Annals of Telecommunications (2024) 79:301–313
https://doi.org/10.1007/s12243-023-00987-2

Experimental assessment of SDR-based 5G positioning: methodologies and insights

Ivan Palamà[1] · Stefania Bartoletti[1] · Giuseppe Bianchi[1] · Nicola Blefari Melazzi[1]

Received: 7 March 2023 / Accepted: 16 August 2023 / Published online: 15 September 2023

Abstract
While GPS has traditionally been the primary positioning technology, 3GPP has more recently begun to include positioning services as native, built-in features of future-generation cellular networks. With Release 16 of the 3GPP, finalized in 2021, a significant standardization effort has taken place for positioning in 5G networks, especially in terms of physical layer signals, measurements, schemes, and architecture to meet the requirements of a wide range of regulatory, commercial and industrial use cases. However, experimentally driven research aiming to assess the real-world performance of 5G positioning is still lagging behind, root causes being (i) the slow integration of positioning technologies in open-source 5G frameworks, (ii) the complexity in setting up and properly configuring a 5G positioning testbed, and (iii) the cost of a multi-BS deployment. This paper sheds some light on all such aspects. After a brief overview of state of the art in 5G positioning and its support in open-source platforms based on software-defined radios (SDRs), we provide advice on how to set up positioning testbeds, and we demonstrate, via a set of real-world measurements, how to assess aspects such as reference signal configurations, localization algorithms, and network deployments. Our contribution further includes an assessment of the efficacy of utilizing measurements obtained from a single-link limited-size testbed to forecast localization performance in more elaborate (and hence more expensive) multi-node network settings. We posit that our methodological insights can assist in lowering the entry cost barriers associated with conducting 5G positioning experiments and, consequently, promote additional experimental research in this domain.

Keywords 5G · Network · Positioning · Software-defined-radio

1 Introduction

Starting with Release 16, the 3GPP is enhancing 5G networks and devices with localization functionalities targeting a very high level of location accuracy thanks to the larger bandwidths and flexible numerology enabled at the 5G physical layer, thus enabling a plethora of new applications [1, 2].

Indeed, the procedures and signals related to 5G positioning have already been defined within the 3GPP, together with the architectural aspects, including the dedicated network functions [3]. 5G technical reports and specifications propose implementations that leave many degrees of freedom regarding the algorithms for extracting the position-related features for each gNodeB-User Equipment (gNB-UE) link (e.g., time-of-arrival, angle estimation) as well as for estimating the UE position by leveraging the features from several links. In [4], the performance of 5G positioning is obtained through simulation by comparing several positioning methods. Results take synchronization errors into account and are obtained using standardized channel models and reference operating environments [5, 6].

The development of advanced techniques for time-of-arrival (ToA) and position estimation is a fervent research area, where the scope is to mitigate the effects of challenging propagation environments, such as non-line-of-sight conditions, poor signal quality, multipath propagations, and interference which results in a degradation of the localization performance [7–11]. Nevertheless, the performance assess-

✉ Ivan Palamà
ivan.palama@uniroma2.it

Stefania Bartoletti
stefania.bartoletti@uniroma2.it

Giuseppe Bianchi
giuseppe.bianchi@uniroma2.it

Nicola Blefari Melazzi
blefari@uniroma2.it

[1] University of Rome "Tor Vergata" and CNIT, Rome, Italy

ment of 5G positioning, to date, has been almost exclusively limited to simulations with channel models specified in the standard by using simulators that are not open-source or preliminary experimental set-up with 5G-like signals [4, 7, 9–13].

Many open-source platforms (such as OpenAirInterface [14], srsRAN [15], Aether [16]) have gained popularity in the academic and industrial environment to implement and simulate the 3GPP stack. Such software suites can provide researchers with access to a range of tools and libraries that can be used to implement and test 5G localization algorithms. This can help to accelerate the research process, as researchers can leverage the work of others and can also promote collaboration and sharing within the research community. Such software platforms are able to run on general-purpose computing platforms and interface with a wide variety of SDRs. SDR platforms allow researchers to flexibly implement and test different localization algorithms without being tied to a specific hardware platform. This can save time and resources, as researchers can quickly and easily switch between different algorithms and configurations. Therefore, they represent an invaluable tool for research and development, enabling researchers to rapidly prototype new algorithms and paradigms and test them in real-world over-the-air conditions. Despite the long-term goal of enabling widespread use of these tools, to date, their use still requires significant effort in terms of hardware and software set-up and configuration.

More specifically, in the context of 5G positioning, some of these open-source platforms have already implemented dedicated 5G positioning reference signals according to the latest 3GPP standards; however, their use is not straightforward. Also, emulating an entire positioning system requires the creation of a network with multiple perfectly synchronized gNBs, which is expensive and not readily available. As a result, several research groups are forced to implement their systems with one or two radios and long development times.

This paper represents an extension of our previous work [17], where we conducted initial exploration and experimentation on 5G positioning using SDR. In the preliminary work, our primary focus was to showcase the technical procedures and available resources for conducting 5G positioning experiments utilizing open-source platforms. In this extended contribution, we go beyond the initial exploration and provide more comprehensive measurements and experiments, particularly in multi-link scenarios. Moreover, we place a strong emphasis on quantitatively assessing the effectiveness of utilizing single-link measurements obtained from a limited-size testbed to predict localization performance in multi-link scenarios. By addressing this crucial aspect, we aim to enhance further our understanding of the intricacies and challenges associated with 5G positioning and its applicability in real-world scenarios.

We would like to emphasize that our goal is not to provide an evaluation of 5G localization performance, as the first real commercial implementations should be available soon, but to provide simple, low-cost, and effective methodologies that enable researchers and industry to test and validate algorithms and research results using measurements of 5G positioning signals transmitted over the air, taking into account standardized localization procedures and real operating conditions.

The key contributions of this paper are as follows:

- Provide an overview of the current state of play of open-source platforms for 5G positioning.
- Showcase a 5G-positioning testbed with positioning reference signal (PRS) in single-gNB and multi-gNB synchronized scenario using an open-source SDR-based platform.
- Present a statistical characterization of time-based measurements over single-link and multi-link scenarios.
- Propose and validate a methodological approach to overcome the limitations of the single-link scenario and use the measurements of that scenario to simulate a 5G positioning system with multiple gNBs effectively.
- Compare the results obtained in the single-link and multi-link scenarios to assess the effectiveness of the single-link approach quantitatively.

The remainder of the paper is organized as follows. After some necessary background in Sect. 2, we describe the proposed PRS-based localization approach in Sect. 3 and the 5G SDR-based single-link and multi-link 5G localization experimental testbeds in Sects. 3 and 4, respectively. Finally, Sect. 6 draws conclusions and outlines further directions for research.

2 5G positioning

This section provides a brief introduction to the main aspects of 5G positioning, thus laying the foundation for a better understanding of the work presented in subsequent sections. 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.

2.1 5G main architecture components

As described in [18], 5G networks have 2 different possible deployment strategies, non-standalone (NSA) mode and standalone (SA) mode. We focus on 5G SA mode, which supports 5G positioning via standardized dedicated 5G new radio (NR) signals and network functions.

CN: 5G Core network (5GCN) leverages the decomposition of the functions executed by the network nodes of the previous generations leading to a 5G architecture completely defined in terms of network functions (NFs) that are exposed as services. 5GCN is a service-based core with web-oriented service-based interfaces. In the remainder of the paper, we will focus on 5G positioning architecture, leveraging the Access and Mobility Management Function (AMF), Location Management Function (LMF), and reference signals, i.e., the PRS and sounding reference signal (SRS).

RAN: 5G SA radio access network (RAN) uses NR technology. 5G base station, called gNodeB, is responsible for all next-generation RAN (NG-RAN) functionalities, both the user's control and data planes.

2.2 NR physical layer

At the physical layer, UE transmissions are scheduled within continuous sequences called *NR frames*, each lasting 10 ms. The 5G NR improves frequency range support by supporting new frequency ranges (FR), including sub-6 GHz range FR1 and mmWave range FR2 with frequencies above 24 GHz. In addition, 5G NR improves the structure of the physical layer, compared to long-term evolution (LTE) by doubling the maximum FFT size to 4096 and by introducing *flexible numerology*, denoted by $\mu \in \{0, \ldots, 6\}$, which doubles the slot orthogonal frequency-division multiplexing (OFDM) symbols and incorporates a modulation scheme that supports configurable subcarrier spacing (SCS), denoted as $\Delta_f = 2^{\mu} \cdot 15$ kHz. The numerology $\mu = 0$ corresponds to the same SCS 15 kHz as LTE.

The typical NR frame structure, illustrated in Fig. 1-a, consists of $N_{\text{slots}} = 10 \cdot 2^{\mu}$ equally sized *slots* of duration T_{slot} and each slot, in turn, contains fourteen OFDM symbols[1]. As of Release 18, adjusting the numerology μ, the SCS can be customized from the set {15, 30, 60, 120, 240, 480, 960} kHz, which influences the physical parameters' time duration. In the time domain, numerology has an inverse relationship with the slot time duration $T_{\text{slot}} = 2^{-\mu}$ ms, and the number of slots per subframe $N_{\text{slots}} = 2^{\mu}$. Due to the fact that shorter slot durations enable more symbols to be processed within a given time, the choice of μ determines the SCS Δ_f and, consequently, the achievable sampling frequency and channel bandwidth B_{ch}. Indeed, the sampling frequency is obtained as the product of the SCS and FFT size, leading to a minimum sampling frequency of 61.44 MHz ($15\,kHz \cdot 4096$) and a maximum sampling frequency of 3932.16 MHz ($960\,kHz \cdot 4096$). Regarding spectral occupation, the nominal channel bandwidth B_{ch} can be calculated using Eq. 1, which yields a minimum B_{ch} of approximately 5 MHz ($25 \cdot 12 \cdot 15\,kHz + 2 \cdot 242.5\,kHz$) and a maximum B_{ch} of approximately 2000 MHz ($264 \cdot 12 \cdot 960\,kHz + 2 \cdot 9860\,kHz$).

$$B_{\text{ch}} = N_{RB} \cdot N_{sub} \cdot \Delta_f + 2 \cdot B_{\text{guard}} \tag{1}$$

where N_{sub} is fixed to 12, N_{RB} and B_{guard} are, respectively, the maximum transmission bandwidth and the guardband as defined in Tables 5.3.2-1 and 5.3.3-1 in [20, 21], respectively.

The 5G system's adaptability extends to customizing the frame structure, allowing it to be tailored based on specific application requirements, such as maximizing bandwidth (up to 100 MHz in FR1 and up to 2000 MHz in FR2) or minimizing latency, by reaching a minimum NR slot duration of 15.625 μs, a marked difference from the fixed 1 ms of LTE. Within the domain of 5G localization, sampling frequency plays a central role. The 5G network, thanks to its ability to achieve higher sampling frequencies, enables better resolution of temporal measurements, thus leading to greater precision and accuracy in the localization process. Indeed, a higher sampling frequency translates to a finer granularity in capturing temporal variations within the wireless channel. This finer resolution allows for a more precise delineation of signal propagation characteristics, including multipath effects and signal reflections, which are crucial factors influencing temporal measurement estimation.

Figure 1b illustrates the same elements in the typical *fabric*-like structure used to represent NR signals. It depicts a resource element (RE) as the smallest defined unit, consisting of one OFDM subcarrier during one OFDM symbol

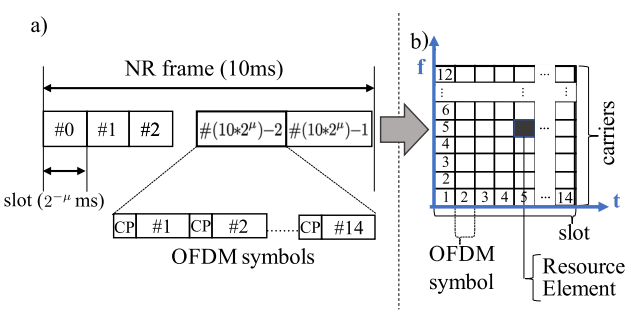

Fig. 1 OFDM modulation in the downlink channel

[1] We report here details of the *normal cyclic prefix* modulation scheme: refer to the 3GPP documentation [19] for the alternative *extended cyclic prefix* format.

interval. A group of 12 REs over the frequency dimension and 14 REs over the time dimension forms a resource block (RB), which represents the smallest unit of resources that can be allocated to a user.

2.3 Architecture and methods for 5G positioning

5G positioning is supported by architectural choices that enable the transceiving of localization signals between gNBs and UEs and the exchange of location measurements to the LMF. This positioning architecture is illustrated in Fig. 2.

The key elements of 5G positioning will be listed below.

5G positioning signals In order to achieve more precise positioning measurements than LTE, new NR reference signals were introduced. These signals are the SRS in the uplink and an enhanced version of the LTE PRS for positioning in the downlink. Although other downlink signals can be used, the 5G NR PRS, defined in [19], is specifically designed to provide the highest possible levels of accuracy, coverage, and interference suppression. The PRS is periodically transmitted by the 5G gNB with the primary purpose of conveying timing and synchronization information to UE for the purpose of positioning estimation. Its function is not to directly provide coordinates or GPS values but rather to encompass distinctive patterns and parameters that facilitate precise estimation of the UE's position. By processing the NR PRS from multiple gNBs, it becomes feasible to compute multiple UE-gNB distances and subsequently employ techniques such as trilateration or other positioning methodologies to determine the location of the user accurately. PRS transmissions in 5G networks are coordinated across multiple gNBs to improve coverage and interference resilience. Selective muting of specific PRS subcarriers during designated timeframes is employed to minimize interference from neighboring cells. Additionally, the signal spanning the full NR bandwidth over multiple symbols enhances its power. These strategies ensure a robust and reliable simultaneous PRS exchange, optimizing positioning accuracy and efficiency.

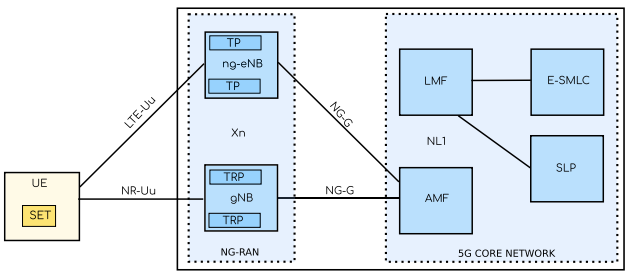

Fig. 2 3GPP 5G positioning architecture [3]

5G positioning schemes 3GPP Rel. 16 5G network introduced some positioning schemes for 5G: downlink time-difference-of-arrival (DL-TDOA), uplink TDOA (UL-TDOA), downlink angle-of-departure (DL-AoD), uplink angle-of-arrival (UL-AoA), multi-round trip time (Multi-RTT) positioning, and NR enhanced cell ID (E-CID). In addition to the radio access technology (RAT) dependent solutions, another group of RAT-independent solutions can be used for positioning, such as global navigation satellite system (GNSS), WLAN, and sensor-based. We will limit our discussion to schemes that are RAT-dependent. In the DL-TDOA scheme, the UE measures the reference signal timing difference (RSTD) or TDOA of the downlink positioning reference signal PRS sent by two base stations and reports to the LMF. The LMF obtains the UE position estimation according to the time difference of multiple downlink reference signals. UL-TDOA is conceptually similar to DL-TDOA; in this case, it is the base station that measures the relative ToAs of uplink SRS sent by the user equipment and reports them to the LMF.

In the DL-AoD scheme, the UE measures and reports the receiving power of the downlink reference signal beam from multiple base stations, estimates the position angle of the terminal based on the direction of the sending beams, and then reports them to LMF. The LMF solves the equations to obtain the UE position according to multiple base station estimates. The principle of the UL-AoA scheme is similar to DL-AoD; the difference lies in the fact that it exploits uplink signals. Multiple base stations measure the arrival angle of terminal uplink signals and report to the LMF. According to the arrival angle measured by multiple base stations, the LMF obtains the UE position.

Multi-RTT positioning is a 5G positioning scheme that uses both uplink and downlink signals. The UE and at least three gNBs send each other reference signals (i.e., SRS and PRS) to measure the RX-TX time difference to obtain the RTT. The RX-TX information is summarized to the LMF that derives the distances between the UE and the gNBs, then estimates the position of the UE as the intersection point of the three circumferences having the derived distances as radii. The NR E-CID positioning approach involves the estimation of the UE position using information about its serving ng-eNB, gNB, and cell. It also utilizes additional UE measurements, NG-RAN radio resources, and other measurements to enhance the accuracy of the UE location estimate.

The 5G network provides support for five distinct positioning modes, namely, hybrid positioning, standalone positioning, UE-based positioning, UE-assisted/LMF-based, and NG-RAN node-assisted/LMF-based. Hybrid positioning

makes use of multiple positioning schemes, while standalone positioning allows the UE to independently use one or more of the positioning methods without any assistance from the network. UE-based positioning allows the UE to compute its position estimate without involving the LMF, and this mode is supported by DL positioning schemes. On the other hand, UE-assisted/LMF-based positioning requires the UE to provide measurements to the LMF for the computation of its position estimate, and so it is supported by DL positioning schemes. Lastly, NG-RAN node-assisted/LMF-based positioning involves the provision of measurements by the NG-RAN node to the LMF for the computation of UE position estimate, and this mode is supported by UL positioning schemes.

5G positioning-enabling NF The 5G positioning architecture contains 2 network functions: the AMF and LMF. When a location request is received, the AMF selects the LMF that is best suited to perform the location determination for that request and uses its location service to trigger that process. The LMF manages the resources and timing of positioning activities and exposes the location service to the AMF for location information requests.

2.4 5G open-source platforms

We now describe the leading existing open-source software platforms/tools for implementing a 5G SA mobile network infrastructure including RAN and core network. The main features will be analyzed focusing on the positioning aspects.

OpenAirInterface OpenAirInterface (OAI) is an open-source project that provides an SDR-compliant platform for mobile wireless networks. OpenAirInterface includes a full stack of software components, from the physical layer up to the application layer, as well as a set of tools and APIs for development and testing. It provides implementations of 5G Core, gNB, and UE compliant with NR Release 15 (with an additional subset of NR Release 16 features). The OAI source code is written in C to ensure real-time performance and is distributed under the OAI Public License. Both gNB and UE implementations are compatible with Intel and ARM architectures running Linux distributions and support general-purpose SDR platforms such as EXMIMO, BladeRF, USRP, and LimeSDR. Several kernel and BIOS modifications are recommended for real-time performance, including installing a low-latency kernel and disabling power management and CPU frequency scaling features. In the last period, OpenAirInterface implemented both DL PRS and UL SRS, making it the ideal candidate platform for testing 5G positioning.

srsRAN srsRAN provides RAN solution (gNB and UE) compliant with 3GPP and O-RAN [22] alliance specifications with features up to NR Release 15. Unlike OAI, it does not provide an implementation of 5GCN but uses Open5GS, an open-source 3GPP compliant 5G Core implementation written in C language. srsRAN is written in C and C++ and is distributed under the GNU AGPLv3 license. srsRAN is compatible with the most popular Linux distributions (i.e., Ubuntu and Fedora) and, like OAI, is compatible with the most popular SDR platforms. It is a relatively more stable project than OAI but offers fewer functionalities, among which support for 5G positioning signals is missing.

Aether Aether is a project promoted by the Open Networking Foundation (ONF) for the simplified implementation of private cellular networks. Unlike OAI and srsRAN, Aether not only offers an implementation of the RAN and 5G Core, integrating SD-RAN [23] and SD-CORE [24] respectively, but also provides a control and orchestration interface for the RAN, a cloud edge platform with support for cloud computing, and a central cloud. The source code is released under the Apache 2.0 open-source license. SD-RAN's main focus is to provide an O-RAN-compliant micro-ONOS-based near-real-time RAN Intelligent Controller (RIC) and a platform for xAPPS. SD-RAN relies on OAI gNB and UE implementations. Since we were not interested in Aether's additional features, we decided in our experimental setup to use OAI directly.

UERANSIM UERANSIM [25] is another well-known open-source project enabling very simple and functional UE and gNB. Unlike the previously mentioned platforms, it is not SDR compatible and simulates the 5G NR interface between UE and gNB over the UDP protocol.

3 System model for PRS-based positioning

We consider a network of neighboring N_g gNBs, one of which serves the UE in a monitored environment. The ith gNBs is at $\mathbf{p}_{\text{gNB}}^{(i)} = [\mathbf{x}_{\text{gNB}}^{(i)} \quad \mathbf{y}_{\text{gNB}}^{(i)}]$, while the true unknown position of a generic user is at $\mathbf{p}_{\text{UE}}$. A location-dependent measurement is performed for each gNBs.

3.1 ToA estimation for DL-TDOA

The DL-TDOA technique uses the PRS transmitted by the set of neighboring gNBs and received by the UE. Specifically, the RSTD or TDOA is measured for each pair of gNBs. Then, multilateration or trilateration is carried out based on

the theory of hyperbolas. Without loss of generality, we consider the gNB with index $i = 1$ as a reference cell for the RSTD measurements.

Each measurement from the ith gNB can be expressed as follows:

$$t_i(\mathbf{p}) = \frac{\|\mathbf{p}_{\text{gNB}}^{(i)} - \mathbf{p}_{\text{UE}}\|}{c} + n^{(i)}(\mathbf{p}) \tag{2}$$

where c is the speed of light, and $n^{(i)}(\mathbf{p})$ accounts for measurement noise and uncertainties. Essentially, $t_i(\mathbf{p})$ corresponds to the relative ToA for the signal transmitted by the gNB and received by the UE. Then, the RSTD is the relative timing difference between the neighboring gNB and the reference gNB (TS 38.215 Section 5.1.29) and is calculated as $t_i(\mathbf{p}) - t_1(\mathbf{p})$. The measurement noise $n^{(i)}(\mathbf{p})$ is generally dependent on the position, on the LOS conditions between the transmitter and receiver, and the SNR of the received signal. Note that to avoid a synchronization error in RSTD measurements, all of the gNBs transmit the PRS simultaneously (which means synchronized transmission from all gNBs).

As measurements are collected per resource, more measurements can be collected at the same gNB to improve positioning accuracy by repeating the transmission of PRS resources, e.g., N_{rep} times [4]. The DL PRS resources can be repeated up to $N_{\text{rep}} \leq 32$ times within a resource set period, either in consecutive slots or with a configurable gap between repetitions.

3.2 Positioning algorithm

Then, from the vector of RSTD measurements from each pair of gNBs, we obtain an estimate of the UE position as $\hat{\mathbf{p}}_{\text{UE}}$. In particular, in the absence of any error and in ideal conditions, the ith RSTD value corresponds to a hyperbola equation where the UE is assumed to be located, with foci located at $\mathbf{p}_{\text{gNB}}^{(i)}$ and $\mathbf{p}_{\text{gNB}}^{(1)}$. Then, a set of hyperbola equations are deduced from a set of RSTD values, which are solved to estimate the UE position. This process is called multilateration. At least two equations are needed for 2D UE positioning.

Then, the $\hat{\mathbf{p}}_{\text{UE}}$ is obtained as the point that intersects the hyperbolas defined as the set of points whose distances from the reference gNB and the ith gNB is equal to $(t_i(\mathbf{p}) - t_1(\mathbf{p}))\, c$. Then, the positioning error is defined as the Euclidean distance between the true and estimated UE position, i.e., $e(\mathbf{p}_{\text{UE}}, \hat{\mathbf{p}}_{\text{UE}}) = \|\mathbf{p}_{\text{UE}} - \hat{\mathbf{p}}_{\text{UE}}\|$. There exists a plethora of sub-optimal algorithms for solving the system of non-linear equations. More advanced algorithms can merge the measures with prior knowledge about the environment or with the availability of other measures [9]. Using a least-square approach, the estimated position can be found as

$$\hat{\mathbf{p}}_{\text{UE}} = \arg\min_{\mathbf{p}} \sum_{i=1}^{N_{\text{gNB}}} \Big[\big(\|\mathbf{p} - \mathbf{p}_{\text{gNB}}^{(i)}\| - \|\mathbf{p} - \mathbf{p}_{\text{gNB}}^{(1)}\| \big) - (t_i(\mathbf{p}) - t_1(\mathbf{p}))c \Big]^2 \tag{3}$$

where the first gNB is used as reference gNB. As another example, a closed and linear form of the least square algorithm, which aims at solving a linearized version of the equations system, can also be used in the form $\mathbf{Ax} = \mathbf{b}$ where the ith row of the matrix $\mathbf{A}$ is

$$\mathbf{a}_i = \begin{bmatrix} x_{\text{gNB}}^{(1)} - x_{\text{gNB}}^{(i)} & y_{\text{gNB}}^{(1)} - y_{\text{gNB}}^{(i)} & d_{1,i} \end{bmatrix} \tag{4}$$

and $\mathbf{x} = [\mathbf{p}_{\text{UE}}^{\text{T}} \quad \mathbf{d}_1^{\text{T}}]^{\text{T}}$, with $\mathbf{d}_1 = \begin{bmatrix} d_{1,2}\, d_{1,3}, \ldots, d_{1,N_{\text{gNB}}} \end{bmatrix}$ and $d_{1,i} = \|\mathbf{p}_{\text{gNB}}^{(1)} - \mathbf{p}_{\text{gNB}}^{(i)}\|$ is the Euclidean distance between the 1st and ith gNB; the ith element of the column vector $\mathbf{b}$ is

$$b_i = \frac{1}{2}\big[(x_{\text{gNB}}^{(1)})^2 - (x_{\text{gNB}}^{(i)})^2 + (y_{\text{gNB}}^{(1)})^2 - (y_{\text{gNB}}^{(i)})^2 + d_{1,i}^2 \big]. \tag{5}$$

4 Single-link approach

In this section, we first describe how we implemented our single-link 5G SDR-based experimental localization system, then the experimental dataset collection and the data calibration processing, and finally the main results for ranging and positioning, following the processing scheme depicted in Fig. 3. To overcome the excessive cost and size of traditional telecommunications equipment, we adopted an SDR approach utilizing commercially accessible devices.

4.1 Experimental setup

The experimental testbed consists of two customized workstations and two radio transceivers that emulate the operator's network (5GCN and gNB) and the user terminal.

Radio transceiver As radio front-end, we used two USRP X310 devices [26] with UBX160 [27] daughterboard. The Ettus Research X310 is a high-performance, modular SDR platform. It is designed to support a wide range of applications, including wireless communications, radar, and satellite communications. As they can be tuned over a wide radio frequency range, from 10 MHz to 6 GHz, they cover all the NR FR1 frequency bands with up to 160 MHz of instantaneous bandwidth. By using the high-speed 10 GbE interface, we can achieve 184.32 MHz as the sampling frequency, thus allowing time measurements with a resolution of approximately

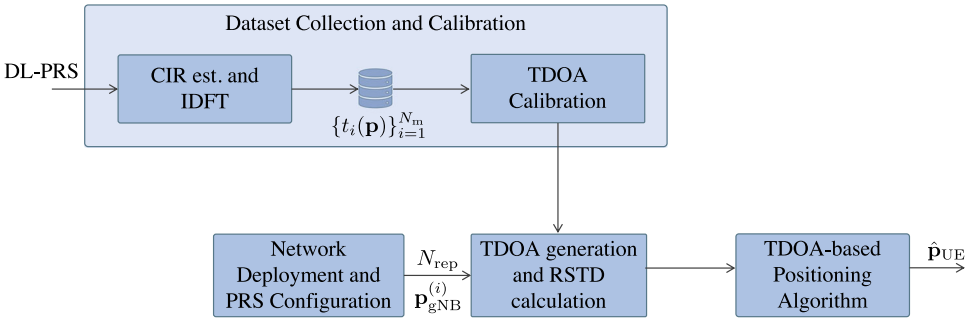

Fig. 3 Illustration of the main step for dataset collection, calibration, and simulation of multiple links

5.43 ns. Given the speed of light, this equates to a ranging accuracy, of about 1.63 ms. We used NR-specific Linx ANT-5GWWS3 SMA multiband antennas.

Workstation For the localization experiments, we used workstations powered by Intel Core i9 CPUs with 18 cores clocked at 3 GHz. As OS, we used Ubuntu 18.04 LTS with kernel version 5.4.0-109-lowlatency.

Network software platform In our single-link testbed we used OAI open-source project to implement the 5G network and the UE. OAI implements both DL PRS and UL SRS. We decided to focus on the DL PRS to validate and propose the tool, but it is possible to apply the same tool using the UL SRS as the positional signal. In the experimental phase, we used the latest commit from the OAI dedicated branch for early-stage PRS integration. As of now, the dedicated PRS development branch has been merged with the main OAI development branch.

RF compatibility We note here that we carried out all the experiments avoiding disturbing other UEs by either running tests inside the lab during weekends or stopping the experiments when other people were getting close to the lab. Considering the SDR radios' output power, we verified that the 5G NR signal does not create interference outside the lab's testing area.

NR channel In our experimental localization testbed, we configured a 5G NR time division duplex (TDD) channel in the N78 (3500 MHz) frequency band with an instantaneous bandwidth of 80 MHz (217 RBs) and SCS of 30 kHz.

4.2 Experimental and simulation results

4.2.1 Dataset collection

We have collected a series of datasets containing the time of arrival measurements from the gNB to the user equipment as the distance varies. In particular, several datasets were obtained for $d_{\text{true}} = 1, 2, \ldots, 7$ m in LOS conditions. We repeated the measurement for each distance as the number of repetitions N_{rep}, which represents the number of PRS resources repetitions within a resource set period. Specifically, we performed the measurement for each distance with $N_{\text{rep}} = 1, 2, \ldots, 8$ repetitions. Fixed d_{true} and N_{rep}, approximately 1500 measures of arrival time were performed. More specifically, when the UE receives the PRS from the gNB, it buffers the channel impulse response, applies the IDFT, and estimates the ToA $t_i(d_{\text{true}}, N_{\text{rep}})$ from the maximum peak of the channel impulse response in time.

4.2.2 Calibration and time estimation

As discussed in Sect. 2, the RSTD is calculated as the difference between the arrival times obtained by two gNBs. If the experimentation is carried out through two gNBs, it will be necessary to synchronize these to transmit the signal simultaneously. In the presence of a single gNB and to evaluate the localization process in the absence of synchronization errors, we calibrated the measurements to compensate for any synchronization error at the transmission between gNBs. Considering this error as static, a calibration phase was carried out for each dataset. Note that this is a common approach in the presence of static timing error; see, e.g., [28]. The calibration considered the first 100 measurements of the dataset.

$$\tilde{t}_i(d_{\text{true}}, N_{\text{rep}}) = t_i(d_{\text{true}}, N_{\text{rep}}) - \frac{1}{N_{\text{cal}}} \sum_{i=1}^{N_{\text{cal}}} (t_i(d_{\text{true}}, N_{\text{rep}}) - d_{\text{true}}/c)\,. \tag{6}$$

Note that such calibration eliminates any static source of error and that the measurements are all taken in LOS conditions.

Figure 4 presents the estimated RSTD as a function of the true RSTD, varying the reference node and dataset. As demonstrated, the estimated RSTD closely aligns with the ideal bisector, which represents the theoretical scenario where the estimated TDOA exactly matches the true TDOA. This showcases the promising level of precision in the TDOA

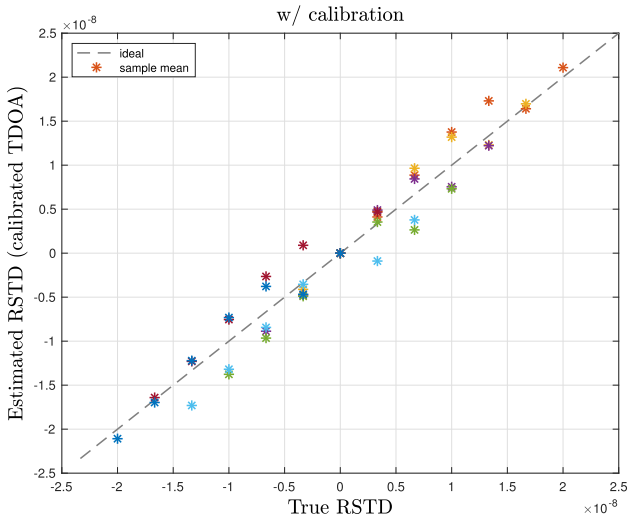

Fig. 4 True vs. estimated range difference with calibrated data. The stars represent the sample mean for different datasets and are compared with the ideal bisector line

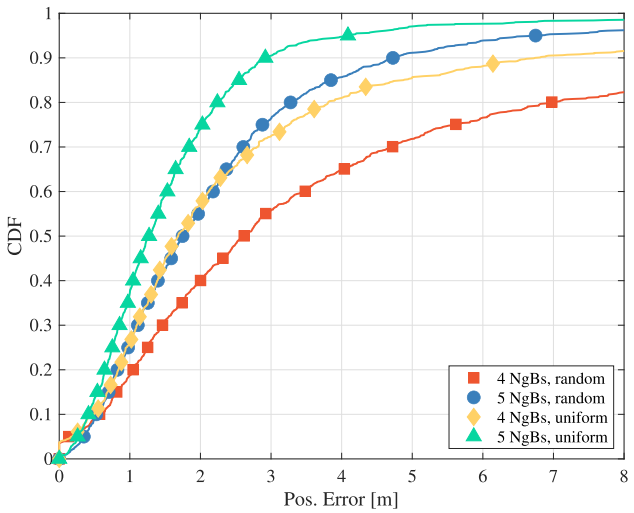

Fig. 5 CDF of the positioning error varying the number of NgNBs and using a uniform or random angular distance between them

estimates, reflecting the overall good performance and calibration effectiveness of the system. It suggests that the implemented algorithms and calibration techniques provide accurate TDOA measurements, despite potential variations in reference node and dataset.

4.2.3 Simulation of the positioning system

To evaluate localization performance, we simulated a system with N_g gNBs around a central UE. Each gNB's position was given by $[d_{1,i}\cos(\alpha_i), d_{1,i}\sin(\alpha_i)]$, with $d_{1,i}$ being the distance from the UE, and α_i, the angular distance from the semi-axis of the positive abscissa and i-th gNB, specifying the gNB's position in a polar coordinate system centered at the UE. We examined two α_i configurations: one random between 0 and 360° and one with equal angular spacing between gNBs. For each implementation of the position estimation, we have chosen a random measure from the dataset $\tilde{t}_k(d_{1,i}, N_{\text{rep}})$ with k random, as N_{rep} varies.

Figure 5 presents the empirical cumulative distribution function (CDF) of the localization error, calculated using a linearized least squares algorithm, while varying the number of gNBs and their angular distribution, either equal (uniform) or random. From the results, we can see that the uniform distribution of gNBs generally leads to superior positioning performance compared to random distribution. For instance, in 80% of cases, the uniform distribution results in a positioning error of approximately 2 ms. In contrast, the random distribution results in a positioning error of over 3 ms in 80% of cases. This underscores the impact of both the number and deployment strategy of gNBs on the system's positioning accuracy. The data suggests that a uniform distribution strategy may yield better performance in minimizing localization error.

5 Multi-link approach

In this section, we describe how we implemented our 5G multi-link SDR-based experimental localization system, then processing for data calibration, and finally the main results for ranging and positioning. The goal of such a multi-link testbed is to create ranging and TDOA measurements through which we can experimentally verify the validity of the proposed single-link based approach.

5.1 Experimental setup

The experimental multi-link testbed is an evolution of the single-link testbed. As illustrated in Fig. 6, it is constituted by two custom workstations, a powerful portable workstation, four USRP X310 with UBX160 daughter cards used as radio transceivers emulating the operator's network with three gNBs, and the user terminal. With the aim of validating the proposed approach, the network software platform and 5G NR channel are the same as the single-link testbed. Thus, the major differences are the use of a gNBs synchronizer and the experimental area.

Base station synchronizer Our localization system employs the Ettus Octoclock [29] to ensure stringent synchronization among the gNBs. This high-precision clock generator and distribution unit is crucial in maintaining synchronization in wireless communication systems. Each USRP board connected to the Octoclock shares a common clock, enabling synchronized signal transmission. The Octoclock

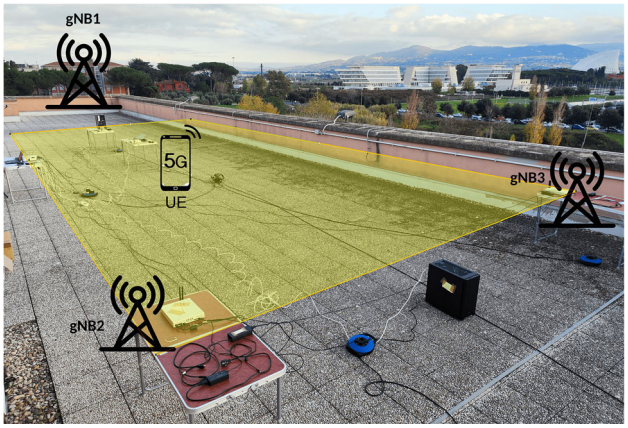

Fig. 6 Multi-link scenario, experimental area in yellow with gNBs and UE

excels in timing synchronization, with a pulse-per-second (PPS) accuracy—a common timing signal used in precision applications—confining synchronization to a stringent 50-ns window. Moreover, its frequency stability, rated at 1 part per billion (ppb)—a unit that describes precision within one billionth of a second—guarantees consistent accuracy. It has eight independent clock outputs, each with a phase-locked loop (PLL) and voltage-controlled crystal oscillator (VCXO) for high-frequency stability and accuracy. These features ensure precise time alignment across the gNBs, making simultaneous transmission possible. Additionally, the Octoclock incorporates a GPS receiver for enhanced synchronization and timing.

UE simultaneous PRS processing OAI-based UE implements a PRS-based ToA estimation 3GPP standard compliant. The procedure starts generating and modulating pilots, then calculating the RE offset of the PRS. Subsequent steps involve SNR estimation and PRS channel estimates conversion into FFT format. UE then computes the channel impulse response (CIR) in the time domain using IDFT oversampling up to 16×. Finally, ToA is estimated by locating the peak of the CIR as the maximum absolute value. For simultaneous reception of multiple synchronized PRS, each gNB utilizes a distinct PRS Resource Offset and NPRS ID. The PRS resource offset is crucial as it enables the differentiation of PRS transmissions from various gNBs by adding a slot offset of each PRS resource, while the NPRS ID plays a vital role in the initialization of a pseudo-random binary sequence that generates the PRS symbols, as defined in the 3GPP standard [19]. This results in accurate and efficient ToA estimation for multiple signals, allowing the UE to receive and process each signal individually yet concurrently.

Experimental area The outdoor experimental area is rectangular 13 m × 7 m and covers a surface of almost 90 m^2. The 13 network deployments are shown in Fig. 7.

5.2 Experimental and simulation results

In the following subsections, we present the results derived from our extensive experimental and simulation activities. Table 1 summarizes the parameters of the experimental activities.

5.2.1 Dataset collection

We collected a series of data sets containing measurements of the arrival time from the gNBs to the user equipment as the user's position $\mathbf{p}_{\mathrm{UE}}$ changes under LOS conditions. Figure 7 presents the various network configurations with different UE positions. We repeated the measurement for different user positions, and the number of repetitions is $N_{\mathrm{rep}} = 16$. For each $\mathbf{p}_{\mathrm{UE}}$, approximately 1500 arrival time measurements were made for each gNB in the same manner as the user in the single-link approach.

5.2.2 Calibration and time estimation

In this section, we present the results of our experiment conducted on a multi-link SDR-based positioning testbed. The accuracy of the TDOA estimation and positioning results were evaluated and compared with those obtained from the single-link approach. Furthermore, to apply the single-link measurements calibration approach in a comparable way to the multi-link measurements, two calibration methods were implemented:

- *Calibration with 1 position:* A subset of 100 measurements between all the gNBs and a single UE position is used for calibration.
- *Calibration with all positions:* A subset of 100 measurements between all the gNBs and all the considered UE positions is used for calibration.

Figure 8 presents the estimated TDOA (empirical mean) as a function of the true TDOA in the multi-link testbed, comparing the results with both calibration approaches. It is evident that the performance of TDOA estimation is highly dependent on the calibration approach used. In particular, the TDOA error is dependent on the UE position, i.e., when possible, using measurements from all the positions for the calibration phase leads to better performance.

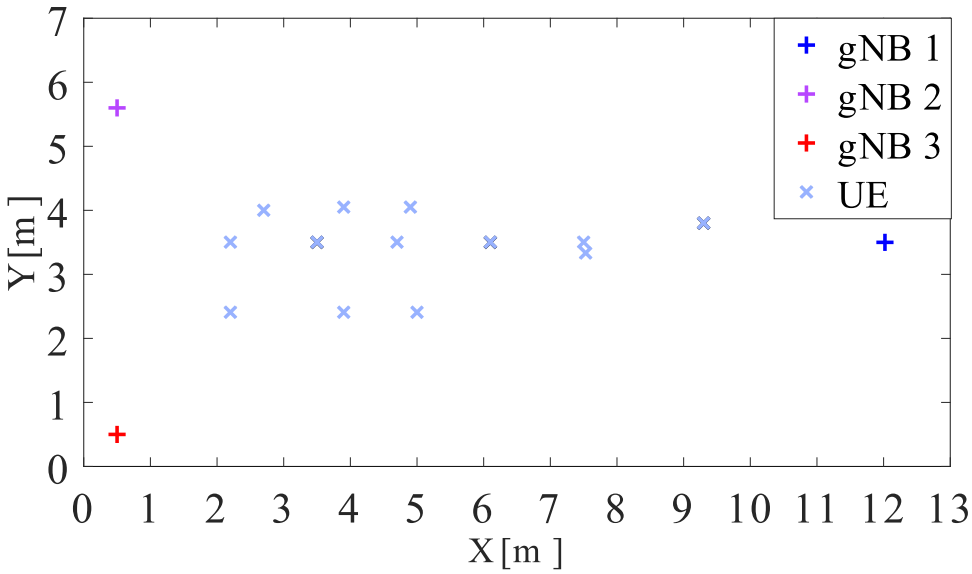

Fig. 7 Multi-link approach experimental area with gNBs and UE positions

Figure 9 presents the empirical CDF of the TDOA error, comparing the results obtained with the two types of calibration with the non-calibrated case. Results show that the calibration changes the mean value of the TDOA error in both cases, i.e., leads to a zero-mean error. In addition, the use of measurements from all the positions also reduces the empirical variance.

With respect to position estimation, we conducted a thorough analysis of the multi-link testbed's performance. Then, we compared the results obtained with multi-link measurements with those obtained using the single-link measurements for simulating a multi-link scenario. This analysis aims to understand if using a smaller testbed with a single-link can be sufficient for having insights into positioning performance in a multi-link scenario. Figure 10 depicts the CDF of the positioning error using non-linear LS algorithm for both approaches and considering the two types of calibrations. Our findings indicate that the two approaches (single-link and multi-link) are comparable in terms of positioning performance. When all the positions are used in the calibration phase, the single-link approach slightly underestimates the performance, while with the calibration based on a single position, the two results are even more comparable.

Finally, Fig. 11 compares the multi-link and single-link approaches when two different algorithms are used, i.e., the non-linear and linear least square. For the linear least-square case, the difference between the results obtained with the multi-link and single-link approaches is negligible.

6 Conclusion

In this paper, we analyzed the main aspects and the state of play to experiment with 5G positioning via SDR-based open-source platforms. We exemplified the use of SDR and OpenAirInterface for 5G positioning evaluation in two scenarios: (i) using only two radios configured as gNB and

Table 1 Summary of experiment parameters

Parameter	Value
Radio transceiver	USRP X310 w/ UBX160 DBoard
5G NR antenna	Linx ANT-5GWWS3
NR band	N78 (3500 MHz)
Bandwidth	80 MHz (217 RBs)
Experimental area	$13\,m \times 7\,m$ (approximately $90\,m^2$)
Number of UE positions/network deployments	13
LOS condition	Yes
Number of PRS repetitions, N_{rep}	4
Number of ToA measurements per gNB	Approximately 1500
Percentage of ToA measurements used for calibration	6.7% (100 ToA measurements)

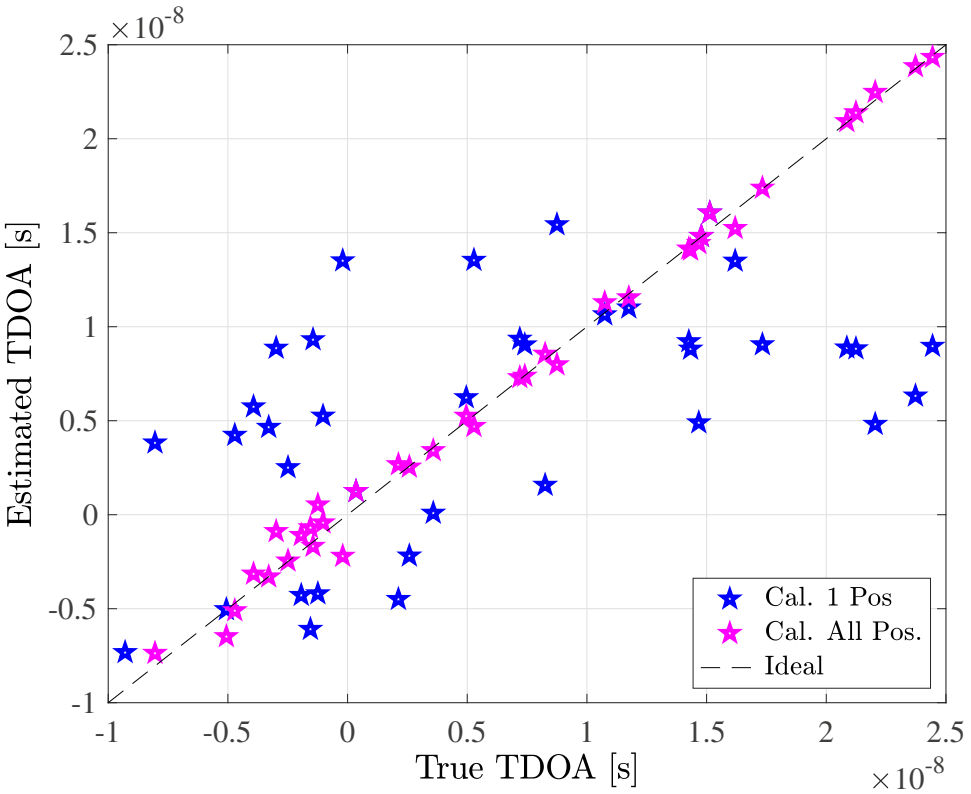

Fig. 8 True vs. estimated TDOA for both calibration methods

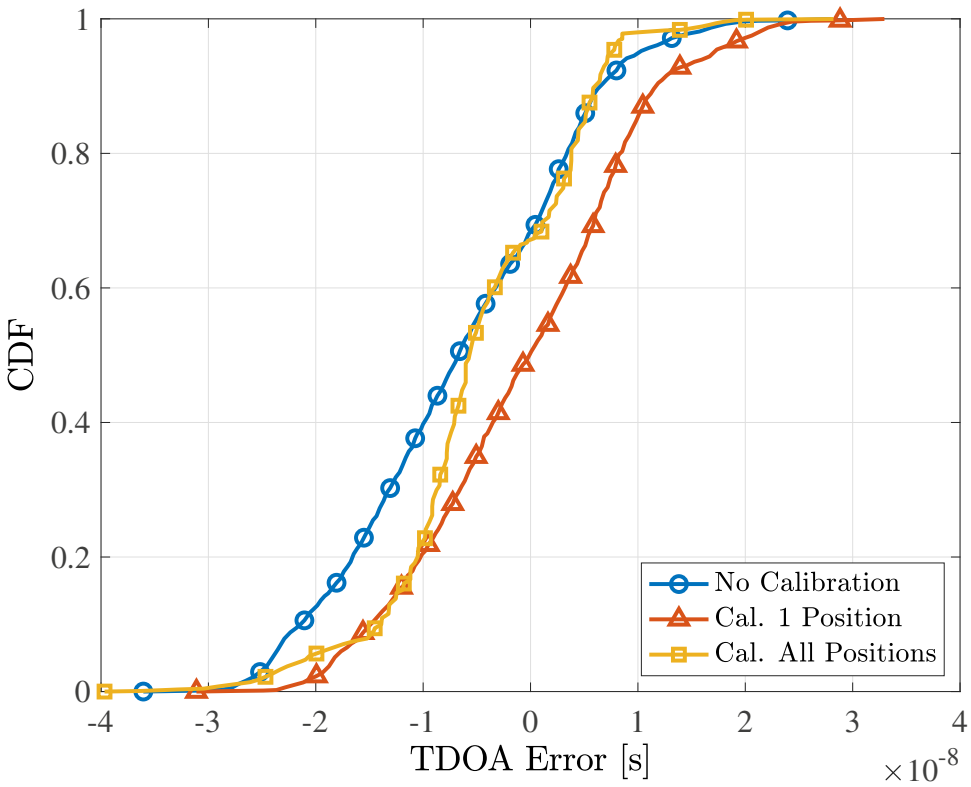

Fig. 9 CDF of the TDOA estimation error, without and with various calibration methods

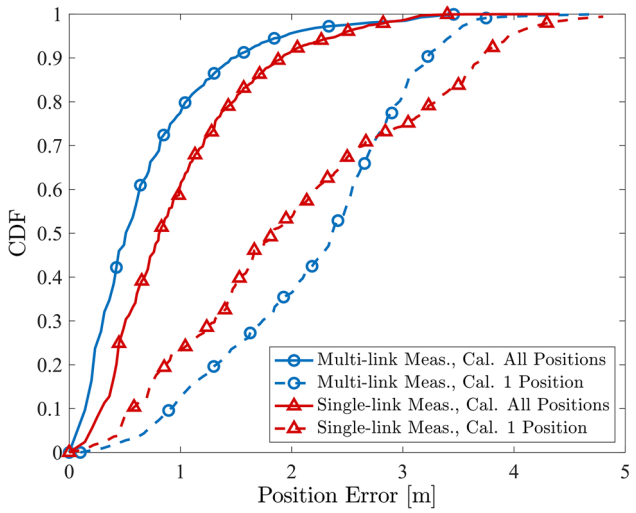

Fig. 10 CDF of position estimation error using non-linear LS algorithm, for both single-link and multi-link approaches, with both calibration methods

user equipment and (ii) using three radios configured as gNB and a single radio as user equipment. In particular, we proposed a simple methodological approach to use a single-link testbed to simulate a multi-node location system and evaluate the effect of network deployment on positioning performance. We then experimentally validate the proposed single-link approach by comparing the simulated results with those obtained with a real multi-link testbed. Results quantitatively evaluate the effectiveness of the proposed approach and show that even with a size-limited and cost-constrained SDR setup, it is possible to investigate the main aspects of 5G positioning, such as the signal structure, TDOA estimation, and positioning algorithm.

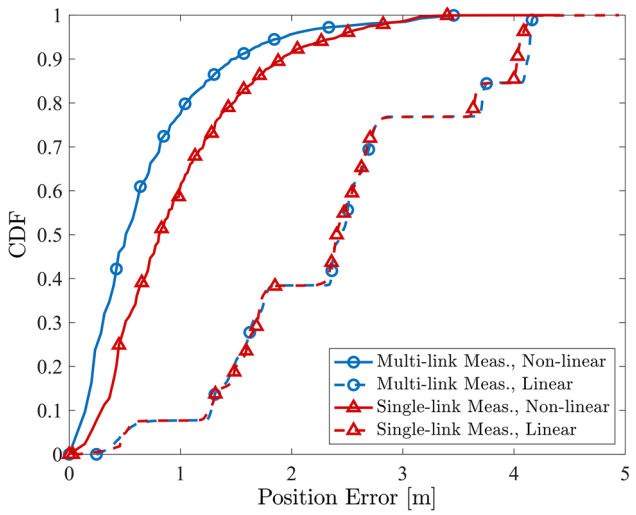

Fig. 11 CDF of position estimation error, using linear and non-linear LS algorithms, assuming one position calibration approach for both single-link and multi-link approach

Funding Open access funding provided by Universitá degli Studi di Roma Tor Vergata within the CRUI-CARE Agreement.

Availability of data and materials Not applicable

Declarations

Conflict of interest The authors declare no competing interests.

References

1. 3GPP (2021) 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. 3GPP (2021) 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. 3GPP (2021) 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
4. Dwivedi S, Shreevastav R, Munier F, Nygren J, Siomina I, Lyazidi Y, Shrestha D, Lindmark G, Ernström P, Stare E, Razavi SM, Muruganathan S, Masini G, Busin A, Gunnarsson F (2021) Positioning in 5G networks. IEEE Commun Mag 59(11):38–44
5. Xhafa A, del Peral-Rosado JA, López-Salcedo JA, Seco-Granados G (2022) Evaluation of 5G positioning performance based on UTDoA, AoA and base-station selective exclusion. Sensors 22(1). [Online]. Available: https://www.mdpi.com/1424-8220/22/1/101
6. Huang S, Chen H-M, Wang B, Chai J, Wu X, Li F (2022) Positioning performance evaluation for 5G positioning reference signal. In: 2022 2nd International Conference on Frontiers of Electronics, Information and Computation Technologies (ICFEICT), pp 497–504
7. Jayawardana PADN, Obaid H, Yesilyurt T, Tan B, Lohan ES (2023) Machine-learning-based LOS detection for 5G signals with applications in airport environments. Sensors 23(3). [Online]. Available: https://www.mdpi.com/1424-8220/23/3/1470

8. Shi J, Zhang G, Lin Y, Li F, Shen C (2022) Positioning of high-speed trains based on PRS. In: 2022 International Wireless Communications and Mobile Computing (IWCMC), pp 578–583
9. Conti A, Morselli F, Liu Z, Bartoletti S, Mazuelas S, Lindsey WC, Win MZ (2021) Location awareness in beyond 5G networks. IEEE Commun Mag 59(11):22–27
10. Kim H, Granström K, Gao L, Battistelli G, Kim S, Wymeersch H (2020) 5G mmWave cooperative positioning and mapping using multi-model PHD filter and map fusion. IEEE Trans Wirel Commun 19(6):3782–3795
11. Palacios J, Bielsa G, Casari P, Widmer J (2018) Communication-driven localization and mapping for millimeter wave networks.In: IEEE INFOCOM 2018 – IEEE conference on computer communications, pp 2402–2410
12. Jia X, Liu P, Liu S, Li X, Qi W (2022) Link-level simulator for 5G localization. In: 2022 IEEE Globecom Workshops (GC Wkshps), pp 401–406
13. Yammine G, Alawieh M, Ilin G, Momani M, Elkhouly M, Karbownik P, Franke N, Eberlein E (2021) Experimental investigation of 5G positioning performance using a mmWave measurement setup. In: 2021 International Conference on Indoor Positioning and Indoor Navigation (IPIN), pp 1–8
14. O (OSA) (2023) OpenAirInterface 5G software alliance for democratising wireless innovation. https://www.openairinterface.org/. Accessed 23 May 2023
15. Software Radio Systems (2023) srsRAN, your own mobile network. https://www.srslte.com. Accessed 14 May 2023
16. O (ONF) (2023) Aether. https://opennetworking.org/aether/. Accessed 14 May 2023
17. Palamá I, Bartoletti S, Bianchi G, Melazzi NB (2022) 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), pp 1–6
18. 3GPP (2022) 3GPP System Architecture Evolution (SAE); Security architecture. 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 28.401. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296
19. 3GPP (2022) 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
20. 3GPP (2022) NR; User Equipment (UE) radio transmission and reception; Part 1: Range 1 Standalone. 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.101-1. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3283
21. 3GPP (2022) NR; User Equipment (UE) radio transmission and reception; Part 2: Range 2 Standalone. 3rd Generation Partnership Project (3GPP). Technical Specification (TS) 38.101-2. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3284
22. O-R Alliance O-ran alliance (2023). url=https://www.o-ran.org/. Accessed 25 Feb 2023
23. Open Networking Foundation (ONF) (2023) SD-RAN. https://opennetworking.org/open-ran/. Accessed 15 May 2023
24. Open Networking Foundation (ONF) (2023) SD-CORE. https://opennetworking.org/sd-core/. Accessed 15 May 2023
25. ALİ GÜNGÖR (2023) UERANSIM. https://github.com/aligungr/UERANSIM. Accessed 15 May 2023
26. Ettus Research, National Instruments (2023) USRP X310. https://www.ettus.com/all-products/x310-kit/. Accessed 08 May 2023
27. Ettus Research, National Instruments (2023) UBX 10-6000 MHz Rx/Tx (160 MHz, X Series only).https://www.ettus.com/all-products/ubx160/. Accessed 08 May 2023
28. Dvorecki N, Bar-Shalom O, Banin L, Amizur Y (2019) A machine learning approach for Wi-Fi RTT ranging. In Proc. of Int. Techn. Meeting of The Institute of Navigation, (ION), Reston,Virginia, pp 435–444
29. Ettus Research, National Instruments (2023) OctoClock-G CDA-2990. https://www.ettus.com/all-products/octoclock-g/. Accessed 22 May 2023