This document is a preprint of: Z. Li, A. Nimr, P. Schroter et al., "Flexible SDR-based Experimental Platform for Realistic Ranging Evaluation in 5G and Beyond," in Proceedings of IEEE Vehicular Technology Conference (VTC Fall 2023), Hong Kong, China, Oct 2023. DOI:10.1109/VTC2023-Fall60731.2023.10333626

Flexible SDR-based Experimental Platform for Realistic Ranging Evaluation in 5G and Beyond

Zhongju Li*, Ahmad Nimr*, Philipp Schröter*, Maximilian Stark†, Gerhard Fettweis*
* Technische Unviversität Dresden, Germany
† Bosch Research Germany

***Abstract*—5G sidelink technology recently presented its unique potential for precise positioning using time delay estimates, although environmental conditions and the reference signal used highly influence the performance. Given the complexity of simulating all potential environmental impacts in a particular scenario, carrying out measurements within the specific environment becomes necessary. This paper introduces a flexible experimental platform to support research in designing the protocol, waveform, and time delay estimation algorithms, offering configurable transmitting signals and radio frequency (RF) parameters. Furthermore, this platform can emulate potential timing errors due to hardware constrains, offering a more practical understanding of 5G sidelink ranging applications.**

***Index Terms*—5G sidelink, experimental platform, two-way ranging**

I. Introduction

The demand for accurate positioning in mobile networks arises from the growing number of services and applications that rely on location information, such as emergency response, industrial automation, asset tracking, autonomous vehicles, and emerging technologies like visual reality (VR) and augmented reality (AR). The level of precision varies depending on the use case, ranging from several meters for information provisioning to several centimeters for safety and tele-operation. While previous generations of cellular networks could provide location information with moderate accuracy, the fifth generation (5G) and beyond aim to deliver significantly improved positioning capabilities, in terms of high accuracy, high integrity, and reduced latency [1].

5G new radio (NR) has supported positioning since Rel-15, relying on previous long term evolution (LTE) positioning and other technologies such as Bluetooth, wireless local area network (WLAN), and global navigation satellite system (GNSS). In Rel-16, NR-based positioning methods were introduced using angle and time measurements, including multi-round-trip-time (RTT), downlink and uplink time-of-arrival (ToA), angle-of-arrival (AoA) and angle-of-departure (AoD) [2], with further enhancements for time-critical use cases introduced in Rel-17 [3]. In Rel-18, standardization of sidelink ranging and positioning is considered to enable user equipments (UEs) to perform ranging without gNB base station. This enables a variety of applications for consumers and industries, such as smart home, smart transportation, and smart retail [4].

The potential of 5G NR sidelink positioning have been studied in several works using simulation tools, such as ray tracing. The work in [5] focuses on evaluating sidelink positioning in an industrial environment using time and angle measurements in the 26 GHz NR band. In [6], an analytical study is conducted on sidelink positioning for vehicular use cases in urban environments, focusing on ToA estimation and RTT-ranging to relax the synchronization. RTT-based ranging is technically equivalent to the two-way ranging (TWR) used in ultra wideband (UWB) standard IEEE Std 802.15.4, which may use one or multiple RTTs [7]. A comprehensive error model for TWR was proposed in [8], addressing various sources of potential errors, including clock drifts among others, and demonstrating the performance variations across different TWR methodologies using measurements form standard UWB equipment. Other experimental studied on TWR have been reported in the literature with certain focus. For instance, [9] presents an software-defined radio (SDR) implementation for TWR using 25 MHz bandwidth in the ISM 2.4 Ghz/5 GHz band, whereas the work in [10] evaluate the performance of TWR using 1 GHz bandwidth at 60 GHz band.

This paper introduces an SDR-based flexible experimental platform for evaluating the realistic performance of various TWR ranging methodologies, including 5G sidelink and other standards. The platform is designed to facilitate research and development in different areas, such as protocol, waveform design, and time delay estimation algorithm. It offers configuration options for a range of transmitting signals and radio frequency (RF) parameters. Additionally, the design enables the emulation and configuration of different errors, such as time synchronization. When accompanied with the processing of measurement data, this allows better understanding of the impact of such errors on the performance of practical systems.

The rest of the paper is organized as follows: Section II presents an overview of several TWR methods and the involved timing parameters. Section III is dedicated to the description of the experimental platform and implementation aspects. In Section IV, an example use case of the platform is presented with illustrative results. The paper is concluded in Section V.

II. Overview of two-way ranging

The range d between two devices in a radio communications system can be estimated by measuring the time τ_{ToF} a signal needs to travel from the transmitting device to the receiving device, which is denoted as the time-of-flight (ToF), such that $d = c\tau_{\text{ToF}}$, where c is the speed of light. However, a direct measuring of ToF at the receiver requires strict synchronization

This document is a preprint of: Z. Li, A. Nimr, P. Schroter et al., "Flexible SDR-based Experimental Platform for Realistic Ranging Evaluation in 5G and Beyond," in Proceedings of IEEE Vehicular Technology Conference (VTC Fall 2023), Hong Kong, China, Oct 2023. DOI:10.1109/VTC2023-Fall60731.2023.10333626

and a common clock to precisely determine the time the signal is transmitted. To overcome these requirements, ToF can be indirectly estimated by means of TWR process, where both devices exchange their local time measurements in one or multiple RTT transmission.

A. TWR Procedures

In the TWR process, as illustrated in Fig. 1, UE1 starts transmitting at time $t_{\text{tx}}^{\text{UE1}} = t_{\text{trigger,tx}}^{\text{UE1}}$ of its local clock, where $t_{\text{trigger,tx}}^{\text{UE1}}$ is the trigger time for transmission. To avoid continuous listening, UE2 starts listening to the received signal at time $t_{\text{trigger,rx}}^{\text{UE2}}$, which is selected with sufficient interval to guarantee receiving the entire transmitted signal from UE1. This only requires coarse synchronization between UE1 and UE2. Once the whole frame is received, UE2 processes the received signal to estimate the delay of the first path $\hat{\tau}_0^{\text{UE2}}$, and then determines the time of receiving in its local clock as $t_{\text{rx}}^{\text{UE2}} = \hat{\tau}_0^{\text{UE2}} + t_{\text{trigger,rx}}^{\text{UE2}}$. Thereafter, UE2 prepares a packet containing the time required for replaying $\tau_{\text{reply}}^{\text{UE2}}$ and starts transmitting at time $t_{\text{tx}}^{\text{UE2}} = \tau_{\text{reply}}^{\text{UE2}} + t_{\text{rx}}^{\text{UE2}} = t_{\text{trigger,tx}}^{\text{UE2}}$. Similarly, UE1 starts listening to the received signal at time $t_{\text{trigger,rx}}^{\text{UE1}}$, estimates the first path $\hat{\tau}_0^{\text{UE1}}$, and calculates the receiving time $t_{\text{rx}}^{\text{UE1}} = \hat{\tau}_0^{\text{UE1}} + t_{\text{trigger,rx}}^{\text{UE1}}$. Accordingly, UE1 can obtain the RTT locally as $\tau_{\text{round}}^{\text{UE1}} = t_{\text{rx}}^{\text{UE1}} - t_{\text{tx}}^{\text{UE1}}$. This time interval is the sum of the reply time at UE2 and twice the ToF. By a successful decoding of the received frame, UE1 gets also $\tau_{\text{reply}}^{\text{UE2}}$. This enables UE1 to estimate the range to UE2 locally using

$$\tau_{\text{round}}^{\text{UE1}} = 2\tau_{\text{ToF}} + \tau_{\text{reply}}^{\text{UE2}}. \tag{1}$$

This is referred as single-sided TWR (SS-TWR), which requires one RTT transmission. The process can be repeated, such that UE1 transmits a new frame containing the measured RTT $\tau_{\text{round}}^{\text{UE1}}$, and the reply time $\tau_{\text{reply}}^{\text{UE1}}$. UE2 can locally measure the RTT of the second round RTT $\tau_{\text{round}}^{\text{UE2}}$, and use the communicated measures from UE1, such that

$$\tau_{\text{round}}^{\text{UE2}} = 2\tau_{\text{ToF}} + \tau_{\text{reply}}^{\text{UE1}}. \tag{2}$$

Using (1) and (2), UE2 can provide enhanced estimation of ToF, which is denoted as double-sided TWR (DS-TWR), and communicates the measure back to UE1. In ideal case, ToF can be computed in SS-TWR as

$$\tau_{\text{ToF}}^{\text{SS-TWR}} = \frac{\tau_{\text{round}}^{\text{UE1}} - \tau_{\text{reply}}^{\text{UE2}}}{2}, \tag{3}$$

and for the case of DS-TWR, as

$$\tau_{\text{ToF}}^{\text{DS-TWR}} = \frac{(\tau_{\text{round}}^{\text{UE1}} - \tau_{\text{reply}}^{\text{UE2}}) + (\tau_{\text{round}}^{\text{UE2}} - \tau_{\text{reply}}^{\text{UE1}})}{4}. \tag{4}$$

In realistic systems, different sources of timing errors arise and need to be considered in deriving advanced estimators.

B. Error Model

Following (1) and (2), the error in estimating ToF is related to the RTT intervals $\{\hat{\tau}_{\text{round}}^{\text{UE}i}\}$ and reply times $\{\hat{\tau}_{\text{reply}}^{\text{UE}i}\}$. As depicted in Fig. 1, for the first RTT,

$$\begin{aligned} \hat{\tau}_{\text{reply}}^{\text{UE2}} &= t_{\text{tx}}^{\text{UE2}} - t_{\text{rx}}^{\text{UE2}} = t_{\text{trigger,tx}}^{\text{UE2}} - t_{\text{trigger,rx}}^{\text{UE2}} - \hat{\tau}_0^{\text{UE2}}, \\ \hat{\tau}_{\text{round}}^{\text{UE1}} &= t_{\text{rx}}^{\text{UE1}} - t_{\text{tx}}^{\text{UE1}} = \hat{\tau}_0^{\text{UE1}} + t_{\text{trigger,rx}}^{\text{UE1}} - t_{\text{trigger,tx}}^{\text{UE1}}. \end{aligned} \tag{5}$$

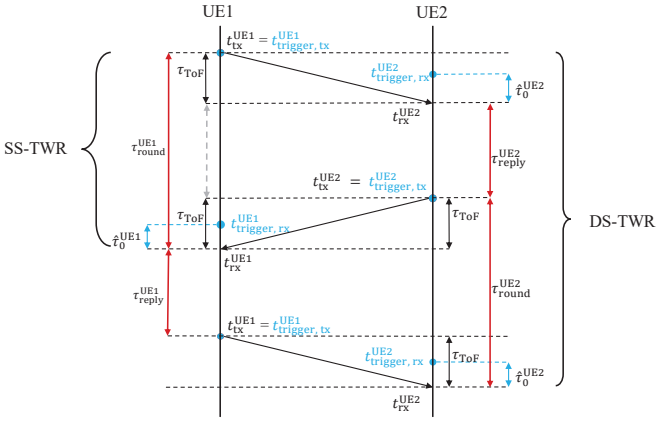


Fig. 1: TWR process timeline.

Accordingly, one source of error is the drift in the triggering clock, and another source is related to the estimation of the first path delay $\hat{\tau}_0^{\text{UE}i}$. Further errors can be introduced because of the propagation delay in the hardware. This errors can be generally modeled as follows:

$$\begin{aligned} \hat{\tau}_{\text{round}}^{\text{UE}i} &= \tau_{\text{round}}^{\text{UE}i} + \xi_{\text{round},i}(\tau_{\text{round}}^{\text{UE}i}), \\ \hat{\tau}_{\text{reply}}^{\text{UE}i} &= \tau_{\text{reply}}^{\text{UE}i} + \xi_{\text{replay},i}(\tau_{\text{reply}}^{\text{UE}i}). \end{aligned} \tag{6}$$

The dependency of errors on the actual value is encountered, for example, in the case of clock drift $\xi_{\text{round}i}(\tau_{\text{round}}^{\text{UE}i}) = \text{clk}_i \tau_{\text{round}}^{\text{UE}i}$ [8], where clk_i defines the relative errors to $\tau_{\text{round}}^{\text{UE}i}$ at UEi. In the proposed experimental platform, timing errors can be emulated by means of configuring the trigger time to artificially induce additional errors, such as emulating hardware delay and higher clock drift as described in Section III-A2.

III. USRP-based Experimental Platform

This section outlines the proposed experimental platform, covering its components, processes, and methods. It offers insight into the system design and function and shares lessons learned from the pre-measurement calibration phase, which is essential for guaranteeing accurate results.

A. USRP-based Experimental Platform

The primary objective of this work is to provide a flexible experimental platform for TWR measurements, designed to operate without being strictly constrained by a specific standard. The platform main component, the universal software radio peripheral (USRP), allows RF parameter configuration like center frequency, sampling frequency, and transmitting power, enhancing its adaptability for diverse wireless communications standards. The proposed platform also supports customized transmitting sequence configurations, increasing its applicability as different standards employ varied methodologies for TWR. The synchronization procedure varies across standards, complicating system design. Instead of conventional received signal-based synchronization, with its inherent challenges and variability among different standards, we use a triggering mechanism for signal transmission and acquisition. This offers a uniform, less standard-sensitive method, increasing our platform flexibility. In summary, Fig. 2 presents the

This document is a preprint of: Z. Li, A. Nimr, P. Schroter et al., "Flexible SDR-based Experimental Platform for Realistic Ranging Evaluation in 5G and Beyond," in Proceedings of IEEE Vehicular Technology Conference (VTC Fall 2023), Hong Kong, China, Oct 2023. DOI:10.1109/VTC2023-Fall60731.2023.10333626

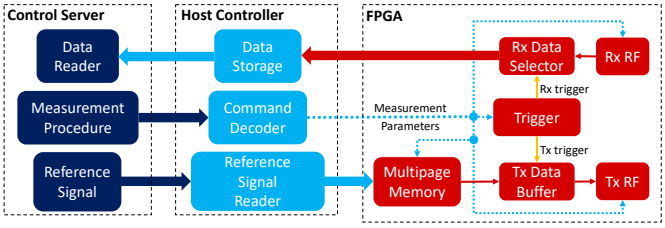


Fig. 2: Block diagram of the proposed experimental platform.

block diagram representing the implemented platform. The subsequent sections will provide detailed explanations of the key components.

1) Reference Sequences

Unique sequences are utilized for ranging estimation across different standards, hence a flexible platform to handle these variations is crucial. Accordingly, the platform should offer the ability to adjust the transmitting sequence to meet specific experimental objectives. However, storing the sequence on the host controller can complicate large bandwidth measurements due to insufficient speed. Our solution is to use a multi-page memory integrated into the field programmable gate array (FPGA) on the USRP, which enables pre-storage and real-time sequences transmission during measurements. Given a higher clock rate of the memory than the sampling frequency, it effectively provides the required data samples. If multiple sequences are needed during the measurement phase, the platform can use a predefined procedure to switch between memory pages for transmitting different sequences, enabling real-time sequence selection during measurement.

2) Device Triggering

TWR requires a coarse clock synchronization among involved entities using different protocols and methods based on the particular standard. Our implementation leverages a triggering system to initiate the signal transmission and acquisition. This local triggering system can be aligned using different approaches. For instance, in indoor scenarios, the alignment can be achieved by a common pulse per second (PPS) signal. In contrast, for outdoor experiments, the triggering system can be synchronized through a GNSS-based PPS signal or an over-the-air synchronization block described in [11]. Our implementation allows triggering time configuration with a resolution of up to 5 nanoseconds, enabling emulation of user timing errors based on a specific error distribution. Additionally, the local clock implemented on the FPGA can be set with a certain drift, allowing emulation of varied user clock drifts and increasing system adaptability. Note that, there is a processing delay on the transmission side, which is discussed in Section III-B1. Due to this delay, a pre-measurement calibration becomes necessary for obtaining an absolute time delay estimation.

3) Data Storage

With the help of the triggering system, the number of samples forwarded to the host controller can be significantly reduced. The number of samples stored per measurement can be configured to fit the needs of an experiment. The data is converted into a binary file to optimize storage use further. The samples obtained from FPGA are represented as a ratio to the peak amplitude of the analog-to-digital converter (ADC). The corresponding amplitude in volt can be calculated as

$$y[k](\mathrm{V}) = 2 \cdot 10^{(g_{\mathrm{rx}}-10)/20} y_{\mathrm{ADC}}[k], \tag{7}$$

where g_{rx}, in dB, represents the gain of receiver chain low noise amplifier (LNA).

Algorithm 1 Measurement procedure of TWR.

Configuration:
1: Generate and pre-store reference signal(s)
2: Configure RF parameters
3: Configure number of samples to be sent/acquired
Measurement Loop:
4: Configure Tx and Rx triggering time
5: Trigger TWR process
Post Processing:
6: Download and convert received samples from USRP
7: Compute distances according utilizing the algorithm under test for TWR
8: Evaluate results

4) Remote Controlling

An accurate evaluation of an algorithm often requires a large number of measurements. This is facilitated in our implementation by an automated user datagram protocol (UDP)-based command protocol that controls the process. The protocol uses command packets with a two-byte header indicating the type, and a variable-length content field detailing the configuration value. The host controller initializes and sets parameters for the FPGA, while a control server provides necessary measurement parameters and allows for designing diverse testing procedures, making for a flexible platform. An example for TWR measurement procedure, used in this study, is shown in Algorithm 1.

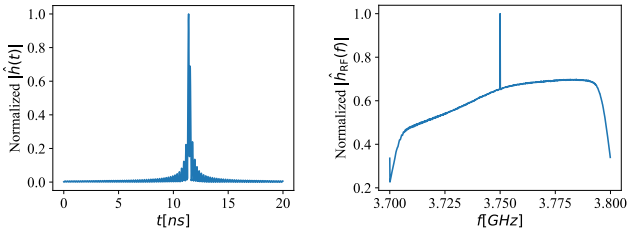
B. Calibration Before Measurement

In the previous section, we highlighted the crucial role of calibration measurements in ensuring the measurement data accurately represents the intended scenario, and mitigating potential interference from hardware impairments. In this section, we present a detailed discussion on the specific calibrations that need to be conducted prior to the actual measurements.

1) Processing Delay Calibration

Fig. 3a depicts the estimated impulse response, revealing the impact of processing delays on the USRP. When the trigger is engaged, a distinct processing delay occurs, following which the analog signal is radiated from the transmitting antenna. To illustrate this, we performed a calibration measurement by directly connecting the transmitter (Tx) and receiver (Rx) ports of the USRP using a 20 centimeter SubMiniature version A (SMA) cable. Given that the Tx trigger is set to zero, the results indicate a peak corresponding to the absolute delay of

This document is a preprint of: Z. Li, A. Nimr, P. Schroter et al., "Flexible SDR-based Experimental Platform for Realistic Ranging Evaluation in 5G and Beyond," in Proceedings of IEEE Vehicular Technology Conference (VTC Fall 2023), Hong Kong, China, Oct 2023. DOI:10.1109/VTC2023-Fall60731.2023.10333626



(a) Estimated impulse response. (b) Estimated freqency response.

Fig. 3: Calibration: Tx and Rx are connected with SMA cable.

11.4 nanoseconds, including the processing delay. This delay needs to be subtracted from the actual measurement results to discount the processing delay and maintain the integrity of the ToF estimation.

2) USRP Frequency Response Calibration

Another essential calibration measurement is to obtain the RF components response of the USRP when the Tx and Rx ports are directly connected via a SMA cable. This procedure plays a critical role in accurately estimating the characteristics of the over-the-air channel. As illustrated in Fig. 3b, a typical frequency response of USRP suggests that it is not flat in the frequency domain, with an evident direct current (DC) component. This significant DC component implies that the carriers around the center frequency should be avoided to maintain the channel estimation performance. Accordingly, the frequency domain channel estimates for obtaining ranging calibrated by the USRP RF response $\tilde{h}_{\mathrm{RF}}[k]$ is given by $\hat{\tilde{h}}[k] = \hat{\tilde{h}}_{\mathrm{raw}}[k]/\tilde{h}_{\mathrm{RF}}[k]$, where $\hat{\tilde{h}}_{\mathrm{raw}}[k]$ is computed with the data samples from FPGA.

3) Antenna Cable Length Calibration

Fig. 4 demonstrates that the measurement antennas employed for the measurements are not connected directly to the Tx and Rx ports, requiring cable lengths to be considered for precise ranging results. The cable length is measured using a network analyzer, which can be challenging to calibrate for zero length. To address this, (9) proposes a method to obtain calibration length, thereby eliminating the need for network analyzer calibration and simplifying the process. Taking into account the RF response and antenna cable length calibration, d_{cali} is defined as the calibration length. Specifically, the estimated ranging distance, denoted as $\hat{d}_{\mathrm{TWR}}$, is expressed as

$$\hat{d}_{\mathrm{TWR}} = \hat{d}_{\mathrm{raw}} + d_{\mathrm{cali}}, \tag{8}$$

where $\hat{d}_{\mathrm{raw}}$ represents the estimated distance directly obtained from $\hat{\tilde{h}}$, and

$$\begin{aligned} \hat{d}_{\mathrm{cali}} &= d_{\text{Cali Cable}} - d_{\text{Ant Cable}} \\ &= d_{\text{NA, Cali Cable}} - d_{\text{NA, Ant Cable}} \end{aligned}. \tag{9}$$

Note that $d_{\text{NA, Cali Cable}}$ and $d_{\text{NA, Ant Cable}}$ denote the measured lengths of the calibration cable and the antenna cable respectively, as determined by the network analyzer. The process of subtracting these measurements effectively bypasses the need for zero length calibration of the network analyzer.

TABLE I: Measurement parameters.

Parameter	ref sig	
	PRS	chirp
f_c [GHz]	3.75	
$f_{s,\mathrm{tx}}$ [MHz]	122.88	122.88
$f_{s,\mathrm{rx}}$ [MHz]	122.88	122.88
signal bandwidth [MHz]	98.28	98.28
subcarrier spacing [KHz]	60	60
block length	4096	2048
reference sequence length	1638	1638

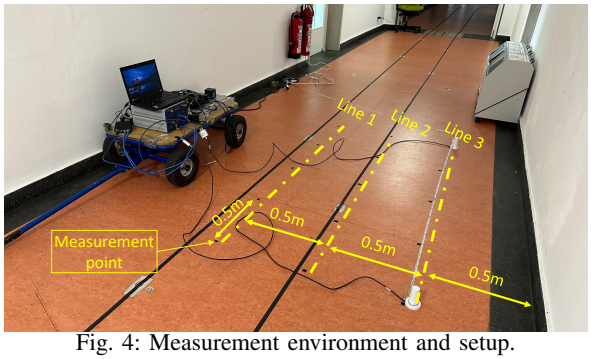


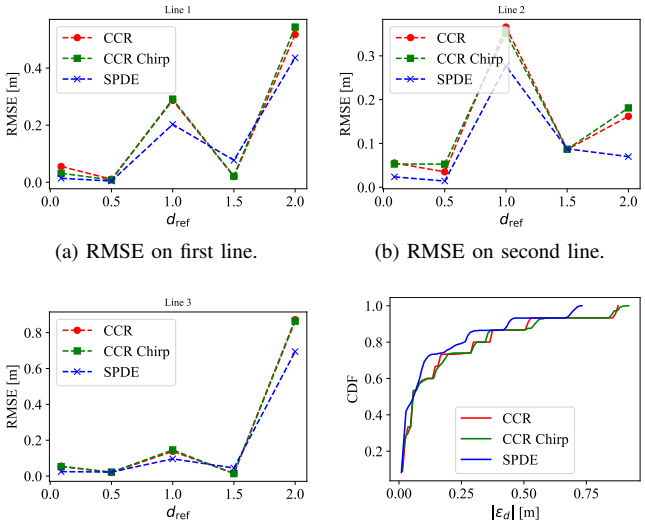
Fig. 4: Measurement environment and setup.

Following the calibration measurements outlined above, the actual TWR measurements are conducted. The results of these measurements, along with their analysis, are presented in the following section.

IV. Measurement Results

In this work, we provide an example of the application of our experimental platform through an indoor TWR measurement. The measurement demonstrates the configurability of the reference sequence required for ranging acquisition. Additionally, we conduct an evaluation of both the conventional cross-correlation (CCR)-based and the superresolution algorithm, proposed in [12]. The parameters utilized for the measurement are documented in Table I. The block length of the 5G positioning reference signal (PRS) is defined in [13]. The sequence length is set as 1638, representing the upper limit of allocation. However, given that they allocated to every other subcarrier, the actual subcarrier spacing for the PRS is 60 KHz, despite the 30 KHz subcarrier spacing in the sub-6 GHz system. The signal occupies a bandwidth around 100 MHz. For comparison, we utilize the same bandwidth to the chirp reference signal. The block length for chirp sequence is defined as the nearest power of two relative to 1638. At the transmitter, frequency domain zero padding is deployed to restrict the bandwidth of the chirp signal. Fig. 4 presents a visual representation of the measurement environment. The measurements took place within a confined corridor, characterized by the presence of metallic reflectors which contribute to the complexity of the channel. This complexity is further highlighted in the subsequent analysis. The PRS is pre-stored on the FPGA. The utilized chirp signal is defined by $c[n] = \exp\left(-\mathrm{j}2\pi\frac{n^2}{N}\right)$.

As visualized in Fig. 4, the measurements are conducted along three lines at different distances from a corridor wall, re-



(a) RMSE on first line. (b) RMSE on second line.

(c) RMSE on third line. (d) CDF over all ranging errors.

Fig. 5: Measurement results.

sulting in unique multipath channels. Each measurement point involves 800 captures, divided into 80 groups for unique channel realizations, with ten measurements per group to improve the processing signal-to-noise ratio (SNR) using averaged data blocks. Performance evaluation is primarily driven by the root mean squared error (RMSE) metric. The error cumulative density function (CDF) of all measurements demonstrates the statistical performance of different methods. Within measurement, the performance of various reference sequences under CCR-based methods is evaluated. Moreover, a comparison is made with the superresolution delay estimation technique proposed by [12], where the PRS serves as the reference signal. Fig. 5 shows that all tested methodologies can achieve centimeter-level accuracy with around 100 MHz bandwidth. However, the notable outliers, mostly due to the underlying multipath channel, can introduce significant errors, observed at the 2m distance in the first and third lines. Environmental factors, such as the unique corridor layout and reflective metal surfaces, as shown in Fig. 4, complicate accurate ranging performance predictions, as these heavily depend on specific channel characteristics. Moreover, indoor scenarios tend to be more complex than their outdoor counterparts due to the presence of a higher number of strong channel paths. Thus, focusing solely on synchronization errors does not adequately represent the actual performance of the TWR accuracy. Another interesting observation from the results is the superior performance of the superresolution algorithm compared to the CCR-based approach. This finding is further confirmed by the result shown in Fig. 5d. In our corridor environment, the superresolution algorithm displayed an average error of 0.3 m, while the CCR approach exhibited an error of 0.4 m for 80% of the tested realizations.

V. Conclusion

In conclusion, we propose an experimental platform with a high degree of flexibility and adaptability in this work. This platform is designed to facilitate ranging-related experiments, featuring a range of adjustable parameters associated with various methodologies. The platform supports different experiments, including but not limited to evaluating different protocols, waveforms, and estimation algorithms designs for two-way ranging (TWR). An implemented synchronized trigger allows one to emulate potential hardware limitations in a practical system. An indoor TWR experiment is presented as an example to illustrate the impact of different reference sequences and delay estimation algorithms. Notably, the platform is not restricted to indoor environments. The triggers in the implementation can be synchronized using global navigation satellite system (GNSS)- or signal-based techniques, allowing for outdoor measurements, such as investigations of 5G sidelink-enabled V2X applications. Thus, the platform is a versatile tool that can cater to a wide variety of experimental requirements in both indoor and outdoor contexts.

Acknowledgment

This work was funded and supported by the project ”Industrial Radio Lab Germany” under contract 16KIS1010K, funded by the Federal Ministry of Education and Research, Germany.

References

[1] 3GPP, “Study on scenarios and requirements of in-coverage, partial coverage, and out-of-coverage NR positioning use cases,” TR 38.845, Technical Report 17.0.0, 2021.

[2] 3GPP, “Study on NR positioning support,” TR 38.855, Technical Report 16.0.0, 2019.

[3] J. Peisa, P. Persson, S. Parkvall, E. Dahlman, A. Grøvlen, C. Hoymann, and D. Gerstenberger, “5g evolution: 3GPP releases 16 and 17 overview,” *Ericsson Technology Review*, vol. 2020, no. 2, pp. 2–13, 2020.

[4] 3GPP, “Study on architecture enhancement to support ranging based services and sidelink positioning,” TR 23.700, Technical Report 18.0.0, 2023.

[5] Y. Lu, M. Koivisto, J. Talvitie, E. Rastorgueva-Foi, T. Levanen, E. S. Lohan, and M. Valkama, “Joint positioning and tracking via NR sidelink in 5G-empowered industrial IoT: Releasing the potential of V2X technology,” *arXiv preprint arXiv:2101.06003*, 2021.

[6] Y. Ge, M. Stark, M. F. Keskin, F. Hofmann, T. Hansen, and H. Wymeersch, “Analysis of V2X sidelink positioning in sub-6 GHz,” in *2023 IEEE 3rd International Symposium on Joint Communications & Sensing (JC&S)*, 2023, pp. 1–6.

[7] IEEE Standards Association and others, “IEEE Std 802.15.4-2011, IEEE standard for local and metropolitan area networks part 15.4: Low-rate wireless personal area networks (LR-WPANs),” 2011.

[8] C. Lian Sang, M. Adams, T. Hörmann, M. Hesse, M. Porrmann, and U. Rückert, “Numerical and experimental evaluation of error estimation for two-way ranging methods,” *Sensors*, vol. 19, no. 3, p. 616, 2019.

[9] V. Sark, N. Maletic, J. Gutiérrez, and E. Grass, “An approach for implementation of ranging and positioning methods on a software defined radio,” in *2017 14th Workshop on Positioning, Navigation and Communications (WPNC)*, 2017, pp. 1–6.

[10] V. Sark, N. Maletic, M. Ehrig, J. Gutiérrez, and E. Grass, “Achieving millimeter precision distance estimation using two-way ranging in the 60 GHz band,” in *2019 European Conference on Networks and Communications (EuCNC)*, 2019, pp. 310–314.

[11] I. Gaspar and G. Fettweis, “An embedded midamble synchronization approach for generalized frequency division multiplexing,” in *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015, pp. 1–5.

[12] Z. Li, A. Nimr, P. Schulz, and G. Fettweis, “A flexible matrix structure for superresolution delay estimation,” in *WS13 ICC 2023 2nd Workshop on Synergies of communication,localization, and sensing towards 6G (WS13 ICC’23 Workshop - SynComm6G)*, Rome, Italy, Jun 2023.

[13] 3GPP TS 38.211, “NR: Physical channels and modulation (Release 16),” 2022.