From Experiments to Insights: A Journey in 5G New Radio Localization

Ivan Palamà*, Giuseppe Santaromita§, Yago Lizarribar§, Lorenzo Maria Monteforte*,
Stefania Bartoletti*, Domenico Giustiniano§, Giuseppe Bianchi*, and Nicola Blefari Melazzi*
*University of Rome Tor Vergata and CNIT, Rome, Italy, email: ivan.palama@uniroma2.it
§IMDEA, Madrid, Spain

***Abstract*—The 3GPP has recently made the inclusion of positioning services a priority in future generations of cellular networks, thus providing an opportunity for these networks to serve as fertile ground for the emergence of new service-based applications. With the release of 3GPP Release 16 there has been an extensive standardization effort aimed at improving positioning capabilities in 5G networks, particularly in terms of physical layer signals, measurement techniques, and network architecture. Despite these advances, the experimental evaluation of 5G positioning in real-world scenarios is still lagging behind, due to factors such as the slow integration of positioning technologies into open-source 5G frameworks, the complexity of setting up a testbed for 5G positioning with multiple base stations (BSs), and the high cost associated with such a deployment. This article offers a comprehensive review of these factors and provides a state-of-the-art overview of 5G positioning and its support in SDR-based platforms. In addition, we present guidance on the proper setup and configuration of a testbed for SDR-based multi-BS synchronized 5G positioning, the lessons we have learnt in the process, and through a series of time-based real-over-the-air measurements, we demonstrate how localization design choices can be effectively evaluated even with limited-size and low-cost SDR-based testbed.**

***Index Terms*—5G, Positioning, Localization, SDR**

I. Introduction

The 3rd Generation Partnership Project (3GPP)'s standardization efforts regarding localization for 5G networks continually progress with each new release. Starting from Release 16, the 3GPP is augmenting the capabilities of 5G networks and devices by incorporating localization features. This integration aims to achieve high level location accuracy by using greater bandwidths and adaptive numerology implemented in the 5G physical layer. This provides a wide variety of innovative applications [1], [2]. Release 17 further elevates the performance of 5G positioning to meet stringent use case requirements, such as centimeter-level accuracy. It introduces additional improvements to reduce positioning latency to facilitate time-critical use cases such as remote control applications. 3GPP Release 18 (called 5G Advanced) further boosts the availability of 5G positioning services through sidelink positioning and ranging in out-of-range conditions and improves the accuracy of 5G positioning services with Radio Access Technology (RAT)-dependent positioning techniques, such as aggregation of reference signal bandwidth, carrier phase measurements and exploitation of AI / ML under heavy non-line of sight (NLOS) conditions [3]. More recently, the topic of wireless sensing has become part of study in the recently started Release 19 [4]. The continued efforts of 3GPP standardization highlight the increasing importance of localization and positioning services in 5G networks.

The 3GPP has defined procedures, signals, and architectural elements for 5G positioning, as well as specialized network functions [5]. Technical reports and specifications for 5G offer flexibility in implementing algorithms to extract position-related features, such as time-of-arrival (TOA) and angle estimation, and determining user equipment (UE) position by combining features from multiple links. Despite active research to improve time-of-arrival and position estimation techniques and mitigate challenges in challenging propagation environments, such as non-line-of-sight and multipath conditions [6]–[9], 5G positioning performance has mainly been assessed through simulation-based studies using standardized channel models and closed-source simulators or preliminary experimental set-up with 5G-like signals [6], [7], [10]–[16], except for few isolated works performing experiments with 5G signals [17], [18].

OpenAirInterface (OAI) [19], srsRAN [20], and Aether [21] are popular open-source platforms that provide network solutions used for implementing, simulating and testing the 3GPP stack in both industrial and academic communities. These platforms offer an open-source implementation of the 5G 3GPP stack and can be executed on general-purpose computing platforms, interfacing with a wide range of SDR boards. SDR technology has gained significant traction in the academic research community due to its versatility and cost-effectiveness. Examples of widely utilized SDR devices include the 4G-oriented Ettus USRP B210, HackRF One, LimeSDR, BladeRF, and the 5G-oriented Ettus USRP X310 [22] and N310 [23], among others. The combination of open-source cellular network platforms and SDR provides a valuable research and development tool that enables rapid prototyping and testing of new algorithms and paradigms in real-world, over-the-air conditions. However, despite their potential, their use currently requires substantial hardware and software setup and configuration effort. Additionally, the incompatibility between different SDRs, and the different options in terms of open-source platforms present further difficulties for researchers. Despite these challenges, as demonstrated in the preliminary work from Palamà et al. [17], the benefits of mobile network open-source-platforms and SDR technology in terms of research and development are undeniable, making them valuable tools for advancing the field of 5G positioning and localization. This area of investigation and development is evolving at fast pace.

Among the various open-source platforms, only OAI has recently implemented the reference signals specified in compliance with the most current 5G positioning 3GPP standards. However, its deployment is not straightforward. Emulating

Copyright © 2023 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

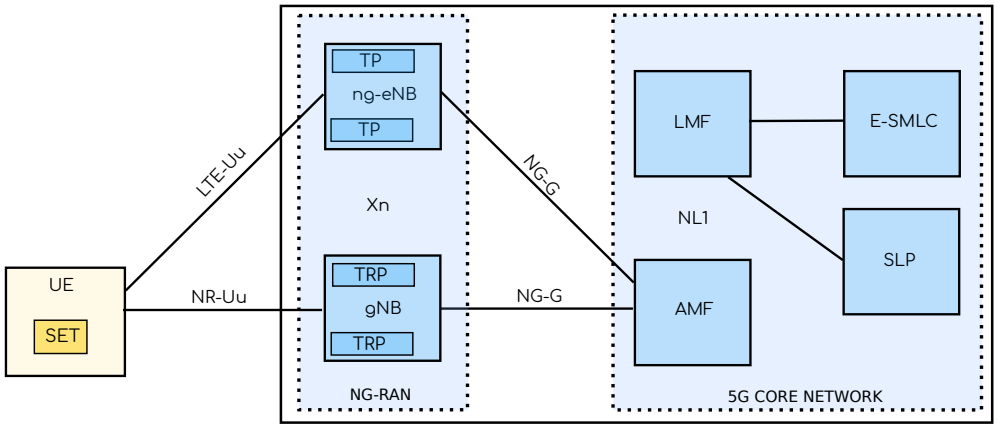


Figure 1: 3GPP 5G Positioning architecture [5].

an entire positioning system would involve setting up a network of multiple gNBs, proving financially prohibitive and presenting logistical challenges. In this article, our goal is not to provide a study on achievable accuracy using 5G localization, but rather *guide the scientific community and industry to understanding how to perform 5G localization, providing an effective methodology* to deploy an experimental testbed, examine and validate algorithms and research results using measurements of 5G localization signals transmitted over the air, taking into account standardized localization procedures and real operating conditions. This paper makes several contributions. Firstly, we conduct a thorough analysis of the current status of open-source platforms and related hardware for 5G localization, highlighting the main technical elements. Secondly, we demonstrate the effectiveness of a positioning reference signal (PRS) testbed for 5G localization using an open-source PRS-based platform. Thirdly, we propose a solution to address synchronization and limited hardware performance issues that arise in multi-gNB link scenarios. Additionally, we perform a statistical evaluation of time-based multi-link measurements and conduct an in-depth investigation of potential localization algorithms using experimental time-based measurements.

The article is organized as follows. After some necessary background in Section I, we analyze the 5G positioning state-of-the-art and our 5G localization system model in Sections II and III, respectively. In Section IV we present a description of the implemented 5G localization SDR-based experimental testbed while in Section V we analyze and discuss the experimental results obtained. Finally Section VI provides conclusions.

II. 5G Positioning: State of the Art

This section introduces and describes the main elements of the 3GPP standardization of 5G localization and explores the latest advancements in open-source platforms for implementing location services within 5G mobile networks.

A. 5G Architecture

The implementation of 5G positioning is facilitated through the use of an optimized architectural design for the transmission of location signals between gNB and UE and the exchange of location measurements with the Location Management Function (LMF). The architectural specifications for the positioning of 5G are contained in [5].

As depicted in Figure 1, the composition of the 5G positioning architecture encompasses the following components:

- User equipment (UE) that may carry out measurements of downlink signals from the Next Generation Radio Access Network (NG-RAN), which may be time- or angle-based, depending on the chosen positioning methodology;
- NG-RAN, comprised of gNB and next generation-evolved NodeB (ng-eNB) network elements, which may contribute to the calculation of position estimates through radio signal measurements and convey these measurements to the LMF;
- The Access & Mobility Management Function (AMF), which is responsible for handling connection and mobility management tasks including positioning for a target UE;
- LMF, which is responsible for managing and supporting a range of location services for target UEs, including computation of user position and the delivery of assistance data.
- The Enhanced Serving Mobile Location Centre (E-SMLC) provides location information to the network, processes and combines location data from multiple sources, and transmits the position information to the requesting entity;
- The SUPL Location Platform (SLP) is a server-based technology for providing secure and accurate location services to mobile devices. It is part of the Secure User Plane Location (SUPL) specification developed by the Open Mobile Alliance (OMA) for delivering Location-Based Services (LBS) in mobile networks.

In particular, the LMF receives location requests for a target UE from the serving AMF and interacts with the NG-RAN to obtain both uplink and downlink position measurements. The LMF may also directly engage with the target UE to provide requested assistance data or calculate a location estimate. The LMF determines the positioning methods to be employed based on various factors such as the LoCation Service (LCS) Client type, the desired Quality of Service (QoS) class [24], UE positioning capabilities, and NG-RAN

positioning capabilities, and invokes these methods in the UE and serving NG-RAN. The positioning methods may result in location estimates for UE-based methods and positioning measurements for UE-assisted and network-based methods.

5G positioning signals: 5G positioning signals have been introduced to achieve higher accuracy compared to LTE positioning. These signals include the uplink Sound Reference Signal (SRS) and an improved LTE Positioning Reference Signal (PRS) version for the downlink. The latter signal provides superior accuracy through the use of a diagonal or staggered physical layer resource element scheme and superior coverage and interference suppression through the coordinated transmission of gNBs. This coordinated transmission avoids interference from adjacent cells and maximizes signal strength over multiple symbols across the entire NR bandwidth. PRS is based on Gold sequences, which are pseudo-random sequences with constant amplitude and orthogonal to each other. The 5G NR PRS features are defined in [25]. PRS is defined by the 3GPP standard as $r(m)$ and is given by:

$$r(m) = \frac{1}{\sqrt{2}}(1 - 2c(2m)) + j\frac{1}{\sqrt{2}}(1 - 2c(2m-1)) \quad (1)$$

where j is the imaginary unit, m is the subcarrier index and the pseudo-random sequence $c(i)$ adopts the 31st-order Gold sequence. The generating equation of the initial sequence of $c(i)$ in [25] is:

$$c_{\text{init}} = \left[2^{22}\left\lfloor \frac{n_{\text{ID,seq}}^{\text{PRS}}}{1024}\right\rfloor + 2^{10}\left(N_{\text{symb}}^{\text{slot}} n_{\text{s,f}}^{\mu} + l + 1\right)\right.$$
$$\left.\cdot\left(2\left(n_{\text{ID,seq}}^{\text{PRS}} \bmod 1024\right) + 1\right) + \left(n_{\text{ID,seq}}^{\text{PRS}} \bmod 1024\right)\right] \bmod 2^{31} \quad (2)$$

where $n_{\text{ID, seq}}^{\text{PRS}} \in \{0, 1, \ldots, 4095\}$ is the PRS sequence ID uniquely identifying a downlink PRS resource, $N_{\text{symb}}^{\text{slot}}$ is the number of symbols per time slot, $n_{s,f}^{\mu} \in \left\{0, \ldots, N_{\text{slot, frame}}^{\mu} - 1\right\}$ is the number of time slots within a frame, assuming the subcarrier spacing configuration μ and the number of time slots per frame $N_{\text{slot, frame}}^{\mu}$, and l is the number of OFDM symbols in the time slot to which the sequence is mapped.

5G Positioning Schemes: As of Release 16, 3GPP has standardized the following 5G positioning schemes [5]: Downlink Time Difference of Arrival (DL-TDOA), Uplink Time Difference of Arrival (UL-TDOA), Downlink Angle of Departure (DL-AOD), Uplink Angle of Arrival (UL-AOA), Multi-Round Trip Time (Multi-RTT) and NR Enhanced Cell ID (E-CID). In addition to the RAT-dependent solutions, another group of RAT-independent solutions can be used for positioning, such as Global Navigation Satellite System (GNSS), WLAN, Bluetooth, barometric pressure, and terrestrial beacon system (TBS). In the following, we focus only on RAT-dependent schemes. The 5G network supports 5 positioning modes:

- Hybrid positioning: 5G network employs multiple positioning schemes.
- Standalone positioning: UE autonomously, without network assistance, uses one or more methods from the mentioned schemes.
- UE-based: UE computes its position estimate using measurements provided by the LMF. It is supported by DL positioning schemes.
- UE-assisted/LMF-based: measurements are provided by the UE to the LMF to be used in the computation of a position estimate. It is supported by DL positioning schemes.
- NG-RAN node-assisted/LMF-based: measurements are provided by the NG-RAN node to the LMF to be used in the computation of a position estimate. It is supported by UL positioning schemes.

In the DL-TDOA scheme, the UE measures the reference signal timing difference (RSTD) or TDOA of the PRS positioning signal from two base stations, which is then communicated to the LMF. The LMF uses these timing differences to estimate the UE's position. The UL-TDOA scheme is conceptually similar but uses uplink signals, and the base station measures the relative time of arrival (RToA) of multiple SRS signals from UEs, which are communicated to the LMF. In the DL-AOD scheme, the UE measures and communicates the received power of downlink reference signal beams from multiple base stations, which are used to estimate the UE position angle and communicated to the LMF. The LMF then solves the equations to determine the UE's position based on the estimates from multiple base stations. The UL-AoA scheme works similarly but with uplink signals. The base station measures the angle of arrival of UE uplink signals, which are communicated to the LMF, and the UE's position is determined from these multiple-angle measurements. In the Multi-RTT positioning scheme, both uplink and downlink signals are used, with the UE and at least three gNBs sending reference signals (SRS and PRS) to measure the RX-TX time difference and obtain the RTT. The RX-TX information is then summarized for the LMF, which derives the distances between the UE and gNBs and estimates the UE's position as the point of intersection of the three circles with the distances derived as radii. The CID positioning technique involves the estimation of the UE position using information about its serving ng-eNB, gNB, and cell. This information can be acquired through paging, registration, or other similar methods. On the other hand, the NR E-CID positioning approach utilizes additional UE measurements, NG-RAN radio resources, and other measurements to enhance the accuracy of the UE location estimate.

B. Mobile Network Synchronization Solutions

In the context of 5G localization, synchronization is a critical aspect to guarantee precise RSTD and RToA time measurements in downlink and uplink, respectively. A lack of high-precision network synchronization would inevitably affect the overall location accuracy, making the overall effort for 5G positioning ineffective.

Various existing solutions for mobile network Internet Service Provider synchronization are available to achieve this. The most popular solution is utilizing the Global Navigation Satellite System (GNSS) signals, such as GPS, to synchronize in time and frequency. However, GNSS can be susceptible to environmental factors and cannot be used standalone as Primary Reference Clock (PRC).

For providing PRC signal to the network, the older ITU-T G.811 was suitable only for frequency synchronization. More recently, the G.8272.1 ePRTC (enhanced Primary Reference Time Clock) is a newer, more specialized solution standardized by the ITU-T for network synchronization which requires usage of cesium clocks for centralized grand master clocks and quartz/rubidium for distributed master clocks and boundary clocks [26]. ePRTC offers sub-nanosecond accuracy, with time, phase, and frequency aligned and calibrated to the GNSS signal over time. This makes ePRTC well-suited for 5G positioning.

For the RAN domain, an option is using the Precision Time Protocol (PTP) and Synchronous Ethernet (SyncE) technologies to enable synchronization with high accuracy and stability between network nodes at the edge. Using this combined approach, PTP provides time-of-day information and phase while SyncE provides highly stable frequency synchronization. ITU-T has defined a set of telecom standards for 5G networks that are built on top of PTP, namely G.8275.1 and G.8275.2. While G.8275.1 is the most accurate solution, G.8275.2 is more practical to implement. Both deliver highly accurate frequency synchronization, phase synchronization and time of day from the PRC signal. Furthermore, in the RAN domain, over-the-air synchronization could provide a valid alternative as it based on round-trip time measurement sent over the radio interface between neighboring base stations [27]. However, it lacks of work in standardization.

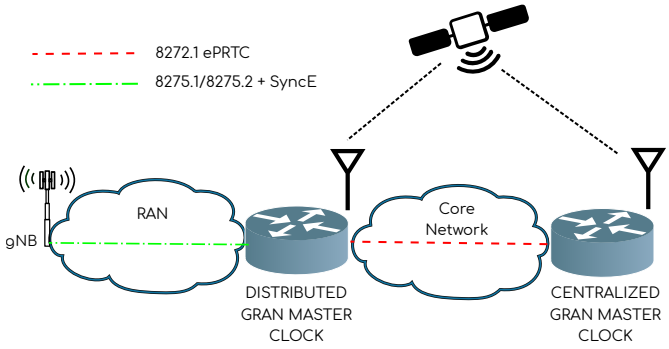


Figure 2: Mobile network syncronization for 5G networks.

In conclusion, and as summarized in Fig. 2, while each synchronization solution has its own advantages and disadvantages, the combination of ePRTC in the 5G Core Network (5GCN) with ITU G.8275.1/G.8275.2 in the RAN domain provides a promising solution for ensuring precise synchronization in 5G positioning and advanced mobile network applications due to its excellent performance, being also the most suitable approach for supporting positioning services based on very accurate timing information.

C. Open-source platforms

We now describe the main open-source SW platforms/tools available to implement a 5G SA mobile network infrastructure, including the NG-RAN and the 5GCN. The main features will be analyzed, focusing on the positioning aspects and referring to the standardized 5G positioning architecture.

OpenAirInterface: OpenAirInterface (OAI) provides NR Release 15/16 compliant 5G Core, gNB and UE implementations. The OAI source code is written in C for real-time performance purposes and is distributed under the OAI Public License. OAI is compatible with Intel and ARM architectures running Linux distributions and support the most commonly used SDR platforms (e.g., BladeRF, USRP, and LimeSDR). In recent times, OpenAirInterface has implemented both DL PRS and UL SRS positioning signals, providing time-of-arrival (ToA) estimation based on channel impulse response (CIR) and finer ToA estimation using IDFT with 16x oversampling for CIR. It allows receiving DL PRS from multiple gNBs synchronized via GPSDO. This makes OAI the ideal platform to test 5G positioning.

srsRAN: srsRAN is the most similar platform to OAI, as the latter provides software implementations of the gNB and UE with functionality up to NR Release 15 but it does not implement its own 5GCN, and instead relies on Open5GS, an open-source implementation of the 5G Core conforming to 3GPP Release 16 written in C language. srsRAN is written in C and C++ and is distributed under the GNU AGPLv3 license. srsRAN also provides a complete ORAN-native 5G CU/DU solution compliant with 3GPP and O-RAN Alliance specifications via a dedicated new srsRAN project [28]. Like OAI it is compatible with popular Linux distributions and supports the most popular SDR platforms. It is a relatively more stable project than OAI but offers fewer features, including 5G positioning signals support.

Aether: Aether is a project promoted by the Open Networking Foundation (ONF) for the implementation of private cellular networks. Unlike OAI and srsRAN, Aether not only offers an implementation of RAN and 5GCN, integrating SD-RAN [29] and SD-CORE [30], respectively, but also provides a control and orchestration interface for RAN, a cloud edge platform with support for cloud computing and a central cloud. The source code is released under an open-source Apache 2.0 license. The main goal of SD-RAN is to provide a micro-ONOS-based, O-RAN-compliant, near-real-time intelligent RAN controller (RIC) and an O-RAN-compliant platform for xAPPS. SD-RAN is based on OAI gNB and UE implementations. Since Aether's RAN is based on OAI and we were not interested in the O-RAN functionalities, we decided to use OAI directly in our experimental setup.

III. System Model

This section introduces the main elements of the location system model and signal processing. We consider a network of neighboring N_{g} gNBs, which estimates the position of N_u users. The ith gNBs is at $\mathbf{p}_{\mathrm{gNB}}^{(i)} = \left[\mathbf{x}_{\mathrm{gNB}}^{(i)}\ \mathbf{y}_{\mathrm{gNB}}^{(i)}\right]$, while the true unknown position of the ith UE is at $\mathbf{p}_{\mathrm{u}}^{(i)}$. A location-dependent time-based measurement is performed for each gNB. Fig. 3 illustrates an example of network deployment with this system model.

A. TOA Estimation

In OpenAirInterface PRS-based TOA estimation is implemented through a series of well-defined steps in accordance with the 3GPP standards for 5G positioning. First, the procedure generates and modulates Pilots, which are then used as references for subsequent processing. Next, the Resource Element (RE) offset of the PRS is calculated, followed by channel estimation and interpolation in the frequency domain. Next, the signal-to-noise ratio (SNR) is estimated, and the

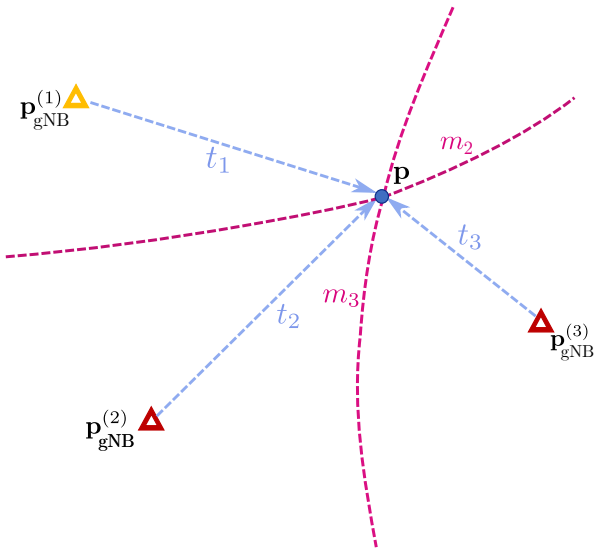


Figure 3: Example network deployment with $N_g = 3$ gNBs (triangles) and $N_u = 1$ UE (circle). The TDOA $m_2 = t_2 - t_1$ and $m_3 = t_3 - t_1$ are measured considering the first anchor as the reference (yellow triangle). The corresponding hyperbola is illustrated in magenta.

PRS channel estimates are entered into the translated format of the fast Fourier transform (FFT). The procedure then calculates the CIR in the time domain with IDFT oversampling up to 16x. Finally, the TOA is estimated by finding the peak estimate of the CIR as the maximum identified absolute value.

B. TDOA-Based Positioning Algorithm

The DL-TDOA technique leverages the PRS signal transmitted by a set of neighboring gNBs and received by the UE, to measure the relative reference signal timing difference (RSTD) or TDOA between each pair of gNBs. This measurement is then employed in the multilateration or trilateration calculation, based on the principles of hyperbolic geometry. As a convention, the gNB with index $i = 1$ is designated as the reference cell for RSTD measurements. The relative TOA for the signal transmitted by the ith gNB and received by the UE is expressed as:

$$t_i(\mathbf{p}) = \frac{\|\mathbf{p}_{\text{gNB}}^{(i)} - \mathbf{p}_{\text{UE}}\|}{c} \tag{3}$$

where c is the speed of light.

The RSTD, as described in [31] Section 5.1.29, represents the relative time difference between the ith neighboring gNB and the reference gNB and is calculated as $m_i = t_i(\mathbf{p}) - t_1(\mathbf{p})$. Therefore, the measurement model for the TDOA is as follows.

$$m_i = \left\|\mathbf{p}_{\text{gNB}}^{(i)} - \mathbf{p}_{\text{UE}}\right\|/c - \left\|\mathbf{p}_{\text{gNB}}^{(1)} - \mathbf{p}_{\text{UE}}\right\|/c + n^{(i)}(\mathbf{p}) \tag{4}$$

Measurement noise $n^{(i)}(\mathbf{p})$ is inherently dependent on the UE position, the SNR of the received signal, and the LOS conditions. To mitigate the risk of synchronization errors in RSTD measurements, all gNBs transmit the PRS simultaneously, thereby ensuring synchronized transmission from all gNBs.

IV. Experimental Setup

This section describes how we implement our 5G SDR-based experimental localization system.

A. Mobile Network Software

In our experimental setup we use OAI open-source framework to implement both RAN (gNB and 5G UE) and 5GCN for its more advanced development concerning reference signals for positioning. We decided to focus on the DL PRS signal to test 5G positioning; however, applying the same procedures using the UL SRS signal is possible. The OAI tag *2022.w51* is utilized.

B. Hardware

The experimental testbed utilized in this study consists of two customized workstations, one powerful laptop, and four SDRs, which are utilized to emulate the operator's network (5GCN and gNB) and the user terminal.

SDR: The SDRs utilized in this study comprises four USRP X310 devices [22] with UBX160 daughterboards [32]. These devices are capable of tuning over a wide radio frequency range, from 10 MHz to 6 GHz, and thus cover all NR FR1 frequency bands with up to 160 MHz of instantaneous bandwidth. Using the high-speed 10 GbE interface, a sampling rate of 184.32 MS/s can be achieved, providing a theoretical localization accuracy of 1.62 m. NR-specific 5G antennas are attached to the SMA connectors of SDR devices. The Ettus USRP N310 was also tested but was found to be non-interoperable with the X310, probably due to different master clock rates.

Base station synchronizer: To provide high-accuracy synchronization between the gNBs, the Ettus Octoclock [33] is utilized. This device is a high-precision clock generator and distribution unit designed for wireless communication systems. It features eight independent clock outputs, each with its own phase-locked loop (PLL) and voltage-controlled crystal oscillator (VCXO) for frequency stability and accuracy. The Octoclock also includes a GPS receiver for enhanced synchronization and timing. This versatile device is ideal for our mobile network localization experimental setup. According to the specifications, the accuracy of the 1 PPS of the built-in GPSDO is within ±50 ns of the UTC RMS, with frequency accuracy of 1 ppb after the GPS is locked. A relative frequency tolerance of 1 ppb means a maximum time offset of 1 nanosecond in one second.

Workstation: Two workstations powered by Intel Core i9 CPUs with 18 cores @3 GHz with Ubuntu OS 18.04 LTS with kernel low latency are utilized to emulate 5GCN and three gNBs. To emulate the UE, the HP "ZBook Power G9 Mobile Workstation" powered by Intel Core i7 CPUs with 14 cores (6 high-performance cores clocked at up to 4.8 GHz and 8 efficient cores clocked at up to 3.7 GHz) with Ubuntu OS 22.04 LTS is utilized.

C. Calibration

Despite the synchronization of gNBs, it is imperative to consider the possibility of additional sources of timing errors in complex real-world scenarios. These could include, but are not limited to, clock drifts between SDRs and servers, causing offset errors in timing, faulty cables, interference

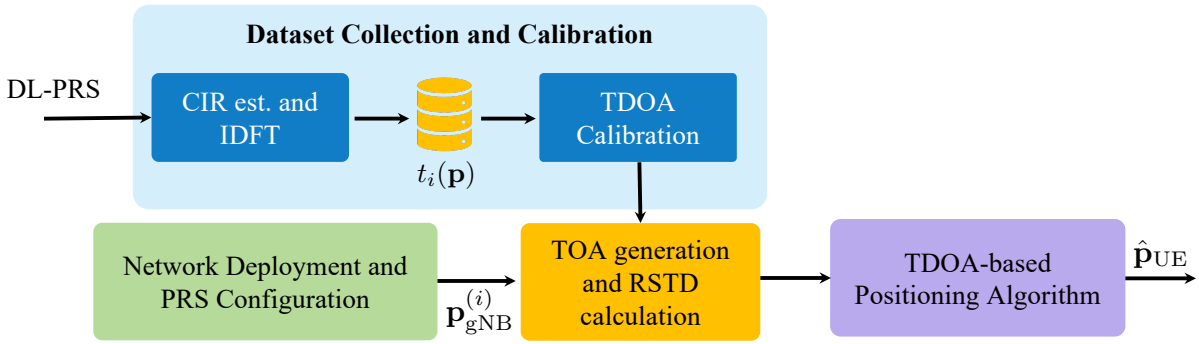


Figure 4: Illustration of the main step for dataset collection, calibration, and TDOA-based positioning.

from external sources, loss or degradation of the signal path, leading to reduced amplitude and phase accuracy, inadequate calibration of SDRs and hardware, resulting in incorrect timing information extraction, and limitations in GPS accuracy. To mitigate these potential errors, it is essential to calibrate the measurements. The calibration process helps to correct any measurement inaccuracies and helps to counteract any systematic biases that may have arisen during the data collection process. Additionally, calibrated measurements can be used as a reference for future experimental studies, helping to improve the overall understanding of the testbed.

To carry out the calibration process, we utilize one position of the UE as reference and calculate the offset denoted by c_{1i} between the expected and measured TDOA values for all pairs. Subsequently, we apply the calibration to each TDOA value as follows: $\hat{m}_i = m_i + c_{1i}$.

D. Moving Average and Oversampling

Moving Average: The experimental instability of 5G localization using open-source SDR-based frameworks and the inherent variability of the outdoor experimental environment pose significant challenges to accurately evaluating positioning performance that can affect the accuracy and stability of positioning results. However, the use of moving average techniques can help eliminate the impact of outlier measurements and improve the overall accuracy of the positioning procedure. Moving average techniques can improve the reliability, robustness, and stability of 5G localization results by smoothing out extreme time-based ranging measurements.

Oversampling: Regarding 5G PRS TOA measurements, one of the major issues is the presence of multipath interference, leading to significant errors in the TOA estimates. To overcome these issues, oversampling can prove to be a useful approach. Oversampling is a technique used to improve the accuracy of TOA estimation by increasing the number of samples collected. In the context of 5G technology, CIR oversampling can be crucial in obtaining finer TOA estimation. The CIR provides information about the time-varying characteristics of the radio channel, including reflections and multipath interference. When CIR is oversampled, the number of samples increases, providing a more detailed representation of the channel response. This results in a higher signal-to-noise ratio, allowing for a more accurate and robust estimate of the TOA.

In OpenAirInterface, oversampling is implemented using a technique called zero-padding. This involves inserting additional zeros on both sides of the baseband frequency-domain representation of the signal and then performing the IDFT, effectively increasing the sampling rate without adding any new information. By oversampling the CIR, it is possible to mitigate the effects of multipath interference, random noise, and other distortions that can affect the accuracy of TOA estimation. This leads to a more reliable and accurate estimate of the TOA, improving the performance of ranging measurements in 5G networks.

V. Experimental Validation

In this section, we present and discuss the experimental results obtained.

A. Deployment Scenario

As illustrated in Figure 5, experiments were performed in an outdoor scenario, a rooftop at the University of Rome, Tor Vergata. Experiments are conducted outdoors under clear GPS satellite visibility to ensure proper synchronization. The experimental testbed area is shown in Figure 6. Our testbed covers a surface of almost 60 m^2. We use 13 different selected UE locations to test our experimental positioning system.

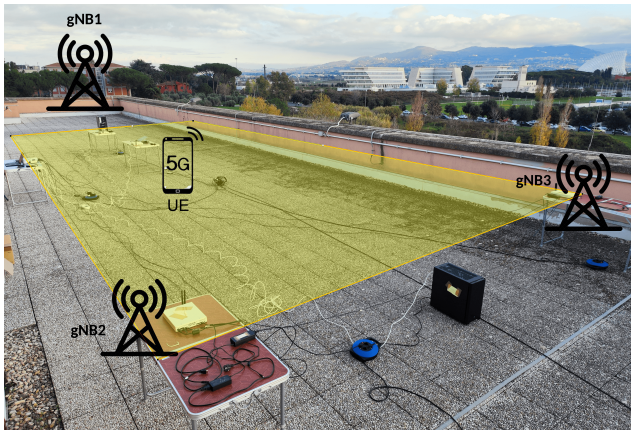


Figure 5: Outdoor scenario, experimental area in yellow with gNBs and UE.

In order to prevent any disruption to other users, all tests are conducted with the caution of stopping the experiments when people approach the testbed. Additionally, the output power of the SDR radios used in the experiments is thoroughly verified to ensure that the 5G NR signal emitted did not cause any interference outside the designated testing area.

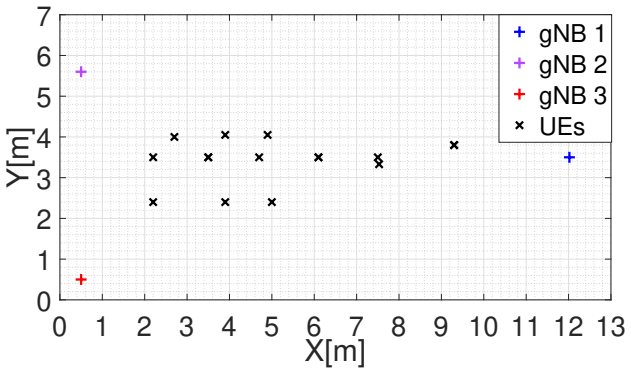


Figure 6: Experimental area with gNBs and UE positions.

The 5G NR TDD channel has been configured in the N78 (3500 MHz) frequency band for the experimental localization testbed. The channel has an instantaneous bandwidth of 80 MHz (217 RBs) and a subcarrier spacing of 30 KHz.

B. Calibration effect

Despite of the synchronization accuracy of the PPS and frequency of the OCTOCLOCK-G CDA-2990, on the order of 50 ns and 1 ppb, respectively, it is still necessary to conduct calibration of the measurements. As demonstrated in Figure 7, the calibration process is critical to measure the TDOA between the two PRS gNBs accurately.

The results show that when comparing the experimentally measured TDOA with the ideal predicted TDOA, significant non-marginal offsets are present if calibration is not performed. Although these offset values remained stable in each individual experiment, variation is observed between experiments. This variability may be explained by the fact that the SDR front ends are closed and opened after each experimental position measurement and by the fact that despite the use of high-level clock synchronization, the measured TDOA may still exhibit an offset from the ideal one due to SDR clock drift. In support of this hypothesis, Figure 7 shows how TDOA measurements turn out to be particularly susceptible to the impact of SDR clock drift of gNB1. Therefore, we conclude that *a calibration process is critical to ensure accurate and consistent TDOA measurements, and verify potential changes in SDR front ends between experiments, and that clock of each gNB is within the expected tolerance for positioning measurements*.

C. Oversampling improvement

To effectively showcase the impact of oversampling on location estimation accuracy, we present Figure 8, which illustrates the localization errors by implementing different oversampling factors.

As shown in Figure 8, by implementing a 16x oversampling rate, we can reduce the localization error to 4 meters in 80% of cases, as compared to 9 meters without oversampling. This notable improvement is attributed to the *ability of oversampling to generate more precise TOA values, which are indispensable in location estimation algorithms*. These outcomes collectively establish the efficacy of oversampling as a methodology to augment the accuracy of location estimation in wireless communication systems.

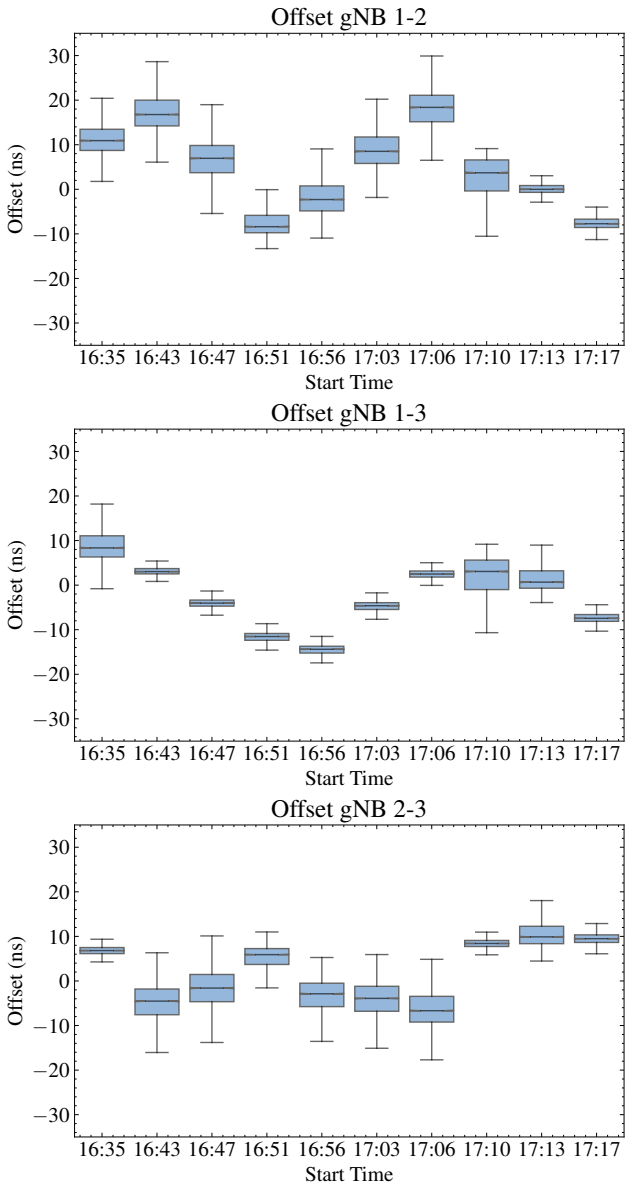


Figure 7: Offset between measured and ideal TDOA without calibration, presented in box plots for multiple location measurement campaigns.

D. Results

We evaluated the accuracy of localization using various algorithms, namely the Closed-Form Solution, Brute-Force, and Non-Linear Least Squares (NLLS). The Closed-Form Solution involves the algebraic resolution of TDOA equations, which require three receivers for a 2D scenario. In contrast, both Brute-Force and NLLS algorithms determine the minimum 2-norm discrepancy between the ideal predicted and estimated TDOA values.

The Brute-Force algorithm discretizes the 2D space into a uniformly distributed grid and evaluates the cost function at each point. However, accuracy depends on the grid size, with finer grids requiring more processing time. To speed up the algorithm, a technique used in this paper is to begin with a coarser grid and refine on the blocks with the lowest value. The space is initially divided into a $15 \times 15, \mathrm{m}^2$ grid with a step size of $0.5\mathrm{m}$, and at each iteration, the grid point with the

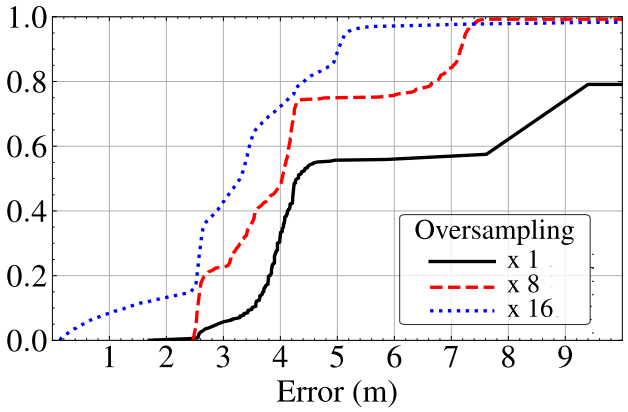


Figure 8: CDF of the positioning error using NLLS localization algorithm and varying the oversampling factor.

lowest objective function value and its neighbors are selected, and the step size is reduced to maintain a constant number of grid points. We set the maximum number of iterations to 10 and the tolerance to 1×10^{-4}.

The NLLS algorithm leverages iterative optimization routines based on gradient-based techniques to determine the direction of maximum descent. Compared to the Brute-Force method, this method is more efficient and retains accuracy. However, the main drawback of NLLS methods is the initial point estimation, which can be overcome by performing an initial estimation using the coarse grid defined with the Brute-Force method. Implementations of successive points can then be achieved through methods such as Levenberg-Marquardt [34], BFGS [35], or Gradient-Descent and its variants [36], with similar results. In the continuation, the positioning results presented by varying the localization algorithm are obtained using the BFGS method.

In general, NLLS/Brute Force perform better than the Closed-Form solution. This is due to the fact that for the former, a main sensor is needed with which the TDOA values are calculated. That means that if the sensor used as reference contains any offset in the timing information, that translates into higher positioning errors. NLLS/Brute Force methods can work with all combinations of time measurements and thus errors from one sensor are averaged out with the other receivers.

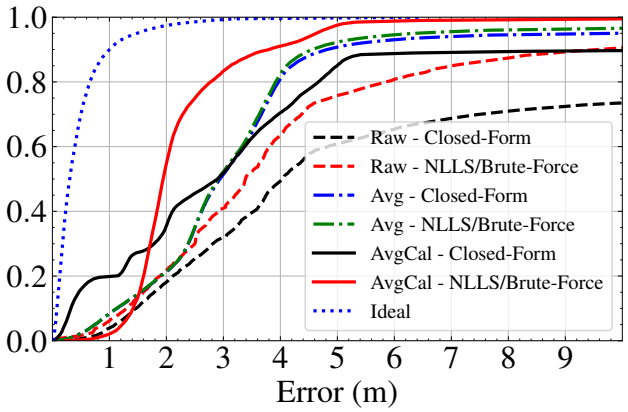


Figure 9: CDF of the positioning error varying the localization algorithm.

Figure 9 depicts the impact of averaging and calibration on performance as the localization algorithm varies. It is evident that the use of averaging facilitates superior performance compared to the use of raw measurements, leading to comparable results regardless of the algorithm employed. The calibration of the measures also exerts a clear influence on the positioning performance: in the absence of calibration, the NNLS, Brute Force and Closed Form algorithms show equivalent performance, whereas with calibrated measurements, the Closed-Form algorithm deteriorates while the NNLS/Brute-Force algorithms exhibit significant improvement, achieving a positioning error of approximately 3,m in 90% of cases.

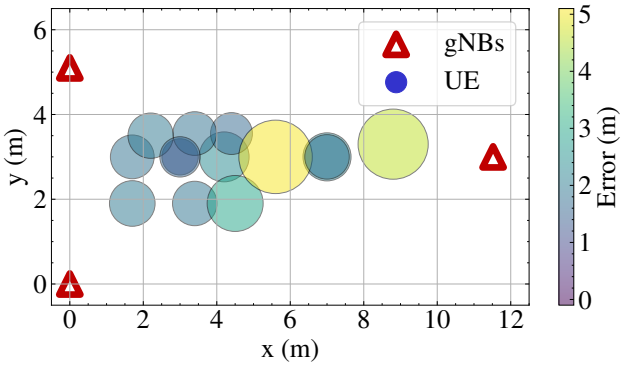


Figure 10: Spatial distribution of gNBs and UE positions. For each UE position, the NLLS localization error is given.

A heatmap depicting the location error associated with each user location for the NLLS algorithm is presented in Figure 10 to gain a more comprehensive understanding of the spatial distribution of errors. As demonstrated, the error is lower in the area near the center of gravity of the testbed area; specifically, it is less than 3 meters. Whereas when the user moves away from the center of gravity and approaches the edges of the testbed area, as expected such spatial configuration results in non-negligible localization errors and the error exceeds 4.5 meters. Only in one position, the user, while far from the center of gravity, experiences a low error; this can be explained by possible synchronization or external factors.

VI. Conclusion

This article presented a thorough examination of the essential components and current state of experimentation with 5G positioning using open-source platforms based on SDR technology. We showcased the usage of SDR and OpenAirInterface to assess 5G positioning by setting up a testbed consisting of four synchronized radios. Our findings revealed that establishing such a testbed can be quite challenging; nevertheless, we were able to provide a number of valuable insights regarding the critical need for localization accuracy, including the importance of precise synchronization of SDRs, the benefits of oversampling, and the necessity of calibration of measurements. Despite the limitations inherent in using open-source software and SDR configuration, this study demonstrates that such methodology can be effectively utilized to explore various aspects of 5G positioning, such as the impact of gNB synchronization accuracy, the structure

design of the positioning signal, and the performance of localization algorithms. It is crucial to note that the aim of this research is not to showcase the 5G localization performance of the testbed, but to demonstrate its potential as a valuable tool that enables researchers and industry to experiment and validate algorithms and research results through the measurement of real over-the-air transmitted 5G positioning signals, while taking into account standardized localization procedures and real-world operating conditions.

ACKNOWLEDGEMENT

The research conducted was sponsored by the European Union's Horizon 2020 research and innovation programme under Grant No. 871249 (LOCUS). CNIT was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU and University of Rome Tor Vergata was partially supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART"). The work at IMDEA Networks was sponsored in part also by the project MAP-6G, reference TSI-063000-2021-63, granted by the Ministry of Economic Affairs and Digital Transformation and the European Union-NextGenerationEU through the UNICO-5G R&D program of the Spanish Recovery, Transformation and Resilience Plan, and in part by the Regional Government of Madrid and the European Union through the European Regional Development Fund (ERDF) as part of the response from the European Union to the COVID-19 pandemic in the context of REACT-CONTACT-CM-23479 research project.

REFERENCES

[1] 3GPP, "Study on NR positioning support," 3rd Generation Partnership Project (3GPP), Technical Report (TR) 33.855. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3501

[2] ——, "Study on NR positioning enhancements," 3rd Generation Partnership Project (3GPP), Technical Report (TR) 33.857. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3732

[3] *Study on expanded and improved NR positioning*, 3rd Generation Partnership Project 3GPP™ 3GPP TR 38 859 V18.0.0 (2023-01), 2022, release 18.

[4] 3GPP, "Study on Integrated Sensing and Communication," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 22.837. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4044

[5] ——, "NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.305. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3310

[6] P. A. D. N. Jayawardana, H. Obaid, T. Yesilyurt, B. Tan, and E. S. Lohan, "Machine-Learning-Based LOS Detection for 5G Signals with Applications in Airport Environments," *Sensors*, vol. 23, no. 3, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/3/1470

[7] A. Xhafa, J. A. del Peral-Rosado, J. A. López-Salcedo, and G. Seco-Granados, "Evaluation of 5G Positioning Performance Based on UTDoA, AoA and Base-Station Selective Exclusion," *Sensors*, vol. 22, no. 1, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/1/101

[8] A. Conti, F. Morselli, Z. Liu, S. Bartoletti, S. Mazuelas, W. C. Lindsey, and M. Z. Win, "Location Awareness in Beyond 5G Networks," *IEEE Communications Magazine*, vol. 59, no. 11, pp. 22–27, 2021.

[9] H. Kim, K. Granström, L. Gao, G. Battistelli, S. Kim, and H. Wymeersch, "5G mmWave Cooperative Positioning and Mapping Using Multi-Model PHD Filter and Map Fusion," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 3782–3795, 2020.

[10] X. Jia, P. Liu, W. Qi, S. Liu, Y. Huang, W. Zheng, M. Pan, and X. You, "Link-Level Simulator for 5G Localization," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2023.

[11] S. Dwivedi, R. Shreevastav, F. Munier, J. Nygren, I. Siomina, Y. Lyazidi, D. Shrestha, G. Lindmark, P. Ernström, E. Stare, S. M. Razavi, S. Muruganathan, G. Masini, Busin, and F. Gunnarsson, "Positioning in 5G Networks," *IEEE Communications Magazine*, vol. 59, no. 11, pp. 38–44, 2021.

[12] G. Yammine, M. Alawieh, G. Ilin, M. Momani, M. Elkhouly, P. Karbownik, N. Franke, and E. Eberlein, "Experimental Investigation of 5G Positioning Performance Using a mmWave Measurement Setup," in *2021 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2021, pp. 1–8.

[13] S. Huang, H.-M. Chen, B. Wang, J. Chai, X. Wu, and F. Li, "Positioning Performance Evaluation for 5G Positioning Reference Signal," in *2022 2nd International Conference on Frontiers of Electronics, Information and Computation Technologies (ICFEICT)*, 2022, pp. 497–504.

[14] J. Shi, G. Zhang, Y. Lin, F. Li, and C. Shen, "Positioning of High-speed Trains Based on PRS," in *2022 International Wireless Communications and Mobile Computing (IWCMC)*, 2022, pp. 578–583.

[15] J. Zhang and H. Wang, "Online Learning Based NLOS Ranging Error Mitigation in 5G Positioning," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, 2022, pp. 6487–6492.

[16] C. Jin, I. Bajaj, K. Zhao, W. P. Tay, and K. V. Ling, "5G Positioning Using Code-Phase Timing Recovery," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, 2021, pp. 1–7.

[17] I. Palamà, S. Bartoletti, G. Bianchi, and N. B. Melazzi, "5G Positioning with SDR-based Open-source Platforms: Where do We Stand?" in *2022 IEEE 11th IFIP International Conference on Performance Evaluation and Modeling in Wireless and Wired Networks (PEMWN)*, 2022, pp. 1–6.

[18] L. Chen, X. Zhou, F. Chen, L.-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, 2022.

[19] OpenAirInterface Software Alliance (OSA), "OpenAirInterface, 5G software alliance for democratising wireless innovation," https://www.openairinterface.org/, Last accessed on 2023-03-08.

[20] Software Radio Systems, "srsRAN," https://github.com/srsran/srsRAN_4G, Last accessed on 2023-03-02.

[21] "Getting Started with Aether," https://docs.aetherproject.org/master/index.html, last accessed on 2022-04-20.

[22] Ettus Research, National Instruments, "USRP X310," https://www.ettus.com/all-products/x310-kit/, Last accessed on 2023-03-08.

[23] ——, "USRP N310," https://www.ettus.com/all-products/usrp-n310/, Last accessed on 2023-03-08.

[24] Samsung, Ericsson, "Support for Multiple QoS Class in deferred location requests," 3GPP SA2 144e CR, S2-2103085.

[25] 3GPP, "NR; Physical channels and modulation," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.211. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3213

[26] ITU-T, ""timing characteristics of enhanced primary reference time clocks"," International Telecommunication Union, Recommendation G.8272.1/Y.1367.1, Nov. 2016.

[27] S. Ruffini, M. Johansson, B. Pohlman, and M. Sandgren, "5G synchronization requirements and solutions," *Ericsson Technology Review*, vol. 2021, no. 1, pp. 2–13, 2021.

[28] Software Radio Systems, "srsRAN Project," https://github.com/srsran/srsRAN_Project, Last accessed on 2023-03-02.

[29] Open Networking Foundation (ONF), "SD-RAN," https://opennetworking.org/open-ran/, Last accessed on 2023-03-08.

[30] ——, "SD-CORE," https://opennetworking.org/sd-core/, Last accessed on 2023-03-08.

[31] 3GPP, "NR; Physical layer measurements," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.215. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3217

[32] Ettus Research, National Instruments, "UBX 10-6000 MHz Rx/Tx (160 MHz, X Series only)," https://www.ettus.com/all-products/ubx160/, Last accessed on 2023-03-08.

[33] ——, "OctoClock-G CDA-2990," https://www.ettus.com/all-products/octoclock-g/, Last accessed on 2023-03-08.

[34] H. P. Gavin, "The Levenberg-Marquardt algorithm for nonlinear least squares curve-fitting problems," *Department of Civil and Environmental Engineering, Duke University*, vol. 19, 2019.

[35] C. A. Floudas and P. M. Pardalos, *Encyclopedia of Optimization*. Springer Science & Business Media, 2008.

[36] S. Ruder, "An overview of gradient descent optimization algorithms," *arXiv preprint arXiv:1609.04747*, 2016.