A USRP-Based Testbed for Wideband Ranging and Positioning Signal Acquisition

Cherif Diouf, Gerard J. M. Janssen, *Member, IEEE*, Han Dun, Tarik Kazaz, and Christian C. J. M. Tiberius

***Abstract*— For validation and demonstration of high accuracy ranging and positioning algorithms and systems, a wideband radio signal generation and acquisition testbed, tightly synchronized in time and frequency, is needed. The development of such a testbed requires solutions to several challenges. Tight time and frequency synchronization, derived from a centrally distributed time-frequency reference signal, needs to be maintained in the hardware of the transmitter and receiver nodes, and wideband signal acquisition requires sustainable data throughput between the receiver and host PC as well as data storage at GB level. This article presents a testbed for wideband radio signal acquisition, for validation and demonstration of high accuracy ranging and positioning. It consists of multiple Ettus X310 universal software radio peripherals (USRPs) and supports high accuracy (<100 ps) time-deterministic, sustainable signal transmission and acquisition, with a bandwidth up to 320 MHz (in dual channel mode) and frequencies up to 6 GHz. Generation and processing of wideband arbitrary signal waveforms is done offline. To realize these features, radio frequency on chip (RFNoC) compatible HDL units were developed for integration in the X310 SDR platform. Wideband transmission and signal acquisition at a lower duty cycle is applied to reduce the data offloading throughput to the host's personal computer (PC). Benchmarking of the platform was performed to demonstrate sustainable long duration dual channel acquisition. Indoor range measurements with the synchronous operation of the testbed show a decimeter-level accuracy.**

***Index Terms*— Burst transmission, data acquisition, Ettus X310, ranging and positioning, universal software radio peripheral (USRP), wideband radio testbed.**

I. Introduction

GLOBAL navigation satellite systems (GNSS), being currently the most popular positioning technology, performs well, at meter level accuracy, in open environments. Despite its proven track record and high economic value, GNSS has a number of serious limitations, in particular in areas where it is needed most, namely in built-up areas (urban canyons) and indoor, where people live, work, and travel. In such areas, GNSS performance is degraded as satellite signals are blocked by buildings and other objects, and GNSS receivers may get "confused" by multipath reflections of the ranging signals. Besides this, GNSS is also vulnerable to unintentional or intentional interference (spoofing and jamming) [1].

Novel ranging and location-based services, as used for navigation, sensing, automated-driving, smartphone localization, and augmented reality, demand for increased accuracies at decimeter and subdecimeter level, and also need to operate in GNSS denied areas. Several terrestrial indoor and outdoor ranging systems are available on the market and novel algorithms, techniques, and platforms are developed, to achieve higher accuracies [2]–[5]. Typically, ranging is done based on estimating the time duration between transmission of the signal at the transmitter and arrival of this signal at the receiver. In a dense multipath radio channel, i.e., with a lot of reflections, the receiver may lock on a reflected signal instead of the desired direct path or line-of-sight (LoS) signal. In addition, it may not be able to distinguish the direct path signal from close-in reflections with a slightly longer delay, which then will cause an offset in the estimated time-of-arrival (ToA) of the signal. Since the precision of ToA estimation [6] and the separability of the multipath reflections is inversely proportional to the signal bandwidth, to achieve a high ranging and positioning accuracy wideband ranging signals are needed. Apart from a high range resolution, transmitters and receivers should also be accurately time-aligned, and in case phase-based ranging is applied, also accurate radio frequency synchronization is needed. This can be obtained by connecting the transmitters to an accurate time-frequency reference signal, like a 1 pulse per second (1PPS) timing signal and 10-MHz frequency reference. An accurate time alignment of the transmitters and receivers is important, since even a small error of, e.g., 1 ns already causes a range error of 0.3 m. For the development of high accuracy ranging and position algorithms, a flexible validation and demonstration testbed setup, to collect experimental data within real-life environments, and to demonstrate proof of concept, is highly desirable. The internal errors of such a system should be (substantially) smaller than those aimed at by the algorithm or system to be evaluated.

For the project at hand, the following system requirements are aimed for:-time synchronization between different devices better than 100 ps,-time and frequency references originating

Manuscript received November 27, 2020; revised February 24, 2021; accepted February 27, 2021. Date of publication March 10, 2021; date of current version March 24, 2021. This work was supported by the Netherlands Organization for Scientific Research (NWO) through the Project SuperGPS under Grant 13970. The Associate Editor coordinating the review process was Dr. Huang-Chen Lee. *(Corresponding author: Cherif Diouf.)*

Cherif Diouf, Han Dun, and Christian C. J. M. Tiberius are with the Department of Geoscience and Remote Sensing, Delft University of Technology, Delft 2628 CN, The Netherlands (e-mail: c.e.v.diouf@tudelft.nl; h.dun@tudelft.nl; c.c.j.m.tiberius@tudelft.nl).

Gerard J. M. Janssen and Tarik Kazaz are with the Circuits and Systems Group, Delft University of Technology, Delft 2628 CD, The Netherlands (e-mail: g.j.m.janssen@tudelft.nl; T.Kazaz@tudelft.nl).

Digital Object Identifier 10.1109/TIM.2021.3065449

from the same source,-wideband signal transmission with a bandwidth > 100 MHz, simultaneous transmission in multiple bands,-tuning band: 1–5 GHz,-sustainable offloading of acquired signals,-standalone operation of the anchor stations (transmitters).

To tackle the subject of wideband data transmission and acquisition, a system may be developed for a specific application. In [7], a data acquisition platform based on sub-Nyquist sampling is designed to test wideband multistandard receivers. An IR-UWB transmission and acquisition platform with the periodic transmission of pulses and equivalent time sampling signal acquisition is shown in [8].

Software defined radio (SDR) systems are flexible programmable hardware devices that can be used for prototyping of very diverse radio technologies. SDR devices are available from low complexity and low cost to very advanced and expensive equipment [9], [10]. These devices have a DSP unit for signal processing operations and separate ADC/DAC units and RF frontends for transmission and reception of radio signals. More advanced SDRs also contain an FPGA for implementing custom on-device signal processing algorithms. An SDR can be configured and controlled through a connected (PC). Data processing can be performed in the SDR, or the data can be offloaded to the PC (by a high speed connection) for further offline processing.

Examples of SDR systems for prototyping, validation, and demonstration related to, ranging and positioning can be found in [11]–[13]. For instance, an SDR-based TDoA indoor localization system using WiFi signals is presented in [11]. Multichannel-based ranging techniques for narrowband wide area networks are demonstrated in [12]. In [13], an SDR architecture for navigation using CDMA signals is presented. Many of these works, while using the flexibility of the SDRs, are very application specific. The whole platform is generally built to validate or demonstrate specific ranging or positioning techniques.

In this article, we discuss the development and testing of a more general SDR-based generic radio signal transmission and acquisition testbed, using high-end Ettus X310 Universal Software Radio Peripheral (USRP). This device consists of two radio frequency (RF) channels with a bandwidth of 160 MHz, which can be simultaneously used in either transmit or receive mode (2× 200-MSPS sampling rate), and a maximum combined bandwidth of 320 MHz. The most challenging requirements of the development process are: 1) the critical timing constraints, which have to be maintained from reference input through the hardware to the input–output signal time stamping and 2) sustainable signal acquisition at very high sampling rates and the related high data rate throughput and storage.

The main contributions of this work are the design, development, and validation of three radio frequency on chip (RFNoC) compatible logic units that allow for sustainable, time deterministic, synchronous transmission, and both synchronous and asynchronous acquisition of dual-band signals, sampled at a total rate of 400 MSPS. The developed blocks have been integrated through RFNoC within the X310 USRPs and are GNU Radio compatible. Indoor ranging experiments with 160-MHz wideband signals using this testbed show a decimeter level accuracy. Furthermore, it is demonstrated that the platform can be used for sustainable dual channel wideband signal acquisition.

The remainder of this article is organized as follows. Section II presents the signal model for ranging based on time delay estimation, and discusses the need for wideband signals. The challenges of wideband signal acquisition are presented in Section III, along with the required functionalities and specifications of the testbed. In Section IV, the X310 USRP and the development context are introduced. In Section V, the design and development of the logic units are described in detail. Benchmarking results of the testbed coarse synchronization and the long duration dual channel acquisition are presented in Section VI. In Section VII, experimental indoor ranging results, obtained with the test platform, are presented. Finally, in Section VIII conclusions are drawn and an outlook on future works is given.

II. Ranging Accuracy and Wideband Signal

A. Signal Model

For ranging based on time delay estimation, a baseband signal model is used. The transmitted bandpass signal at a frequency f_c for the baseband signal $s(t)$ is given by $x(t) = \mathrm{Re}\{s(t)e^{j2\pi f_c t}\}$, in which $\mathrm{Re}\{\cdot\}$ indicates the real part of a complex value. We assume an ideal channel impulse response (CIR) for a static single path channel, given by

$$h(\tau, t) = a\delta(t - \tau) \tag{1}$$

with a is the attenuation of the signal due to propagation losses and τ is the propagation time between transmitter and receiver. The received baseband signal is then given by

$$\begin{aligned} r(t) &= (s(t) * h(\tau, t))e^{j2\pi f_D(t-\tau)+\theta_0} + n(t) \\ &= a\delta(t - \tau)e^{j2\pi f_D(t-\tau)+\theta_0} + n(t) \end{aligned} \tag{2}$$

where $*$ indicates convolution, θ_0 is the phase offset between transmitter and receiver at $t = 0$, f_D is the frequency difference between the received signal and the receiver frontend, i.e., due to a frequency offset between transmitter and receiver or due to Doppler shift, and $n(t)$ is noise with a zero-mean Gaussian distribution and variance σ_n^2. For a sampled system, the sampled received signal can be represented as

$$r[k] = (s[k] * h[\tau, k])e^{j2\pi f_D(kT_s-\tau)+\theta_0} + n[k] \tag{3}$$

where k represents the discrete time variable and T_s is the sample time.

B. Time Delay-Based Ranging: Accuracy and Bandwidth

For ranging, the variable of interest is the time delay τ. From the estimated value $\hat{\tau}$ of τ, the estimated distance $\hat{d}$ between transmitter and receiver is found as $\hat{d} = c \times \hat{\tau}$, where $c = 3 \times 10^8$ m/s is the speed of light. The precision that can be obtained when performing ranging based on unbiased time delay estimation can be bounded by the Cramer-Rao Lower

Bound (CRLB), which defines a lower bound on the variance of the estimation error $\sigma_\tau^2 = \overline{(\hat{\tau} - \tau)^2}$ as

$$\sigma_\tau^2 \geq \frac{1}{\mathrm{SNR}\overline{F^2}} \tag{4}$$

and is determined by the signal-to-noise ratio (SNR) and mean square bandwidth or Gabor bandwidth $\overline{F^2}$ of the signal [6] defined as

$$\overline{F^2} = \frac{\int_{-\infty}^{\infty} (2\pi f)^2 |S(f)|^2 df}{\int_{-\infty}^{\infty} |S(f)|^2 df} \tag{5}$$

where $S(f)$ is the Fourier transform of $s(t)$. Equation (5) shows that the Gabor bandwidth is related to the signal bandwidth. In a single path LoS channel, the variance of the range estimate becomes: $\sigma_d^2 = c^2\sigma_{\hat{\tau}}^2$. So, in order to reduce the range estimation error variance, a larger Gabor bandwidth is needed and/or the SNR has to be increased. As we saw in Section I, the time resolution, which determines how well multipath components that arrive with short time differences can be separated, also is inversely proportional to the signal bandwidth. So the use of wideband signals is essential for accurate ToA estimation and ranging in a multipath channel. The CRLB for such a scenario also depends on the channel characteristic and on the ranging algorithms used to perform the estimation, which is outside the scope of this article.

III. Wideband Ranging Signal Acquisition

Acquiring wideband radio signals for prototyping of ranging algorithms can be a hurdle due to the high amount of generated data. For sparse channels, sub-Nyquist sampling and compressive sensing techniques have been proposed that can operate at sample rates less than the Nyquist rate, and therefore partially overcome this issue [14], [15]. Such techniques can only be applied when sufficient *a priori* knowledge of the channel is available. Therefore, in the following, we only consider full rate wideband signal acquisition.

Bearing in mind the computational cost and data throughput of such full rate acquisition, one may alleviate the problem by implementing and testing all the algorithms directly on-device with real-time signals acquired by the RF hardware system in the testbed in concern. This online processing option could nevertheless turn out to be very time-consuming and not without implementation hardship, particularly due to FPGA and ASIC hardware development constraints. Moreover, such implementation is generally very inappropriate in the early stages of development, when algorithms and techniques are not reliably validated.

In this situation, the common practice is to first implement and test the techniques on a computer, in scientific software or libraries (MATLAB, Python/Numpy) with: 1) models of signals and then 2) signals acquired from real-life environments. This allows to have a faster initial assessment of the performance. Then, if needed, in a later stage hardware implementation for further validation can be done.

In this work, we are thus targeting full rate acquisition and transfer to PC of wideband signals for offline prototyping of ranging algorithms using an SDR-based testbed.

TABLE I

Characteristics of Some SDR Devices Capable of Dual-Band Wideband Signal Acquisition

Device	Maximum . bandwidth (MHz)	Maximum sampling Rate (MSPS)	Frequency Range (GHz)
Crimson TNG [16]	1200 (4 dual RX channels)	1480 (4 x 370)	DC to 6
AARONIA Spectran V6 [10]	490 (2 x 245)	500 (2 x 250)	0.01 to 6
Ettus N320/N321	400 (2 x 200)	500 (2 x 250)	0.003 to 6
Ettus N300/N310	400 (4 x 100)	> 600	0.003 to 6
Ettus X300/X310	320 (2 x 160)	400 (2 x 200)	0.01 to 6

TABLE II

Data Throughput in One and Two Channels Configuration for Duty Cycle Equal to 1 and to 0.1

	MSPS	Throughput	File Size (1 min)
Duty Cycle = 1	200	800 MB/s	48 GB
	400	1600 MB/s	96 GB
Duty Cycle = 0.1	200	80 MB/s	4.8 GB
	400	160 MB/s	9.6 GB

Table I presents characteristics of five SDR devices capable of dual-band wideband signal acquisition. The maximum bandwidth is varying from 320 to 1200 MHz, and sampling rates are varying from 400 to 1480 MSPS.

Let us take the X310, used in our testbed, as an example to study the computational requirements and acquisition issues.

This X310 allows for a maximum sample rate of 200-MSPS per channel, where one sample occupies 4 bytes (16 bits-I, 16 bits-Q). The equivalent data throughput to the host-PC is 800 MB/s for the one-channel configuration, and 1.6 GB/s if the X310 is operated with two channels (Table II). To handle this throughput, a PC with two high-end 10-Gb/s Ethernet cards is required. A total of 2.5 GB/s can be theoretically handled using such a configuration.

A 1.6-GB/s data throughput also requires the use of NVMe-type SSD disks that can support a theoretical writing speed at GB/s level. It should be noted, however, that the common host-PC runs on a nonreal time operating system (OS) that may introduce latencies and delays, with process scheduling that reduces the effective throughput. Hence, even if the hard drive and the network link support 1.6 GB/s, a continuous acquisition without data losses can hardly be guaranteed. Besides throughput considerations, 10 min of data acquisition at 1.6 GB/s will generate a data file size of 960 GB (or 5.76 TB for 1 h). This renders long-duration experiments and further post processing very unpractical.

A. Bursts Transmission and Acquisition Scheme for Reduced Throughput Operations

The high amount of data transfer and the required transfer rate needed for continuous acquisition of wideband ranging

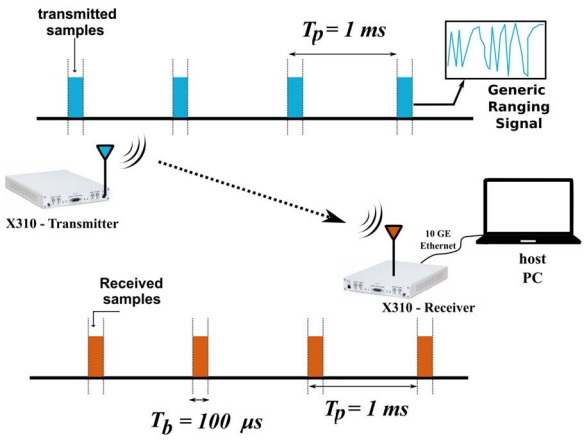

Fig. 1. Low duty cycle ranging signal transmission and reception, with a transmission period of $T_p = 1$ ms and a burst duration of $T_b = 100$ μs.

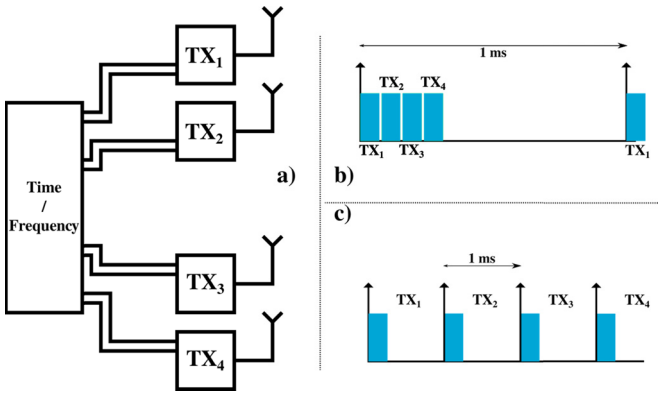

Fig. 2. (a) Configuration to synchronize multiple transmitters, (b) and TDM within one transmission period, and (c) within different transmission periods.

signals can be largely relaxed when a wideband but low duty cycle ranging signal is used, i.e., periodic burst transmissions. Such a ranging scheme will allow data transfer from the receiving USRP to the host PC at a reasonable and sustainable throughput.

Fig. 1 shows a low duty cycle-based setup for ranging, where a first X310 acts as a transmitter, and a second X310 acts as a receiver, which forward the ranging samples to a host-PC, through a 10 GE link. Let T_b be the burst duration and T_p the transmission period, then the resulting duty cycle is $\alpha = (T_b/T_p)$. A too large duty cycle may cause an unsustainable throughput. We have specified a default transmission period of $T_p = 1$ ms and a duration $T_b = 100$ μs for a duty cycle of $\alpha = 0.1$. In this way, 1000 range estimates can be obtained per second. A car driving at 30 m per second will move by 3 cm during a $T_p = 1$ ms period. At a rate of 200 MSPS, 20 000 samples are transmitted in a single burst.

For two channels operating at full sampling speed, the throughput is reduced to 160 MB/s, a value well below the maximum ten GE Ethernet speed and the writing speed of a performant SSD. Moreover, one minute of data recording then results in a file size of 9.6 GB, see Table II. When an even lower duty cycle is acceptable, the throughput and file size will accordingly decrease.

The testbed is designed to support generic format signals (Fig. 1) that meet the frontend bandwidth limits. As the X310 is the device in use, the transmitted signal can have a maximum contiguous bandwidth of 320 MHz when the two 160-MHz channels are combined. Ranging signals can vary from phase shift-keying (PSK) signals to more advanced signal designs such as orthogonal frequency-division multiplexing (OFDM). Signal samples are provided to the transmitter in $I - Q$-format in a raw file, and the received samples are available in $I - Q$-format for post processing.

B. Testbed Synchronization Requirements and Solutions

Synchronization is a critical issue in ranging. As wideband ranging signals are used to attain decimeter or even centimeter-level accuracy, a small timing mismatch, occurring within the transmission or acquisition chain, will significantly degrade the ranging performance. We have opted for synchronization based on the use of an external (1PPS/PPS) time reference and a 10-MHz frequency reference. This allows to align the transmitting and the receiving windows in time for proper ranging signals recording at the receiver side, Fig. 1. The 1PPS and 10 MHz may be derived from various sources.

When the testbed receiver and transmitter(s) are relatively close together, the synchronization source can be a clock distributor which electrical 1PPS and 10-MHz outputs are conveyed via coaxial cables to the SDRs. When the testbed devices are more distant, GPS-based synchronization could seem to be a solution. However, GPS timing accuracy is in the order of 10 ns and therefore not suitable for decimeter level precision. High accuracy wireless-based synchronization may provide sub-nanosecond synchronization [17], [18] and could be used to synchronize the testbed devices.

White Rabbit (WR)-based synchronization over optical fiber networks is also a promising solution to distribute accurate synchronization reference signals over large areas. Time-frequency reference distribution, over tens of kilometers with sub-nanosecond synchronization accuracy, has been demonstrated [19]. High timing accuracy, at the 100-ps level, has already been demonstrated with WR [20], [21]. A 100 ps of timing error will generate 3 cm of ranging bias which may be acceptable for a decimeter level ranging or positioning system [22]. In the proposed testbed, time-frequency reference signals are distributed over a small optical fiber link using WR nodes.

In a multiple transmitter scenario, as shown in Fig. 2(a), accurate synchronization allows several X310 USRPs of the testbed to start transmitting ranging signal samples at predefined time instants. Moreover, the testbed will support time-division-multiplexing (TDM), as shown in Fig. 2(b), where different X310 devices can transmit within the same burst period, or successively within different timed bursts [Fig. 2(c)].

The receiver of the testbed can operate in synchronous mode, sharing the same time and frequency reference signals with the transmitter(s), or it can operate in a standalone asynchronous mode, which is more suitable for a mobile scenario. In asynchronous mode, a matched filter-based technique is

used to detect the arrival time of the incoming ranging bursts and time-align the acquisition windows to the transmission windows.

The synchronous operating mode hardly causes any time delay impairments; however, synchronized frontends may still present phase offsets or a subsample bin level difference in transmitting/receiving time. For asynchronous mode operation, however, the impact of time delay impairments is much more significant. Moreover, a frequency offset by the free running receiver oscillator is also introduced. The matched filter-based synchronization is not totally comparable to a synchronization based on an external 1PPS/10-MHz signals, being less accurate.

C. Platform Specifications

The full specifications and functionalities of the testbed are summarized as follows:

1) multiple transmitters/receivers support, for ranging and positioning experiments;
2) time-frequency synchronization between the devices of the testbed. Synchronization based on a 10 MHz/1PPS external time-frequency reference signal.

The previous features are generally common to SDR systems and may be already available or very easy to implement. The development we present is mainly focused on the following:

1) deterministic timing from transmitter(s) to the receiver, in particular in the custom units in hardware;
2) dual channel, full bandwidth (160 MHz per channel) and at full sample rate (200 MSPS per channel) sustainable periodic generic signal transmission, and acquisition;
3) hardware-based transmission and acquisition control and specialized time control units in hardware, in order to limit PC-SDR interaction.
4) support of synchronous and asynchronous operating modes for the receiver. The latter allows to move the receiver freely from the transmitter(s);
5) sustainable offload throughput and reduced experimental data file size (low duty cycle ranging signals);
6) time-division multiplexed transmissions for positioning applications;
7) configurability of transmission and recording packets sizes and periods.

IV. X310 SDR Platform And Context

A. X310 USRP System

The Ettus X310 USRP has two individually configurable RF channels, each of which can be used either as a transmitter or a receiver, operating at a maximum sample rate of 200 MSPS. Each RF channel has an effective bandwidth of 160 MHz. By combining the signals from two frontends, a total bandwidth of 320 MHz can be covered, resulting in a total sample rate of 400 MSPS. The central frequency of each RF frontend can be tuned from 10 MHz to 6 GHz.

Several X310 units may be associated within a synchronized network to form a flexible array. The Ettus X310 USRP is compatible with the GNU Radio and the universal hardware (UHD)/RFNoC software environments. This compatibility allows to develop and integrate C++/Python digital signal processing units. Moreover, the X310 features an embedded Xilinx Kintex7 XC7K410T FPGA. This allows for the implementation of on-device digital signal processing units. The main advantage of an FPGA implementation is that it allows for much faster and time deterministic on-device processing operations. Hardware acceleration tasks can thus be implemented in the Kintex7.

B. Dual-Channel Transmission and Acquisition With the X310: Current Options

Due to the USRP's flexible software/hardware environment, very diverse radio/signal processing features have been already implemented and are publicly available. In the following, we put forward the context of the developed solutions as well as alternative solutions for dual-channel transmission and acquisition with the X310 devices.

1) At the Transmitter Side: Using the USRP to transmit synchronized generic signals is not straightforward due to the high sample rate and throughput, and the required accuracy. Several solutions may, however, be considered.

1) For direct transmission of a 2× 200 MSPS signal from the host-PC to the RF frontends, a rate of 1.6 GB/s should be sustainably supported from the PC to the X310 RF frontends. If possible at all, this requires the installation and use of the Intel Data Plane Development Kit (DPDK) on the host PC and tuning operations, such as changing the CPU policy to performance, enabling the POSIX threads, disabling hyperthreading, and increasing Ethernet Buffers size for better caching. The DPDK is a set of libraries that allows to process network data in batches and keeps these operations out of the OS kernel [23], [24]. However, there is still no guarantee that the data transmission will always be performed without issues. Moreover, if the same sequence has to be periodically transmitted, the solution is not very efficient.
2) Direct 2× 200 MSPS signal transmission from the USRP hardware to the RF frontends. For identical signals to be transmitted periodically, the best solution is to have the samples available on the device for maximum throughput to the RF frontends. In that case, several RFNoC CE (hardware processing block) may exist. Ettus is providing an arbritatry waveform generator (AWG) CE (signal generator); however, this block has a limited number of supported waveforms. In [25], a custom AWG-like CE, also known as *wavegen*, supporting the transmission of generic samples was used, and its code made available. Alternatively, Ettus has also proposed a software/hardware block that supports periodic transmission of generic signals: the replay-block. At the time of development (UHD 3.15) the original replay-block did not support dual channel transmission. With UHD 4.0.0 [26], the replay-block has been upgraded to support the dual-channel transmission of generic signals. Considering UHD 4.0.0, the proposed

solution has the following advantages over the replay-block. The replay-block basically loads the samples from the host PC to the device's external 1-GB DRAM, from which the samples are periodically streamed to the RF frontends. The solution we propose relies on the Xilinx internal BRAM and is fully compatible with GNU Radio and has configurability options such as: defining the transmission and receiving periods, the ranging packet size and it implements time division multiplexing (TDM) for multiple transmitters.

2) At the Receiver Side: At the receiver side, and still considering dual channel acquisition at full sample rate (1.6-GB/s throughput), using DPDK is still a possible solution. However, assuming that the acquisition is without issues due to OS scheduling and latencies, this solution is rather inefficient as 10 min of data recording will fill a 1 TB hard drive. Moreover, if the transmitted signals are low duty cycle bursts, which is the likely approach, the solution is inefficient as the signal is being continuously acquired while only a small part of its samples is relevant.

Another option allowed by the X310 is to save the received samples in the external 1-GB DRAM. However, 1 GB only allows for 0.625 s of dual channel recording. Up to now, we did not come across a solution developed, tested, and benchmarked allowing for a longer duration, 400-MSPS dual channel synchronous or asynchronous sustainable data acquisition using the X310 USRP platform.

V. USRP System Block Development

In this section, we present the specific blocks developed to implement the testbed. The development software environment is first introduced before focusing on the actual architecture of design and implementation.

A. GNU Radio, UHD, RFNoC

GNU Radio is a free and open-source software development and control toolkit that provides signal processing blocks for SDR systems [27]. These blocks are written in C++ or Python. GNU radio is compatible with a large number of SDR systems available on the market. GNU Radio blocks can also be used with the X310 USRP through the USRP Hardware Driver (UHD) layer. The UHD framework provides drivers, libraries, and basic terminal commands to directly operate USRPs from a host PC, or do so via GNU Radio.

Moreover, it is also possible to implement hardware DSP units in the USRP Kintex7 FPGA. While software DSP blocks can be implemented through the GNU Radio framework, hardware DSP blocks, also called computation engines (CEs), are implemented on the USRP through the radio frequency network on chip (RFNoC) development framework [28], [29].

RFNoC allows data streaming between DSP blocks running on hardware, but also between hardware and host PC blocks (through the UHD). The RFNoC framework allows the implementation of up to ten logic CEs in the X310 Kintex7 [30].

B. Terminology

In the sequel, we specifically define the following.

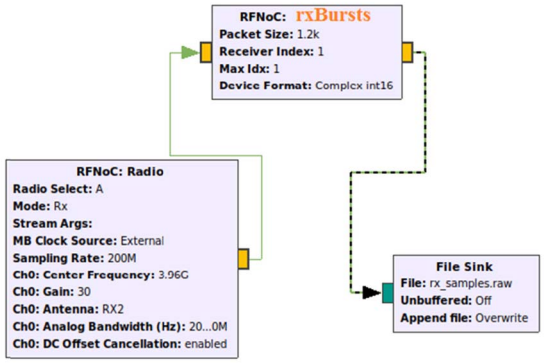

Fig. 3. Example of a GNU Radio flow-graph allowing to program the USRP as a burst receiver.

1) *Block:* an SDR C++/Python unit that performs software processing.
2) *CE:* a USRP-hardware unit, implemented in the X310 Kintex7, that performs a hardware processing task. Thus an RFNoC CE is a unit that performs an on-device operation.
3) Blocks can run independently on the host PC. On the other hand, each CE needs an associated block, which forms the software interface to the CE.
4) Three standard blocks/CEs will be used while three custom blocks/CEs were developed to build up the testbed. The standard blocks/CEs that are used, are as follows.
   a) *File Source Block:* A block which reads a data file from the host PC and outputs the raw samples.
   b) *File Sink Block:* A block which takes samples as inputs and saves them to a file on the host PC.
   c) *RFNoC Radio-Block and RFNoC Radio-CE:* These units are Software/Hardware interfaces to configure and use the X310 RF frontends.

The carrier frequency, its operating mode (transmitting/receiving), and the frontend sample rate are defined through the RFNoC Radio-Block.

The developed blocks/CEs are as follows.

1) *rxBursts-Block and rxBursts-CE:* These units were developed for synchronously receiving the ranging bursts and optimized for high data rate throughput. The host PC interface of the rxBursts-CE is the rxBursts-Block.
2) *arxBursts-Block and arxBursts-CE:* Custom developed unit for asynchronously receiving bursts optimized for high data rate throughput.
3) *txBursts-Block and txBursts-CE:* Developed units for burst transmission. The main development was carried out on the txBursts-CE while the txBursts Block is the CE host PC interface.

C. Development of the Synchronous Receiver

The receiver flowgraph in GNU Radio is shown in Fig. 3. It contains the frontend, a file-sink block that points to the data file path and the rxBursts-CE, shown on top, which is

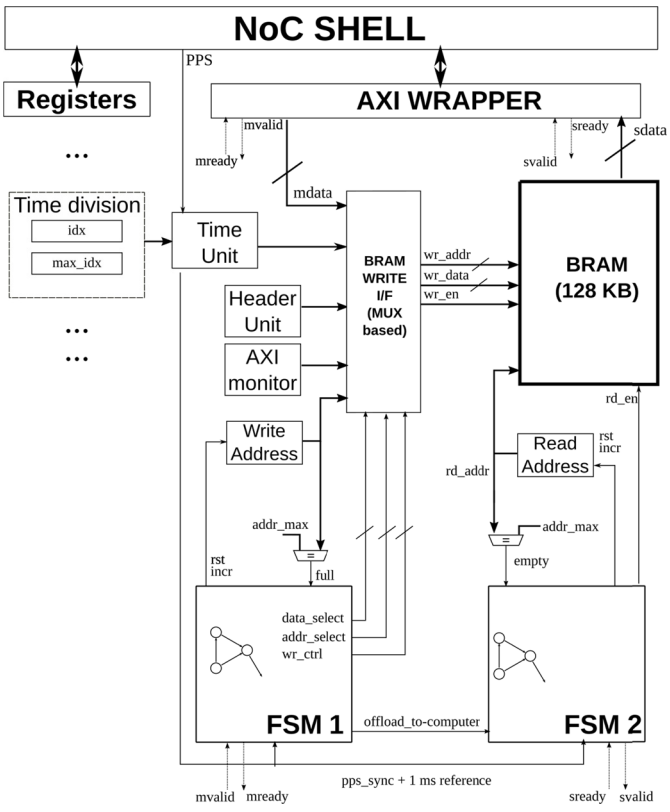

Fig. 4. rxBursts-CE logic architecture, for burst receiving.

handling the periodic transfer of received bursts to the host PC. The rxBursts-CE continuously receives samples from the RF frontend but only forward the time-aligned samples to the host-PC (Fig. 1). The default acquisition period is 1 ms. In the acquisition process, the CE will first move the time-aligned received samples to a 128-KB FPGA BRAM memory. When the BRAM memory is filled with the time-aligned samples, the CE acknowledges the PC of data availability. When ready, ranging samples contained in the BRAM are then forwarded to the host PC and saved to the data file. If, for instance a $\alpha = 0.1$ (adjustable) duty cycle is considered, the recording duration is 100 μs (equal to 20 000 samples per channel), and the host PC has 900 μs to fully offload the 20 000 ranging samples in BRAM. The cycle is restarted each 1 ms. Here it is assumed that the transmission and the receiving windows are time-aligned. Asynchronous operation, when the transmitter and the receiver are operating on independent oscillators, is considered later in this article.

1) Architecture: A detailed block diagram of the rxBursts-CE is shown in Fig. 4. The architecture includes the default RFNoC layers, such as the NoC Shell, the AXI wrapper, and the configuration registers, and shows the core logic architecture for burst acquisition using the 128-KB BRAM memory. The logic can be divided into six parts: two finite state machine (FSM) units, a header unit, a timing unit, a multiplexing unit, and the 128-KB BRAM memory where the samples to be forwarded to PC are temporarily stored. A 128 KB of memory can hold in total 32 768 samples, i.e., a maximum burst length of 163.8 μs.

FSM1 is the main state machine. It controls the storing to BRAM and also triggers the transfer of samples to the PC. The BRAM interface (I/F) allows to add metadata such as headers, timing information, and even addresses to the data forwarded to the host PC.

For time coordination, a key sub-block is the time unit which provides the following

1) the 1-ms reference;
2) the 5-ns counter reference;
3) time synchronization between the 1PPS and 1-ms signals and other control signals in the logic;
4) FSM2 controls the sample-by-sample transfer of the BRAM data to the host PC.

Once the time-aligned samples are fully transferred to PC, the state machine returns to its idle state and waits for the next transfer trigger from FSM1 to restart the offload process.

2) Time Synchronization Inside the FPGA: To ensure time alignment, the 1-ms reference is synchronized to the frontend time counter (*vitatime* counter) and to the 1PPS external reference. Thus, several USRPs will have all their time references synchronized and their processes time-aligned.

3) Packets Offloading Period: The received packets are, by default, transferred to the PC every 1 ms. Two configuration registers (idx/max idx), are available to increase this period by a natural integer value L. In that case the offload process will be restarted every $L\times$ 1 ms instead of every 1 ms, thus further reducing the duty-cycle and the average throughput and data file size.

4) RFNoC Crossbar Backpressuring: The RFNoC crossbar is a "smart" bus that links different CEs, relying on the VITA Radio Transport (VRT [31]), and Condensed Hierarchical Datagram for RFNoC (CHDR, [32]) transport protocols and the AXI communication interface. VRT defines a radio transport-layer protocol that facilitates signal and context data (timing) sharing between or within radio frequency equipment. CHDR is a protocol that defines the fundamental unit of data transfer in an RFNoC network.

The crossbar controls the sample by sample transfer between different RFNoC CEs. An important consideration is that the RFNoC crossbar can interrupt a stream of samples between a transmitting CE and a receiving CE for several clock periods when the crossbar is adjusting to cope with the high data throughput. This phenomenon is also known as backpressuring.

However, such an interruption will cause a shift in the samples' timestamps. Therefore, we added logic in the design to monitor when these streaming interrupts happen. For each acquisition period, the start of the data transfer from the RF frontends and the number of clock periods of interruption is inserted as metadata in the received packet. This information can then be used offline to correct for any mismatch, in particular when ranging is based on ToA techniques which require all hardware delays to be fixed.

5) Received Packet Format: A received ranging packet contains 30 samples of metadata consisting of: ten samples of header, seven samples of timing and packet context, and 13 samples which are currently not filled in, see Fig. 5.

ADDR 0-9	ADDR 10	ADDR 11		ADDR 25	ADDR 26	ADDR 27	ADDR 28	ADDR 29
Header	Period Counter (1 ms)	1rst Sample Time (ns)		1PPS Counter (s)	Sync. Reference Time (ns)	Actual Trigger Time (ns)	Crossbar GAPs count	Ranging Packet Size
Value					ASYNC	ASYNC		
0xAAAA								

Fig. 5. For each received packet a header of 30 samples contains context metadata of the acquisition. The header is inserted by the rxBursts-CE.

D. Development of the Asynchronous Receiver

The rxBursts-CE only enables burst acquisition in a synchronized ranging/communication scenario, i.e., in case the transmitter and receiver are synchronized to the same reference.

In a realistic situation, there is no time-frequency synchronization between the transmitter and the receiver, and the transmission and receiving windows are not deterministically aligned and are continuously sliding with respect to each other. Having the option to work in an asynchronous configuration allows for a more flexible testbed as the receiver can be mobile. Therefore, we developed the arxBursts-CE, which is based on the rxBursts-CE. The main difference is that the asynchronous CE has a Time-Unit, associated with a 512 sample length correlation-based coarse synchronizer, to align the receive window with the incoming ranging packets. Once the GNU-Radio flowgraph is launched, the CE is continuously performing a Schmidl&Cox-based correlation on the samples provided by the RF frontend [33], [34]. After ten consecutively detected synchronization frames with consistent timing, the CE will lock on the last detection time and launch the record-to-BRAM and offload-process. This detection time is also tracked and updated to keep the receive windows aligned with the transmitted bursts. The situation can be compared to the synchronous mode where the record to BRAM and the transfer-to-PC process is triggered by the 1-ms time reference pulse. An asynchronous receiver uses a GNU Radio flow graph similar to the one presented in Fig. 3, only the synchronous CE, the rxBursts, is replaced by the asynchronous one, the arxBursts.

E. Development of the Transmitter

The transmitter flowgraph in GNU Radio is illustrated in Fig. 6. It contains a file-source block which represents the samples to be streamed, the txBursts-CE which schedules and controls the periodic transmission of the ranging signal and the RFNoC Radio which represents the RF frontend.

The transmitter USRP operates as follows. The generic ranging samples are received from the host PC (raw file source) and moved into a block RAM (BRAM) memory encapsulated by the txBursts-CE, in the FPGA. These samples are then periodically streamed out through the RF frontend at a default interval of 1 ms. The ranging burst has an adjustable duration of, by default, 100 μs ($\alpha = 0.1$, 20 000 samples), and zero-valued samples are streamed for the rest of the 1-ms transmission period. This is done by using a multiplexing mechanism which first connects the output of the txBursts-CE to the output of the BRAM memory. Then when all the samples in the BRAM have been transmitted, the output of

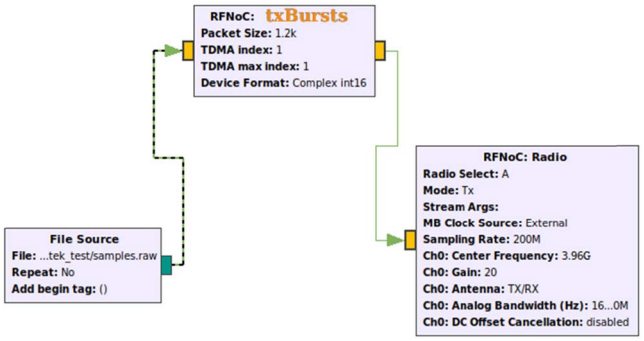

Fig. 6. Example of a GNU Radio flowgraph allowing to implement the burst transmitter.

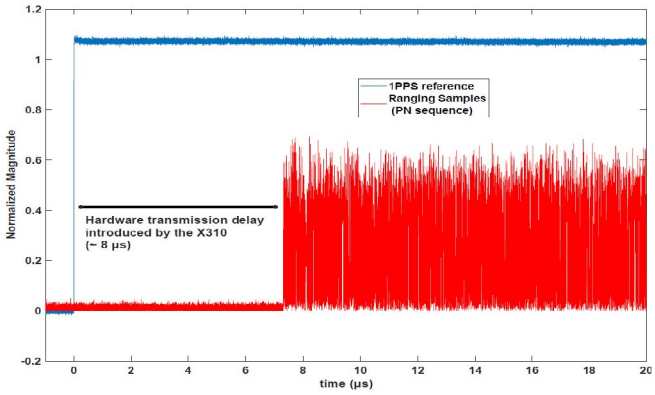

Fig. 7. Outgoing ranging samples timing (red), with reference to the 1PPS signal (blue).

the CE is connected to a still zero-value sample through the multiplexing mechanism. Thus zero-value samples will be transmitted until the next transmission period. This ensures an uninterrupted data stream between the CE and the RF frontend in order to avoid timing issues due to ON and OFF switching between streaming periods. The txBursts-CE forward ranging packets to the RF frontend with hardware generated timestamps relative to the 1PPS and the frontend time counter (*vitatime* counter). This allows transmission time synchronization with respect to the external reference and to other devices in the setup. Fig. 7 shows the transmitted signal and the 1PPS reference signal, as observed by an oscilloscope. A delay of about 8 μs between the two signals can be seen, which is caused by a constant hardware latency in the transmission chain [35] which can be calibrated out in the off-line processing afterward.

1) Architecture: The txBursts-CE has a similar architecture as the rxBursts-CE (Fig. 4). The main difference between the two blocks lies in its functionalities. The rxBursts-CE periodically receives signal samples and transfers this data to the host PC, while the txBursts-CE receives the signal samples once and periodically transfers the samples to the transmitting RF frontend. Hence, the FSM of the two CE is slightly different.

2) Time Division Multiplexing: To associate several synchronized transmitting frontends, channels or devices, code division multiplexing (CDM), or TDM within the same transmission period can be implemented by signal design, see Fig. 2(b). We have chosen to also implement a TDM transmission scheme where 1-ms transmission slots are successively allocated to different transmitters, as shown in Fig. 2 (c). By default, sample transmission is retriggered every 1 ms. When TDM is used, the transmission of the samples is retriggered every $K \times 1$ ms, where K is defining the total number of transmitters. For each transmitter, the *idx* (transmitter index) parameter, indicating the actual transmitter index in the TDM chain, and the *max idx* parameter, which corresponds to K, are configured before running the flowgraph. Referring to Section V-C3, L has to be a multiple of K.

VI. Characterization

In the following, we characterize the implemented testbed by means of some benchmark tests.

A. Packet Detection Performance

The performance of the asynchronous receiver detector is assessed by means of simulation using the receiver operating characteristics (ROC) metric [36] which links the probabilities of detection (PD) and false alarm (PFA) for different SNR and threshold values. The full detection stage was implemented in MATLAB and the computations were performed in integer format, as implemented in the hardware.

The received signal is based on the model as presented in (3). The frequency and phase offsets that occur in the asynchronous mode, are embedded in the received baseband signal variables f_D and θ_0, respectively. In the simulations, the frequency offset is randomly chosen between 0 and 10 kHz, which corresponds to values observed in practice. For the assessment, 1000 simulations are run. For each simulation, a random noise signal, frequency offset, and phase offset are generated. The ROC characteristic is presented in Fig. 8(a). Synchronization performance can be optimized by carefully adjusting the threshold value. As indicated before, for initial synchronization, the detection stage of the CE waits for ten consecutive positive detection events with consistent timing before providing the actual trigger to start the arxBursts-CE signals' recording and transfer process. This avoids locking on false positives in the initial phase. For instance, with SNR $=$ 15 dB and $P_D = 0.8$, $P_{\text{FA}} = 0.5$, the probability of having ten consecutive false positives spaced by the 1-ms bursts period is $P_{FA}^{10} \approx 0.001$, the probability of correctly locking to ten consecutive bursts is $P_D^{10} \approx 0.1$.

B. Dual Channel Acquisition Benchmarking

We now present transfer and storage benchmarks of the system with dual channel acquisition, where a single X310 samples incoming signals from its two channels and forward the data to a connected PC through a 10-Gb/s optical Ethernet link. Every $T_p = 1$ ms, a burst of $T_b = 125$ μs is transmitted per channel, resulting in a total data throughput between USRP and PC of 200 MB/s, as each packet per channel holds 25 000 samples (100 kB). The main interest is to monitor the number of packet drops over a substantial number of acquired packets ($>$1e6 packets on each channel) to assess the sustainability of long duration acquisition.

TABLE III
Benchmarking of Long Duration Dual Channel Acquisition

Run	1	2	3	4	5
Duration (min)	10	17	25	30	13
Total file size (GB)	125	207	300	362	155
Nbr. Packets (x1000)	1200	2040	3000	3600	1560
Losses (x1000)	0	0.08	0	0	0
Overruns	0	2	0	6	0

The host-PC is an 8-core, 3.6-GHz Intel Xeon W-2123 Dell Precision 5820, having 16 GB of RAM and running on Ubuntu 18.04. Packets forwarded by the X310 are saved on a Samsung 970 pro SSD drive that has been benchmarked to support a writing speed higher as 2.5 GB/s. The latter is well over the needed 200-MB/s throughput. Nevertheless, having an Ethernet connection and an SSD writing speed that can handle 1.25 and 2.5 GB/s, respectively, does not guarantee reliable acquisition. Indeed the OS is standard and not a real-time system tailored for high throughput data acquisition. The system was not particularly tuned, but the maximum transmission unit (MTU) was set to 9000 to allow for Jumbo Ethernet packets and the maximum socket receive buffer was set to its maximum of 2 GB. On the X310 side, an important parameter to configure is the rxBursts-CE *RFNoC spp* (samples per packet) value. This was set to 7800, close to the maximum value which is 8000. Higher *spp* values result in a higher throughput that can be delivered by the CE. Other Ethernet connections were disconnected while running the test to avoid interrupts from the network.

Table III presents the benchmark results for five different acquisition sequences of different duration, varying from 10 to 30 min. Along with the acquisition duration, we show in the table the total amount of the received data, the number of received and lost packets, and the number of overrun errors. An overrun error is sent by the X310 to the terminal when the USRP is providing more data than the PC can handle. Overruns indicate that samples are likely to be dropped between the X310 and the PC. Looking at the Table III, we can see that packet drops were only observed during the second recording session where a total of 80 packets are lost or corrupted out of 2 040 000 received packets.

Fig. 8(b) shows the flushing of the received data from RAM to SSD storage during acquisition. Over the two minutes of observation, we observe that the flushing is not deterministic, but there is a pattern of peak flushing every 11 s where an amount of data up to 1.5 GB is written to SSD. Since the whole process is controlled by the OS, packets drop and corruption are to be expected if other processes are running during acquisition.

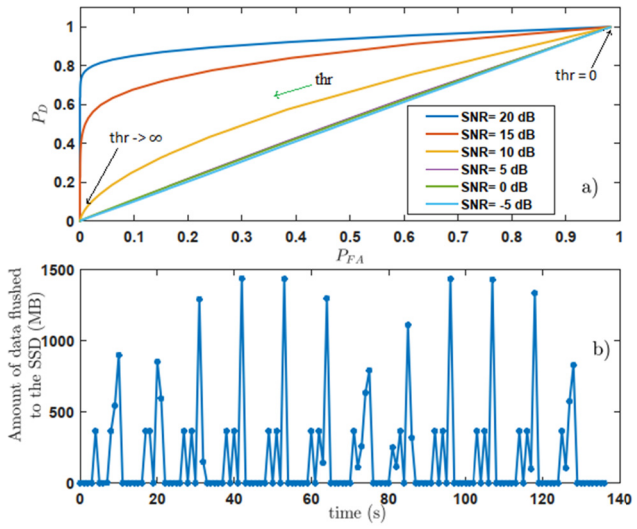

Fig. 8. (a) ROC of implemented packet synchronizer and (b) amount of data (MB) per second written to SSD during the dual channel acquisition.

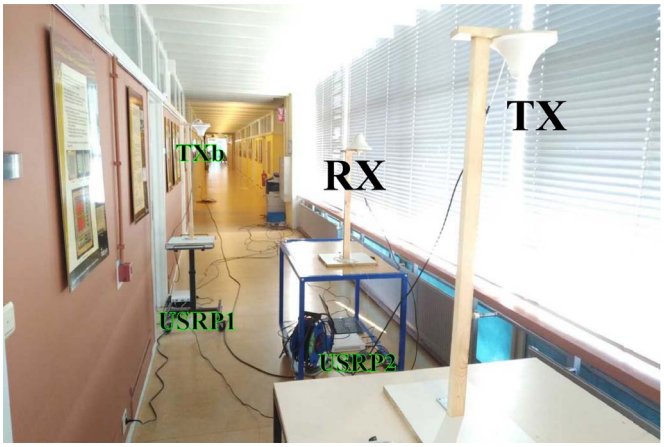

Fig. 9. Experimental setup in the corridor of the 17th floor of the Electrical Engineering, Mathematics and Computer Science (EEMCS) building of TU-Delft.

Overall, from the benchmarking presented in Table III, it can be concluded that long duration acquisition can be successfully performed in a sustainable way.

VII. ToA Ranging Experiments

The platform has been tested and validated through indoor ToA ranging experiments in a corridor located at the TU Delft campus. More experimental results using this testbed can be found in [37] and [38]. In [37], a ranging system based on the sparse selection of narrow signal bands is presented and validated using the testbed. This work aims at increasing the bandwidth occupancy efficiency using a CRLB constrained convex optimization to select the frequency bands. In [38], a positioning system using carrier phase measurements is validated using the testbed.

The setup of the current experiment is shown in Figs. 9 and 10(a) and consists of two X310 USRPs and a time-and-frequency reference source and distributor. The distributor

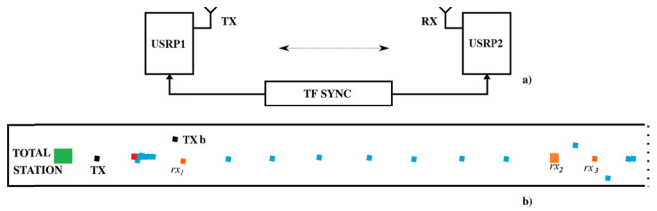

Fig. 10. (a) USRPs TX-RX configuration, (b) Corridor geometry and measurement locations: rx1, rx2 and rx3 are locations where specific CIRs where extracted for illustration.

TABLE IV
RANGING USING AN ARTIFICIAL CABLE-BASED CHANNEL

Ranging method based on	ToA	TDoA
Error (mm)	13.5	3.1
STD (mm)	8.4	1.3

provides the 1PPS and 10 MHz reference signals to the USRPs for synchronization. The first USRP (USRP1) implements a synchronized transmitter with antenna TX connected to the first RF frontend (channel 0). The transmitter streams a 160-MHz pseudorandom noise (PRN) sequence. The second USRP (USRP2) is the receiver with antenna RX, which operates on a single channel (channel 0) in synchronous mode.

The antennas are commercially available ceiling mountable Taoglas wideband antennas (bandwidth: 700 MHz–6 GHz, gain 3 dBi). The TX antenna points to the floor and is set up higher than the RX antenna, which points upward to the ceiling. The carrier frequency $f_c = 3.96$ GHz and the EIRP transmit power is about 7 dBm.

The measurement geometry is presented in Fig. 10(b). The corridor has a width of 2 m and a height of 3 m. The TX location is given in black. The receive antenna RX is moved along 32 measurements points in the corridor (indicated in blue and orange), from short range close to the transmitter, up to a distance of 23 m. A land-surveying Total Station is used to establish the ground truth distances at mm-level accuracy.

The positions of the first cluster of measurement points, close to the transmitters, are separated by less than 5 cm. A second series of measurement points, separated by about 2 m, are taken up to a distance of 23 m with respect to the TX antenna. From each measurement point the following information is extracted: signal attenuation, CIR, and the estimated distance based on ToA.

A. Channel Impairments and Multipath Components

Initial results from an RF cable-based 160-MHz artificial channel have shown that the system can achieve cm-level accuracy, using ToA and TDoA range estimates [39]. In the latter case, the channel is a single path channel without reflections and the SNR was as high as 50 dB. As indicated in Table IV, centimeter and millimeter level accuracy were, respectively, obtained in ToA- and TDoA-based ranging.

In indoor ranging the situation is less ideal because signal attenuation, impairments due to the antennas, reflections

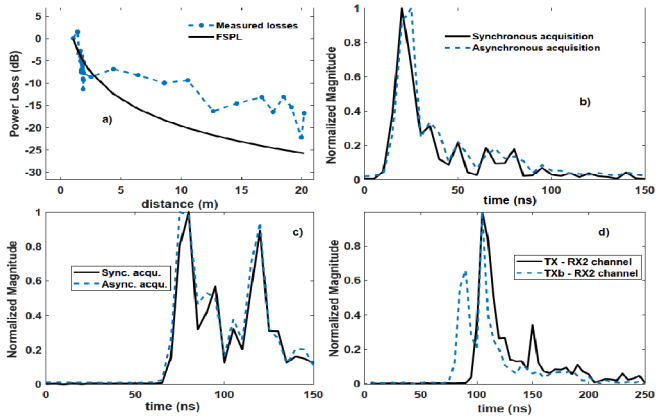

Fig. 11. (a) Power loss observed in the corridor (dashed blue) and comparison with the free space propagation loss (black), (b) Example of extracted channel response close to the transmitters (RX1), (c) Example of extracted channel response far away from the transmitter (RX3), (d) Extracted channel response at measurement location 29, TX–RX2 channel response in solid black, TXb–RX2 channel response in dashed blue, where TXb is an alternative position of the transmitter. Time delays are not representative-the two curves have been realigned to ease their comparison.

against walls and obstacles which cause multipath propagation, significantly degrade the ranging performance, even in a LoS situation. Fig. 11(a) shows the propagation loss as a function of distance. The two sets of measurement locations close (about 2 m) and far (>2 m) from the transmitter can be observed. An attenuation of about 20 dB is observed from the reference location [Fig. 10(b), in red, 1.8 m from the TX] to the furthest measurement location. Over a 23 m distance, less attenuation is observed compared to the free space path loss. This is caused by the waveguide effect due to the propagation of the signal in the corridor.

Fig. 11(b) and (c) shows extracted CIR at the rx_1 and rx_2 positions [see Fig 10(b)]. In Fig. 11(b), we can distinguish the LoS component (first peak) from the delayed multipath components (MPCs). In Fig. 11(c), at 19 m from the transmitter, the response shows two strong peaks. The first peak is due to the LoS component followed by a cluster of MPCs. The second strongest peak occurs 40 ns later and is followed by a second cluster of MPCs. Here we can also see the clear advantage of having a large signal bandwidth, which allows for separation of MPCs with small delay differences. Compared to a standard bandwidth, such as 10 MHz, which allows for a 100-ns resolution only. the LoS component would not be distinguishable from the following close-in reflections.

Fig. 11(b) and (c) shows also two CIRs obtained by a synchronous and asynchronous receiver (in black and in dashed blue, respectively). The measured CIRs for both cases are very similar but CIRs measured by the asynchronous receiver have been realigned in time to facilitate easier comparison. Fig. 11(d) shows the CIR between the TX and the receiver located at a RX2. For the same receiver location, the dashed blue curve shows a CIR in which the LoS component is not the strongest one, where the transmit antenna was placed at TXb.

B. Ranging Techniques

From the transmit time and the estimated ToA of the received signals, the propagation delay between TX and RX is estimated, and used to compute an estimate of the distance between the TX and RX antenna with $\hat{d} = c \cdot \hat{\tau}$. The ranging performance can now be assessed by comparing the range estimates to the ground truth values measured by the Total Station. In the following, we present the signal processing to obtain the ToA.

1) ToA-Based Ranging Using Cross Correlation: From the transmitted and received sequences, $s_0[k]$ and $r[k]$, respectively, we extract the discrete time CIR using the following equation:

$$h[k] = \mathrm{IFFT}\left\{\frac{R[n]}{S_0[n]}\right\} \tag{6}$$

where $R[n]$ and $S_0[n]$ are the fast Fourier transform (FFT) of the $r[k]$ and $s_0[k]$, with n the discrete frequency variable. The inverse FFT is indicated as IFFT. The ToA is estimated by performing cross correlation between the extracted channel response and a template channel response $h_{\mathrm{ref}}[k]$ extracted at a distance $d_{\mathrm{ref}} = 1$ m between transmitter and receiver. The template CIR $h_{\mathrm{ref}}[k]$ embeds impairments from the RF frontends, cables, and antennas, as well as hardware delays introduced by the transmitter and the receiver.

The sample index of the maximum of the magnitude of the cross correlation is used to determine the range estimate. In addition, we apply an oversampling (zero-padding) factor of $F_{\mathrm{ovs}} = 100$ to achieve a 50-ps bin resolution. Since the LoS or cross correlation peak is usually located in between two samples, oversampling allows to obtain the ToA estimate closer to its actual value.

At each location, $M = 10$ CIRs $h_m[k']$, are measured and used to compute an average ToA estimate $\hat{\tau}$. With $h_{\mathrm{ref}}[k']$ the reference CIR and $h_m[k']$ the mth CIR for a certain location, k' being the sample index after oversampling, the propagation delay τ between TX and RX is estimated using the cross correlation between $h_{\mathrm{ref}}[k']$ and $h_m[k']$ as

$$\hat{\tau} = \frac{T_s}{M \cdot F_{\mathrm{ovs}}} \sum_{m=0}^{M-1} \left(\arg\max_{l} \left\{ \left| \sum_{k'=0}^{\mathrm{NF_{ovs}}-1} h_{\mathrm{ref}}[k'] h_m^*[k'-l] \right| \right\} \right). \tag{7}$$

Here, l is the sample index of the maximum, $T_s = 5$ ns is the sampling period and N is the number of samples in the CIR, and $*$, used as a superscript, indicates the conjugate operator. The range estimate $\widehat{d}$, in meter, is now given by

$$\hat{d} = \hat{\tau} \cdot c + 1 \tag{8}$$

where $c = 3 \cdot 10^8$ m/s is the speed of light and the " $+1$" compensates for the $d_{\mathrm{ref}} = 1$-m reference distance. It turns out that the M ToA estimates from the CIRs $h_m[k']$ at each location show a very small standard deviation (often at the mm level) due to the high SNR at those short distances.

2) ToA-Based Ranging: Quadratic LS-Fitting: Besides the cross correlation, quadratic LS fitting, applied on the LoS component of the CIRs, is used to estimate the time delay $\widehat{\tau}$,

with

$$\hat{\tau} = \frac{T_s}{M} \sum_{m=0}^{M-1} (l_0 - l_{\text{ref}} - u_m(l_0)) \tag{9}$$

where

$$u_m(l_0) = \frac{|h_m(l_0+1)| - |h_m(l_0-1)|}{2|h_m(l_0-1)| - 4|h_m(l_0)| + 2|h_m(l_0+1)|} \tag{10}$$

with

$$l_0 = \left(\arg\max_l \{|h_m(l)|\} \right) \tag{11}$$

and

$$l_{\text{ref}} = \left(\arg\max_l \{|h_{\text{ref}}(l)|\} \right) - u_{\text{ref}} \left(\arg\max_l \{|h_{\text{ref}}(l)|\} \right) \tag{12}$$

the estimated range $\widehat{d}$ is found with (8).

3) ToA-Based Ranging Using Peak Search: Finally, we use a peak search to compute the range estimate. Since the first peak is not necessarily the highest peak, the first peak of each $h_m[k']$ above a preset threshold value is selected as the LoS path, and the sample number $\hat{l}_m$ where the LoS component crosses the threshold is selected. The sample index l_{ref} of the LoS component of $h_{\text{ref}}[k']$ is similarly determined. Now, the difference in sample number, $\hat{l}_m - l_{\text{ref}}$, is used to compute the time delay $\widehat{\tau}$ with

$$\hat{\tau} = \frac{T_s}{M \cdot F_{\text{ovs}}} \sum_{m=0}^{M-1} \left(\hat{l}_m - l_{\text{ref}} \right) \tag{13}$$

and the estimated range $\widehat{d}$ is found with (8).

C. Ranging Results

To assess the ranging accuracy in the corridor, the ToA-based range estimates are compared to the ground truth values as measured by the Total Station. Quantification of the accuracy is performed using the average error which characterizes the mean offset between the estimates and the ground truth values, which asymptotically will correspond to the range bias. Moreover, the spread in the estimates is characterized by the standard deviation of the error as well as by the average of the error magnitude.

In Fig. 12(a), the range estimates using cross correlation (in blue) and the ground truth values (in black) are plotted. A good agreement between the two curves is observed. Fig. 12(b) shows the range error ε, between the estimated and the ground truth distances. In most cases, the ranging error is at the decimeter level. The outlier of 2 m, shown in the histogram [Fig. 12(c)] corresponds to the position 22. The first set of 17 measured positions are at a distance less than 2 m from the transmitter TX, while the second set of 15 measurements is taken at distances from 2 to 23 m.

Taken over all 32 locations, the average of the error magnitude is 36.3 cm and the standard deviation is 53.9 cm (see Table V). For the first set of positions, the average of the error magnitude is 21.8 cm and the standard deviation is 17.8 cm.

The second set of positions shows the average error magnitude is 52.7 cm and the standard deviation is 66.3 cm.

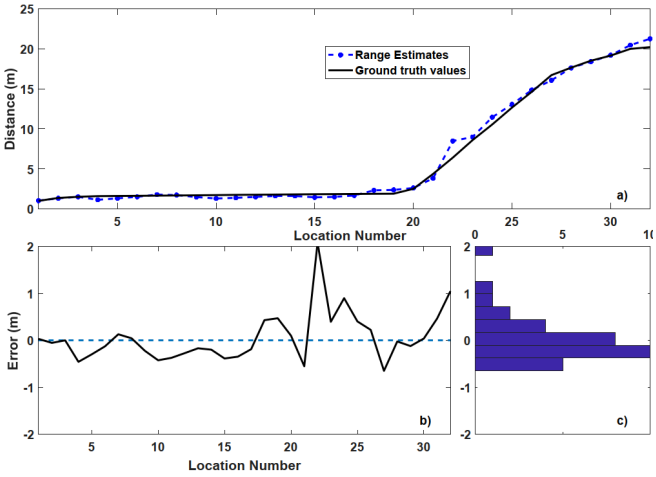

Fig. 12. (a) Comparison between the ToA range estimates and the reference ground truth values, (b) error between ToA range estimates and the ground truth values, and (c) histogram of the error.

TABLE V

TOA RANGING ERROR ε (IN cm) OVER 32 LOCATIONS, ESTIMATION BASED ON CROSS CORRELATION TECHNIQUE

	AVG(ε)	AVG($\lvert\varepsilon\rvert$)	STD(ε)
Overall	6.0	36.3	53.9
Range (< 2m)	-19.4	21.8	17.8
Range (> 2m)	34.8	52.7	66.3

TABLE VI

TOA RANGING ERROR ε (IN cm) OVER 32 LOCATIONS, ESTIMATION BASED ON LS-FITTING

	AVG(ε)	AVG($\lvert\varepsilon\rvert$)	STD(ε)
Overall	3.3	40.9	54.1
Range (< 2m)	-30.3	33.3	26.8
Range (> 2m)	41.3	49.6	52.3

The ranging performance is better for the positions at a short distance from the TX. Ranging accuracy is mainly related to the channel behavior at the measurement points. Near the transmit antenna the extracted CIRs are close to the reference CIR $h_{\text{ref}}[k']$ and the LoS path is much stronger than reflected paths, while further away from the transmitter, ranging is less immune to close-in MPCs arriving at the receiver within a few sampling periods.

D. Comparison of Cross Correlation, LS-Fitting, and Peak-Search

The range error statistics for cross correlation, LS-fitting and peak-search are shown in Tables V–VII, respectively. Comparing these results shows that the differences between the different ToA estimation techniques is small and they all achieve decimeter level accuracy, but the peak-search algorithm shows a lower standard deviation than cross correlation and LS-fitting, which show about equal performance. The peak-search algorithm, however, is sensitive to the selected

TABLE VII

TOA RANGING ERROR ε (IN cm) OVER 32 LOCATIONS, ESTIMATION BASED ON PEAK SEARCH TECHNIQUE

	AVG(ε)	AVG($\lvert\varepsilon\rvert$)	STD(ε)
Overall	-9.4	31.2	39.0
Range (< 2m)	-27.4	27.4	11.8
Range (> 2m)	11.0	35.4	48.7

TABLE VIII

TOTAL BANDWIDTH AND RANGING PERFORMANCE, ERROR IN cm

BW (MHz)	160	80	40	20	10
AVG(ε)	6	33.2	58.4	28.5	-12.0
AVG($\lvert\varepsilon\rvert$)	36.3	81.2	95.7	165.5	284.2
STD(ε)	53.9	111.4	128.35	302.4	473.8

threshold level. Here a threshold level normalized to the peak-level of 0.7 is used.

E. Effect of the Ranging Bandwidth

Finally, the effect of bandwidth on the ranging accuracy is investigated. From the initial 160-MHz channel frequency responses, we extract limited bandwidth baseband channel responses and perform ranging using the cross correlation technique as previously presented. The following bandwidths are compared: 160, 80, 40, 20, and 10 MHz. The results are shown in Table VIII.

With decreasing bandwidth from the standard deviation increases by almost a factor of 8 (from 53.9 to 473.8 cm), as predicted by the CRLB (see Section II-B) while the average of the error magnitude increases by a factor of 7 (from 36.3 to 284.2 cm).

VIII. CONCLUSION

This article presents a testbed for wideband radio signal acquisition, for validation and demonstration of high accuracy ranging and positioning. For this platform, the Ettus USRP X310 was used, which can either transmit or receive with a bandwidth of 160 MHz, simultaneously on two channels. By associating these two channels, a contiguous bandwidth of 320 MHz, or a much larger virtual bandwidth can be achieved, at a total sampling rate of 400 MSPS. At the receiver side, we particularly target data acquisition of dual channel ranging signals for further offline processing. The receiving device will record and forward samples to a connected host-PC. However, the very high sample rate results in a very high throughput, hardly sustainable even for high-end computers, a high probability of packet loss due to nondeterministic OS scheduling, and a huge data file size, rendering long duration experiments very unpractical.

To overcome this, we propose a burst mode transmission and acquisition platform. The USRP hardware units and developments that meet the acquisition requirements are discussed. The proposed platform is fully implemented and allows for accurate time-deterministic experiments that can be run for longer duration (more than 1 h, depending on the available memory). The system can be used to perform positioning experiments as several USRPs can operate synchronously. The platform also supports asynchronous operation where all transmitters are synchronized, but the receiver runs on an independent clock, like a regular mobile user.

The synchronization performance in noncoherent mode has been benchmarked as well as reliable data acquisition and data transfer in dual channel operation. Indoor ranging experiments, based on ToA, were performed using a PRN sequence with a bandwidth of 160 MHz as a ranging signal. The ranging accuracy was assessed by comparing the range estimates for three detection schemes: cross correlation, LS-fitting, and peak-search, with the ground truth values obtained by a land-surveying Total Station. The results show a decimeter level accuracy, where the peak-search algorithm (with a range error standard deviation of $\sigma_\varepsilon = 39$ cm) outperformed cross correlation and LS-fitting.

Thanks to the wide bandwidth and related high time resolution, the testbed can be used to perform research on ranging and positioning in dense multipath environments. Accurate time-frequency references are needed for synchronization. The platform, in this article, has been developed within the scope of the SuperGPS project and uses WR timing nodes connected to an optical network to provide and distribute a time-frequency reference with 100-ps level uncertainty.

With accurate time-frequency references available, signal designs and ranging algorithms toward centimeter or even millimeter-level accuracy can be assessed. Such techniques could rely on multiband signals. The platform is also suitable to perform CIR measurements at multiple signal bands simultaneously. With small changes in the developed hardware, this setup can also support two-way ranging.

REFERENCES

[1] E. Schmidt, Z. Ruble, D. Akopian, and D. J. Pack, "Software-defined radio GNSS instrumentation for spoofing mitigation: A review and a case study," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 8, pp. 2768–2784, Aug. 2019, doi: 10.1109/TIM.2018.2869261.

[2] J. Barnes, C. Rizos, M. Kanli, and A. Pahwa, "A positioning technology for classically difficult GNSS environments from locata," in *Proc. IEEE/ION Position, Location, Navigat. Symp.*, Coronado, CA, USA, 2006, pp. 715–721, doi: 10.1109/PLANS.2006.1650665.

[3] K.-M. Mimoune, I. Ahriz, and J. Guillory, "Evaluation and improvement of localization algorithms based on UWB pozyx system," in *Proc. Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Split, Croatia, Sep. 2019, pp. 1–5, doi: 10.23919/SOFTCOM.2019.8903742.

[4] G. Kahe and F. Masoumi Ganjgah, "MAKAN: A low-cost low-complexity local positioning system," *Navigation*, vol. 66, no. 2, pp. 401–415, Jun. 2019, doi: 10.1002/navi.308.

[5] K. Shamaei, J. Khalife, and Z. M. Kassas, "Exploiting LTE signals for navigation: Theory to implementation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2173–2189, Apr. 2018.

[6] S. M. Kay, "Fundamentals of statistical signal processing," in *Estimation Theory*, vol. 1. Upper Saddle River, NJ, USA: Prentice-Hall, 1993, p. 53.

[7] J. R. G. Oya, F. Munoz, A. Torralba, A. Jurado, A. J. Garrido, and J. Banos, "Data acquisition system based on subsampling for testing wideband multistandard receivers," *IEEE Trans. Instrum. Meas.*, vol. 60, no. 9, pp. 3234–3237, Sep. 2011, doi: 10.1109/TIM.2011.2128710.

[8] M. Cervetto, E. Marchi, and C. G. Galarza, "A fully-configurable SoC-based IR-UWB platform for data acquisition and algorithm testing," *IEEE Embedded Syst. Lett.*, early access, May 26, 2020, doi: 10.1109/LES.2020.2997660.

[9] *HackRF One SDR*. Accessed: Mar. 17, 2021. [Online]. Available: https://greatscottgadgets.com/hackrf/one/

[10] *Aaronia Sprectan V6 SDR*. Accessed: Mar. 17, 2021. [Online]. Available: https://aaronia-shop.com/products/spectran-v6-rsa-500x

[11] T. Xie, C. Zhang, and Z. Wang, "Wi-Fi TDoA indoor localization system based on SDR platform," in *Proc. IEEE Int. Symp. Consum. Electron. (ISCE)*, Kuala Lumpur, Malaysia, Nov. 2017, pp. 82–83.

[12] J. Khalife, K. Shamaei, and Z. M. Kassas, "A software-defined receiver architecture for cellular CDMA-based navigation," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Savannah, GA, USA, Apr. 2016, pp. 816–826, doi: 10.1109/PLANS.2016.7479777.

[13] F. Wolf, J.-B. Doré, X. Popon, S. D. Rivaz, F. Dehmas, and J.-P. Cances, "Coherent multi-channel ranging for narrowband LPWAN: Simulation and experimentation results," in *Proc. 15th Workshop Positioning, Navigat. Commun. (WPNC)*, Oct. 2018, pp. 1–6.

[14] Y. C. Eldar and T. Michaeli, "Beyond bandlimited sampling," *IEEE Signal Process. Mag.*, vol. 26, no. 3, pp. 48–68, May 2009, doi: 10.1109/MSP.2009.932125.

[15] M. Mishali and Y. Eldar, "Sub-nyquist sampling," *IEEE Signal Process. Mag.*, vol. 28, no. 6, pp. 98–124, Nov. 2011, doi: 10.1109/MSP.2011.942308.

[16] *Crimson TNG SDR*. Accessed: Mar. 17, 2021. [Online]. Available: https://www.pervices.com/documentation-tng/

[17] S. Prager, M. S. Haynes, and M. Moghaddam, "Wireless subnanosecond RF synchronization for distributed ultrawideband software-defined radar networks," *IEEE Trans. Microw. Theory Techn.*, vol. 68, no. 11, pp. 4787–4804, Nov. 2020, doi: 10.1109/TMTT.2020.3014876.

[18] C. Rizos and L. Yang, "Background and recent advances in the locata terrestrial positioning and timing technology," *Sensors*, vol. 19, no. 8, p. 1821, Apr. 2019.

[19] P. Moreira, J. Serrano, T. Wlostowski, P. Loschmidt, and G. Gaderer, "White rabbit: Sub-nanosecond timing distribution over Ethernet," in *Proc. Int. Symp. Precis. Clock Synchronization Meas., Control Commun.*, Brescia, Italy, Oct. 2009, pp. 1–5, doi: 10.1109/ISPCS.2009.5340196.

[20] E. Dierikx *et al.*, "Optical fiber trans-national time transfer for comparing two UTC realisations," in *Proc. Joint Conf. IEEE Int. Freq. Control Symp. Eur. Freq. Time Forum (EFTF/IFC)*, Orlando, FL, USA, Apr. 2019, pp. 1–2, doi: 10.1109/FCS.2019.8856091.

[21] N. Sotiropoulos, C. M. Okonkwo, R. Nuijts, H. de Waardt, and J. C. J. Koelemeij, "Delivering 10 Gb/s optical data with picosecond timing uncertainty over 75 km distance," *Opt. Exp.*, vol. 21, no. 26, pp. 32643–32654, 2013.

[22] C. Diouf, H. Dun, T. Kazaz, G. Janssen, and C. Tiberius, "Demonstration of a decimeter-level accurate hybrid optical-wireless terrestrial positioning system," in *Proc. 33rd Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS)*, Oct. 2020, pp. 2220–2228.

[23] A. Williams, "UHD streaming with DPDK: Raising the throughput ceiling with drivers in user space," in *Proc. GNU Radio Conf.*, Huntsville, AL, USA, Sep. 2019. Accessed: Mar. 17, 2021. [Online]. Available: https://www.gnuradio.org/grcon/grcon19/presentations/UHD_Streaming_with_DPDK_Raising_the_Throughput_Ceiling_with_Drivers_in_User_Space/

[24] S. Gallenmüller, P. Emmerich, F. Wohlfart, D. Raumer, and G. Carle, "Comparison of frameworks for high-performance packet IO," in *Proc. ACM/IEEE Symp. Archit. Netw. Commun. Syst. (ANCS)*, Oakland, CA, USA, May 2015, pp. 29–38, doi: 10.1109/ANCS.2015.7110118.

[25] S. Prager, T. Thrivikraman, M. S. Haynes, J. Stang, D. Hawkins, and M. Moghaddam, "Ultrawideband synthesis for high-range-resolution software-defined radar," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 6, pp. 3789–3803, Jun. 2020, doi: 10.1109/TIM.2019.2937423.

[26] H. Nelson. *UHD 4.0 Announcement*. Accessed: Mar. 17, 2021. [Online]. Available: https://www.ettus.com/announcing-uhd4/

[27] M. Abirami, V. Hariharan, M. B. Sruthi, R. Gandhiraj, and K. P. Soman, "Exploiting GNU radio and USRP: An economical test bed for real time communication systems," in *Proc. 4th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Tiruchengode, India, Jul. 2013, pp. 1–6, doi: 10.1109/ICCCNT.2013.6726630.

[28] L. Benini and G. De Micheli, "Networks on chips: A new SoC paradigm," *Computer*, vol. 35, no. 1, pp. 70–78, 2002, doi: 10.1109/2.976921.

[29] M. Braun and J. Pendlum, "A flexible data processing framework for heterogeneous processing environments: RF network-on-chip," in *Proc. Int. Conf. FPGA Reconfiguration Gen.-Purpose Comput. (FPGA4GPC)*, Hamburg, Germany, 2017, pp. 1–6.

[30] *RF Network-On-Chip (RFNoC) Getting Started*. Accessed: Mar. 17, 2021. [Online]. Available: https://kb.ettus.com/Getting_Started_with_RFNoC_Development

[31] T. Cooklev, R. Normoyle, and D. Clendenen, "The VITA 49 analog RF-digital interface," *IEEE Circuits Syst. Mag.*, vol. 12, no. 4, pp. 21–32, 4th Quart., 2012, doi: 10.1109/MCAS.2012.2221520.

[32] *RF Network-On-Chip (RFNoC) Specification*. [Online]. Available: https://files.ettus.com/app_notes/RFNoC_Specification.pdf

[33] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Commun.*, vol. 45, no. 12, pp. 1613–1621, Dec. 1997, doi: 10.1109/26.650240.

[34] X. Mei, Z. Ding, and L. Pan, "FPGA implementation of frame synchronization in burst OFDM communication based on IEEE802.11a," in *Proc. 8th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Shanghai, China, Sep. 2012, pp. 1–4, doi: 10.1109/WiCOM.2012.6478525.

[35] N. B. Truong, Y.-J. Suh, and C. Yu, "Latency analysis in GNU radio/USRP-based software radio platforms," in *Proc. MILCOM IEEE Mil. Commun. Conf.*, San Diego, CA, USA, Nov. 2013, pp. 305–310, doi: 10.1109/MILCOM.2013.60.

[36] S. M. Kay, "Fundamentals of statistical signal processing," in *Detection Theory* (Prentice-Hall Signal Processing Series), vol. 2. Upper Saddle River, NJ, USA: Prentice-Hall, 1993, p. 74.

[37] H. Dun, C. C. J. M. Tiberius, C. Diouf, and G. J. M. Janssen, "Sparse signal bands selection for precise time-based ranging in terrestrial positioning," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Portland, OR, USA, Apr. 2020, pp. 1372–1380, doi: 10.1109/PLANS46316.2020.9110197.

[38] H. Dun, C. C. J. M. Tiberius, C. Diouf, and G. J. M. Janssen, "Terrestrial precise positioning system using carrier phase from burst signals and optically distributed time and frequency reference," in *Proc. Int. Tech. Meeting Inst. Navigat.*, Feb. 2021, pp. 510–524, doi: 10.33012/2021.17846.

[39] C. Diouf, G. J. M. Janssen, T. Kazaz, H. Dun, F. Chamanzadeh, and C. C. J. M. Tiberius, "A 400 Msps SDR platform for prototyping accurate wideband ranging techniques," in *Proc. 16th Workshop Positioning, Navigat. Commun. (WPNC)*, Bremen, Germany, Oct. 2019, pp. 1–6, doi: 10.1109/WPNC47567.2019.8970251.

Cherif Diouf received the Ph.D. degree in system modeling of electronic circuits from the Université de Bretagne Occidentale, Brest, France, in 2014.

He later carried out research on optical communication and seabed power-over-fiber systems. More recently, he was an Embedded Systems Engineer on deep-sea autonomous floats at the French Oceanographic Institute. He is currently working with the Department of Geoscience and Remote Sensing, Delft University of Technology, Delft, The Netherlands, on the development of an accurate optical-wireless terrestrial positioning system demonstrator.

Gerard J. M. Janssen (Member, IEEE) received the Ph.D. degree from the Delft University of Technology, Delft, The Netherlands, in 1998.

He is currently an Associate Professor with the Circuits and Systems Group, Delft University of Technology. His research interests include wireless communication, particularly narrowband multiuser detection, digital modulation techniques, channel modeling, diversity techniques, and ultra wideband communications and positioning.

Han Dun received the B.Sc. degree in communication engineering and the M.Sc. degree in communication and information engineering from Shanghai University, Shanghai, China, in 2013 and 2016, respectively. He is currently pursuing the Ph.D. degree with the Department of Geoscience and Remote Sensing, Delft University of Technology, Delft, The Netherlands.

From 2013 to 2016, he also worked at the Key Laboratory of Specialty Fiber Optics and Optical Access Network, Shanghai University, where he contributed to the real-time optical OFDM-PON. His research interests include wireless localization, and statistical signal processing.

Tarik Kazaz received the M.Sc. degree (*cum laude*) in electrical engineering from the Department for Telecommunications, University of Sarajevo, Sarajevo, Bosnia and Herzegovina, in 2012. He is currently pursuing the Ph.D. degree with the Circuits and Systems Research Group, Delft University of Technology (TU Delft), Delft, The Netherlands.

In 2013, he joined BH Mobile, where he was a Radio Access Network Engineer, while at the same time he was a Part Time Teaching Assistant at the Faculty of Electrical Engineering, University of Sarajevo. In 2015, he joined the Department of Information Technology, Ghent University, as a Ph.D. Researcher. He was active in several national and international research projects including EU H2020 ORCA, WiSHFUL, iMinds' IoT Strategic Research Program and NWO SuperGPS. His main research interests are wireless networks, signal processing for communications, software defined radio and cognitive radio, and hardware-software co-design.

Christian C. J. M. Tiberius received the Ph.D. degree from the Delft University of Technology, Delft, The Netherlands, in 1998, with a focus on recursive data processing for kinematic GPS surveying.

He is currently an Associate Professor with the Geoscience and Remote Sensing (GRS) Department, Delft University of Technology. His research interest lies in navigation, with GNSS and high-accuracy terrestrial radio positioning.