G) of wireless access technology [4].

Low latency and high data rate are among the main characteristics of 5G signals. To achieve these characteristics, higher transmission bandwidth is essential. However, unlicensed spectrum in lower frequencies is scarce. Due to this limitation, using millimeter waves (mmWaves) for 5G signal transmission has been considered. But, mmWaves suffer from high signal path loss, which can be compensated by beamforming techniques and massive multiple-input multiple-output (mMIMO) antenna structure. Beamforming requires the knowledge of the user’s location. Therefore, 5G-based positioning is not only a service that is provided to users, but also a key enabler to high data rates via proactive resource allocation and beamforming [5].

The 3GPP has evaluated different types of positioning techniques including timing, angle, carrier phase, and received reference signal power-based techniques for 5G downlink and uplink signals in Release 15 and 16 [6]. Positioning performance evaluation of 5G signals is not only limited to 3GPP reports. For example, mmWaves signals’ characteristics were evaluated for positioning in [7]. Position and orientation error bounds were derived in [8], [9] as a function of the Cramér-Rao lower bounds (CRLBs) of the direction-of-departure (DOD), direction-of-arrival (DOA), and time-of-arrival (TOA) for both uplink and downlink communications, showing sub-meter position error, and sub-degree orientation error for mmWaves. A methodology to design 5G networks for precise positioning was proposed in [10] and was evaluated with simulation results showing achievable localization accuracies below 30 centimetres by using cellular ranging measurements with 50 and 100 MHz of system bandwidth. Several channel estimation algorithms were...
proposed in [11]–[13] to estimate DOD, DOA, and TOA of the user equipment (UE) by means of compressed sensing tools, which exploit the sparsity of mmWaves’ channels, showing sub-meter level position error in simulation results. The received reference signal strength from multiple base stations was used in [14] to estimate the DOD and position of the UE in a two-stage Kalman filter, showing sub-meter 3-dimensional (3-D) position accuracy for mmWaves using numerical results. In [15], a method was proposed to jointly estimate the position and orientation of the UE, as well as the location of reflectors or scatterers in the absence of the line-of-sight (LOS) path, showing less than 15 m position root-mean-squared error (RMSE) and less than 7 degree orientation RMSE. To remove the effect of the clock bias, a two-way distributed localization protocol was proposed in [16] and its position and orientation error bounds were derived showing that their proposed approach has identical performance to the synchronized one-way localization approach. A positioning method for multiple-input single-output was proposed in [17], where the DOD and TOA of the received signal is used to localize a mobile receiver. Estimation of signal parameters via rotational invariant techniques (ESPRIT) algorithm was used in [18] to estimate DOA and DOD of the signal.

All the proposed approaches in the literature can be categorized as network-based approaches, since they require communication with the network to transmit a pre-specified reference signal, namely positioning reference signal (PRS), and the systems’ parameters (e.g., number of transmission antennas and beamforming matrix). Although network-based positioning capabilities of wireless communication systems have been defined since 4G systems, cellular providers have practically failed to implement them for two main reasons: (1) additional bandwidth is required to accommodate the PRS, which caused the majority of cellular providers to choose not to transmit the PRS in favor of dedicating more bandwidth for traffic channels, and (2) network-based positioning jeopardizes the UE’s privacy since its location is revealed to the network. This paper proposes an opportunistic navigation with 5G signals to overcome the challenges of network-based positioning, where the positioning is performed at the UE and 5G reference signals that are broadcast to the UE are exploited for navigation purposes. Therefore, the UE’s location is not revealed to the network and the privacy of the UE is protected. Besides, the UE does not require any communication with the network to obtain additional signals or system’s information, which results in no additional overhead for the system. Moreover, the proposed receiver is capable of extracting navigation observables from all the gNBs in the environment, including the ones that are not providing communication service to the UE. This improves the geometric diversity of the exploited gNBs, resulting in a more accurate position estimate.

Over the past decade, opportunistic navigation has been demonstrated in the literature with different types of radio frequency (RF) signals, also known as signals of opportunity (SOPs). SOP examples include cellular [19], [20], digital television [21], [22], AM/FM [23], [24], Wi-Fi [25], [26], and low-earth orbit (LEO) satellite signals [27], [28]. Among SOPs, cellular signals have attracted considerable attentions due to their desirable attributes, including: (1) large transmission bandwidth, (2) high carrier-to-noise ratio (C/No), and (3) favorable geometric diversity [29]. The potential of using cellular code-division multiple access (CDMA) [30]–[35] and long-term evolution (LTE) [36]–[41] have been thoroughly studied in the literature. Experimental results demonstrated meter-level accurate navigation with CDMA and LTE signals indoors [42]–[46] and on ground vehicles [47]–[51] and centimeter-level accurate navigation on aerial vehicles [52]–[54]. CDMA and LTE are the standards of the 3rd and 4th generations (3G and 4G) of wireless communication systems, respectively. The structure of 5G signals was finalized in 2019, and since then, only a few operators have started implementing this standard mainly in major cities around the world. Since 5G signals are new to the field, the literature lacks a thorough study on the potential of 5G signals for opportunistic navigation.

There are several challenges for an opportunistic navigation with 5G signals: (1) low-level 5G frame structure and signaling processing are scattered in several technical reports, which makes them confusing and tiresome to follow for one without proper background, (2) potential reference signals for opportunistic navigation with 5G signals have not been investigated, (3) specialized receivers to opportunistically extract navigation observables from 5G signals have not been developed, and (4) achievable ranging and positioning accuracy with these signals have not been analyzed. This paper tackles these challenges by

- providing the low-level 5G signal structure and describing important parameters for opportunistic navigation,
- presenting potential signals for opportunistic navigation and their related coding and decoding procedure,
- developing a software-defined receiver (SDR) to extract navigation observables from 5G signals,
- deriving ranging and positioning accuracy with 5G signals via numerical simulations, and
- evaluating 5G signals ranging accuracy experimentally.

Experimental results with real 5G signals are provided showing a standard deviation of 1.19 m for the estimated range with the proposed SDR. To the authors’ knowledge, this is the first time that navigation observables are extracted from real 5G signals.

The structure of this paper is organized as follows. Section II discusses the opportunities and challenges of navigation with 5G signals. Section III presents 5G frame structure and the potential reference signals for opportunistic navigation. Section IV shows the structure of the proposed SDR to extract navigation observables from 5G signals. Section V derives the ranging precision of the 5G signals. Section VI analyzes the statistics of the position estimation error. Section VII demonstrates the experimental results. Finally, Section VIII concludes the paper.

II. OPPORTUNISTIC NAVIGATION WITH 5G SIGNALS: OPPORTUNITIES AND CHALLENGES

This section discusses the opportunities and challenges associated with opportunistic navigation with 5G signals.
A. Opportunities

5G signals possess multiple desirable characteristics for opportunistic navigation, which are summarized next.

- **Operating at high frequency bands**: 5G is designed to support transmission at different frequency ranges (FRs). According to the 5G specifications, these FRs can be divided into two main ranges: (1) FR1, which is also known as sub-6 GHz, corresponds to 450 MHz to 6 GHz and (2) FR2, which is also known as mmWaves, corresponds to 24.25 GHz to 52.6 GHz [55]. Due to the high path loss in mmWaves, the received signal will contain a LOS signal with a few dominant multipath components. Therefore, multipath effect on the navigation observables is lower for mmWaves compared to low frequency signals. This will yield a more accurate TOA estimation [7]. Moreover, due to high path loss, 5G networks have higher density to provide a reliable coverage, which results in a desirable geometric diversity for navigation purposes.

- **mMIMO structure**: mMIMO structure in 5G is advantageous for navigation purposes, since (1) the large number of antennas increases the received signal’s carrier-to-noise ratio ($C/N_0$), which has direct relationship with ranging precision and (2) highly directional signals reduce the interference of other 5G base stations (also known as next generation NodeBs or gNBs), which increases the ranging accuracy.

- **Large transmission bandwidth**: A single 5G signal can have a maximum of 100 MHz and 400 MHz bandwidth in sub-6 GHz and mmWaves, respectively. The large transmission bandwidth of 5G signals enables differentiating multipath from LOS, which improves the accuracy of TOA estimation. Besides, the estimated LOS TOA has higher precision with larger transmission bandwidth [39].

B. Challenges

To exploit 5G signals for navigation, the following challenges must be tackled.

- **Ultra-lean transmission**: Inopportunist navigation, a broadcast reference signal is used to derive navigation observables such as TOA and DOA. This signal is known at the UE and is independent of the network operator. Therefore, the UE can exploit it opportunistically for navigation without being a network subscriber. In cellular LTE signals, several reference signals, such as cell-specific reference signal (CRS), are broadcast at regular time intervals even when there is no UE in the environment. This reduces the network energy efficiency and increases the network operational expenses and interference. One of the main features of 5G is its ultra-lean transmission, which minimizes the transmission of these “always-on” signals. 5G has four main reference signals: demodulation reference signals, phase tracking reference signals, sounding reference signals, and channel state information (CSI) reference signals. These reference signals are only transmitted when necessary, making practical implementation of previously developed opportunistic navigation approaches with the frequency-scattered reference signals impossible [56]. This limits opportunistic navigation with 5G signals to only synchronization signal and physical broadcast channel (SS/PBCH) block, which is always-on. As SS/PBCH block is not transmitted on the whole signal’s bandwidth, therefore, one cannot exploit the full ranging accuracy that can be achieved by 5G signals. Besides, SS/PBCH does not have a frequency-scattered structure and the previous techniques for exploiting frequency-scattered reference signals for navigation must be modified for SS/PBCH signals. It is worth noting that since SS/PBCH block is transmitted periodically, it does not introduce any delay on generating the navigation solution.

- **Unknown mMIMO structure**: As discussed in Section I, mMIMO is a requirement for 5G transmission to overcome high path loss, increase throughput, and reduce interference. In a conventional MIMO structure, all signal processing is performed in baseband and each antenna has a separate RF chain. In mmWaves, antenna elements must be placed close to each other to avoid grating lobes. Therefore, allocating one RF chain to each antenna element is impossible for mmWave mMIMO due to space limitations. Moreover, large number of RF chains increases the power consumption, which is a limiting factor [57]. Due to these limitations, hybrid analog-digital precoding and combining has been proposed for 5G transmission. As a result, the channel measured in the digital baseband is intertwined with the choice of analog precoding and combining vectors and the entries of the channel matrix are not directly accessible. Therefore, existing approaches to estimate angles and TOA, such as the ones presented in [11]–[13], [15], are not straightforwardly applicable, since the choice of hybrid-digital precoding structure, the number of antennas at the gNB, and the structure of array depend on the network provider, and are unknown to the UE.

- **Need for specialized receiver structure**: A specialized receiver is required to extract navigation observables from 5G signals, since these signals are not designed for navigation purposes.

- **Unknown gNBs’ clock biases**: 5G signals are designed for communication purposes. Therefore, a stringent level of synchronization between gNBs is not required. Technical literature have shown that 1 μs and higher timing synchronization can satisfy the communication application requirements for 5G, while that can introduce more than 300 m ranging error in positioning applications [58]. In order to achieve an accurate navigation solution with 5G signals, the gNBs’ clock biases must be known and removed from the pseudorange measurements. However, these clock biases are unknown at the UE and must be estimated.

This paper addresses the first three aforementioned challenges by: (1) exploiting SS/PBCH block, which is always-on, to extract navigation observables from 5G signals, (2) limiting the navigation observables to only TOA, and (3) proposing an
III. 5G Signal Structure

This section presents the low-level models of 5G signals and frame structure.

A. 5G Frame Structure

5G downlink transmission is based on orthogonal frequency division multiplexing (OFDM) modulation with cyclic prefix (CP). A 5G frame has a duration of 10 ms and consists of 10 subframes with durations of 1 ms. A frame can also be decomposed into two half-frames, where subframes 0 to 4 form half-frame 0 and subframes 5 to 9 form half-frame 1. This structure enables the coexistence of LTE and 5G systems.

In the time-domain, each subframe breaks down into numerous slots, each of which contains 14 OFDM symbols for a normal CP length. The number of slots per subframe depends on the subcarrier spacing. In contrast to LTE, which has a constant subcarrier spacing of 15 kHz, 5G defines different numerologies $\mu \in \{0, \cdots, 4\}$ to support flexible subcarrier spacing $\Delta f = 2^\mu \cdot 15$ [kHz]. As a result, there are $2^\mu$ slots in each subframe and the CP is down-scaled by a factor of $2^\mu$ compared to the LTE signal’s CP length [59]. Subcarrier spacings of 15 and 30 kHz are more suitable for FR1 since the signal’s attenuation is lower and the cell size can be larger, while higher subcarrier spacings are more applicable to FR2.

In the frequency-domain, each subframe is divided into numerous resource grids, each of which contains 14 OFDM symbols for a normal CP length. The number of slots per subframe depends on the subcarrier spacing. In contrast to LTE, which has a constant subcarrier spacing of 15 kHz, 5G defines different numerologies $\mu \in \{0, \cdots, 4\}$ to support flexible subcarrier spacing $\Delta f = 2^\mu \cdot 15$ [kHz]. As a result, there are $2^\mu$ slots in each subframe and the CP is down-scaled by a factor of $2^\mu$ compared to the LTE signal’s CP length [59]. Subcarrier spacings of 15 and 30 kHz are more suitable for FR1 since the signal’s attenuation is lower and the cell size can be larger, while higher subcarrier spacings are more applicable to FR2.

In the frequency-domain, each subframe is divided into numerous resource grids, each of which contains 14 OFDM symbols for a normal CP length. The number of slots per subframe depends on the subcarrier spacing. In contrast to LTE, which has a constant subcarrier spacing of 15 kHz, 5G defines different numerologies $\mu \in \{0, \cdots, 4\}$ to support flexible subcarrier spacing $\Delta f = 2^\mu \cdot 15$ [kHz]. As a result, there are $2^\mu$ slots in each subframe and the CP is down-scaled by a factor of $2^\mu$ compared to the LTE signal’s CP length [59]. Subcarrier spacings of 15 and 30 kHz are more suitable for FR1 since the signal’s attenuation is lower and the cell size can be larger, while higher subcarrier spacings are more applicable to FR2.

B. 5G SS/PBCH Block

When a UE receives a 5G signal, it must first convert the signal into the frame structure to be able to extract the transmitted information. This is achieved by first identifying the frame start time. Then, knowing the frame start time, the UE can remove the CPs and take a fast Fourier transform (FFT) to construct all the OFDM symbols in the frame.

C. PSS and SSS Sequence Generation

The PSS and SSS are two orthogonal maximum-length sequences (m-sequences) of length $N_{SS} = 127$, which are transmitted on contiguous subcarriers. The PSS is transmitted in one form of three possible sequences, each of which maps to an integer representing the sector ID of the gNB, i.e., $N_{ID}^{(2)} \in \{0, 1, 2\}$. To provide frame timing to the UE, a gNB broadcast synchronization signals (SS) on pre-specified symbol numbers, which are known at the UE. The UE can obtain frame start time by acquiring the SS. An SS includes a primary synchronization signal (PSS) and a secondary synchronization signal (SSS), which provide symbol and frame timing, respectively. The PSS and SSS are transmitted along with the physical broadcast channel (PBCH) signal and its associated demodulation reference signal (DM-RS) on a block called SS/PBCH block. The SS/PBCH block consists of four consecutive OFDM symbols and 240 consecutive subcarriers. Fig. 2 demonstrates an SS/PBCH block structure and Table I shows the subcarriers and symbols allocated to each symbol in the SS/PBCH block.

The frequency location of the SS/PBCH block depends on the 5G high-level signallings. The SS/PBCH block has a periodicity of 20 ms and is transmitted numerous times on one of the half frames, which is also known as SS/PBCH burst. Each SS/PBCH block is transmitted in a different direction using beamforming techniques. The OFDM symbol numbers on which the SS/PBCH block starts and the number of SS/PBCH blocks per frame depend on the numerology and transmission frequency $f_c$ of the signal. Table II summarizes these values based on Section 4.1 of [60]. Index 0 in this table represents the first symbol of the half frame containing SS/PBCH blocks. Note that in the 5G protocol, SS/PBCH is not transmitted on subcarrier spacing of 60 kHz.

![5G frame structure](image-url)
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             | \( f_c \leq 3 \text{ GHz} \) | \( 3 < f_c \leq 6 \text{ GHz} \) | \( \{2, 8\} + 14n \) | \( \{0, 1\} \)
|                         |                   |              | \( \{0, \cdots, 3\} \) |           |
| Case B: 30             | \( f_c \leq 3 \text{ GHz} \) | \( 3 < f_c \leq 6 \text{ GHz} \) | \( \{4, 8, 16, 20\} + 28n \) | \( \{0\} \)
|                         |                   |              | \( \{0, 1\} \) |           |
| Case C: 30             | \( f_c \leq 3 \text{ GHz} \) | \( 3 < f_c \leq 6 \text{ GHz} \) | \( \{2, 8\} + 14n \) | \( \{0, 1\} \)
|                         |                   |              | \( \{0, \cdots, 3\} \) |           |
| Case D: 120            | \( f_c > 6 \text{ GHz} \) | \( \{4, 8, 16, 20\} + 28n \) | \( \{0, \cdots, 3, 5, \cdots, 8, 10, \cdots, 13, 15, \cdots, 18\} \) |           |
| Case E: 240            | \( f_c > 6 \text{ GHz} \) | \( \{8, 12, 16, 20, 32, 36, 40, 44\} + 56n \) | \( \{0, \cdots, 8\} \) |           |

The SS/PBCH block structure.

Fig. 2. SS/PBCH block structure.

The SSS is transmitted in one of 336 possible forms, each of which maps to an integer representing the gNB’s group identifier, i.e., \( N_{ID}^{(1)} \in \{0, \cdots, 335\} \). The values of \( N_{ID}^{(2)} \) and \( N_{ID}^{(1)} \) define the physical cell identity of the gNB according to

\[
N_{Cell}^{ID} = 3N_{ID}^{(1)} + N_{ID}^{(2)}.
\]

The instructions to generate the PSS and SSS sequences are provided in Section 7.4.2 of [59].

D. PBCH Sequence Generation

PBCH is a physical channel to transmit essential system information for establishing a connection between the gNB and UE. These parameters are sent in a block called master information block (MIB). An MIB is a 23 bits message containing: (1) frame number (6 bits), (2) subcarrier spacing (1 bit) (this bit shows subcarrier spacing of 15 or 30 kHz for FR1 and subcarrier spacing of 60 or 120 kHz for FR2), (3) subcarrier offset between the first subcarrier of SS/PBCH block and the first subcarrier of the resource grid containing the SS/PBCH block \( k_{SSB} \) (4 bits), (4) position of the DM-RS corresponding to physical downlink shared channel (PDSCH) (1 bit), (5) parameters related to the physical downlink control channel (PDCCH) and system information block (SIB) (8 bits), (6) a flag showing if the cell is barred or not (a UE may not use a barred cell for cell selection/reselection) (1 bit), (7) a flag to allow intra frequency reselection (1 bit), and (8) a spare bit (1 bit) [61]. PBCH also contains 1 bit message representing the type of message in PBCH, which can be either MIB or a messageClassExtension. Therefore, the size of PBCH message is 24 bits [61]. Once the PBCH message is generated at the higher layers, it is encoded and transmitted on physical resources. Fig. 3 shows the block diagram of PBCH coding stages, in which PBCH message is denoted by vector \( \vec{a} \) of length \( A = 24 \) [59], [62].

In the payload generation stage, PBCH message \( \vec{a} \) is first extended to length \( A = A+8 \) and then interleaved according to Section 7.1.1 in [62]. Next, the resulting vector \( \vec{a} \) is scrambled to \( \vec{a}' \) of size 32 based on Section 7.1.2 of [62]. Then, the entire vector is used to generate cyclic redundancy check (CRC) parity bits of length 32 according to Section 7.1.3 of [62]. The resulting CRC is attached to vector \( \vec{a}' \), resulting in vector \( \vec{c} \) of length 64. The vector \( \vec{c} \) is then passed to the channel coding block, where a polar coding is used to code the message according to Section 7.1.4 of [62]. The output of channel coding block is passed to the rate matching block, resulting in vector \( \vec{f} \) of length 864 as discussed in Section 7.1.5 in [62]. Then, the vector \( \vec{f} \) is scrambled, modulated to quadrature phase-shift keying (QPSK) symbols, and mapped to physical resources according to Section 7.3.3 in [59]. The scrambling code at this stage depends on the SS/PBCH block index. Therefore, by decoding PBCH message, the exact symbol number can be obtained. The final PBCH sequence \( \vec{d}_{PBCH} \) with length of 432 is transmitted on the symbols allocated to this message, which are shown in Fig. 2.

E. DM-RS for PBCH Sequence Generation

A DM-RS is a reference signal, which is transmitted to the UE to provide an estimate of the channel frequency response. In 5G, each physical channel has a DM-RS signal, which is used for decoding that specific physical channel, and also providing some system parameters. The DM-RS is transmitted on only specific symbols and subcarriers (not the whole transmission band). A DM-RS for PBCH depends on the half frame containing the SS/PBCH block \( n_{hf} \), the number of SS/PBCH block transmission per frame, and the SS/PBCH block index \( k_{SSB} \). The structure of DM-RS sequence is shown in Section 7.4.1.4 of [59].

IV. RECEIVER STRUCTURE

This section presents the structure of the proposed SDR to opportunistically extract TOA from 5G signals. The proposed SDR consists of three main stages: (1) carrier frequency extraction, (2) acquisition, and (3) tracking. Each of these stages are discussed in details next.

A. Carrier Frequency Extraction

When a UE is activated, it first needs to perform a blind search over all possible frequencies in order to find any
available SS/PBCH block. In 5G, only specified channel raster can carry SS/PBCH blocks, which is called synchronization raster. The center frequency of the synchronization channel raster, which is equivalent to the frequency of the 121st subcarrier of the SS/PBCH block, is denoted by \( S_{\text{ref}} \). The value of \( S_{\text{ref}} \) is a function of a parameter called global synchronization channel number (GSCN). This function depends on the frequency band of the signal and is presented in Section 5.4.3.1 of [55].

It is worth mentioning that if a UE knows \( S_{\text{ref}} \) a priori, it can skip this stage.

**B. Acquisition**

Once the UE determines the SS/PBCH block center frequency \( S_{\text{ref}} \), it starts sampling at a minimum rate equal to the SS/PBCH transmission bandwidth. Next, it wipes off the carrier frequency to convert the samples into the baseband domain. The resulting samples are correlated with all possible PSS sequences and the PSS sequence corresponding to the highest correlation peak determines the \( N_{1D}^{(1)} \). The location of the peak of the correlation represents the SS/PBCH symbol start time and can be used to control the FFT window. Then, the cyclic prefix is removed from the signal and by taking the FFT from the received samples, the signal is converted into the frame structure. At this stage, the UE can extract the SS/PBCH block. Next, the received SSS signal is correlated with all possible SSS sequences and the one corresponding to the highest correlation peak determines the value of \( N_{1D}^{(2)} \).

Knowing \( N_{1D}^{(1)} \) and \( N_{1D}^{(2)} \), the UE can calculate the cell ID \( N_{1D}^{\text{Cell}} \). The cell ID is used to map the subcarriers allocated to the DM-RS. An exhaustive search must be performed over all possible DM-RS sequences and the one with the highest peak is selected. Once the DM-RS sequence is detected, it can be used to estimate the channel frequency response (CFR). The next stage is to decode the PBCH message. For this purpose, the effect of CFR on the received PBCH message is removed using a channel equalizer. Then, the resulting PBCH message is decoded by following the steps in Fig. 3 in reverse order.

After obtaining the PBCH message, the UE can reconstruct the SS/PBCH block locally. Then, the resulting code on the second or fourth symbol of the SS/PBCH block is used to estimate the CFR and refine the frame start time, which is called TOA in this paper. The TOA refinement can be performed using a super resolution algorithm such as ESPRIT [64]. The phase difference between the CFR on the second and fourth symbols of the PBCH is used to provide a coarse estimate of Doppler frequency \( f_D \). Fig. 4 summarizes the structure of the acquisition stage.

**C. Tracking**

After obtaining a coarse estimate of the TOA, a tracking loop can be used to refine the TOA estimate and keep track of any changes. The tracking loop is composed of a phase-locked loop (PLL)-aided delay-locked loop (DLL) to track the code and carrier phase measurements. Code phase tracking estimates the TOA by estimating the delay of the received pseudo-random code, which is an SS/PBCH block in this manuscript; while carrier phase tracking estimates the TOA from the received carrier waveform. The main components of the PLL and DLL are: a discriminator function, a low-pass filter (LPF), and a numerically-controlled oscillator (NCO). Fig. 5 shows the structure of the proposed tracking loop.

At each tracking loop iteration, the estimated phase, which is obtained by integrating the Doppler frequency \( f_D \) over time, is removed from the baseband signal. Then, the estimated TOA, which is normalized by the sampling time \( T_s \), is divided into a fractional part \( \frac{\text{Frac}\{\cdot\}}{\frac{\text{Int}\{\cdot\}}{\text{Ref}}} < 1 \) and an integer part \( \text{Int}\{\cdot\} \). The integer part is used to control the FFT window, while the fractional part is removed from the signal in the frequency domain using a phase rotation. Then, the DLL and PLL are used to estimate the remaining code and carrier phase errors, respectively.

It has been shown that the PLL discriminator function can be the phase of the integrated CFRs over the entire subcarriers [50]. An early-power-minus-late-power discriminator function can be used for the DLL discriminator function to derive the normalized timing error \( \hat{\epsilon}_n \) [64]. Since a shift in the time-domain is equivalent to a phase rotation in the frequency-domain, the locally generated early and late code signals for the OFDM symbol can be obtained respectively as

\[
S_{\text{early}}(k) = e^{-j2\pi k/k} S(k), \quad S_{\text{late}}(k) = e^{j2\pi k/k} S(k),
\]

for \( k = 0, \cdots, K - 1 \).

where \( S(k) \) is the locally generated SS/PBCH symbol at the \( k \)-th subcarrier, \( K = 240 \) is the number of subcarriers allocated to the SS/PBCH block at each symbol, and \( 0 < \xi < 1/2 \) is the normalized time shift. The early and late correlations in the frequency-domain can be expressed respectively as

\[
R_{\text{early}} = \sum_{k=0}^{K-1} R'(k) S_{\text{early}}(k), \\
R_{\text{late}} = \sum_{k=0}^{K-1} R'(k) S_{\text{late}}(k),
\]
where \( R'(k) \) is the received signal at the \( k \)-th subcarrier after phase shift. The DLL discriminator function is defined as
\[
D_{\text{DLL}} \triangleq |R_{\text{early}}|^2 - |R_{\text{late}}|^2 \triangleq K^2C\Lambda_{\text{DLL}}(\tilde{\tau},\xi) + N_{\text{DLL}},
\]
where \( C \) is the received signal power, \( \Lambda_{\text{DLL}}(\tilde{\tau},\xi) \) is the normalized S-curve function, defined as
\[
\Lambda_{\text{DLL}}(\tilde{\tau},\xi) \triangleq \left[ \frac{\sin(\pi(\tilde{\tau} - \xi))}{K\sin(\pi(\tilde{\tau} - \xi))/K} \right]^2 - \left[ \frac{\sin(\pi(\tilde{\tau} + \xi))}{K\sin(\pi(\tilde{\tau} + \xi))/K} \right]^2,
\]
and \( N_{\text{DLL}} \) represents the noise with zero-mean and variance
\[
\text{var}[N_{\text{DLL}}] \leq 2K^2\sigma^4 \left[ 1 + \frac{C}{K\sigma^2} \left( \frac{\sin(\pi(\tilde{\tau} - \xi))}{\sin(\pi(\tilde{\tau} - \xi))/K} \right)^2 + \frac{C}{K\sigma^2} \left( \frac{\sin(\pi(\tilde{\tau} + \xi))}{\sin(\pi(\tilde{\tau} + \xi))/K} \right)^2 \right],
\]
where equality holds for \( \xi = 0.5 \) and \( \sigma^2 \) is the variance of the received signal’s noise [64]. In the following analysis, \( \xi \) is set to 0.5.

The output of the discriminator functions are first normalized by the slope of the discriminator functions at zero error. Then, a loop filter is used to achieve zero steady-state error. It can be assumed that the symbol timing error has linear variations and a second-order loop filter can be used to achieve zero steady-state error. Therefore, a first-order LPF can be used with a transfer function given by
\[
F(s) = 2\zeta\omega_L + \frac{\omega_L^2}{s},
\]
where \( \omega_L \) is the undamped natural frequency of the delay loop and \( \zeta \) is the damping ratio. The damping ratio was set to 1/\( \sqrt{2} \) to have a step response that rises fast enough with little overshoot [65]. Therefore, the noise-equivalent bandwidth is \( B_L = 0.53\omega_L \) [66]. The loop filter transfer function in (3) is discretized and realized in state-space. The loop update rate was set to two frame duration, i.e., \( T_f = 20 \) ms since SS/PBCH block has periodicity of 20 ms.

Finally, the TOA estimate \( \tilde{\tau} \) is updated according to
\[
\tilde{\tau} \leftarrow \tilde{\tau} + \frac{T_f}{T_s}(v_{\text{DLL}} - v_{\text{PLL}}),
\]
where \( v_{\text{DLL}} \) and \( v_{\text{PLL}} \) are the outputs of the DLL and PLL filters, respectively.

V. CODE PHASE ERROR STATISTICS

In this section, the SS/PBCH block open-loop code phase error is evaluated. For this purpose, a generic model for the channel impulse response (CIR) is considered, as
\[
h(\tau) = \sum_{l=0}^{L-1} \alpha_l \delta(\tau - \tau_l),
\]
where \( L \) is the number of multipath components and \( \alpha_l \) and \( \tau_l \) are the relative attenuation and delay components, respectively, of the CIR’s \( l \)-th path. The code phase error statistics are evaluated in the absence and presence of multipath, i.e., when \( L = 1 \) and \( L \neq 1 \), respectively.

A. Code Phase Error in Multipath-Free Environment

In a multipath-free and noise-free environment, the point at which the discriminator function is zero represents the TOA. However, noise can move the zero crossing point as
\[
\tilde{\tau} = \frac{N_{\text{DLL}}}{k_{\text{DLL}}},
\]
where
\[
k_{\text{DLL}} = \frac{\partial D_{\text{DLL}}(\tilde{\tau},\xi)}{\partial \tilde{\tau}} \bigg|_{\tilde{\tau} = \tau_L / 2} = \frac{4\pi C \cos(\pi K)}{K (2\pi K)^3}. \tag{5}
\]
It has been shown that the open-loop code phase error due to noise is a random variable with zero-mean [64]. The open-loop code phase error variance can be shown to be
\[
\sigma^2 \approx \frac{c^2\pi^2}{128\Delta f^2 K^3 T_{\text{sub}} N_0} \tag{6}
\]
where \( c \) is the speed of light, \( T_{\text{sub}} = 20 \) ms is the subaccumulation time interval, and the approximation is obtained by assuming \( K \gg 1 \) and \( C/N_0 \gg 1 \) dB-Hz and defining the double-sided power spectral density of noise as \( S_n(f) \triangleq N_0/2 \) [50]. Note that carrier-to-noise ratio is defined as \( C/N_0 \triangleq C/T_{\text{sub}}\sigma^2 \), while signal-to-noise ratio is defined as \( \text{SNR} \triangleq (C/N_0)/(1/B_n) \), where \( B_n \) is the noise equivalent bandwidth.

Fig. 6 compares the standard deviation of the code phase error for different values of \( C/N_0 \) and for different numerologies. It can be seen that due to the large transmission bandwidth of higher numerologies, the standard deviation of code phase error is an order of magnitude lower compared to lower numerologies.
It can be seen that (8) not only depends on the multipath delay and in a multipath-free environment, for different values of $C/N_0$, and for different numerologies (i.e., $\mu$).

B. Code Phase Error in a Multipath Environment

In a multipath fading environment, the discriminator function can be expressed as in [64]

$$D_{\text{DLL}} = K^2 A_{\text{DLL}}(\bar{e}_\tau, \xi) + N_{\text{DLL}} + \chi_1 + \chi_2,$$  \hspace{1cm} (7)

where

$$\chi_1 = \left| \sum_{k=0}^{K-1} \sum_{l=1}^{L-1} \alpha_l e^{-j2\pi(k/K)(\tau_l/T_\tau - \xi)} \right|^2 - \left| \sum_{k=0}^{K-1} \sum_{l=1}^{L-1} \alpha_l e^{-j2\pi(k/K)(\tau_l/T_\tau + \xi)} \right|^2,$$

$$\chi_2 = 2\Re \left\{ \left| \sum_{k=0}^{K-1} e^{j2\pi(k/K)\xi} \right| \left( \sum_{k=0}^{K-1} \sum_{l=1}^{L-1} \alpha^*_l e^{j2\pi(k'/K)(\tau_l/T_\tau - \xi)} \right) \right\} - 2\Re \left\{ \left| \sum_{k=0}^{K-1} e^{-j2\pi(k/K)\xi} \right| \left( \sum_{k=0}^{K-1} \sum_{l=1}^{L-1} \alpha^*_l e^{j2\pi(k'/K)(\tau_l/T_\tau + \xi)} \right) \right\},$$

where $\Re\{\cdot\}$ denotes the real part; $\alpha_0 = 1$ and $\tau_0 = 0$; and $\xi = 0.5$. The additional terms $\chi_1$ and $\chi_2$, which are caused only by multipath (not noise), introduce a bias in the estimated open-loop code phase error given by [64]

$$b = \frac{e \left( \sin \left( \frac{\pi}{2R} \right) \right)^3}{4\pi a_\mu \Delta f \cos \left( \frac{\pi}{2R} \right)} (\chi_1 + \chi_2).$$  \hspace{1cm} (8)

It can be seen that (8) not only depends on the multipath delay $\tau_l$, but also on the attenuation of the delays $\alpha_l$ and sampling time, which depends on the numerologies.

In the rest of this subsection, first, the effect of multipath delay is evaluated in Fig. 7 by considering a constant multipath amplitude and increasing the multipath delay for a simplified CIR model. Next, two more realistic CIRs are considered and the statistics of the multipath bias are compared for different numerologies.

To evaluate the effect of multipath delay on the SS/PBCH block ranging error, a channel with only one LOS and one multipath component is considered, where the multipath component has 6 dB lower amplitude than the LOS signal, i.e., $|\alpha_0| = 1$ and $|\alpha_1| = 0.2512$. Fig. 7 shows the results. The solid and dashed lines represent the results for constructive and destructive multipath, respectively, where for constructive multipath $\alpha_0 = 1$ and $\alpha_1 = 0.2512$ and for destructive multipath $\alpha_0 = 1$ and $\alpha_1 = 0.2512e^{j\pi}$. When multipath delay tends to zero, multipath signal traverses the same path as the LOS signal. Therefore, multipath no longer introduces any bias on the pseudorange. It can be seen that although multipath can cause high error on low numerologies, higher numerologies are more robust to multipath. This is due to the fact that the transmission bandwidth is larger for higher numerologies, which makes it possible to differentiate multipath from LOS. Note that in the presented results in this section, the effect of noise is completely neglected. Therefore, the ranging bias in only due to the multipath effect.

A proper channel model is essential for evaluating the effect of multipath on the SS/PBCH ranging performance. The existing channel models must be modified to be adopted for mmWaves, since they have different radio propagation characteristics than sub-6 GHz signals. Over the past years, several channel models have been proposed to model radio propagation characteristics of different frequency bands [67]. In this paper, tapped delay line (TDL) 3GPP channel model is used, which is a proper model for simplified evaluations, e.g., non-MIMO evaluations, and is valid for a frequency range between 0.5 GHz and 100 GHz [68].

Among TDL channel models, TDL-A, TDL-B, and TDL-C represent three different channel profiles with non-LOS (NLOS) propagation. In these channel models, both the LOS path and
Fig. 8. Histogram of multipath-induced code phase error for different numerologies and for (a) TDL-A, (b) TDL-B, (c) TDL-C, (d) TDL-D, and (e) TDL-E channel models with nominal delay spread.

Fig. 9. Mean and standard deviation of the code phase error for different values of delay spread for a TDL-A channel model. TDL-A channel model and delay spreads are presented in Table 7.7.2-1 of [68] and Table III, respectively.

Table III
Scaling Parameters for TDL Channel Models according to Table 7.7.3-1 of [68]

<table>
<thead>
<tr>
<th>Model</th>
<th>Delay Spread [ns]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very short delay spread</td>
<td>10</td>
</tr>
<tr>
<td>Short delay spread</td>
<td>30</td>
</tr>
<tr>
<td>Nominal delay spread</td>
<td>100</td>
</tr>
<tr>
<td>Long delay spread</td>
<td>300</td>
</tr>
<tr>
<td>Very long delay spread</td>
<td>1000</td>
</tr>
</tbody>
</table>

Fig. 9-13 illustrate the mean and standard deviation of the code phase error for each channel model. Fig. 9-11 show that in the NLOS condition, the multipath bias can be significantly large, resulting in large position estimation error. Here, it is

 multipath follow Rayleigh distribution. Therefore, there is no dominant signal along the LOS path and the LOS signal may or may not exist. These channels model heavily built-up urban environments (e.g., Manhattan, New York, USA). In contrast, TDL-D and TDL-E channel profiles are considered to model a LOS propagation environment, where there is a dominant signal along the LOS path. In these channels, the LOS signal follows a Rician fading distribution and the multipath follows Rayleigh distribution. TDL-D and TDL-E channels represent different environments with $K$-factors of $K_1 = 13.3$ dB and $K_1 = 22$ dB, respectively. Channel delay’s taps can have different delay spreads from very short to very long as explained in Table III. For each channel model, $10^5$ channel taps are randomly generated according to the specified distributions in Section 7.7.2 of [68]. Then, multipath error is calculated according to (8). Fig. 8 shows the histogram of the code phase error for different numerologies and for different TDL channel profiles with nominal delay spread. Similar figures can be plotted for the rest of the delay spreads. It can be seen that the distribution has slightly heavier tail for positive multipath errors, which is due to the fact that multipath delays are always larger than the LOS delay. By comparing Fig. 8(a)-(c) with Fig. 8(d) and 8(e), it can be seen that when LOS is blocked or multipath dominates LOS signal (as in TDL-A, TDL-B, and TDL-C channel profiles), a large bias with nonzero-mean is introduced to the measured pseudoranges.
imperative to identify and remove the erroneous measurements from the set of measurements to reduce the location estimation error. Numerous techniques have been developed on how to identify this type of measurements \[69\], \[70\]. This topic is out of the scope of this paper and is deferred for future work. Note that in practical scenarios, the NLOS bias is expected to be lower than what is presented in Fig. 9-11. This is due to the fact that the receiver continuously estimates the received carrier-to-noise ratio and it stops tracking the signal when the received carrier-to-noise ratio is low. This condition is not considered in the generated simulation results presented in Fig 9-11. Fig. 12 and Fig. 13 show that for each channel model, e.g., a TDL-D with short delay spread, increasing subcarrier spacing (i.e., increasing numerologies) reduces the mean and standard deviation of the error. This is due to the fact that for larger subcarrier spacing, the SS/PBCH signal bandwidth is larger, which provides higher resolution to differentiate the LOS from multipath. Fig. 7, 12, and 13 also
show that pseudorange error does not decrease monotonically with the multipath delay. This is due to the limited band of the received signal, which causes a sinc autocorrelation function in the time-domain.

VI. POSITION ESTIMATION ERROR STATISTICS

The structure of the proposed SDR to extract navigation observables from 5G signals was discussed in Section IV. Then, the achievable ranging precision and the model of multipath error were derived in Section V. In this section, these results are used to derive the statistics of the position estimation error.

A. TOA Measurement Model

Consider a 2-dimensional (2D) network of $U \geq 3$ gNBs, which are distributed independently and uniformly around the UE with a binomial point process (BPP) model [71]. The minimum distance between the UE and the gNBs for far-field assumption to hold is assumed to be $d_{\text{min}}$. The maximum distance for which ranging signals can be detected by the UE is assumed to be $d_{\text{max}}$. The location of the $u$-th gNB can be presented by $(d^{(u)}, \phi^{(u)})$, where $d^{(u)} = \| r_s - r_s^{(u)} \|_2$ is the distance between the $u$-th gNB and the UE and $\phi^{(u)} = \arctan \left( \frac{y_s^{(u)} - y_s}{x_s^{(u)} - x_s} \right)$, where $r_s = [x_s, y_s]^T$ and $r_s^{(u)} = [x_s^{(u)}, y_s^{(u)}]^T$ are the locations of the UE and the $u$-th gNB, respectively.

The UE makes TOA measurements to all gNBs. Each TOA measurement contains the distance of the UE to each gNB (i.e., true range), the difference of the clock bias between the UE and the gNB, multipath-induced error, and measurement noise. For simplicity, it is assumed that the gNBs and UE are synchronized and their clock biases do not affect the TOA measurements. By multiplying the estimated TOAs to the speed of light, pseudorange measurements can be obtained according to

$$\rho = d + b + \varepsilon,$$

where $\rho \triangleq [\rho^{(1)}, \ldots, \rho^{(U)}]^T$ is the vector of pseudorange measurements; $d \triangleq [d^{(1)}, \ldots, d^{(U)}]^T$ is the vector of ranges; $b \triangleq [b^{(1)}, \ldots, b^{(U)}]^T$ is the vector of biases caused by multipath according to (8), with mean $\mu_b$ and covariance matrix $\Sigma_b$; and $\varepsilon \triangleq [\varepsilon^{(1)}, \ldots, \varepsilon^{(U)}]^T$, where $\varepsilon^{(u)}$ is the measurement noise, which is modeled as zero-mean Gaussian random variable with standard deviation of $\sigma_\varepsilon^{(u)}$. Since the effect of multipath and noise on TOA measurements are independent, the covariance matrix of $\rho$ can be obtained according to

$$\Sigma_\rho \triangleq \text{cov} \{ \rho \} = \Sigma_\varepsilon + \Sigma_b,$$

where $\Sigma_\varepsilon \triangleq \text{cov} \{ \varepsilon \} = \text{diag} \left[ \sigma_\varepsilon^{(1)^2}, \ldots, \sigma_\varepsilon^{(U)^2} \right]$ and $\text{diag}$ represents diagonal matrix.

Denoting the received carrier-to-noise ratio from the gNB located at distance $d_{\text{min}}$ to the UE by $C/N_0$, and using the path-loss model, it can be shown that the carrier-to-noise ratio of the $u$-th gNB follows

$$(C/N_0)^{(u)} = \left( \frac{d_{\text{min}}}{d^{(u)}} \right)^a C/N_0,$$

where $a$ is the path-loss exponent, which depends on the propagation environment [72]. Therefore, using the results of (6), the $u$-th gNB’s TOA measurement noise variance can be modeled according to

$$\sigma_\varepsilon^{(u)^2} = \frac{2 \pi^2}{128 \Delta f^2 R^3 T_{\text{sub}} C/N_0} \left( \frac{d^{(u)}}{d_{\text{min}}} \right)^a [m^2].$$

B. Position Estimation Error Statistics

The UE can obtain an estimate of $\Sigma_\varepsilon$ using the correlation function. However, the UE does not have any information about the multipath bias on its estimated TOA, since the channel impulse response parameters are not estimated in the DLL. Therefore, $b$ is unknown at the UE and is assumed to be zero.

Since the pseudorange measurements are nonlinear functions of the UE’s position (cf. (11)), one can readily estimate the UE’s position via a weighted nonlinear least squares (WNLS) estimator. Of course, more sophisticated estimators can be also employed. Utilizing a WNLS, if $b$ is nonzero, it can be shown that the UE’s position estimation error $\hat{r}$ has the following mean and covariance matrix

$$\mathbb{E} \{ \hat{r} \} = (G^T \Sigma_\varepsilon^{-1} G)^{-1} G^T \Sigma_\varepsilon^{-1} \mu_b,$$

$$\text{cov} \{ \hat{r} \} = (G^T \Sigma_\varepsilon^{-1} G)^{-1} + (G^T \Sigma_\varepsilon^{-1} \Sigma_b \Sigma_\varepsilon^{-1} G) \times (G^T \Sigma_\varepsilon^{-1} G)^{-1},$$

where

$$G \triangleq \begin{bmatrix} \cos \phi^{(1)}, & \cdots, & \cos \phi^{(U)} \\ \sin \phi^{(1)}, & \cdots, & \sin \phi^{(U)} \end{bmatrix}^T.$$
TABLE IV

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency band</td>
<td>mmWave</td>
</tr>
<tr>
<td>antenna configuration</td>
<td>SISO</td>
</tr>
<tr>
<td>$C/N_0$</td>
<td>${50, 60, 70}$ [dB-Hz]</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>3.7</td>
</tr>
<tr>
<td>$d_{min}$</td>
<td>10</td>
</tr>
<tr>
<td>$d_{max}$</td>
<td>200</td>
</tr>
<tr>
<td>$U$</td>
<td>${5, 10, 15}$</td>
</tr>
<tr>
<td>gNBs density</td>
<td>${40, 80, 120}$ gNBs/km$^2$</td>
</tr>
</tbody>
</table>

SISO: single-input single-output

TABLE V

<table>
<thead>
<tr>
<th>$\mu$</th>
<th>$\eta_{TDL-D}$</th>
<th>$\eta_{TDL-E}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>26.85</td>
<td>29.74</td>
</tr>
<tr>
<td>1</td>
<td>9.75</td>
<td>13.98</td>
</tr>
<tr>
<td>2</td>
<td>3.24</td>
<td>8.06</td>
</tr>
<tr>
<td>3</td>
<td>0.74</td>
<td>0.46</td>
</tr>
<tr>
<td>4</td>
<td>0.48</td>
<td>0.36</td>
</tr>
</tbody>
</table>

In order to evaluate the proposed receiver, an experiment was performed with real 5G signals in the Anteater parking structure at the University of California, Irvine, USA. In this section, the experimental hardware and software setup are first presented. Then, the experimental results are presented.

A. Experimental Hardware and Software Setup

Since 5G protocol has been finalized very recently, it has not been fully implemented by all operators. The U.S. operators AT&T, Verizon, and Sprint have partially implemented their 5G networks in some areas of a few major cities. On December 6th, 2019, T-Mobile announced a nationwide 5G implementation on its band 71 (i.e., frequency range of 600 MHz). At the time and location of this paper’s experiment, only T-Mobile was transmitting 5G signals and the available gNBs were limited to only this operator. Therefore, extracting a position estimate from one pseudorange measurement was infeasible. Hence, the experimental results were confined to evaluating the pseudorange measurements.

In order to perform the experiment, a ground vehicle was equipped with 1 cellular Laird antenna to receive 5G signals at a center frequency of 630.05 MHz, which was obtained by searching over all possible frequency candidates as discussed in Section IV-A [74]. Using Table 5.4.3.3-1 of [55], it can be seen that the SS/PBCH block can only accept Case A on band 71, which has 15 kHz subcarrier spacing. Therefore, the SS/PBCH block at this band has 3.6 MHz bandwidth. The cellular antenna was connected to a National Instrument (NI) universal software radio peripheral (USRP)-2955, driven by a GPS-disciplined oscillator (GPSDO) to down-mix and sample 5G signals at 5 MSps [75]. A laptop was used to record the samples using LabVIEW [76]. The recorded samples were processed with MATLAB offline [77]. A Septentrio AsteRx-i V, which was equipped with dual antenna multi-frequency GNSS receiver with real-time kinematic (RTK) and a Vectornav VN-100 micro electromechanical systems (MEMS) inertial measurement unit (IMU), was used to estimate the position of the ground vehicle, which was used as the “ground truth” [78]. The ground vehicle traversed a loop path four times over 135 seconds. The code and carrier loop bandwidth were set to 0.1 and 4 Hz, respectively. Fig. 15 shows the experimental hardware setup, the location of the gNB, and the traversed trajectory.

B. Experimental Results

First, the received signal was correlated with all possible PSS sequences and the one with the highest peak was selected resulting in $N_{1D}^{(2)} = 1$. Fig. 16(a) shows the maximum of the PSS correlations, which is normalized by the highest value. Next, the signal was converted to the frame structure and the SS/PBCH block was extracted. Then, the received SSS signal was correlated with all possible SSS sequences and the one with the highest peak was selected resulting in $N_{1D}^{(1)} = 1$. The signal was then demodulated to extract the data. The pseudorange measurements were then extracted and a WNLS is used to solve for the position of the UE. Table IV summarizes the values of the Monte Carlo simulation parameters.

Fig. 14 shows the resulting cumulative distribution function (CDF) of the position estimation error. Table V shows the 95% probability position estimation error bounds for $U = 5$ and $\mu = 0, \cdots, 4$. It can also be seen that increasing the numerologies (i.e., increasing the bandwidth) has the highest effect on the position estimation error, while the effect of the number of gNBs and $C/N_0$ on the error is insignificant compared to the bandwidth.

VII. EXPERIMENTAL RESULTS

In order to evaluate the proposed receiver, an experiment was performed with real 5G signals in the Anteater parking structure at the University of California, Irvine, USA. In this section, the experimental hardware and software setup are first presented. Then, the experimental results are presented.
Fig. 15. (a) Experimental hardware setup and (b) location of the gNBs and the traversed trajectory.

Fig. 16. (a) Maximum of correlation of the received signal with all possible PSS sequences, (b) maximum of correlation of the received signal with all possible SSS sequences, and (c) correlation of the received signal with the selected PSS and SSS sequence in time domain.

A two-state model, which is composed of a clock bias \( \delta t \) and a clock drift \( \dot{\delta}t \), can be used to model the clock dynamics in the estimated pseudorange at time-step \( k \), according to

\[
\rho(k) = d(k) + c \left( kT_{sub}\dot{\delta}t(0) + \delta t(0) \right) + \varepsilon(k),
\]

where \( d(k) \) is the actual range at time-step \( k \) and \( \varepsilon \) is the measurement noise [79]. The clock bias was found to be \( c\delta t(0) \approx \rho(0) - d(0) = 5.37 \times 10^6 \text{ m} \). Fig. 17(a) shows \( \rho(k) - c\delta t(0) \) with orange marked line. The actual range \( d(k) \) is plotted with yellow solid lines. It can be seen that there is a mismatch between \( \rho(k) - c\delta t(0) \) and the actual range \( d(k) \), which is shown in Fig. 17(b) with the blue line. The pseudorange model (14) shows that this mismatch is due to the noise and clock drift (i.e., \( \delta t(0) \)), which increases over time. In the pseudorange model, it is assumed that the clock has a constant drift over time and a first-order polynomial was fitted to estimate this drift. For this purpose, at each time-step, a first-order polynomial was fitted to the difference of the actual range and pseudorange from the initial time-step to the current time-step. The resulting polynomials at each time-step were used to remove the effect of clock bias and drift from the estimated pseudorange at that time-step. The polynomial that was fitted to the difference of actual range and pseudorange over the whole experiment, estimated the clock drift to be \( c\delta t(0) = -0.16 \text{ m/s} \). The orange line in Fig. 17(b) shows the resulting first-order polynomial and the green line shows the difference of the pseudorange and range after removing the effect of the clock. The results showed that the estimated range has a standard deviation of 1.19 m. Since the experimental environment was a relatively open area, the received signal had less multipath than the TDL-D and TDL-E channel models. Therefore, the resulting standard deviation was less than the results presented in Fig. 12 and 13 and it can be assumed that the pseudorange measurement noise has zero mean.

Note that in practical scenarios, one can use the actual range measurements obtained from a GNSS receiver before the GNSS signal cutoff to estimate the clock bias and drift. Another approach is to estimate the clock bias and drift simultaneously with the position of the UE in an extended Kalman filter (EKF) [49]. The remaining error in the pseudorange, after removing the clock bias and drift, is the effect of multipath and noise, which can cause error on the estimated location as discussed in Section VI.

C. Comparison With ESPRIT Algorithm

In this subsection, the performance of the proposed receiver is compared with the ESPRIT algorithm proposed in [63]. The ESPRIT algorithm is a super-resolution algorithm that can obtain an estimate of the channel impulse response LOS and multipath delays given the length of the channel. The minimum descriptive length (MDL) criterion is one approach to estimate the length of the channel [80]; but, the MDL
method tends to overestimate the channel length. As a result, the ESPRIT TOA estimation has an outlier. In this subsection, the MATLAB function “filloutliers” with linear method was used to reduce this outlier effect on the ESPRIT algorithm’s estimated pseudorange. A similar approach to the one presented in Subsection VII-B was used to remove the effect of the clock bias and drift from the ESPRIT algorithm’s estimated pseudorange. Fig. 17 shows the results of the ESPRIT algorithm’s pseudorange before and after removing the clock bias and their corresponding errors. The standard deviation of the ESPRIT algorithm’s estimated pseudorange after removing the effect of the clock bias was measured to be 34.42 m, which is significantly higher than the proposed approach standard deviation of 1.19 m.

VIII. Conclusion

This paper proposed an opportunistic framework to exploit 5G signal for navigation and presented the first published experimental results that demonstrate ranging with real 5G signals. For this purpose, first, low-level models of 5G signals and possible reference signals that can be exploited for navigation were presented. Next, an SDR structure was proposed to extract navigation observables from these signals. Implementing the proposed SDR on an embedded device is practically achievable, but this will require further research and development to optimize the design for size, power consumption, among other engineering considerations. Then, the accuracy of the code phase measurements were analyzed in a multipath free environment and in the presence of multipath. Then, the results were used to derive the statistics of the position estimation error. Simulation results were presented for different channel models. Finally, real 5G signals were used to evaluate the performance of the proposed SDR. The results showed a standard deviation of 1.19 m for the estimated pseudorange using a SS/PBCH signal.

APPENDIX A

PROOF OF (12) AND (13)

It is assumed that the UE uses a WNLS to estimate its location, where an iterative algorithm is used according to

$$\hat{r}_t^{(k+1)} = \hat{r}_t^{(k)} + \left( G^T \Sigma_e^{-1} G \right)^{-1} G^T \Sigma_e^{-1} \left( \rho - \hat{d}^{(k)} \right),$$

(15)

where $k$ represents the iteration number. Using a first-order Taylor polynomial to approximate the range, the vector of pseudoranges (9) can be rewritten as

$$\rho = d^{(k)} + G^{(k)} (r_t - \hat{r}_t^{(k)}) + b + \varepsilon.$$  

(16)

By inserting (16) into (17), the estimation error can be obtained as

$$\hat{r}_t \triangleq \hat{r}_t^{(k+1)} - r_t = \left( G^T \Sigma_e^{-1} G \right)^{-1} G^T \Sigma_e^{-1} \left( b + \varepsilon \right).$$  

(18)

Therefore, the mean and covariance of the estimation error presented in (12) and (13), can be derived according to

$$\mathbb{E} \{ \hat{r}_t \} = \left( G^T \Sigma_e^{-1} G \right)^{-1} G^T \Sigma_e^{-1} \left( \mathbb{E} \{ b \} + \mathbb{E} \{ \varepsilon \} \right) = \left( G^T \Sigma_e^{-1} G \right)^{-1} G^T \Sigma_e^{-1} \mu_b,$$

$$\text{cov} \{ \hat{r}_t \} = \mathbb{E} \{ \hat{r}_t \hat{r}_t^T \} = \left( G^T \Sigma_e^{-1} G \right)^{-1} G^T \Sigma_e^{-1} \left( b + \varepsilon \right) \left( b + \varepsilon \right)^T + \Sigma_e^{-1} G \left( G^T \Sigma_e^{-1} G \right)^{-1} = \left( G^T \Sigma_e^{-1} G \right)^{-1} G^T \Sigma_e^{-1} \left( b + \Sigma_e \right) \Sigma_e^{-1} G \left( G^T \Sigma_e^{-1} G \right)^{-1}.$$  

REFERENCES


Kimia Shamaei received the B.S. and M.S. degrees in electrical engineering from the University of Tehran, and the Ph.D. degree from the Department of Electrical Engineering and Computer Science, University of California, Irvine, CA, USA. She is a recipient of the 2018 Institute of Navigation (ION) Samuel Burk a Award and the 2020 ION Bradford Parkinson Award.

Zaher (Zak) M. Kassas (Senior Member, IEEE) received the B.E. degree in electrical engineering from the Lebanese American University, the M.S. degree in electrical and computer engineering from The Ohio State University, and the M.S.E. degree in aerospace engineering and the Ph.D. degree in electrical and computer engineering from The University of Texas at Austin. He is currently an Associate Professor with the University of California, Irvine, CA, USA, and the Director of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He is also the 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. His research interests include cyber-physical systems, estimation theory, navigation systems, autonomous vehicles, and intelligent transportation systems. In 2018, he received the National Science Foundation (NSF) Faculty Early Career Development Program (CAREER) Award. In 2019, he received the Office of Naval Research (ONR) Young Investigator Program (YIP) Award. He is a recipient of the 2018 IEEE Walter Fried Award, the 2018 Institute of Navigation (ION) Samuel Burk a Award, and the 2019 ION Col. Thomas Thrulow Award. He is an Associate Editor of the IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS and the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS.