5G Positioning with Software-defined Radios

Ivan Palamà[a], Yago Lizarribar[b], Lorenzo Maria Monteforte[a], Giuseppe Santaromita[b], Stefania Bartoletti[a], Domenico Giustiniano[b], Giuseppe Bianchi[a], Nicola Blefari Melazzi[a]

[a] *University of Rome Tor Vergata and CNIT, Rome, Italy*
[b] *IMDEA Networks Institute, Madrid, Spain*

Abstract

Positioning is a key focus in 5G standardization, starting with 3GPP Release 16. However, most of the effort from the research community and work presented in the technical standardization has been limited mainly to simulation studies. This paper explores the use of software-defined radios (SDRs) platforms for 5G positioning, presenting an overview of the current state-of-the-art and available open-source platforms. Utilizing an advanced SDR-based multi-gNodeBs (gNBs) synchronized testbed, the paper conducts a series of time-based, over-the-air measurements. Results offer insights into the impact of various real-world system parameters, such as the number of gNBs, transmission bandwidth, signal processing techniques, and localization algorithms on positioning accuracy and Time to First Fix (TTFF). These findings provide a pathway for the cost-effective and efficient implementation of high-precision 5G localization systems. The paper contributes to advancing both theoretical understanding and practical applications, serving as a guide for the development of 5G positioning technology.

Keywords: 5G, Positioning, Localization, Signal Processing, SDR

1. Introduction

The evolution of 5G technology, underpinned by the 3rd Generation Partnership Project (3GPP)'s ongoing standardization efforts, marks a pivotal shift in the telecommunications landscape. Beginning with Release 16, the focus has been on enhancing the capabilities of 5G networks to support precise localization services, a critical component for a myriad of emerging applications [1, 2]. The

Email address: ivan.palama@uniroma2.it (Ivan Palamà)

integration of advanced localization features into 5G networks is not just a technological advancement; it represents a paradigm shift in how mobile networks can be leveraged, targeting high-accuracy and low-latency positioning through increased bandwidths and flexible numerology within the 5G physical layer.

The ambition to achieve centimeter-level accuracy, as outlined in Release 17, is a testament to the growing importance of 5G localization accuracy, low latency, network and device efficiency [3], for commercial use cases, Industrial IoT and especially for time-sensitive applications like remote control systems. Release 18, known as 5G Advanced, further enhances these capabilities, introducing improvements such as New Radio (NR) carrier phase measurements and sidelink positioning [4, 5] for out-of-range scenarios and Radio Access Technology (RAT)-dependent techniques for better accuracy under non-line-of-sight (NLOS) conditions [6]. With the initiation of Release 19, the exploration of wireless sensing technologies and mobile XR further emphasizes the strategic role of AI/ML in localization services in the future of wireless networks [7].

While the 3GPP has established a robust framework for 5G positioning with its comprehensive technical reports and specifications [8, 3, 9], the practical realization and evaluation of these technologies in real-world scenarios remains a challenge. This complexity is further accentuated by the diverse range of positioning use cases outlined in 3GPP documents [3, 9], each with distinct performance accuracy and Time to First Fix (TTFF) requirements. Simulations and preliminary experimental setups have been the primary methods for assessing 5G positioning performance to date [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20]. Only a few pioneering studies have begun to conduct experimental research with over-the-air (OTA) 5G signals [21, 22, 23].

In this field, open-source platforms like OpenAirInterface (OAI) [24], srsRAN [25], and Aether [26], when paired with Software-Defined Radio (SDR) devices such as Ettus USRP B210, HackRF One, LimeSDR, BladeRF, and the more advanced 5G-oriented Ettus USRPs X310, N310 and X410 [27], provide a robust framework for implementing and testing the 3GPP stack. These open-source platforms and commercial devices offer a unique opportunity for rapid prototyping and testing new algorithms and paradigms in real-world OTA conditions.

Despite these technologies' potential, their application in 5G localization and positioning demands significant effort in hardware and software setup and configuration. In this work, we provide a deep understanding of 5G positioning in real-world conditions building on our preliminary insights [28], and stressing prior work over three dimensions: 1) We assess the impact of increasing the number of gNBs, a strategy aimed at enhancing the spatial diversity and accuracy

of the localization system. 2) We explore the benefits of expanding the operational bandwidth up to 100 MHz, the largest bandwidth currently allowed by the 3GPP standard for communication below 6 GHz; larger bandwidth is expected to provide finer resolution in time-based measurements, leading to more precise localization. 3) We delve into oversampling and moving average signal processing strategies, examining the effects of sampling rates up to four times at 100 MHz and moving average window up to 50 measurements; these approaches are hypothesized to improve the accuracy of time-of-arrival (TOA) measurements and reduce the effect of quantization errors, a critical factor in precise localization.

The results not only enhance the theoretical understanding of 5G localization but also provide practical insights and methodologies for application and experimentation in real-world settings that can be of interest both for the research community and for the telecommunication engineers that will build new 5G and beyond infrastructures. In fact, we demonstrate how strategic decisions in network infrastructure design and signal processing techniques can be effectively evaluated, offering valuable guidance to researchers and industry professionals seeking to enhance localization performance in contemporary 5G and beyond networks.

The article is organized as follows: we begin with essential background information in Section 1, followed by an analysis of the current state-of-the-art in 5G positioning and a detailed description of our 5G localization system model in Sections 2 and 3, respectively. Section 4 is dedicated to presenting our implementation of the 5G localization SDR-based experimental testbed. The experimental results obtained are thoroughly analyzed and discussed in Section 5. The article concludes with key findings and conclusions in Section 6.

2. 5G Positioning: State of the Art

This section introduces and describes the main elements of the 3GPP standardization of 5G localization and examines the role of existing open-source platforms in implementing location services within 5G mobile networks.

2.1. 5G Positioning Architecture

The implementation of 5G positioning, now advancing with the innovations of 3GPP Releases from 16 to 19, leverages an optimized architectural design for efficient transmission of location signals between gNB and UE, and for the seamless exchange of location measurements with the 5G Core Network. The evolving architectural specifications for 5G positioning, reflecting these technological strides, are detailed in [8].

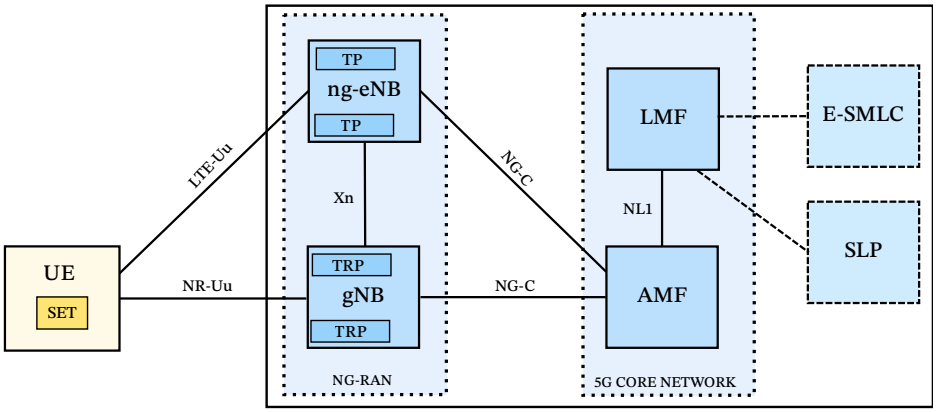


Figure 1: 3GPP 5G Positioning architecture [8].

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 (DL) signals from the Next Generation Radio Access Network (NG-RAN), or may send Reference Signals in uplink for positioning;
- NG-RAN, comprised of gNBs and next generation- evolved NodeB (ng-eNB) network elements, which may contribute through radio signal measurements and convey these measurements to the LMF. A gNB can be composed of one or multiple Transmission-Reception Point (TRP), a set of geographically co-located antennas (e.g. antenna array). In our experimental studies with downlink positioning, TRPs are geographically separated, and therefore we consider one TRP per gNB;
- The Access & Mobility Management Function (AMF), which is responsible for handling connection and mobility management tasks, including positioning for a target UE, as per request for some location service associated or on behalf of a particular target UE;
- Location Management Function (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) was first introduced in Long-Term Evolution (LTE) network architecture. The LMF may

communicate with E-SMLC with a proprietary interface to access location information from older networks;

- The SUPL Location Platform (SLP) is a server-based technology for providing secure and accurate location services to mobile devices on the user plane. The LMF may communicate with the SLP with a proprietary interface.

The LMF plays a crucial role in receiving location requests from the AMF and interacting 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 [29], UE positioning capabilities, and NG-RAN positioning capabilities, and invokes these methods in the UE and serving NG-RAN.

5G positioning signals: 5G positioning signals have been introduced to achieve higher accuracy compared to LTE positioning [30]. These signals include the uplink Sound Reference Signal (SRS) and an improved LTE Positioning Reference Signal (PRS) version for the downlink. In this work, we delve into the latter, as our focus is on downlink positioning methods. PRS 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 throughout the NR bandwidth.

5G Positioning Schemes: As of Release 16, 3GPP has standardized the following 5G positioning schemes [8]: 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). The recent releases have further refined these schemes, enhancing their accuracy and efficiency. 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 five 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.

As mentioned earlier, each gNB consists of one or multiple TRPs. Nevertheless, to simplify the description, we simply refer to gNBs as the element in the NG-RAN involved in the procedures of positioning in the rest of the paper. In the DL-TDOA scheme, the UE calculates the reference signal timing difference (RSTD) or TDOA of the PRSs transmitted by two distinct gNBs. The measured TDOA, is then communicated to the LMF, which uses these timing differences to estimate the UE's position. The UL-TDOA scheme is conceptually similar to DL-TDOA but uses uplink signals and reverses the signal direction. Here, the gNB is responsible for measuring the relative time of arrival (RToA) of multiple SRSs emitted by UEs. The gNB communicates these measurements to the LMF. In the DL-AOD scheme, the UE measures the received power of downlink reference signal beams from multiple gNBs. These power measurements are used to estimate the position angle of the UE and are communicated to the LMF. The LMF then solves the derived equations to determine the UE's position based on these multiple gNBs estimates. Mirroring DL-AOD, UL-AoA utilizes uplink signals. The gNBs measure the angle of arrival of the uplink signal from UE, which is communicated to the LMF, and the UE's position is determined from these multiple-angle multi-gNBs measurements.

In the Multi-RTT positioning scheme, both uplink and downlink signals are used. The UE and a minimum of three gNBs exchange reference signals (SRS and PRS) to measure the Round Trip Time (RTT), deducing the RX-TX time difference. The LMF synthesizes these measurements to calculate the distances between the UE and each gNB, estimating the UE's position at the intersection point of the circles formed with these distances as radii. The CID positioning technique involves the estimation of the UE position using information about its

connected ng-eNB, gNB, and cell. This information can be acquired through paging, registration, or other similar methods. NR E-CID positioning approach takes this a step further by incorporating additional UE measurements, NG-RAN radio resources, and other metrics, significantly enhancing the accuracy of the UE location estimates.

2.2. 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 or disturbance attacks that affect its reliability; consequently, it cannot be used standalone as a 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 the usage of cesium clocks for centralized grand master clocks and quartz/rubidium for distributed master clocks and boundary clocks [31]. 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. Nevertheless, G.8275.1 is recommended to meet the relevant time synchronization requirements [32]. Finally, in the RAN domain, over-the-air synchronization could provide a valid

alternative as it is based on round-trip time measurement sent over the radio interface between neighboring base stations [32]. However, it lacks work in standardization.

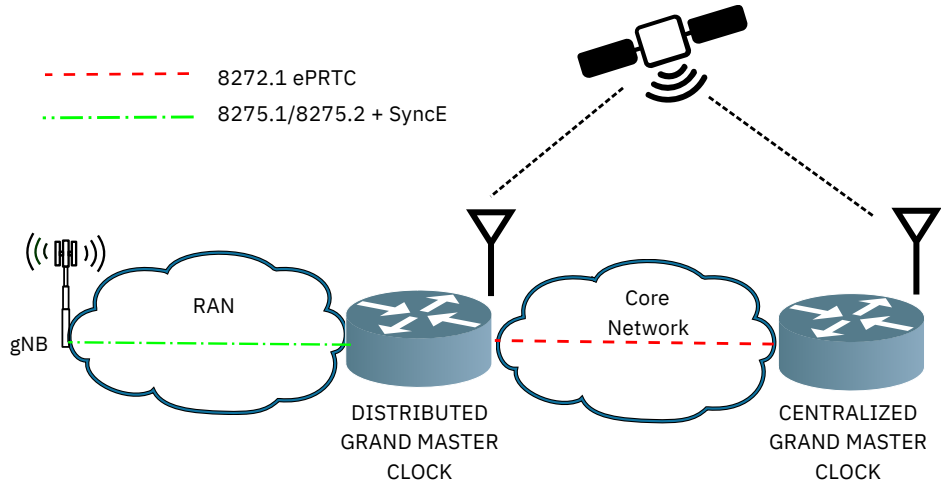


Figure 2: Mobile network synchronization for 5G networks.

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.

2.3. 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. Written in C for real-time performance, OAI is distributed under the OAI Public License. This license allows free redistribution, use, and modification of source and object code for academic and research purposes, but it mandates Fair, Reasonable, and Non-Discriminatory (FRAND) negotiations for commercial or non-research uses, differing from Open

Source Initiative-approved licenses in terms of unrestricted use. OAI is compatible with Intel and ARM architectures running Linux distributions and supports the most commonly used SDR platforms (e.g., USRP and LimeSDR). In recent times, OpenAirInterface has aligned with O-RAN standards through FlexRIC integration and 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 Inverse Discrete Fourier Transform (IDFT) with up to 16x oversampling for CIR. It allows receiving DL PRS from multiple gNBs synchronized via a GPS disciplined oscillator (GPSDO). This makes OAI the ideal platform to test 5G positioning.

srsRAN: srsRAN platform provides software implementations of the gNB and UE with functionality up to NR Release 15. It does not implement its 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. The srsRAN platform comprises two projects: srsRAN 4G[25] and srsRAN Project[33]. The srsRAN 4G project provides an end-to-end 4G and 5G NSA network implementation and a prototyping implementation of 5G SA UE and gNB. Instead, srsRAN Project is an ORAN-native 5G Centralized Unit/Distributed Unit (CU/DU) solution compliant with 3GPP and O-RAN Alliance specifications. srsRAN is the most similar platform to OAI; in fact, it is compatible with Linux distributions and supports the most popular SDR platforms. But, unlike OAI, where development is carried out daily by multiple branches, in srsRAN the release of new features is cadenced approximately semiannually; this makes srsRAN a relatively more stable project than OAI, but offers fewer features, including 5G positioning signal support. In fact, currently, srsRAN does not support positioning signals and protocols.

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 [34] and SD-CORE [35], 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 an O-RAN-compliant, near-real-time intelligent RAN controller (RIC) based on micro-ONOS, a cloud-native variant of the Open Network Operating System (ONOS), and an O-RAN-compliant platform for eXtended applications (xAPPs). SD-RAN is based on OAI gNB and UE implementations. Since Aether's RAN is based on OAI without adding additional positioning support and we were not interested in

the O-RAN extra functionalities, we decided to use OAI directly in our experimental setup.

3. System Model

This section introduces the main elements of our location system model and the associated signal processing methodologies. In the subsequent sections of the paper, we assume a 2D location scenario, i.e., considering only the x and y coordinates while neglecting the z coordinate. Furthermore, assuming a 2D environment, we focus on horizontal positioning accuracy, which is often of primary interest in many practical localization applications. For clarity, it is worth noting that using 5G reference signals dedicated to positioning in a 3D localization scenario is possible.

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 unknown position of the jth UE is at $\mathbf{p}_{\mathrm{UE}}^{(j)} = \left[\mathbf{x}_{\mathrm{UE}}^{(j)}\ \mathbf{y}_{\mathrm{UE}}^{(j)}\right]$. A location-dependent time-based measurement is performed for each gNB. Fig. 3 provides a visual representation of a typical network deployment following our system model.

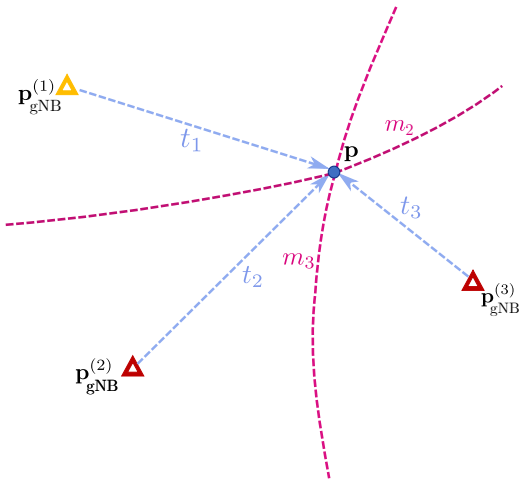


Figure 3: Example network deployment with $N_g = 3$ gNBs (triangles) and $N_u = 1$ UE (circle). The TDOA $m_2 = t_2 - t_1$ and $m_3 = t_3 - t_1$ are measured considering the first anchor as the reference (yellow triangle). The corresponding hyperbola is illustrated in magenta.

3.1. Comparative Analysis of PRS and SRS for Positioning

In the context of utilizing 5G reference signals for positioning, it is essential to distinguish between PRS and SRS. Both signals have unique characteristics and applications within the network, influencing their suitability for positioning tasks.

- Signal Design and Purpose: Specifically designed for positioning, PRS is optimized for time-based measurements, which are crucial for accurate localization. The structure of PRS minimizes ambiguity in detection, making it highly effective for positioning in diverse environments. Hence, SRS primarily aims to estimate uplink channel state information (CSI), facilitating network decisions regarding beamforming, power control, and user scheduling. Although SRS can be repurposed for positioning, its design is not inherently optimized for this application.

- Robustness and Accuracy: PRS exhibits superior robustness to multipath effects and NLOS conditions, critical attributes in urban and indoor environments where direct paths between the transmitter and receiver are often obstructed. SRS, instead, while useful for its intended purpose of channel estimation, is less robust in the face of multipath and NLOS conditions when repurposed for positioning, potentially leading to decreased accuracy.

- Network Resource Utilization: PRS utilizes dedicated resources in the frequency and time domain, ensuring that the signal integrity is preserved for the precise measurement requirements of positioning tasks. SRS instead, though flexible in configuration, using SRS for positioning could lead to increased resource consumption or necessitate trade-offs with its primary function of channel sounding. SRS time-domain and frequency-domain allocation is limited compared to PRS (i.e., max 4 OFDM symbols in 1 slot).

Given these considerations, while SRS presents a theoretically viable option for positioning, its performance, robustness, and efficiency for such applications are inherently constrained by its primary design for channel sounding. Conversely, PRS, with its positioning-optimized design, offers significant advantages in accuracy, reliability, and compliance with positioning standards. Therefore, in our system model and subsequent analyses, we focus on PRS. This choice is motivated by our objective to explore the use of SDR platforms for 5G positioning, leveraging the inherent advantages of PRS designed specifically for this purpose.

3.2. TOA Estimation

The relative TOA for the signal transmitted by the ith gNB and received by the jth UE is expressed as:

$$t_{i,j}(\mathbf{p}) = \frac{\|\mathbf{p}_{\text{gNB}}^{(i)} - \mathbf{p}_{\text{UE}}^{(j)}\|}{c} \tag{1}$$

where c is the speed of light. In OAI, PRS-based TOA estimation is implemented through a series of well-defined steps in accordance with the 3GPP standards for 5G positioning. Initially, Pilots are generated and modulated, serving as references for subsequent processing. Subsequently, the Resource Element (RE) offset of the PRS is calculated, followed by channel estimation and interpolation. Next, signal-to-noise ratio (SNR) estimation is conducted, and PRS channel estimates are transformed into a format suitable for 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.

3.3. 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 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. Conventionally, the gNB with index $i = 1$ is designated as the reference for RSTD measurements.

The RSTD, as described in [36] Section 5.1.29, represents the relative time difference between the ith neighboring gNB and the reference gNB and is calculated by the jth UE as $m_{i,j} = t_{i,j}(\mathbf{p}) - t_{1,j}(\mathbf{p})$. Therefore, the measurement model for the TDOA is as follows:

$$m_{i,j} = \left\|\mathbf{p}_{\text{gNB}}^{(i)} - \mathbf{p}_{\text{UE}}^{(j)}\right\| / c - \left\|\mathbf{p}_{\text{gNB}}^{(1)} - \mathbf{p}_{\text{UE}}^{(j)}\right\| / c + n^{(i,j)}(\mathbf{p}) \tag{2}$$

Measurement noise $n^{(i,j)}(\mathbf{p})$ 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.

3.4. Optimization Model for Positioning

We can formulate the optimization problem as a minimization of the L2-norm of the measured and estimated TDOA:

$$\mathbf{p_{UE}} = \arg\min_{\mathbf{p_{UE}}} S(\mathbf{p_{UE}}) = \frac{1}{2}\sum_{\forall i,j}(\hat{m}_{ij} - m_{ij}(\mathbf{p_{UE}}))^2 = \frac{1}{2}\sum_{\forall i,j} r_{ij}^2 \tag{3}$$

where $\hat{m_{ij}}$ is the measured TDOA between gNBs i and j, $m_{ij}(\mathbf{p_{UE}})$ is the evaluation of Equation 2 at the UE position $\mathbf{p_{UE}}$ and r_{ij} denotes the residual error between them. For this method, the solution lies at the point where the gradient of $S(\mathbf{p_{UE}})$ is 0, which can be computed per transmitter coordinate (x, y) as:

$$\begin{aligned}
\frac{\partial S}{\partial p_{UE,x}} &= \sum_{\forall i,j} r_{ij} \cdot \left(\frac{p_{UE,x} - p_{gNB_i,x}}{d_i} - \frac{p_{UE,x} - p_{gNB_j,x}}{d_j} \right) \\
\frac{\partial S}{\partial p_{UE,y}} &= \sum_{\forall i,j} r_{ij} \cdot \left(\frac{p_{UE,y} - p_{gNB_i,y}}{d_i} - \frac{p_{UE,y} - p_{gNB_j,y}}{d_j} \right)
\end{aligned} \tag{4}$$

The optimization problem for the TDOA equations is non-convex, and requires more complex methods to obtain reliable solutions. There also exist techniques to linearize these equations and obtain fast (but suboptimal) solutions. These approaches are further explained in Section 4.3.

3.5. Geometric Dilution of Precision

The Geometric Dilution of Precision (GDOP) quantitatively represents the impact of the geometric configuration of gNBs on the accuracy of UE localization. It's derived from the Jacobian matrix, which relates the TDOA measurements to the UE's position.

For clarity in our 5G localization system analysis, it's important to note that while we are addressing a two-dimensional positioning problem, we typically refer to the Horizontal Dilution of Precision (HDOP) in such cases. However, for the sake of generality, we choose to use the term GDOP in the following discussion. Given a network of N_g gNBs, with ith position $\mathbf{p}_{\text{gNB}}^{(i)}$, N_u UEs with jth position $\mathbf{p}_{\text{UE}}^{(j)}$ and the TDOA measurement given by Eq. 2, since one gNB is used as a reference, we have $N_g - 1$ independent TDOA measurements for each jth UE. The corresponding Jacobian matrix in two dimensions $\mathbf{J}$, representing the sensitivity of the TDOA measurements to the position considered j UE, is calculated

as follows:

$$\mathbf{J} = \begin{bmatrix} \frac{\partial m_2}{\partial \mathbf{x}_{\mathrm{UE}}} & \frac{\partial m_2}{\partial \mathbf{y}_{\mathrm{UE}}} \\ \vdots & \vdots \\ \frac{\partial m_{N_g}}{\partial \mathbf{x}_{\mathrm{UE}}} & \frac{\partial m N_g}{\partial \mathbf{y}_{\mathrm{UE}}} \end{bmatrix} \tag{5}$$

where each element of $\mathbf{J}$ is the partial derivative of the TDOA measurement $m_{i,j}$, based on the measurement model defined in eq. 2, with respect to the jth UE's coordinates $\mathbf{x}_{\mathrm{UE}}^{(j)}$ and $\mathbf{y}_{\mathrm{UE}}^{(j)}$.

Finally, GDOP is calculated as the square root of the trace of the matrix product $(\mathbf{J}^T\mathbf{J})^{-1}$:

$$\mathrm{GDOP} = \sqrt{\mathrm{trace}((\mathbf{J}^T\mathbf{J})^{-1})} \tag{6}$$

A lower GDOP value implies a more favorable geometric configuration, leading to enhanced accuracy in the UE's position estimation. Conversely, a higher GDOP suggests a less ideal geometry, potentially decreasing the precision of location estimates. This underlines the importance of strategic placement of gNBs in our network. Our experimental setup, featuring four gNBs, aims to minimize the GDOP, thus ensuring a geometrically optimal arrangement for precise localization. In addition to GDOP, the Cramér-Rao Lower Bound (CRLB) provides a more general theoretical benchmark for the minimum variance of an unbiased estimator [37]. The CRLB is defined based on the Fisher Information Matrix (FIM) for the positioning error, and a lower CRLB value indicates a higher potential accuracy in position estimation.

4. Experimental Setup

This section delineates the deployment of our 5G SDR-based experimental localization system, detailing both the software and hardware configurations, along with the network configuration and signal processing methodologies employed.

4.1. Mobile Network Software

In our experimental setup, we use the 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 release tagged *2023.w38* is employed for our experiments. TOA measurement estimation for PRS is executed using the *peak_estimator* function inside the *nr_prs_channel_estimation*

function, located within the *nr_dl_channel_estimation.c* file. To enable TOA measurement estimation for UL SRS in OAI, it would be necessary to integrate the *peak_estimator* function into the *nr_srs_channel_estimation* function, found in the *nr_ul_channel_estimation.c* file.

4.2. Hardware

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

SDR: Five Ettus USRP X310 devices, equipped with UBX160 daughterboards [38], constitute the backbone of our SDR setup. These devices, covering a broad radio frequency spectrum from 10 MHz to 6 GHz, support all NR FR1 frequency bands with up to 160 MHz bandwidth. Using the high-speed 10 GbE interface, a sampling rate of 184.32 MS/s can be achieved, enabling a theoretical localization accuracy of 1.62 m. We used NR-specific Linx ANT-5GWWS3 [39] SMA multiband antennas. While both the Ettus USRP N310 and X310 were evaluated in our experimental setup, we encountered significant interoperability issues due to the differences in their supported master clock rates. Specifically, the USRP N310 supports master clock rates of 122.88 MHz, 125.00 MHz, and 153.60 MHz, while the USRP X310 operates at higher clock rates of 184.32 MHz and 200.00 MHz. This discrepancy in clock rate compatibility presents a challenge for interoperability between the N310 and X310 in a unified experimental setup, as synchronized data acquisition and processing are necessary for communication and positioning.

Base station synchronizer: Precise synchronization between gNBs is achieved using the Ettus Octoclock [40], a high-precision clock generator and distribution unit. With its eight independent clock outputs, GPS receiver, phase-locked loop (PLL), and voltage-controlled crystal oscillator (VCXO) configuration, this device provides exceptional frequency stability and accuracy, essential for our mobile network localization testbed. According to the specifications, the accuracy of the 1 PPS of the built-in GPSDO is within ±50 ns of the UTC RMS, with a 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: The computational backbone comprises two Intel Core i9 powered workstations, each with 18 cores clocked at 3 GHz, running Ubuntu 18.04 LTS Linux operating system with a low-latency kernel. We strategically utilized Ubuntu 18.04 LTS for its proven stability and extensive support for critical legacy hardware and software components. These workstations implement the 5GCN

and four gNBs. To implement the UE, an 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) running Ubuntu OS 22.04 LTS is utilized. For the sake of clarity, initially, our experiments were conducted on a stable setup using Ubuntu 18.04 LTS, prioritizing research continuity over system updates due to time constraints. Recognizing the importance of staying current, we later upgraded the two workstations to Ubuntu 22.04. We validated our setup's compatibility with this newer version, demonstrating our testbed's robustness and adaptability to evolving software environments.

4.3. Signal Processing Techniques and Localization Algorithms

Our experimental approach to assessing how to improve 5G localization accuracy includes the study of advanced signal processing techniques.

Moving Average: Given the experimental challenges and environmental variabilities associated with 5G localization using open-source SDR-based frameworks, achieving consistent positioning performance is a complex task. To address this, we employ moving average techniques, which are instrumental in mitigating the impact of outlier measurements. By averaging out extreme values in time-based ranging data, the moving average method substantially improves the reliability and stability of our localization results, ensuring a more robust performance even in fluctuating outdoor conditions.

Oversampling Techniques: To counteract the presence of multipath interference, which leads to significant errors in the TOA estimates, we implement oversampling. 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 SNR, allowing for a more accurate and robust estimate of the TOA. In OAI, oversampling is implemented using a technique called zero-padding, which 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.

Localization Algorithms: To address the localization challenge in wireless networks, a variety of algorithms are employed, each offering distinct approaches and benefits. These include Linear Least Squares (Linear LS), Non-Linear Least Squares (NLLS), and the Brute-Force algorithm. Each method offers distinct methodologies for estimating the position of UE in a 5G network environment.

Linear LS simplifies the localization problem by linearizing the TDOA equations in a similar manner as [41]. This method assumes a linear relationship between the measured TDOAs and the unknown UE position. It is most effective in environments with minimal signal distortion but tends to be less accurate in scenarios with significant multipath effects or non-line-of-sight conditions.

NLLS directly addresses the non-linear nature of TDOA equations. It leverages iterative optimization routines based on gradient-based techniques to determine the direction of maximum descent and minimize the 2-norm difference between the predicted and actual TDOAs. 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 [42], BFGS [43], or Gradient-Descent and its variants [44], with similar results.

Lastly, the Brute-Force Algorithm takes a comprehensive approach, discretizing the area of interest into a grid and evaluating a cost function at each grid point. Since the estimated position is identified as the point that minimizes the minimum 2-norm discrepancy between the ideal predicted and estimated TDOA values, accuracy depends on the grid size, and the tradeoff between accuracy and processing time became crucial. However, this method, especially for finer grids, offers high accuracy due to its exhaustive search of the solution space.

Each algorithm's suitability varies depending on the specific environmental conditions and system requirements, making it essential to select the appropriate method based on the context of the localization task.

As a benchmark, we define the 'Ideal' case as the theoretical best-case scenario with minimal error influence, utilizing NLLS, chosen because brute force and NLLS yielded nearly equal results in our experiments. For comparative purposes, this scenario is characterized by only process noise and without the constant sampling time offset.

4.4. Network configuration

Our methodology for enhancing 5G localization precision entailed a detailed exploration of various network configurations, specifically examining the impact of different numbers of gNBs and bandwidth parameters.

Network Deployment with Four gNBs: In a TDOA-based system, the localization accuracy heavily depends on the geometry of the gNBs relative to the UE. With three gNBs, TDOA localization is typically reliant on the intersection of hyperbolae formed by the time difference measurements between pairs of gNBs. While effective, this approach can be limited in precision due to factors like signal multipath, non-line-of-sight conditions, and synchronization errors. The addition of a fourth gNB not only provides an extra set of TDOA measurements but also enhances the geometric robustness of the system, introducing new hyperbolic intersections and significantly refining the localization process. The configuration of four gNBs also mitigates the effect of GDOP. By adding the fourth gNB, we lead to a lower GDOP value and, thus, higher accuracy in the calculated position of the UE.

Bandwidth Configurations: We explore the impact of varying bandwidths - 40, 80, and 100 MHz - on the accuracy of localization. Higher bandwidths result in shorter impulse responses in the time domain, improving the precision of TDOA measurements due to more defined signal autocorrelation functions, offering sharper peaks and, consequently, more precise timing estimates. Essentially, increased bandwidth translates to improved time resolution, which leads to enhancing the accuracy of TDOA-based localization systems. This enhancement in time resolution positively affects the FIM, leading to more informative TDOA measurements. Consequently, a larger bandwidth not only enriches the FIM but also reduces the CRLB, indicating less variance in position estimates and thus increasing the overall localization accuracy.

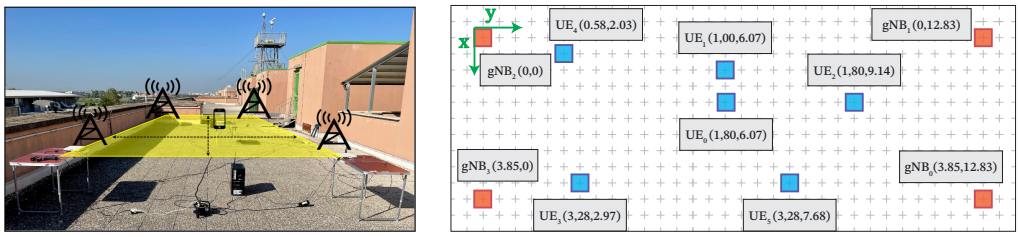
5. Experimental validation

In this section, we present the deployment scenario and the experimentation settings, and discuss the experimental results.

5.1. Deployment Scenario

As illustrated in Figure 4a, experiments were performed on an outdoor setting, a roof of the University of Rome, Tor Vergata. Experiments are conducted outdoors with clear GPS satellite visibility to ensure proper synchronization. The experimental testbed area is shown in Figure 4b. Our testbed covers a surface

of more than 50 m^2. As reported in Figure 4b, we use six different selected UE locations to test our experimental positioning system.



(a) Testbed Setup.

(b) gNB and UE positions.

Figure 4: Experiment setup overview. The experimental area is shaded in yellow (Figure 4a) with four gNBs and UE. Figure 4b shows the positions of the gNBs and the 6 locations for the UE.

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

The 5G NR TDD channel has been configured in the N78 frequency band (3500 MHz) for the experimental localization testbed. The channel has a variable instantaneous bandwidth of 40, 80 and 100 MHz (respectively, 106, 217 and 273 RB) and a sub-carrier spacing of 30 kHz.

NLOS conditions adversely affect TOA measurements for PRS in 5G networks by causing multiple propagation and an alteration of TOA estimates by delayed copies of the signal, which can be misinterpreted as direct signals, leading to incorrect distance estimates. In the following subsections, we will focus on the LOS scenario because our SDR testbed, constrained by low transmission power, is inherently suited for LOS scenarios and lacks the capability to manage the challenges posed by NLOS conditions effectively. Therefore, since we cannot handle NLOS scenarios with the hardware at our disposal, our study does not cover NLOS scenarios, emphasizing an area for future research with more capable hardware.

5.2. Moving Average Experimentation

In this subsection, we examine the influence of applying a moving average filter to Time Difference of Arrival (TDOA) measurements on position estimation accuracy. This analysis is supported by Figure 5, which graphically illustrates the

correlation between increasing average window sizes and the resultant position estimation errors.

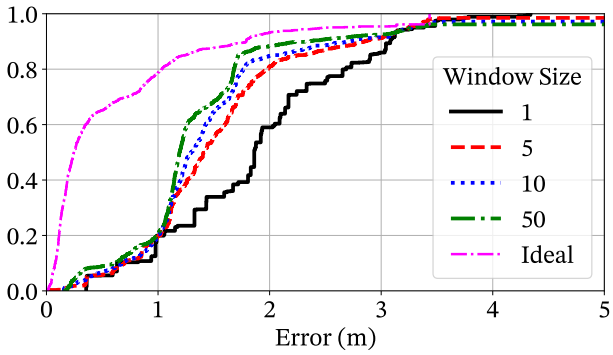


Figure 5: Empirical cumulative distribution function of the error using a Non-Linear Least Squares localization algorithm, four gNBs, no oversampling and 100 MHz BW with varying moving average window sizes applied to TDOA measurements.

As demonstrated in Figure 5, implementing a moving average filter with a window size of up to 50 significantly reduces the localization error. Indeed, by using a Brute Force localization algorithm, four gNBs and 100 MHz BW, it is possible to achieve a localization error of 1.7 meters in 80% of the cases, an improvement of about 37.04% over the case without moving average. This reduction in error demonstrates the filter's efficacy in enhancing the accuracy of position estimations by smoothing out random noise and measurement fluctuations in the TDOA data. The filter effectively smooths out short-term fluctuations and random noise inherent in signal measurements by averaging TDOA measurements over a defined number of samples (the window size).

However, it is important to consider the trade-off between noise reduction and the potential delay introduced by larger window sizes. Especially in dynamic time-critical scenarios, it is crucial to optimize the window size to ensure that the filter does not overly smooth out the TDOA data, which could lead to inaccuracies in triangulation.

5.3. Oversampling improvement

To effectively show the impact of oversampling on location estimation accuracy, we present Figure 6, which illustrates localization errors by implementing different oversampling factors. The oversampling analysis strategically focuses on UE's most representative positions 0, 4, and 5, to illustrate the system's performance across diverse scenarios: position 0 as a baseline, position 4 to assess

performance under conditions close to a receiver, and position 5 to evaluate robustness in a challenging environment at a corner and further from the receivers.

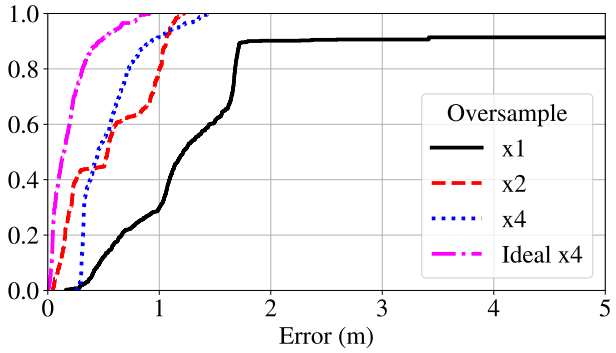


Figure 6: Empirical cumulative distribution function of the error using Non-Linear Least Squares localization algorithm, 100 MHz of BW, moving average window size 50 and varying the oversampling factor.

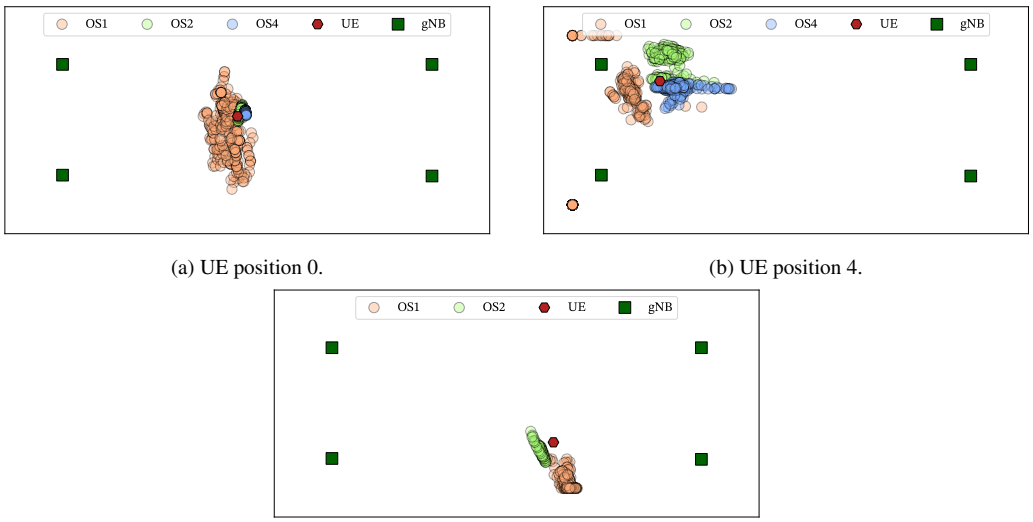
As shown in Figure 6, by implementing a 4x oversampling rate, we can reduce the localization error to 0.7 meters in 80% of the cases, compared to 1.7 meters without oversampling, which results in a localization performance improvement of 58.82%. This notable improvement is attributed to the *ability of oversampling to generate more accurate TOA values, which are indispensable in location estimation algorithms*.

Figure 7 demonstrates the beneficial impact of oversampling on UE position estimations. In fact, the experimental results confirm what was argued in Section 4.3, showing how effectively oversampling enhances the resolution of signal processing, allowing for a more detailed signal representation and, thus, a more precise extraction of timing information. As a result, the variance in position estimations is reduced, thereby improving the overall accuracy of the localization system.

These results collectively establish the efficacy of oversampling as a methodology to increase location estimation accuracy in wireless communication systems.

5.4. Network Configuration Experimentation

This subsection delves into the impact of varying the network configuration, particularly the number of gNBs, on the precision of position estimation in a 5G network. Figure 8 presents a comparative analysis of positioning errors in three and four gNBs scenarios.



(a) UE position 0.

(b) UE position 4.

(c) UE position 5.

Figure 7: Impact of oversampling (OS) on the variance of three selected UE position estimates, with OS1, OS2, and OS4 corresponding to factors 1, 2, and 4, respectively.

Figure 8 shows that the use of four gNBs leads to a reduced localization error of 1.2 meters, an improvement of 29.41% compared to the three gNB setup. When an extra gNB is added, the improvement in positioning accuracy can be attributed to improved network geometry, as previously discussed in GDOP subsection 3.5.

To better understand the impact of the placement of the gNB on the localization accuracy, Figure 9 shows the theoretical HDOP in our experimental setup. Incorporating an additional gNB enhances the spatial distribution of signal sources around the UE, and the system benefits from additional reference points, which helps to refine the triangulation process and reduce the potential for positioning errors.

The findings of this experiment reinforce the concept that network configuration, specifically the number of gNBs and their spatial location, is a critical factor in achieving high accuracy in 5G positioning systems.

5.5. Localization Algorithms

This subsection evaluates the accuracy of localization using various algorithms, namely Linear LS, NLLS, and Brute-Force. Each of these algorithms offers a different approach to resolving the localization problem, with varying degrees of complexity and precision.

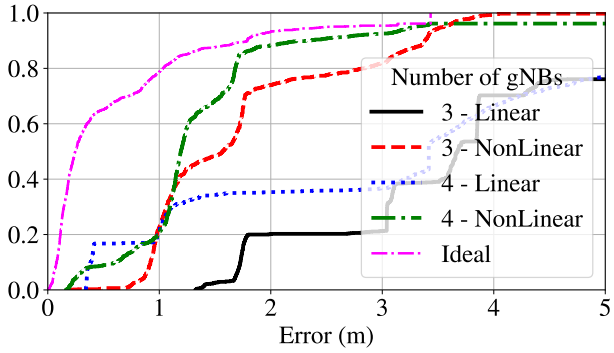


Figure 8: Empirical cumulative distribution function of the error using NonLinear (i.e., Brute Force and NLLS) and Linear (i.e., LS) localization algorithms, with no oversampling 100 MHz of BW, moving average window size 50 and with network configurations of three and four gNBs.

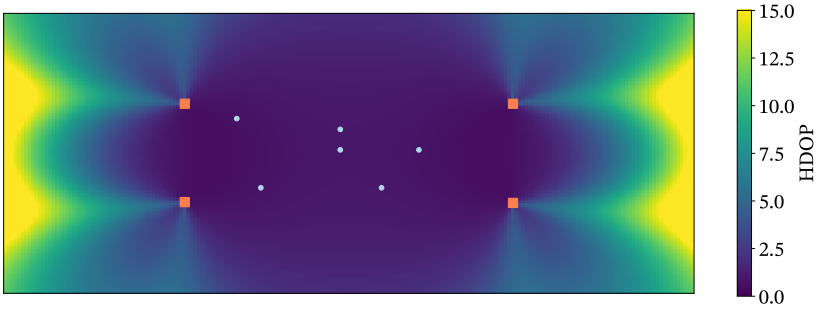


Figure 9: Theoretical HDOP in the experimental setup showing the spatial arrangement of UEs and gNBs.

Since the Brute-Force algorithm discretizes the 2D space into a uniformly distributed grid and evaluates the cost function at each point, a finer grid leads to better accuracy but requires more processing time. To speed up the algorithm, a technique used in this paper is to begin with a coarser grid and refine the blocks with the lowest value. The space is initially divided into a $15{\times}7$ m^2 grid with a step size of 0.5m, and at each iteration, the grid point with the 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}.

Figure 8 demonstrates the performance of these algorithms in terms of localization accuracy. The results indicate that both NLLS and Brute-Force algorithms outperform the Linear LS algorithm, providing more precise location estimates

with both. Furthermore, the performance of NLLS and Brute-Force algorithms is found to be comparable, with both achieving a high level of accuracy in positioning. Notably, with configurations of 4 and 3 gNBs, compared with the case of linear algorithms, the localization error is reduced to 1.3 meters (with a remarkable 65.8% improvement) and 1.7 meters (with a significant 55.3% improvement) in 80 percent of the cases, respectively.

The superior performance of NLLS and Brute-Force over Linear LS can be attributed to their ability to accommodate real-world signal propagation complexities better. These algorithms effectively average the errors of individual measurements, leading to more accurate position estimations.

Our experimentation highlights the effectiveness of NLLS and Brute-Force algorithms in achieving high-precision localization in a 5G network, with both methods showing considerable advantages over the simpler Linear LS approach. This analysis underscores the importance of algorithm selection in designing robust and accurate localization systems for wireless communications.

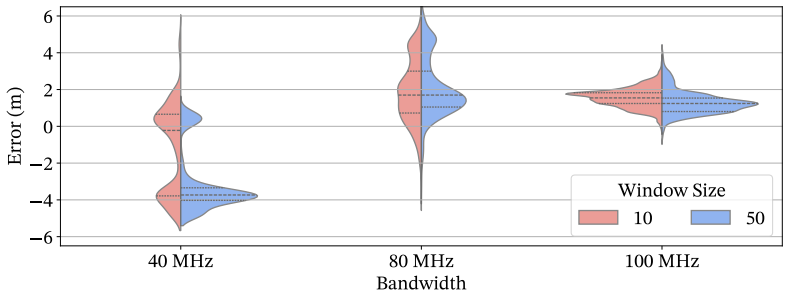


Figure 10: Distribution of error between measured and theoretical TDOAs for gNBs 2/3 at different bandwidths and window sizes.

To show the influence of bandwidth configuration on location estimation accuracy, in Figure 10, we show the evolution of the error between the measured TDOA and the theoretical TDOA for UE positions 0, 4 and 5 and gNBs 2-3 by varying the bandwidth. When we increase the bandwidth, the improvements are two-fold: on the one hand, the estimations are closer to the theoretical value; on the other, the estimations are packed more densely towards the mean of the distribution, confirming the theoretical principles discussed in Sec. 4.4.

5.6. LOS vs NLOS scenarios

This paragraph provides an overview of what would happen in situations where NLOS was present. There could be several scenarios if our system were affected

by NLOS. In the first scenario, one or more paths become blocked, and no PRS is received at the UE. If only one is blocked, the localization performance would revert to the 3 gNB scenario. If 2 or more PRS are blocked, localization would not be possible.

A second possible scenario is that the PRS reached the UE by another path, thus adding a delay to that particular TOA measurement. Since the OAI software is designed to select the highest correlation peak, the UE might latch onto a path different from the LOS one, thus reducing the performance of the localization algorithm. To simulate this with the 4 gNB scenario, we artificially introduce different delays in the TOA belonging to one of the gNBs and show the results in Figure 11.

The TOA delay was increased in our simulations by introducing artificial delays to the TOA that were measured in the LOS/direct signal path. Specifically, we modeled a situation where the signal takes an indirect path to reach the UE, similar to what would happen with a single wall bounce. For instance, a signal reflecting off a surface at a 30º angle would incur a different delay compared to one reflecting at a 40º angle. These artificial delays emulate the effect of the signal taking a longer, indirect route, mimicking real-world NLOS conditions. In the end, since we are dealing with samples, the NLOS effect can be collapsed into a sample delay, simplifying the analysis and reducing the complexity of simulations.

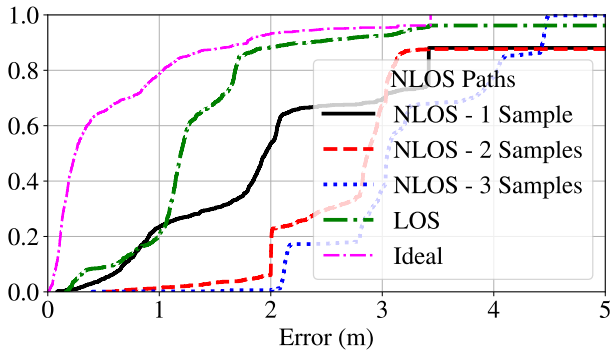


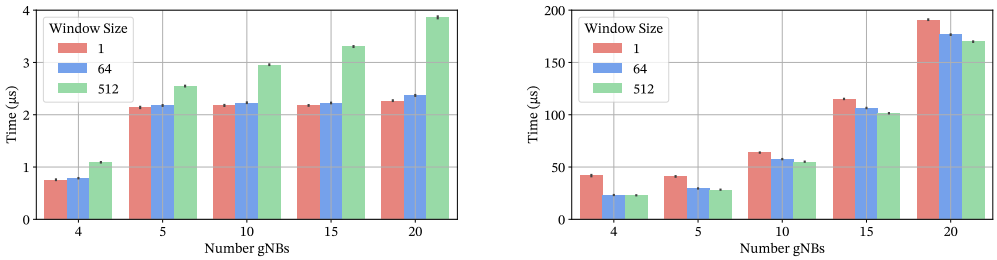
Figure 11: Empirical cumulative distribution function of the error when adding different delays to one of the TOA. Bandwidth is 100 MHz and no oversampling is performed.

As expected, the performance degradation is notable even with 1 sample delay. Currently, the OAI software does not provide reliable tools to detect whether the received PRS comes from an LOS or NLOS path, so performance would be severely degraded.

5.7. *Computational cost and Time to First Fix*

This subsection evaluates the computational aspects of positioning in 5G networks, particularly focusing on the TTFF as defined by 3GPP technical specifications [3, 9]. In the most restrictive positioning cases, the enhanced positioning use case, the TTFF must be provided with a 90% horizontal error of less than 1 meter in less than 1 second. Given enough bandwidth and oversampling levels, we have shown that it is feasible to reach the accuracy goal. In this last section, we evaluate the time it would take to obtain the TTFF.

To assess the time required to obtain the position estimates with different window sizes, we developed a C++ TDOA library. We then generate 10k experiments and vary the number of gNBs from 4 to 20. We test this approach on a Macbook Pro M1 Pro with 10 cores. The results, illustrated in Figure 12b, show the computation time for position estimates when varying the window size. Remarkably, the computation time remains relatively minimal, averaging around ~200 μs even with 20 gNBs, which is practically negligible for most scenarios. Notably, when employing Linear least squares, this computation time further reduces to approximately ~2 μs for up to 20 gNBs, as shown in Figure 12a. This suggests that averaging more TOA measurements for enhanced accuracy, as seen in Figure 5, incurs minimal time cost, except for the time it takes to accumulate enough data to fill the averaging window.



(a) Linear method

(b) Non-Linear method

Figure 12: Time taken to estimate position using (12a) Linear and (12b) Non-Linear methods when varying the window size and the number of gNBs.

From these results, we can deduce that even for large window sizes, the computational time is negligible and could be suitable for most localization use cases specified in [9]. In our setup, the PRS was sent every 5 ms, enabling window sizes up to 128 and still meeting the requirements for a TTFF of less than 1 second. In other deployments, the PRS transmission frequency might vary, and our study in-

dicates that the critical factor in determining TTFF is the PRS frequency, not the computational time for position estimation.

6. Conclusion

In this study, we thoroughly explored the key components and the evolving landscape of 5G positioning, leveraging the capabilities of open-source platforms supported by SDR technology. Our investigation delved into various aspects of 5G positioning, including the application and evaluation of different location algorithms, signal processing techniques such as oversampling and moving averages, practical impairments, and the implications of varying network configuration (i.e., number of base stations and bandwidth). Overcoming the inherent challenges associated with open-source solutions and SDR configurations, this research has demonstrated the versatility and robustness of such an approach in dissecting the multifaceted nature of 5G positioning in a real-world environment and meeting the positioning accuracy and stringent TTFF requirements outlined by industry standards. Experimenting with different configurations and methodologies yielded valuable insights, especially in understanding how the interplay between network geometry, algorithmic choices, and signal processing strategies influence and enhance localization accuracy within 5G networks. Our findings reveal that employing the NLLS or Brute-Force localization algorithm, combined with an averaging window size of 50 and an oversampling factor of 4, enables us to achieve a localization error as low as 0.7 meters in 80% of cases. Additionally, we have attained a TTFF of approximately 25 microseconds, further illustrating the efficacy of our approach. It is important to highlight that while the localization performances and operational efficiency achieved in our testbed are intriguing, the primary objective of this research was not to showcase the ultimate capabilities of the testbed in 5G localization. Instead, the study aimed to demonstrate the testbed's potential as a valuable tool for the research community and industry. This platform enables the experimentation and validation of algorithms and research findings through real over-the-air transmitted 5G positioning signals. In doing so, it accounts for standardized localization procedures and the complexities of real-world operating conditions. This research emphasizes the potential of leveraging open-source, SDR-based platforms as effective practical tools for innovation and exploration, thus paving the way for continued advancements in 5G positioning technology.

Acknowledgement

The research at University of Rome Tor Vergata and CNIT was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU, by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART") and by the European Research Council (ERC) under the European Union's Horizon Europe (Grant agreement No. 101078411). The work at IMDEA Networks was sponsored in part by the project PID2022-136769NB-I00 (6th-SENSE_ELSA) funded by MICIU/AEI/10.13039/501100011033/ and by the ERDF, A way of making Europe, and in part by the project MAP-6G, reference TSI-063000-2021-63, granted by the Ministry of Digital Transformation and Public Service and the European Union-NextGenerationEU through the UNICO-5G R&D program of the Spanish Recovery, Transformation and Resilience Plan (PRTR).

References

[1] 3GPP, Study on NR positioning support, Technical Specification (TS) 33.855, 3rd Generation Partnership Project (3GPP) (Jan. 2023).

[2] 3GPP, Study on NR positioning enhancements, Technical Report (TR) 38.857, 3rd Generation Partnership Project (3GPP) (Mar. 2021).

[3] 3GPP, Service requirements for the 5G system, Technical Specification (TS) 22.261, 3rd Generation Partnership Project (3GPP) (Sep. 2023).

[4] 3GPP, Service requirements for cyber-physical control applications in vertical domains, Technical Specification (TS) 22.104, 3rd Generation Partnership Project (3GPP) (Sep. 2023).

[5] 3GPP, Architectural enhancements to support ranging based services and sidelink positioning, Technical Specification (TS) 23.586, 3rd Generation Partnership Project (3GPP) (Sep. 2023).

[6] 3GPP, Study on expanded and improved NR positioning, Technical Report (TR) 38.859, 3rd Generation Partnership Project (3GPP) (Jan. 2023).

[7] 3GPP, Study on integrated sensing and communication, Technical Specification (TS) 22.837, 3rd Generation Partnership Project (3GPP) (Sep. 2023).

[8] 3GPP, NG radio access network (NG-RAN); stage 2 functional specification of user equipment (UE) positioning in NG-RAN, Technical Specification (TS) 38.305, 3rd Generation Partnership Project (3GPP) (Sep. 2023).

[9] 3GPP, Study on positioning use cases, Technical Specification (TS) 22.872, 3rd Generation Partnership Project (3GPP) (Sep. 2023).

[10] M. Cui, K. Zhao, Z. Zheng, M. Gu, Y. Wang, H. Pan, B. Wang, A Novel Iterative Positioning Method Based on Difference RSS Model With 5G Field Experiments, Vol. 24, 2024, pp. 5466–5475. doi:10.1109/JSEN.2023.3277510.

[11] Z. Li, F. Jiang, H. Wymeersch, F. Wen, An iterative 5G positioning and synchronization algorithm in NLOS environments with multi-bounce paths, Vol. 12, 2023, pp. 804–808. doi:10.1109/LWC.2023.3244575.

[12] P. A. D. N. Jayawardana, H. Obaid, T. Yesilyurt, B. Tan, E. S. Lohan, Machine-learning-based LOS detection for 5G signals with applications in airport environments, Vol. 23, 2023. doi:10.3390/s23031470.

[13] X. Jia, P. Liu, S. Liu, X. Li, W. Qi, Link-level simulator for 5G localization, in: 2022 IEEE Globecom Workshops (GC Wkshps), 2022, pp. 401–406. doi:10.1109/GCWkshps56602.2022.10008769.

[14] 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, A. Busin, F. Gunnarsson, Positioning in 5G networks, Vol. 59, 2021, pp. 38–44.

[15] G. Yammine, M. Alawieh, G. Ilin, M. Momani, M. Elkhouly, P. Karbownik, N. Franke, 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. doi:10.1109/IPIN51156.2021.9662535.

[16] A. Xhafa, J. A. del Peral-Rosado, J. A. López-Salcedo, G. Seco-Granados, Evaluation of 5G positioning performance based on UTDoA, AoA and base-station selective exclusion, Vol. 22, 2022. doi:10.3390/s22010101.

[17] S. Huang, H.-M. Chen, B. Wang, J. Chai, X. Wu, 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. doi:10.1109/ICFEICT57213.2022.00093.

[18] J. Shi, G. Zhang, Y. Lin, F. Li, C. Shen, Positioning of high-speed trains based on PRS, in: 2022 International Wireless Communications and Mobile Computing (IWCMC), 2022, pp. 578–583. doi:10.1109/IWCMC55113.2022.9824177.

[19] J. Zhang, H. Wang, Online learning based NLOS ranging error mitigation in 5G positioning, in: GLOBECOM 2022 - 2022 IEEE Global Communications Conference, 2022, pp. 6487–6492. doi:10.1109/GLOBECOM48099.2022.10000807.

[20] C. Jin, I. Bajaj, K. Zhao, W. P. Tay, K. V. Ling, 5G positioning using code-phase timing recovery, in: 2021 IEEE Wireless Communications and Networking Conference (WCNC), 2021. doi:10.1109/WCNC49053.2021.9417556.

[21] Z. Liu, L. Chen, X. Zhou, Z. Jiao, G. Guo, R. Chen, Machine learning for time-of-arrival estimation with 5G signals in indoor positioning, Vol. 10, 2023, pp. 9782–9795. doi:10.1109/JIOT.2023.3234123.

[22] I. Palamà, S. Bartoletti, G. Bianchi, 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. doi:10.23919/PEMWN56085.2022.9963853.

[23] L. Chen, X. Zhou, F. Chen, L.-L. Yang, R. Chen, Carrier phase ranging for indoor positioning with 5G NR signals, Vol. 9, 2022, pp. 10908–10919. doi:10.1109/JIOT.2021.3125373.

[24] OpenAirInterface Software Alliance (OSA), OpenAirInterface, 5G software alliance for democratising wireless innovation (2023).

[25] Software Radio Systems, srsRAN 4G: Open source SDR 4G software suite from Software Radio Systems (SRS), srsRAN (Dec. 2023).

[26] Open Networking Foundation (ONF), Introduction — Aether Docs 2.2.0-dev documentation, https://docs.aetherproject.org/master/index.html (2023).

[27] Ettus Research, National Instruments, USRP Software Defined Radio (SDR) online catalog, https://www.ettus.com/products/ (2024).

[28] I. Palamà, G. Santaromita, Y. Lizarribar, L. M. Monteforte, S. Bartoletti, D. Giustiniano, G. Bianchi, N. B. Melazzi, From experiments to insights: A journey in 5G new radio localization, in: 2023 21st Mediterranean Communication and Computer Networking Conference (MedComNet), 2023, pp. 74–82. doi:10.1109/MedComNet58619.2023.10168856.

[29] Ericsson, Support for Multiple QoS Class in deferred location requests, Change request (CR) 0491 of technical specification (TS) 29.122, 3rd Generation Partnership Project (3GPP) (2023).

[30] 3GPP, NR; Physical channels and modulation, Technical Specification (TS) 38.211, 3rd Generation Partnership Project (3GPP) (Sep. 2023).

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

[32] S. Ruffini, M. Johansson, B. Pohlman, M. Sandgren, 5g synchronization requirements and solutions, Vol. 2021, 2021, pp. 2–13. doi:10.23919/ETR.2021.9904655.

[33] Software Radio Systems, srsRAN: Open source O-RAN 5G CU/DU solution from Software Radio Systems (SRS), srsRAN (Dec. 2023).

[34] Open Networking Foundation (ONF), SD-RAN, https://opennetworking.org/open-ran/ (2023).

[35] Open Networking Foundation (ONF), SD-CORE, https://opennetworking.org/sd-core/ (2023).

[36] 3GPP, NR; physical layer measurements, Technical Specification (TS) 38.215, 3rd Generation Partnership Project (3GPP) (2017).

[37] M. Z. Win, Y. Shen, W. Dai, A theoretical foundation of network localization and navigation, Vol. 106, 2018, pp. 1136–1165. doi:10.1109/JPROC.2018.2844553.

[38] Ettus Research, National Instruments, UBX 10-6000 MHz Rx/Tx (160 MHz, X series only), https://www.ettus.com/all-products/ubx160/ (2023).

[39] TE Connectivity, ANT-5GWWS3-SMA, https://www.te.com/usa-en/product-ANT-5GWWS3-SMA.html (2023).

[40] Ettus Research, National Instruments, OctoClock-G CDA-2990, https://www.ettus.com/all-products/octoclock-g/ (2023).

[41] H. Sallouha, A. Chiumento, S. Pollin, Aerial Vehicles Tracking Using Non-coherent Crowdsourced Wireless Networks, Vol. 70, 2021, pp. 10780–10791. arXiv:2108.00922, doi:10.1109/TVT.2021.3103315.

[42] H. P. Gavin, The Levenberg-Marquardt algorithm for nonlinear least squares curve-fitting problems, Vol. 19, 2019.

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

[44] S. Ruder, An overview of gradient descent optimization algorithms, 2016. arXiv:1609.04747.