ARL-TR-9837 • Nov 2023

DEVCOM ARMY RESEARCH LABORATORY

A Real-Time Software-Defined Radio Two-Way Ranging Protocol

by Mitchell J Grabner and Michael L Don

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-TR-9837 ● Nov 2023

A Real-Time Software-Defined Radio Two-Way Ranging Protocol

by Mitchell J Grabner and Michael L Don
DEVCOM Army Research Laboratory

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
November 2023	Technical Report	October 2020–October 2022

4. TITLE AND SUBTITLE
A Real-Time Software-Defined Radio Two-Way Ranging Protocol

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Mitchell J Grabner and Michael L Don

5d. PROJECT NUMBER
AH80

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
DEVCOM Army Research Laboratory
ATTN: FCDD-RLA-WE
Aberdeen Proving Ground, MD 21005-5066

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-9837

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
In this technical report, we develop a real-time software-defined radio two-way ranging (TWR) protocol on Ettus Research Universal Software Radio Peripheral (USRP) devices using the USRP Hardware Driver application programming interface. TWR is useful in providing ranging and localization to low-power devices such as unmanned aerial vehicles and embedded sensor nodes that may be deployed in environments where global positioning system is unavailable. The TWR protocol is tested in both controlled and real-world environments, and the results are verified against simulation data. The protocol is capable of a 2-m range accuracy using a narrow bandwidth of only 2 MHz.

15. SUBJECT TERMS
two-way ranging, software-defined radio, localization, synchronization, wireless communications, Weapons Sciences

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Michael L Don
Unclassified	Unclassified	Unclassified	UU	56	19b. TELEPHONE NUMBER (Include area code) 443-846-9550

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures iv

List of Tables vi

1. Introduction 1

2. Overview of TWR 2

3. USRP Hardware Overview 5

4. Timed Sampling in UHD 8

5. Ranging Signal Construction 10

6. Modulation Technique 11

7. Loopback Calibration Procedure 12

8. Transmitter Procedure 14

9. Receiver Procedure 16

10. Range Calculation 18

11. Experimental Results 19

12. Conclusion 42

13. References 43

List of Symbols, Abbreviations, and Acronyms 46

Distribution List 48

List of Figures

Fig. 1 Illustration of a simple TWR protocol ……3

Fig. 2 Illustration of CPC on a square wave ranging signal. The top signal is the initial message from device A. The next signal is at device B, which includes the phase offset due to the travel time from A to B and a clock offset. The bottom signal is the returned signal at device A with the clock offset removed. ……4

Fig. 3 Block diagram of the analog device AD9364 RFIC[17] ……6

Fig. 4 Block diagram of the analog device AD9361 RFIC[17] ……6

Fig. 5 Block diagram of the USRP B200 device[18]……7

Fig. 6 Block diagram of the USRP E312 device[19]……7

Fig. 7 Illustration of the time delays seen in the SDR caused by the RFFE ….. 10

Fig. 8 Block diagram of the loopback calibration procedure …… 14

Fig. 9 Block diagram of the ranging transmitter procedure…… 16

Fig. 10 Block diagram of the unlocked ranging receiver procedure. …… 17

Fig. 11 Block diagram of the locked ranging receiver procedure …… 18

Fig. 12 The USRP E312 devices used for experimentation.…… 20

Fig. 13 The USRP B200 devices used for experimentation …… 21

Fig. 14 Experimental TWR distance estimate samples compared to the true distance of 1.55 m…… 22

Fig. 15 Experimental TWR distance estimate sample errors for a distance of 1.55 m …… 22

Fig. 16 Simulation TWR distance estimate samples compared to the true distance of 1.55 m…… 23

Fig. 17 Simulation TWR distance estimate sample errors for a distance of 1.55 m …… 23

Fig. 18 Experimental TWR distance estimate samples compared to the true distance of 2.46 m…… 24

Fig. 19 Experimental TWR distance estimate sample errors for a distance of 2.46 m …… 24

Fig. 20 Simulation TWR distance estimate samples compared to the true distance of 2.46 m…… 25

Fig. 21 Simulation TWR distance estimate sample errors for a distance of 2.46 m …… 25

Fig. 22 Experimental TWR distance estimate samples compared to the true distance of 3.68 m..... 26
Fig. 23 Experimental TWR distance estimate sample errors for a distance of 3.68 m 26
Fig. 24 Simulation TWR distance estimate samples compared to the true distance of 3.68 m..... 27
Fig. 25 Simulation TWR distance estimate sample errors for a distance of 3.68 m 27
Fig. 26 Experimental TWR distance estimate samples compared to the true distance of 18.92 m 28
Fig. 27 Experimental TWR distance estimate sample errors for a distance of 18.92 m 28
Fig. 28 Simulation TWR distance estimate samples compared to the true distance of 18.92 m 29
Fig. 29 Simulation TWR distance estimate sample errors for a distance of 18.92 m 29
Fig. 30 Experimental and simulation distance estimate mean compared to the true distance for all trials 30
Fig. 31 Simulation TWR distance estimate samples compared to the true distance of 18.92 m for 400 length and 511 length Gold codes..... 30
Fig. 32 Simulation TWR distance estimate sample errors for a distance of 18.92 m for 400 length and 511 length Gold codes 31
Fig. 33 Experimental TWR distance estimate samples compared to the true distance of 18.92 m using 511 maximal length Gold codes 31
Fig. 34 Experimental TWR distance estimate sample errors for a distance of 18.92 m using 511 maximal length Gold codes..... 32
Fig. 35 Outdoor TWR test location and procedure..... 34
Fig. 36 Experimental TWR distance estimate samples compared to the true distance of 1 to 62.5 m 34
Fig. 37 Simulation TWR distance estimate samples compared to the true distance of 1 to 62.5 m 35
Fig. 38 Experimental TWR distance estimate samples compared to the true distance of 1 to 62.5 m 35
Fig. 39 Simulation TWR distance estimate samples compared to the true distance of 1 to 62.5 m 36
Fig. 40 Outdoor "Road Test" TWR test location and procedure..... 37

Fig. 41 Experimental TWR distance estimates versus the true distance 38
Fig. 42 Experimental TWR distance estimates versus range reliability..... 39
Fig. 43 Experimental TWR distance estimates with reliability greater than 80% 39

List of Tables

Table 1 Transmit metadata parameters in UHD 8
Table 2 Stream command parameters in UHD.....8
Table 3 Additional parameters in receive metadata in UHD 9
Table 4 Intrinsic loopback calibration offset parameters saved in the ranging structure 14
Table 5 Round-trip parameters saved into the ranging structure by the transmitter..... 15
Table 6 Controlled experiment system parameters..... 19
Table 7 Outdoor multipath experiment system parameters..... 33
Table 8 Outdoor "Road Test" system parameters..... 37

1. Introduction

Two-way ranging (TWR) is a popular radio frequency (RF) ranging method for low-cost and low-power devices as it removes the need for expensive clock references and synchronization hardware.[1] The simplicity of the protocol allows ranging measurements to be integrated into low-power devices such as unmanned aerial vehicles and embedded sensor nodes. Localization algorithms can use ranging measurements to provide positioning[2–5] in scenarios where localization is traditionally difficult and global positioning system (GPS) may be unavailable.

Software-defined radio (SDR) implementations are a way to further simplify the problem of integrating various system components by defining radio physical and network layer functionality in simple software interfaces that run on a wide variety of hardware from low-power embedded processors to high-power x86 workstations. The SDR implementation can be expanded or modified and redeployed quickly without any direct hardware changes to the radio. In previous research, the US Army Combat Capabilities Development Command Army Research Laboratory used the versatility of SDRs for custom telemetry applications[6–9] and RF angle of arrival measurement.[10]

In this report we discuss the implementation of a custom TWR protocol using the Ettus Research Universal Software Radio Peripheral (USRP) Hardware Driver (UHD) on the embedded series E312 and the bus series B200 devices.[11] The remainder of this report is structured as follows: Section 2 briefly discusses the theory of TWR using RF signals. Section 3 describes the SDR hardware used in this research and their host software interfaces. Section 4 discusses the foundational implementation concerns of timed transmission in a UHD context. Section 5 explains the methods of constructing a useful ranging signal for RF TWR. Section 6 discusses the system's modulation scheme for a low-power embedded system. Section 7 discusses the critical problem of SDR hardware delays and a method to overcome them using a calibration procedure. Section 8 details the TWR protocol from the transmitter device perspective. Section 9 explains the TWR protocol from the receiver device perspective. Section 10 describes the final range calculation procedure on the transmitter. Section 11 details two experiments used to quantify the performance of the TWR method and compares these results to simulation. Performance problems are identified and methods to address them are discussed. Section 12 summarizes

the research and outlines key research questions to address in future work.

2. Overview of TWR

A TWR protocol is a conceptually simple ranging procedure that measures the distance between two devices using the time it takes a message traveling the speed of light $c \approx 3 \times 10^8$ m/s to make a round trip from one agent to the other and back again. The procedure can be expressed mathematically for two devices A and B as

$$d_{TWR} = \frac{t_{AB} + t_{BA}}{2} \times c, \tag{1}$$

where the travel time in seconds from device A to device B is t_{AB} and the travel time in seconds from device B to device A is t_{BA}. Unless device B is a perfect reflector (i.e., it can reflect the incoming ranging signal instantly), there will be some processing delay t_p on device B before a response is sent back to A. This changes our TWR equation to

$$\tilde{d}_{TWR} = \frac{t_{AB} + t_p + t_{BA}}{2} \times c. \tag{2}$$

Obviously, t_p is a source of error in the range calculation unless compensated for by the transmitter device A. The most straightforward approach is to set t_p to a known value by introducing a fixed delay that gives enough time for processing. t_p can then simply be removed after the response has been received by

$$\hat{d}_{TWR} = \frac{t_{AB} + t_{p/B} + t_{BA} - t_{p/A}}{2} \times c. \tag{3}$$

The processing delay applied by device B is $t_{p/B}$ and the same time offset subsequently removed by device A is $t_{p/A}$. If the two t_p times do not match exactly, ranging error will occur. An illustration of a simple TWR protocol can be seen in Fig. 1.

The most attractive feature of TWR is the removal of time synchronization requirements and highly accurate time references. One-way ranging or time of flight protocols like those used in GPS outfit the transmitting satellites with extremely accurate atomic clocks because of this requirement. By using TWR, both transmitting and receiving devices can have inexpensive commercial oscillators.

The consequence of unsynchronized ranging devices is that the sample clocks and

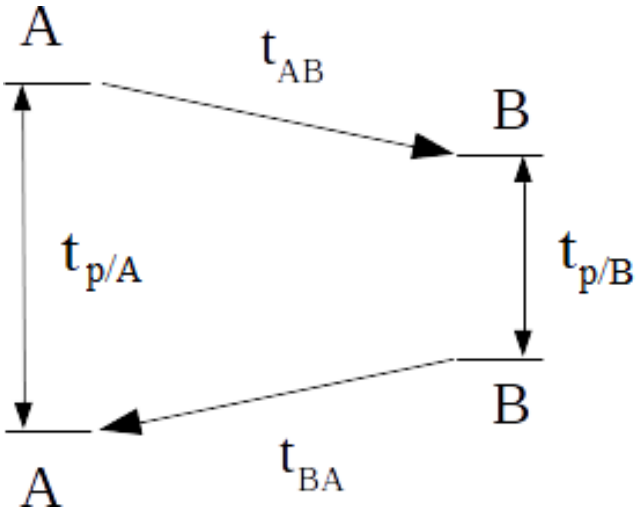

Fig. 1 Illustration of a simple TWR protocol

local times of each device are not guaranteed to be aligned in any way, requiring some additional processing to compensate for this discrepancy.[12] This compensation can be achieved by the receiver/responder device, without simultaneous transmission,[13] by applying a simple circular shift to the incoming ranging signal before responding. If the mathematical representation of clock phase offset is θ_{clk} and the phase difference caused by the travel time t_{AB} is θ_{AB} the circular shifting operation can be described as

$$x_{shift} = xe^{j(\theta_{AB}+\theta_{clk})} \tag{4}$$

where the baseband received, demodulated ranging message is x. The transmitter, who has a clock phase offset of $-\theta_{clk}$ relative to the receiver/responder, will remove this offset after sampling and downconversion to baseband, leaving θ_{AB} and θ_{BA} present in the demodulated response. If x_{AB} is the transmitted ranging signal, then the received ranging signal x_{BA} can be described as

$$x_{BA} = x_{AB}e^{j(\theta_{AB}+\theta_{BA})}. \tag{5}$$

The total round-trip phase difference $\theta_{tot} = \theta_{AB} + \theta_{BA}$ can be resolved in the range $[-\pi, \pi)$. θ_{tot} can be computed from the phase difference of the received signal x_{BA} relative to a x_{ref} signal in the frequency domain using a real-valued discrete Fourier transform (DFT) according to

$$\theta_{tot} = \text{atan}(\max(X_{BA})) - \text{atan}(\max(X_{ref})), \tag{6}$$

where X_{BA} and X_{ref} are the frequency domain representations of x_{AB} and x_{ref} respectively, given by

$$X[k] = \sum_{n=0}^{N-1} x[n] e^{-\frac{2\pi i}{N} kn}, \tag{7}$$

where $\{0 \leq k \leq 2/N - 1\}$ since the real valued DFT is even symmetric. Since this phase difference does not give sample delay information, which is needed to resolve the time difference according to our sample rate, the phase change resulting from a single sample offset, θ_{single}, is computed offline to resolve the total phase in terms of fractional samples. Using this variable, the phase total can be converted to factional samples using $s_{phase} = \theta_{tot}/\theta_{single}$ and converted to time using the sampling rate F_s by $t_{phase} = s_{phase}/F_s$. Thus, if we assume processing delay is accounted for as in equation 3, the TWR distance with clock phase correction (CPC) is

$$d_{CPC} = \frac{t_{phase}}{2} \times c. \tag{8}$$

If the phase calculations are not accurate, large range errors can occur. The most common sources of error in these calculations can be attributed to noise and multipath channel effects,[14,15] but sample quantization and machine precision can also play a part.[16] An illustration of the basics of CPC TWR can be seen in Fig. 2.

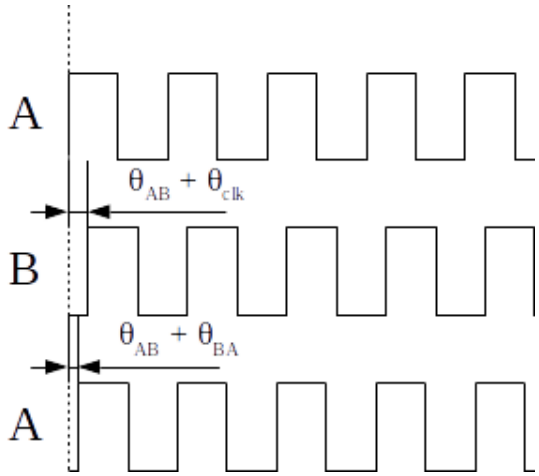

Fig. 2 Illustration of CPC on a square wave ranging signal. The top signal is the initial message from device A. The next signal is at device B, which includes the phase offset due to the travel time from A to B and a clock offset. The bottom signal is the returned signal at device A with the clock offset removed.

3. USRP Hardware Overview

The SDR hardware used in this report consists of the Ettus USRP B200 as well as the E312. Both devices are capable of tuning to a center frequency from 70 MHz to 6 GHz allowing them to cover most licensed and unlicensed frequency bands. The analog devices AD9364 and AD9361 radio frequency integrated circuits (RFICs) on the B200 and E312, respectively, are capable of up to 56-MHz instantaneous bandwidth while the on-board Xilinx field-programmable gate arrays (FPGAs) are capable of streaming up to 61.44 megasamples per seconds (MSps). The high-level block diagram of both RFICs can be seen in Fig. 3 and Fig. 4. We can see from these diagrams that the AD9361 in the E312 is also capable of phase-coherent multiple-input multiple-output operation thanks to the common local oscillator connection on the two TX and two RX ports.

The B200 device uses a SuperSpeed USB3 bus connection and requires a host computer to perform baseband signal processing while the E312 is equipped with an on-board ARM Cortex A9 dual-core CPU processor clocked at 866 MHz. Therefore, the actual baseband signal bandwidth is limited by the transport connection between the SDR device and the host processor. The USB3 protocol max transfer rate of 5 Gbps allows for up to 100 MSps while the AXI connection to the ARM processor is limited to 10 MSps. Lastly, the host CPU is the final limiting factor in signal bandwidth, limiting the sample rate based on the processor's ability to read samples from the transport and apply baseband signal processing. The system level block diagrams for both the B200 and E312 devices can be seen in Fig. 5 and Fig. 6, respectively.

For this report, we found that the host CPU on the E312 limits the sample rate to around 2 MSps for any significant signal processing tasks, such as TWR. Higher sample rates are possible on a host x86 CPU using the B200 devices, but signal processing problems discussed later in Section 11 limit their usefulness.

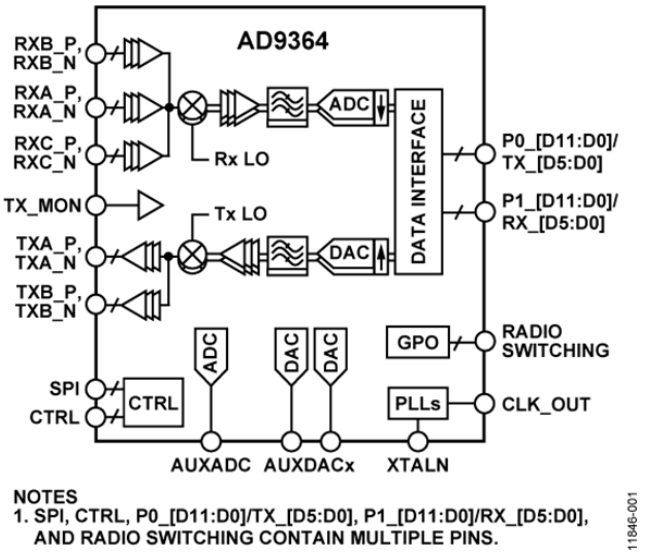

Fig. 3 Block diagram of the analog device AD9364 RFIC[17]

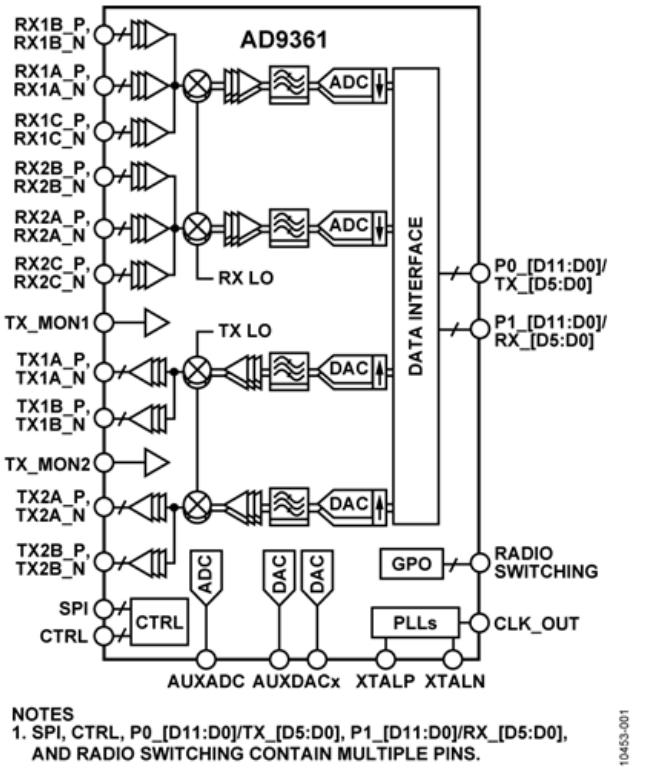

Fig. 4 Block diagram of the analog device AD9361 RFIC[17]

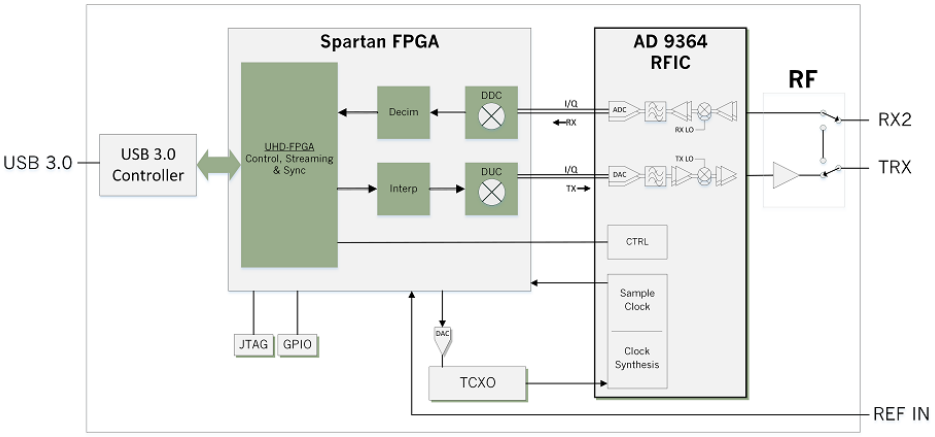

Fig. 5 Block diagram of the USRP B200 device[18]

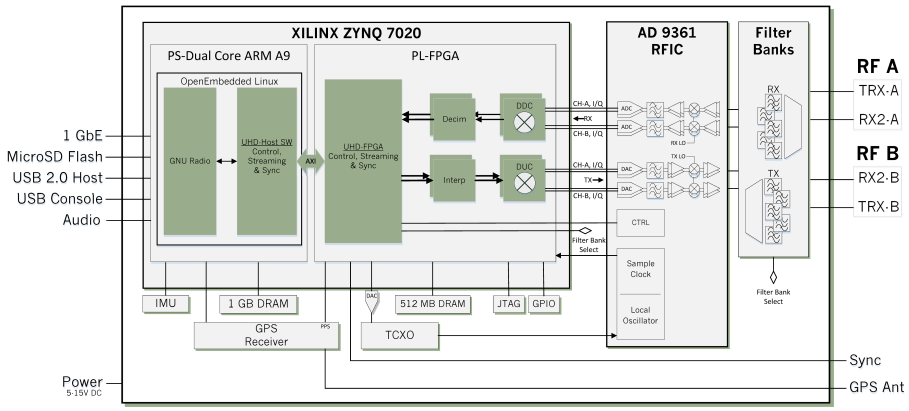

Fig. 6 Block diagram of the USRP E312 device[19]

4. Timed Sampling in UHD

Being able to reliably transmit and receive from a USRP device at a given local reference time is the most fundamental functionality needed to begin implementing a TWR system on the UHD platform. The `tx_metadata_t` structure holds transmission burst information important to the USRP radio. The metadata parameters and their functions can be seen in Table 1.

Table 1 Transmit metadata parameters in UHD

Parameter	Description
`start_of_burst`	Identify if a transport packet is the beginning of a transmission burst.
`end_of_burst`	Identify if a transport packet is the end of a transmission burst.
`has_time_spec`	Identify if this burst should be sent at a given time or sent immediately.
`time_spec`	Specifies the local device time at which to send the data packet.

From the table, we can see that a `tx_metadata_t` structure with `has_time_spec` set to `True` and `time_spec` set to a specific `tx_time` is sufficient to alert the radio that a packet burst is required to leave the FPGA for the RF front-end (RFFE) at a specified time. Additionally, depending on the length of the data packet and the samples per transport packet (`spp`), the first `spp` samples should have `start_of_burst` set to `True` and `end_of_burst` set to `False` while the last `spp` samples should be the opposite. The metadata is sent as an argument to the UHD `send()` function, which sends up to `spp` samples at a time to the USRP radio via the `tx_streamer` interface.

On the receive side, instead of sending metadata to the stream interface, the stream interface creates its own metadata in the form of `rx_metadata_t`. Therefore, a stream command is sent to the receive chain beforehand in the form of `stream_cmd_t`. The UHD stream command parameters are shown in Table 2.

Table 2 Stream command parameters in UHD

Parameter	Description
`stream_mode`	Identify the sample streaming mode, either continuous or burst mode.
`stream_now`	Identify if streaming should start now or wait for a `time_spec`.
`time_spec`	Specifies the local device time at which to send the data packet.

Once a stream command is issued via `issue_stream_cmd()`, the `recv()` function should be called via the `rx_streamer` before the specificed `time_spec` in order to avoid a late command condition. The `rx_metadata_t` parameters filled in by the `recv()` function are the same as `tx_metadata_t` with the additions shown in Table 3. The `rx_metadata_t end_of_burst` parameter is useful for guaranteeing all samples have been received from the radio.

Table 3 Additional parameters in receive metadata in UHD

Parameter	Description
`more_fragments`	`True` if the buffer has insufficient size to hold a full transport packet.
`fragment_offset`	Identifies the sample number at which the next fragment begins.
`error_code`	Identifies any errors in the receive chain.

Since the timed sampling is handled in the USRP FPGA, there is a delay between when the USRP sends the in-phase/quadrature (IQ) samples to the RFFE and when the samples actually leave the antenna. Correspondingly, on the receive side, there is a delay between the USRP initializing the timed sample buffers in the FPGA and the transmitted samples arriving at the antenna and travelling to the FPGA. Intuitively, this delay is proportional to the master clock rate of the FPGA hardware. Through experimental testing, we found that the delay is fixed between power cycles of the device but may be different between each radio. The calibration procedures to account for these delays are discussed later in Section 7. An illustration of the time delay caused by this UHD inplementation can be seen in Fig. 7.

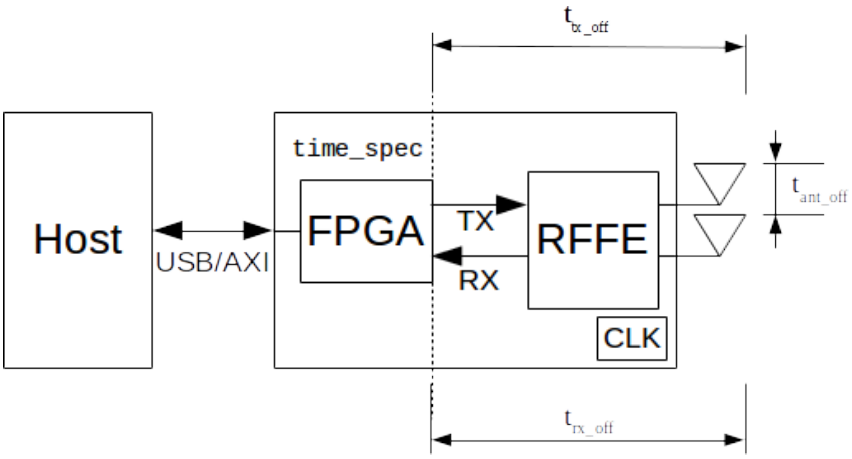

Fig. 7 Illustration of the time delays seen in the SDR caused by the RFFE

5. Ranging Signal Construction

The ranging signal used in a TWR protocol should have good autocorrelation properties such that it is easy to time align the incoming signal to a known copy of itself. This property will aid in accurately measuring the return delay for distance calculations. In addition, the signal should also be highly orthogonal to other ranging codes if other ranging devices are sharing the same broadcast channel. Linear feedback shift register (LFSR) based pseudo-noise (PN) sequences known as Gold sequences[20,21] meet these criteria and are also used in GPS ranging[22] and code division multiple access wireless communication protocols.[23] For simplicity, our TWR protocol uses the Course/Aquisition (C/A) code used in GPS ranging. The discrete C/A code is computed using the exclusive or ($\oplus$) on two LFSR maximum length sequence codes in the form

$$C/A_i[n] = A[n] \oplus B[n - d_i], \tag{9}$$

where $\{0 \leq n \leq 1023\}$, the ith C/A code is C/A_i, the output of the first LFSR with generator polynomial $x^{10} + x^3 + 1$ is A, and the output of the second LFSR with generator polynomial $x^{10} + x^9 + x^8 + x^6 + x^3 + x^2 + 1$ is B. Both LFSRs A and B have the initial state 1111111111_2. The delay d_i is designated in the GPS specifications for each specific C/A code.[24]

6. Modulation Technique

When choosing a modulation technique, it is important to consider all of the system requirements in order to balance throughput, channel bandwidth, complexity, and implementation effort. Since the hardware on this system is a low-power embedded device that cannot handle heavy computational loads, a low-complexity modulation scheme is necessary for acceptable ranging rates. Therefore, the modulation method chosen for this system is Gaussian frequency shift keying (GFSK), which is a popular digital modulation used in many low-power protocols like Bluetooth.[25]

Let the discrete binary information signal to be modulated be $x[n]$. The signal is first converted to non-return to zero (NRZ) format by $x_{NRZ}[n] = 2x[n] - 1$ and then filtered through a polyphase interpolating finite impulse response Gaussian filter, which applies sps samples per information bit. It is created by sampling a continuous-time filter with impulse response

$$h(t) = \frac{\sqrt{\pi}}{a} e^{-\frac{\pi^2 t^2}{a^2}}, \tag{10}$$

where a is related to the filter roll-off BT by

$$a = \frac{1}{BT}\sqrt{\frac{\log 2}{2}}. \tag{11}$$

The filtering procedure is done by time-domain discrete convolution given by

$$m[n] = (x * h) = \sum_{m=-M}^{M} x[n-m]h[m], \tag{12}$$

where M is the overlap size. The Gaussian filtering reduces the out-of-band power in the frequency domain of the transmitted signal by smoothing the discrete jumps in frequency caused by the digital signal at the expense of inter-symbol interference. The filtered interpolated signal is then frequency modulated in the form

$$\phi[n] = k \sum_{n=0}^{N-1} m[n], \tag{13}$$

and converted to polar form by $\theta[n] = \cos(\phi[n]) + \sin(\phi[n])i$. The sensitivity of the modulator is the constant k which changes the total phase deviation on the final

output signal.

The GFSK demodulation procedure used in our system is quadrature demodulation in the form

$$\hat{m}[n] = \text{arctan}(\hat{\phi}[n+1]\hat{\phi}[n]^*) \tag{14}$$

where the complex conjugate of the received signal is $\hat{\phi}[n]^*$ and arctan is the four-quadrant atan function.[26] Before quadrature demodulation, a low-pass filter (LPF) is applied to the incoming signal to remove excess noise outside of the signal bandwidth. Since the signal is not oversampled at the receiver, the LPF's sample rate is F_s and the cutoff frequency is F_s/sps with a transition width of 100 Hz and 30-dB attenuation.

To recover the binary information, if needed, a low-pass decimation filter is applied and sliced at the 0 crossing, which will extract our estimate $\hat{x}[n]$.

7. Loopback Calibration Procedure

To have a reliable TWR protocol, knowledge of when a ranging message leaves and arrives at the USRP radio hardware is needed to, ideally, nanosecond precision. Since the concept of SDR development is to abstract out the radio hardware as much as possible, this is a challenging design problem.

As discussed in Section 4, timed transmit and receive functionality built into the UHD driver alone is not sufficient to meet the nanosecond precision design requirements. Therefore, careful calibration of the individual devices is needed to zero out the delays in the transmit and receive chains as accurately as possible. A loopback calibration procedure attempts to compensate for two types of error in the hardware 1) sample offset and 2) phase offset. The sample offset is easily found by first tuning the USRP transmit frequency to the receive frequency and transmitting a known ranging message at a given device time `txrx_time` and receiving at the same time. The receiver buffer of raw IQ samples, which contains the ranging message, is then correlated in the time domain with a saved template of the transmitted ranging message IQ samples according to the equation

$$corr[n] = (f \star g) = \sum_{m=-M}^{M} f^*[m]g[m+n], \tag{15}$$

where $(\cdot)^*$ denotes the complex conjugate. The sample index of the maximum value of $corr[n]$ is the lag in samples between the ranging message IQ f and the received sample buffer g. This lag is the transmit and receive offset in absolute samples inside the receive buffer. Once the sample offset is identified, the received ranging message is extracted, demodulated, and sample-aligned to a demodulated reference ranging message. The phases of the two demodulated signals $\hat{f}$ and $\hat{g}$ are computed in the frequency domain similar to Eq. 4 in Section 2 by first converting the signals to the frequency domain and then finding the phase angle of the maximum value of the DFT as

$$\hat{\theta}_F = \text{atan}(\max(\hat{F}[k])). \tag{16}$$

The angle difference can then be found by the difference $\hat{\theta}_F - \hat{\theta}_G$. This result is the subsample round-trip loopback phase delay. These two intrinsic round-trip delays are saved to a global structure `ranging_struct` and used in the range calculations. By modifying our TWR distance calculation after CPC from Eq. 8 to include calibration correction from both devices A and B, we get

$$d_{CPC,cal} = \frac{t_{phase} + t_{B,cal} - t_{A,cal}}{2} \times c, \tag{17}$$

where $t_{A,cal}$ and $t_{B,cal}$ are the intrinsic phase offsets for devices A and B, respectively. The calibration phase from device B is added to the range calculation instead of subtracted to account for the circular shift applied according to Eq. 4 from Section 2. The absolute sample offset is removed from the received response message before the range is calculated and the receiver/responder simply sends its response `intrinsic_sample_offset`$/T_s$ fractional seconds early, where T_s is the sampling period. Detailed transmit and receive procedures are explained further in Sections 8 and 9.

An overview of these parameters is shown in Table 4, and the simple block diagram of the loopback calibration procedure is shown in Fig. 8. The dashed lines are saved variables from Table 4 and the solid lines are logic flow.

Table 4 Intrinsic loopback calibration offset parameters saved in the ranging structure

Parameter	Description
`intrinsic_sample_offset`	Absolute sample offset in loopback configuration.
`intrinsic_phase_offset`	Phase offset in loopback configuration.

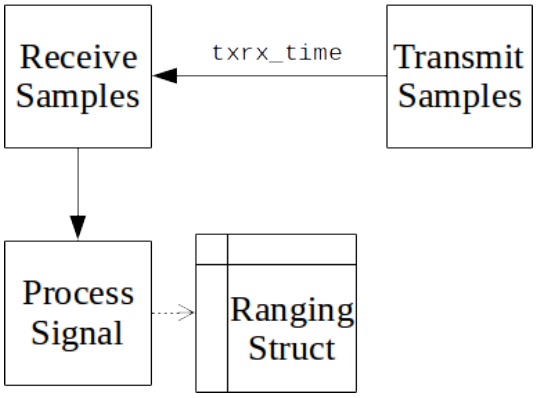

Fig. 8 Block diagram of the loopback calibration procedure

8. Transmitter Procedure

The TWR transmitter is responsible for transmitting a known ranging message, receiving a response ranging message, computing, and saving all relevant information needed for accurate ranging calculations.

The transmitter sends the ranging message at a local device time `tx_time` and begins receiving IQ samples at an `rx_time`, which is equal to `tx_time` plus a known delay agreed upon between the transmitter and receiver. The received message is correlated in the time domain with a template ranging message IQ signal to extract the lag in samples and verify that a response was actually received. Additionally, the magnitude of the peak of the complex correlation is saved and compared to the product of the template energy and received signal energy to provide a reliability estimate. This estimate in percent is computed according to

$$\text{reliability} = 100 \times \frac{|\max(\text{corr}(f, g)|}{E[f]E[g]}, \tag{18}$$

where $E[\cdot]$ is the expected value, f is the the received ranging message, and g is the

received sample buffer as in Section 7. The received ranging message is extracted, demodulated, and sample-aligned to the earliest expected sample, `intrinsic_sample_offset`. The two demodulated signals' phases are computed in the frequency domain and then the difference is calculated. This difference is the overall phase delay without calibration correction applied for device A. The information of the round trip at the transmitter is shown in Table 5. The TWR transmitter procedure block diagram is shown in Fig. 9.

Table 5 Round-trip parameters saved into the ranging structure by the transmitter

Parameter	Description
`tx_time`	Local device time in seconds the ranging message is sent.
`rx_time`	Local device time in seconds the ranging message is received.
`known_delay`	Expected delay in seconds before a response is expected from the receiver/responder.
`transmit_interval`	Delay in seconds between transmit bursts.
`overall_sample_offset`	The total sample offset in the receive buffer where the received range message is located.
`overall_phase_offset`	Total phase diff. between a local demod. ranging message and the received demod. signal.
`corr_norm`	Norm of the max correlation between the local range message and RX IQ samples.
`reliability`	The estimated reliability of the range measurement.

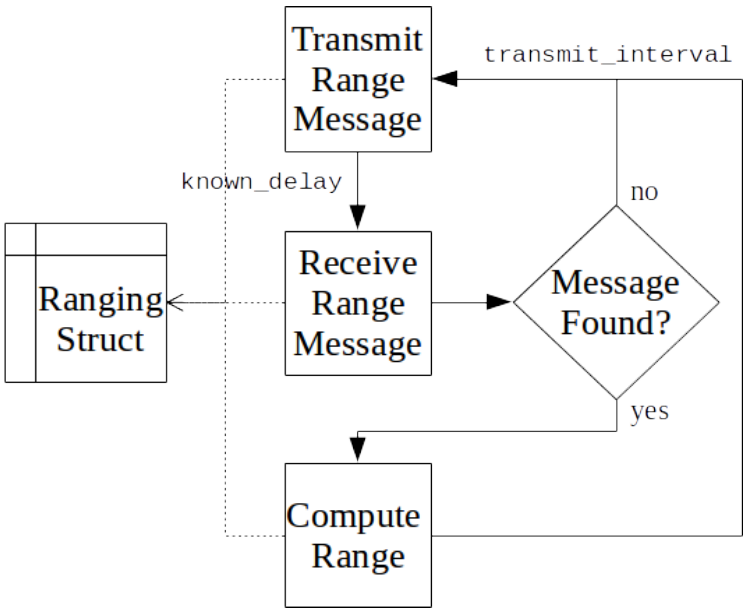

Fig. 9 Block diagram of the ranging transmitter procedure

9. Receiver Procedure

The TWR receiver is responsible for detecting a known range message, computing and compensating for any intrinsic sample and phase delay contributed by the device, and responding to the range request after a known delay agreed upon by both the transmitter and receiver.

The receiver has two main receiver modes, unlocked and locked. In the unlocked mode the receiver is waiting for an initial ranging message to be transmitted over the channel. The receiver continuously streams samples from the radio while polling the received signal strength indicator (RSSI) sensor on the USRP device. If an RSSI above the noise floor is detected, the receiver checks the buffer via time domain correlation to see if a range message was in the packet. If no message is detected, the receiver continues receiving packets until a range message is found or a long timeout is reached. This unlocked mode is used to avoid as much processing between transport packets as possible, therefore increasing the maximum achievable sample rate of the system by avoiding overflow conditions. The unlocked mode receiver block diagram is shown in Fig. 10.

When a ranging message is found in a receive buffer, the receiver goes into locked mode. In locked mode, the receiver expects a range request at known intervals

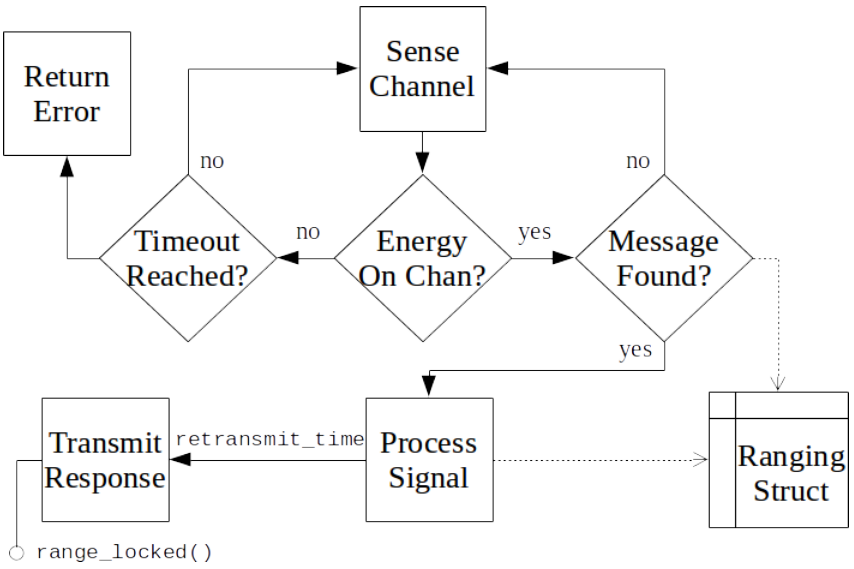

Fig. 10 Block diagram of the unlocked ranging receiver procedure

agreed upon between the transmitter and receiver relative to the first received message. The locked mode restricts received samples to a few packets, which most likely contain the range message. This greatly reduces receiver overhead and allows for an increased ranging interval. If the receiver misses a predefined number of range requests, it returns to unlocked mode, waiting for any attempt to re-lock with the transmitter. The locked mode receiver block diagram can be seen in Fig. 11.

Regardless of a locked or unlocked condition, the receiver must process any incoming ranging message and respond after the appropriate `known_delay`. The received ranging message from the transmitter is correlated in the time domain with a template ranging message IQ signal to extract the lag in samples. The received ranging message is extracted, demodulated, and sample-aligned to a demodulated template ranging message. The two demodulated signals' phases are computed in the frequency domain, and then the difference is computed. This difference is the overall phase delay and sample clock phase offset without calibration correction. The time of retransmission is carefully computed as `rx_time + lag_in_sec + known_delay − intrinsic_sample_offset`. The `intrinsic_sample_offset` is the sample delay computed in Section 7 during loopback calibration.

In order to compensate for the phase offset in retransmission, a known ranging

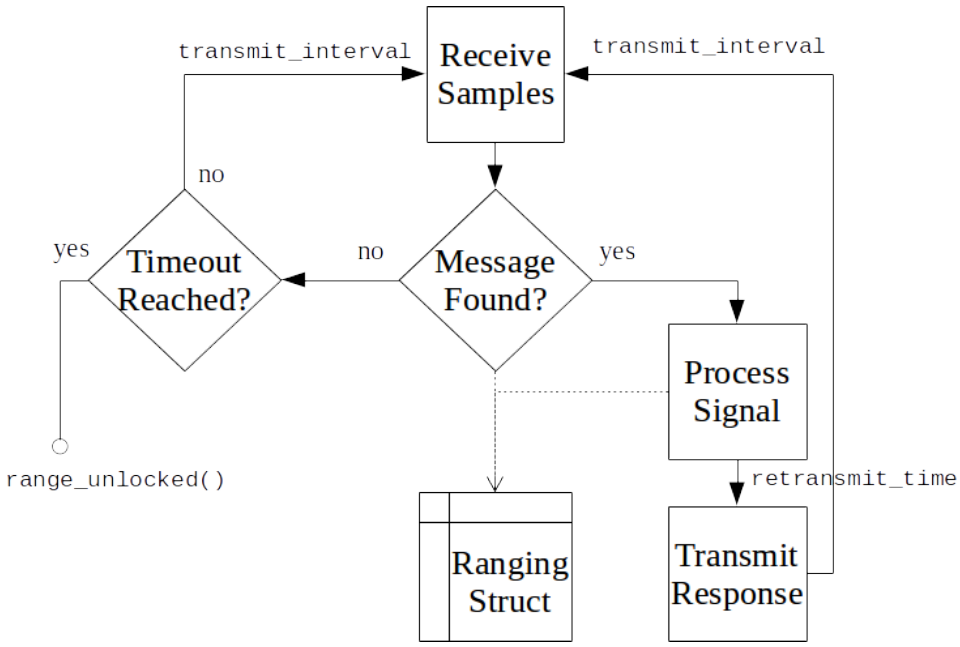

Fig. 11 Block diagram of the locked ranging receiver procedure

message is phase shifted according to `overall_phase_offset` + `intrinsic_phase_offset` before modulation and retransmitted according to Eq. 4. This procedure allows the TWR device's response to be as close to the original message as possible without incurring noise enhancement from simple loopback retransmission.

10. Range Calculation

At the transmitter, after all information in Table 5 is saved to memory, the range can be calculated. The range calculation is done by first applying the calibration correction according to

$$\theta_{range} = \texttt{overall\_phase\_offset} - \texttt{intrinsic\_phase\_offset}, \quad (19)$$

then converting phase to fractional samples

$$s_{range} = \theta_{range}/\theta_{single}, \quad (20)$$

then converting to round trip time

$$rt_{range} = s_{range}/F_s, \quad (21)$$

and finally to one-way distance

$$d_{range} = \frac{rt_{range}}{2} \times c. \tag{22}$$

The distance in meters calculated here is equal to $d_{CPC,cal}$ in Section 7.

11. Experimental Results

In order to verify the accuracy of the SDR TWR method described in this report, we simulate the ranging system without the SDR-specific loopback calibration described in Section 7 and compare the results to a controlled, wired experiment using a slow-ranging rate of 1 Hz. The system parameters used in the simulation and the controlled experiment can be seen in Table 6. Our receive LPF (used before phase comparison) has an aggressive cutoff frequency of 250 kHz. This is done to remove as much noise power as possible from the baseband signal to improve phase accuracy. The devices used in this initial experiment are the USRP B200 devices seen in Fig. 13.

Table 6 Controlled experiment system parameters

Parameter	Value
Ranging device	B200
Sample rate	2 MHz
Symbol rate	1 MHz
Modulation	GFSK
Samples per symbol	2
Modulation sensitivity	2
Gaussian filter length	8
Center frequency	2.5 GHz
PN sequence	Gold code
PN maximal length	1023 bits
Truncated PN length	400 bits
Signal-to-noise ratio	15 dB
Receive LPF cutoff	250 kHz
Ranging rate	1 Hz

The trials in the controlled test vary cable lengths to mimic different real-world distance measurements without the effects of the channel. Figures 14, 15, 18, 19, 22, 23, 26, 27 correspond to the experimental trials while Figs. 16, 17, 20, 21, 24, 25, 28, 29

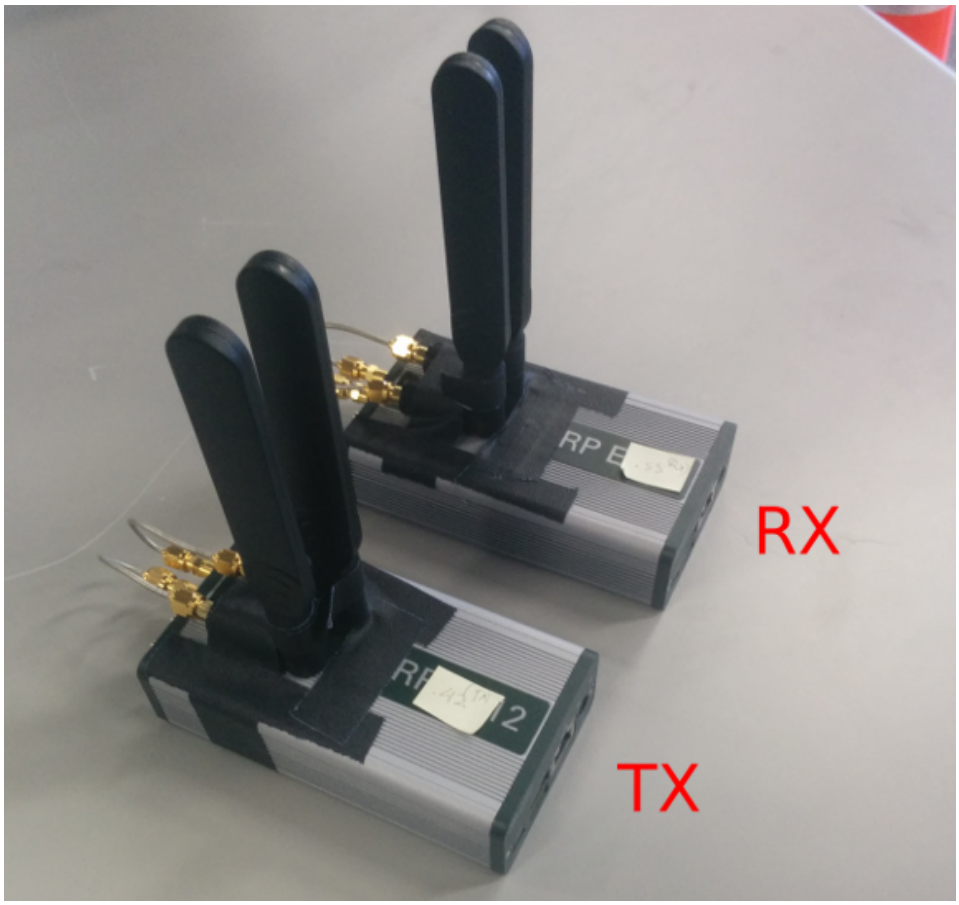

Fig. 12 The USRP E312 devices used for experimentation

are the simulated trials.

Compared to the simulated trials, the experimental trials have larger variations in the distance estimates; however, the root mean square error (RMSE) and standard deviation (std) are still very close. In Fig. 30 the mean distance of all the trials compared to the true distance is shown. We can see that the experimental system follows simulation closely; however, there is still a significant error compared to the true distances. The long-range trial of about 19 m also shows an increased RMSE over the shorter distances.

This behavior was found to be related to the correlation properties of the Gold codes described previously in Section 5. The M-Sequences used to construct the code have optimum correlation properties only at their maximum length.[21] Since we truncated the 1023 length code to 400, our phase calculations exhibit an increasing

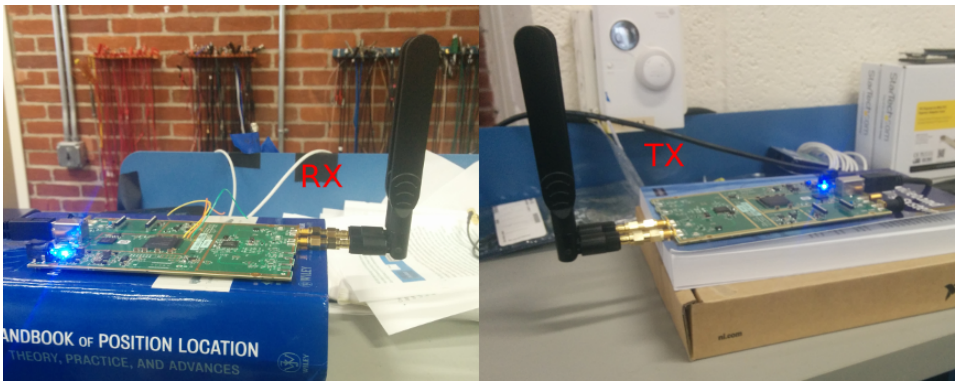

Fig. 13 The USRP B200 devices used for experimentation

error as the transmitted ranging sequence is further out of phase with the reference sequence. To fix this problem, we transmit a new Gold code sequence with length 511 following the same method as Eq. 9 with order 9 polynomials $x^9 + x^4 + 1$ and $x^9+x^6+x^4+x^3+1$. By simulation, we show that using a full length Gold sequence reduces our error considerably at longer distances. In Fig. 31 and Fig. 32 we can see the distance estimates and errors of both the truncated code and full code.

Figures 33 and 34 show experimental results using the new codes at 18.92 m. Interestingly, there was no improvement in RMSE while the standard deviation was significantly reduced. The variation in distance in this test was caused by the test being conducted after a cold start of the device. We believe that the reason the improved codes did not show the same RMSE performance as simulation is related to the frequency offset and phase noise between the devices. The frequency offset applies a constant phase error across the whole length of the ranging sequence while phase noise applies a varying phase error over the ranging sequence. Both of these phenomena are dependent on the carrier frequency and the sample rate of the system. We verified this experimentally by noticing that shorter length codes show higher reliability than longer codes during ranging while staying the same during loopback calibration. This can only be explained by the differences in the oscillators in the two radios. Therefore, the length of ranging code, without receiver correction, is limited by the performance of the device's internal reference phase lock loop (PLL). Experimentally, we found that the ranging code length detection limit is about 1000 samples for the B200 devices and 800 samples for the E312 devices at 2-MHz sample rate. Intuitively, as the sample rate increases, the useful code length also decreases proportionally. Further research is needed to determine

if frequency offset and phase error can be corrected at the receiver.[27]

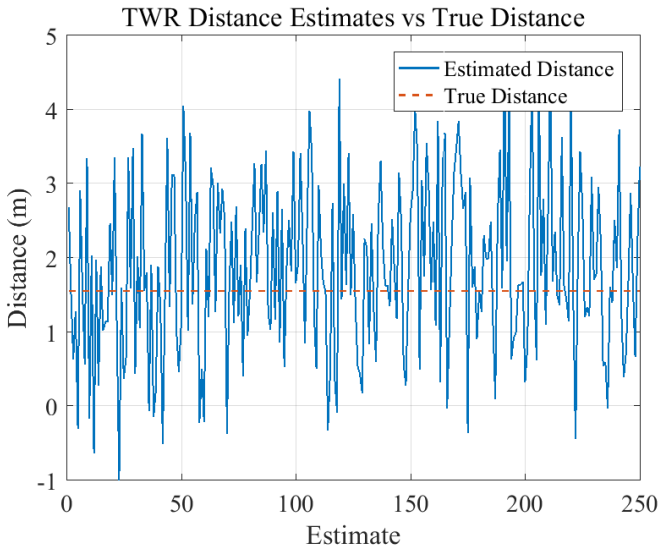

Fig. 14 Experimental TWR distance estimate samples compared to the true distance of 1.55 m

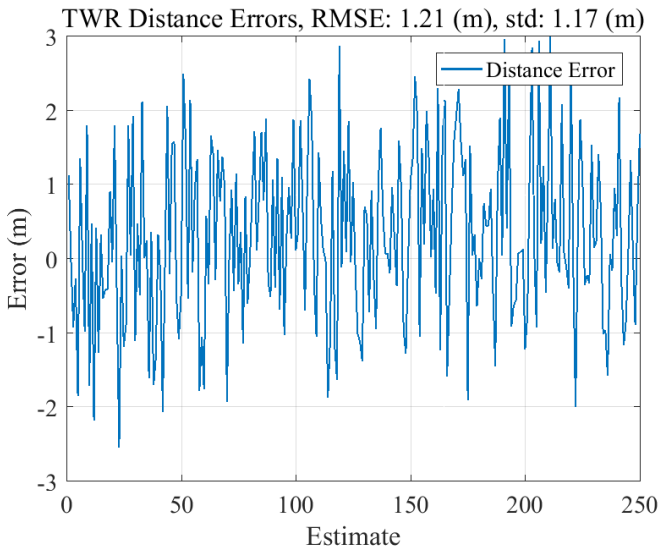

Fig. 15 Experimental TWR distance estimate sample errors for a distance of 1.55 m

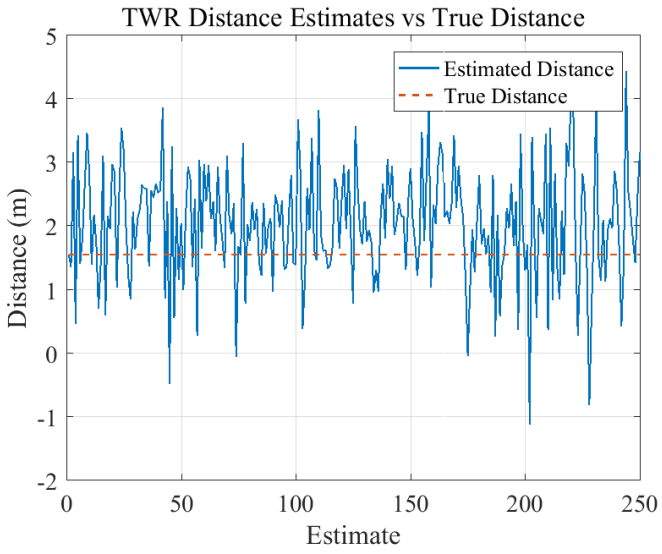

Fig. 16 Simulation TWR distance estimate samples compared to the true distance of 1.55 m

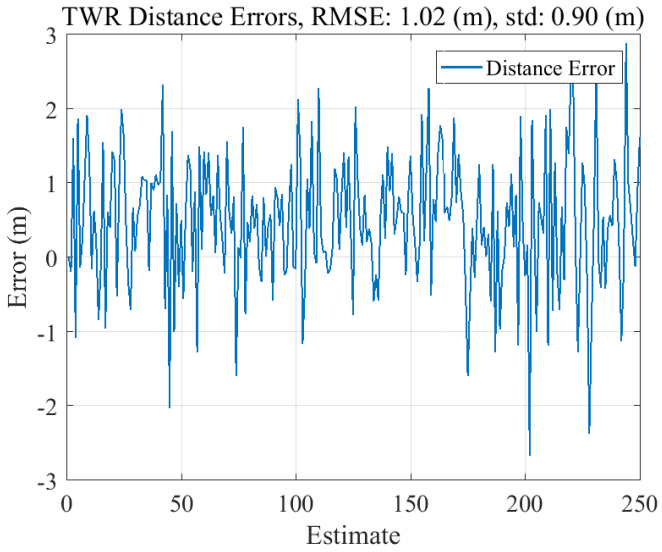

Fig. 17 Simulation TWR distance estimate sample errors for a distance of 1.55 m

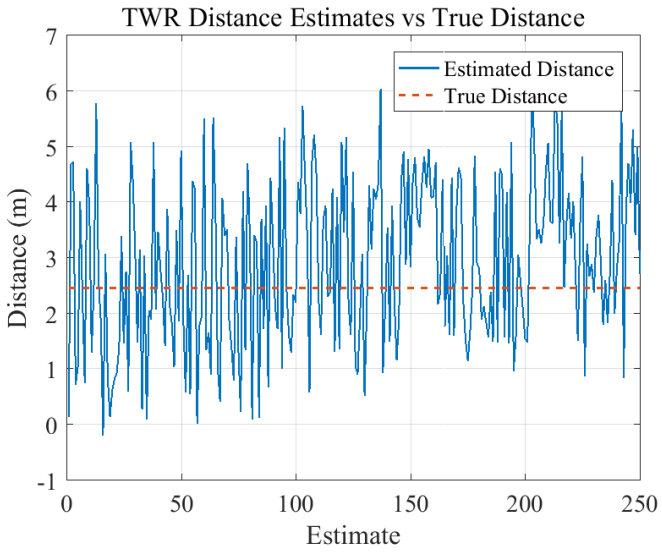

Fig. 18 Experimental TWR distance estimate samples compared to the true distance of 2.46 m

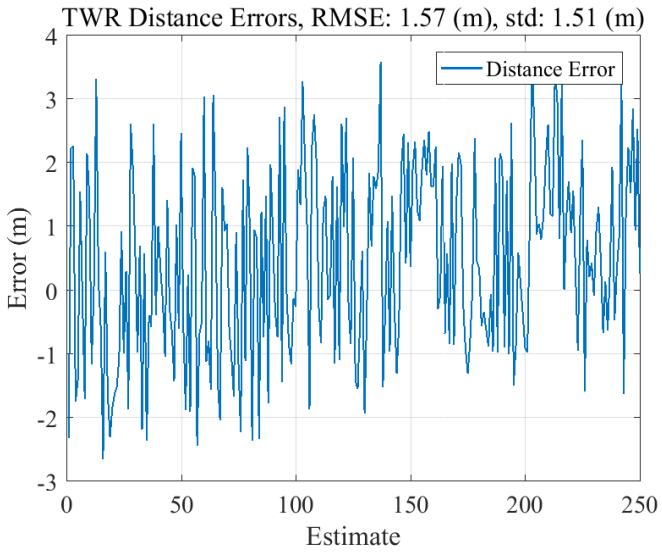

Fig. 19 Experimental TWR distance estimate sample errors for a distance of 2.46 m

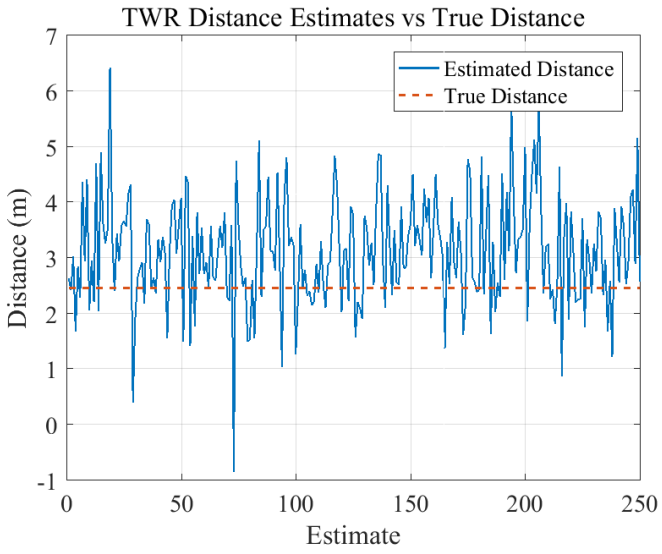

Fig. 20 Simulation TWR distance estimate samples compared to the true distance of 2.46 m

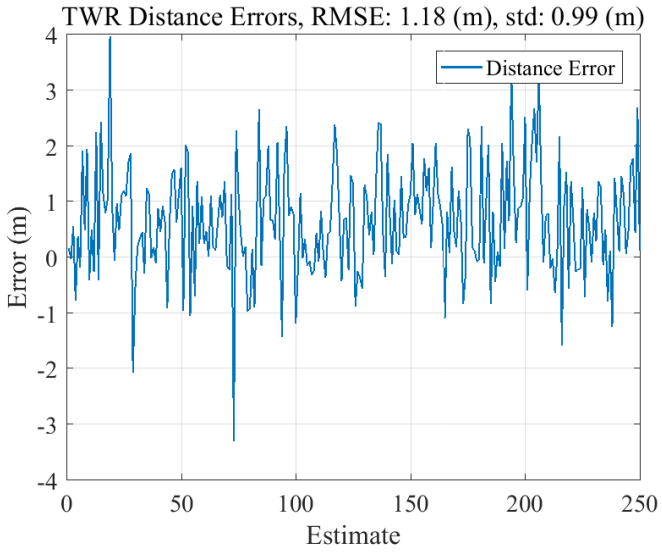

Fig. 21 Simulation TWR distance estimate sample errors for a distance of 2.46 m

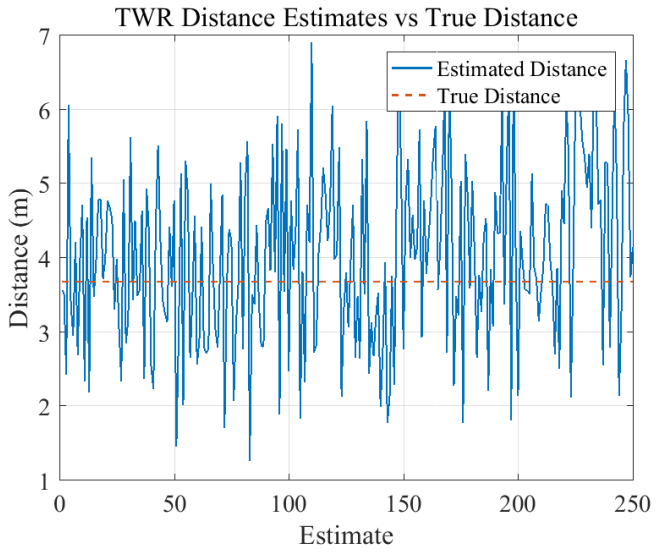

Fig. 22 Experimental TWR distance estimate samples compared to the true distance of 3.68 m

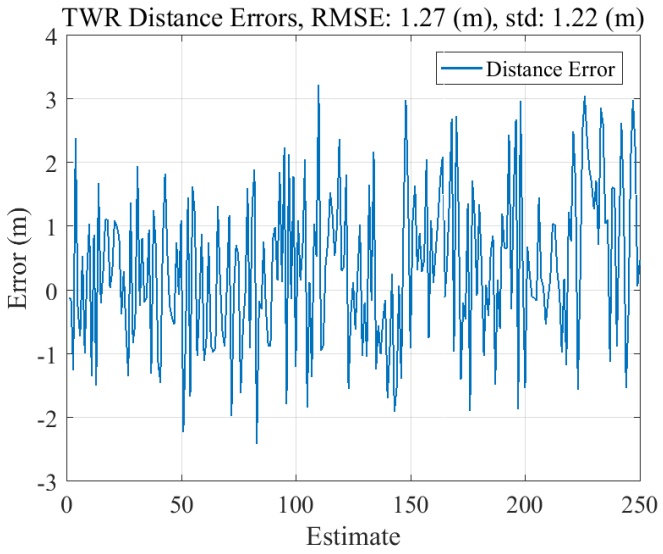

Fig. 23 Experimental TWR distance estimate sample errors for a distance of 3.68 m

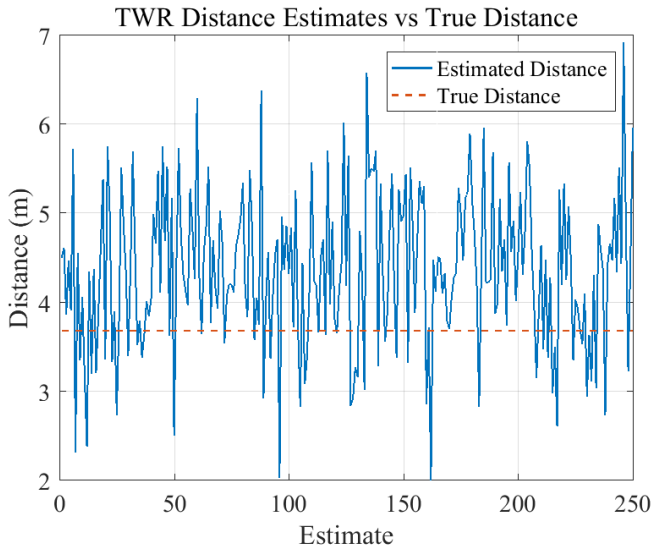

Fig. 24 Simulation TWR distance estimate samples compared to the true distance of 3.68 m

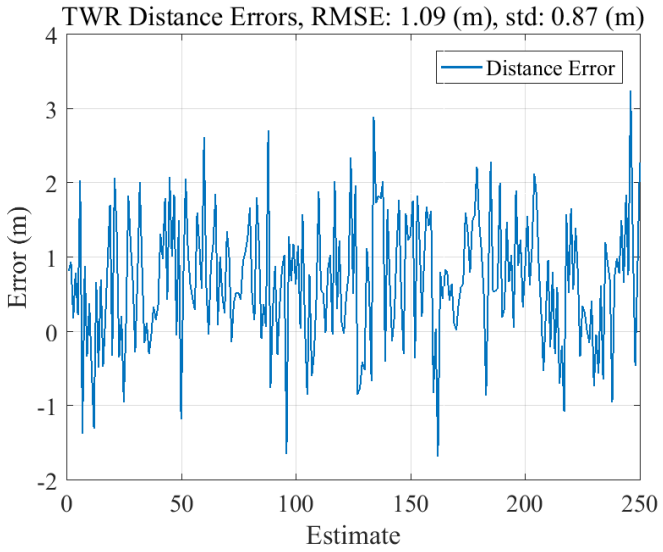

Fig. 25 Simulation TWR distance estimate sample errors for a distance of 3.68 m

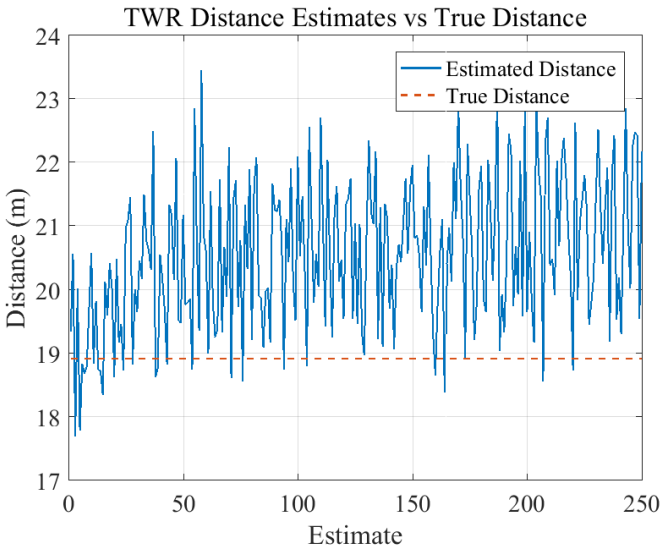

Fig. 26 Experimental TWR distance estimate samples compared to the true distance of 18.92 m

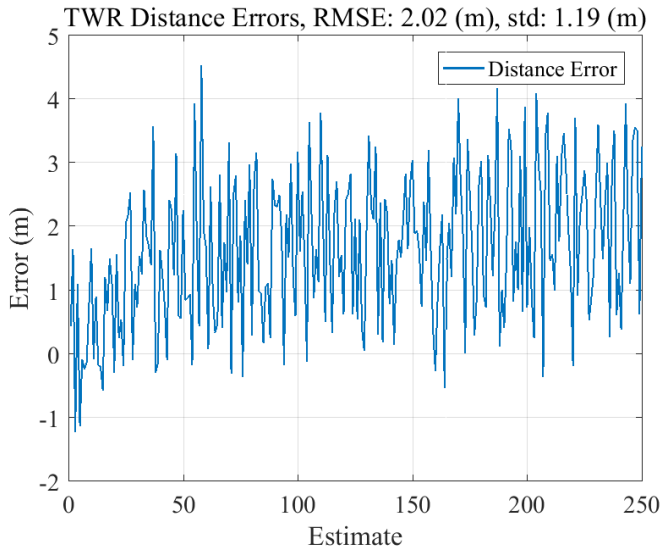

Fig. 27 Experimental TWR distance estimate sample errors for a distance of 18.92 m

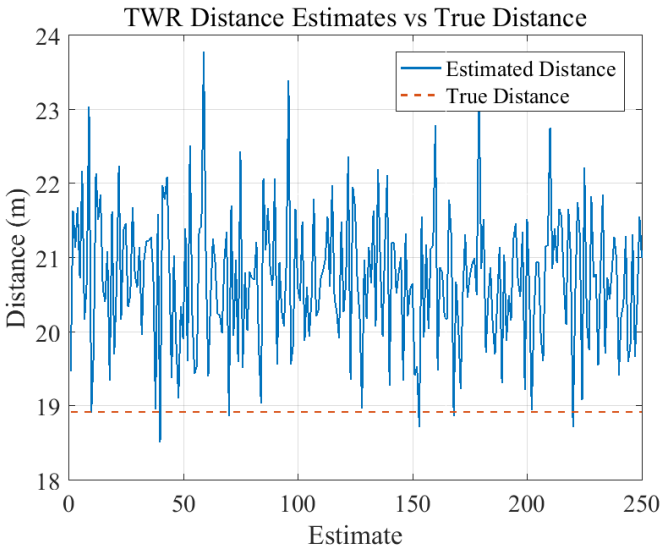

Fig. 28 Simulation TWR distance estimate samples compared to the true distance of 18.92 m

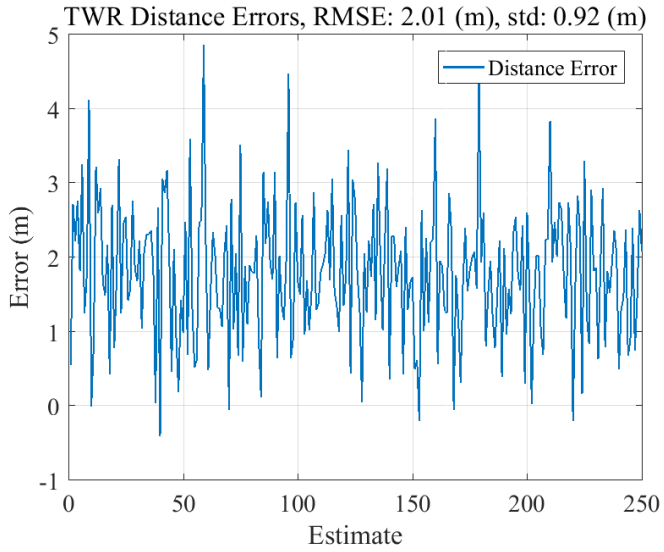

Fig. 29 Simulation TWR distance estimate sample errors for a distance of 18.92 m

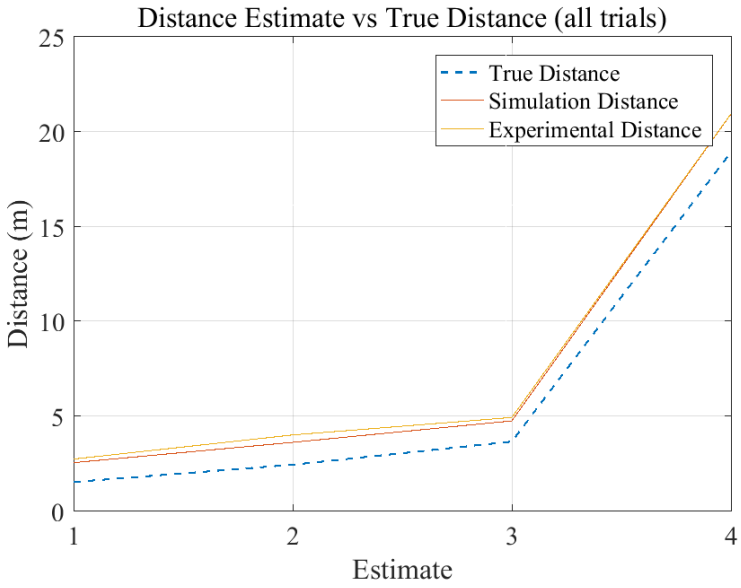

Fig. 30 Experimental and simulation distance estimate mean compared to the true distance for all trials

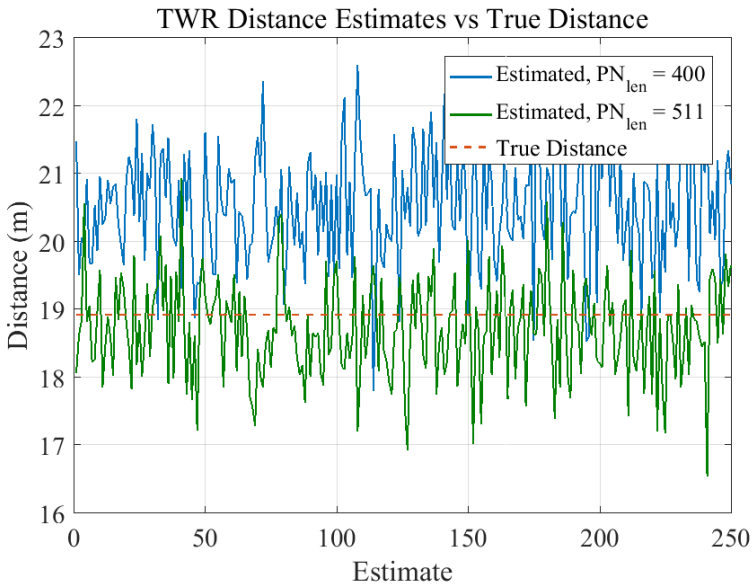

Fig. 31 Simulation TWR distance estimate samples compared to the true distance of 18.92 m for 400 length and 511 length Gold codes

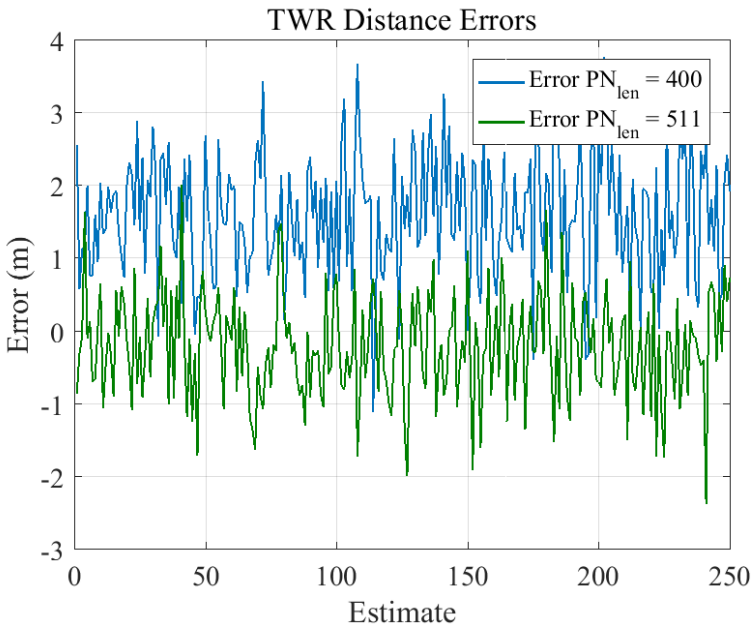

Fig. 32 Simulation TWR distance estimate sample errors for a distance of 18.92 m for 400 length and 511 length Gold codes

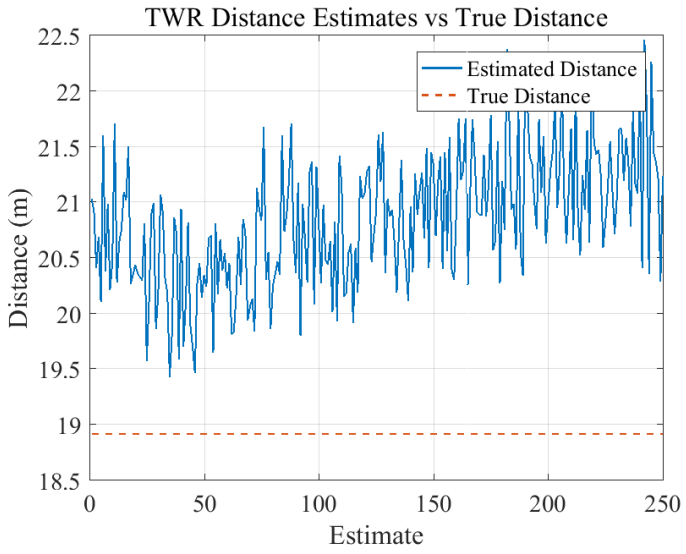

Fig. 33 Experimental TWR distance estimate samples compared to the true distance of 18.92 m using 511 maximal length Gold codes

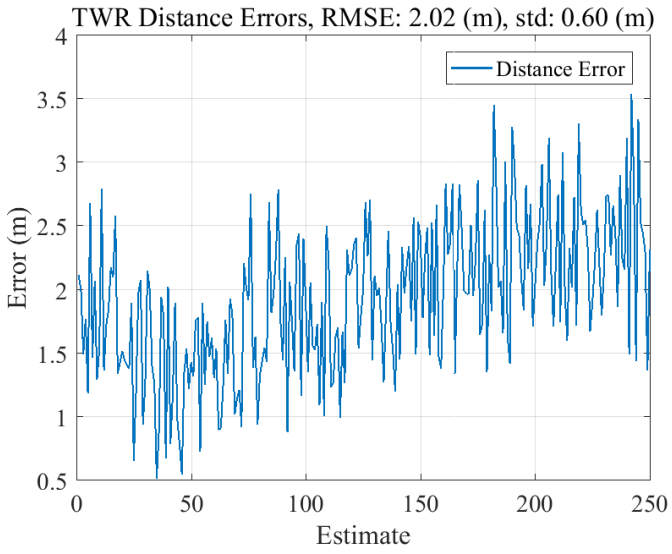

Fig. 34 Experimental TWR distance estimate sample errors for a distance of 18.92 m using 511 maximal length Gold codes

We performed a second test to evaluate the performance of the TWR system in a multipath environment. The satellite image of the outdoor test location can be seen in Fig. 35. The procedure used for the test is as follows: the transmitter E312 device labeled TX in Fig. 12 is placed at the start location, and the receiver E312 device labeled RX in Fig. 12 is moved from 1 m away from the transmitter out 62.5 m to the designated end location and then returned to the start location. The relevant system parameters used in this outdoor test can be seen in Table 7. To simulate the multipath channel in our simulated system, we use a Rician line-of-sight (LOS) model using a tapped delay line with taps at 0, 10 and 20 μs with power in decibels of 0, -11.4 and -15.2, respectively. Lastly, the Rician K-Factor was set to 9 to ensure a strong LOS path to the simulated devices. We can see in Fig. 36 that the multipath channel causes the correlation detector to miss the LOS path much of the time. This behavior roughly matches our simulation in Fig. 37 although with less frequency.

In order to easily filter out the missed detections, we can filter the data in postprocessing by first removing any estimates below 0 and any estimates over a whole sample delay, which is 150 m at 2-MHz sample rate. This simple filter gives us a closer look at the error in a multipath fading channel. The experimental and simulation data post-filter is shown in Fig. 38 and Fig. 39, respectively. We can see

Table 7 Outdoor multipath experiment system parameters

Parameter	Value
Ranging device	E312
Sample rate	2 MHz
Symbol rate	1 MHz
Modulation	GFSK
Samples per symbol	2
Modulation sensitivity	2
Gaussian filter length	8
Center frequency	2.5 GHz
PN sequence	Gold code
PN maximal length	1023 bits
Truncated PN length	400 bits
Signal-to-noise ratio	15 dB
Receive LPF cutoff	250 kHz
Ranging rate	10 Hz

there is still significant error caused by the channel, and both experimental and simulation data show the increasing error with distance caused by our truncated codes as this test was performed using the 400-bit length code. Additionally, we can see in the outdoor experiment that channel effects only present themselves at the extreme distances of the test. This is most likely due to the LOS path becoming weaker relative to the increasing number of multipath signals as we employ a custom software-defined automatic gain control (AGC), which attempts to maintain a SNR of around 15 dB.

Fig. 35 Outdoor TWR test location and procedure

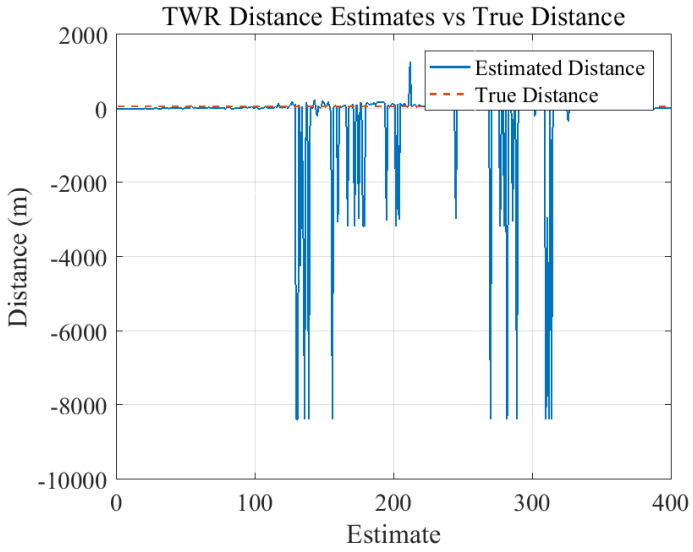

Fig. 36 Experimental TWR distance estimate samples compared to the true distance of 1 to 62.5 m

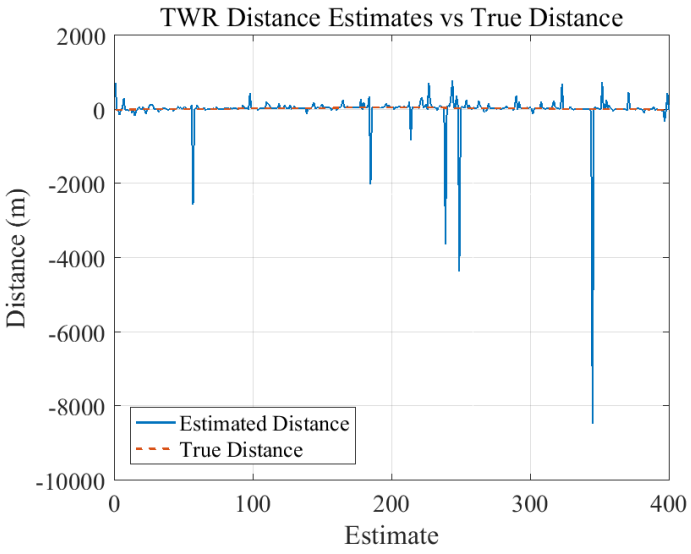

Fig. 37 Simulation TWR distance estimate samples compared to the true distance of 1 to 62.5 m

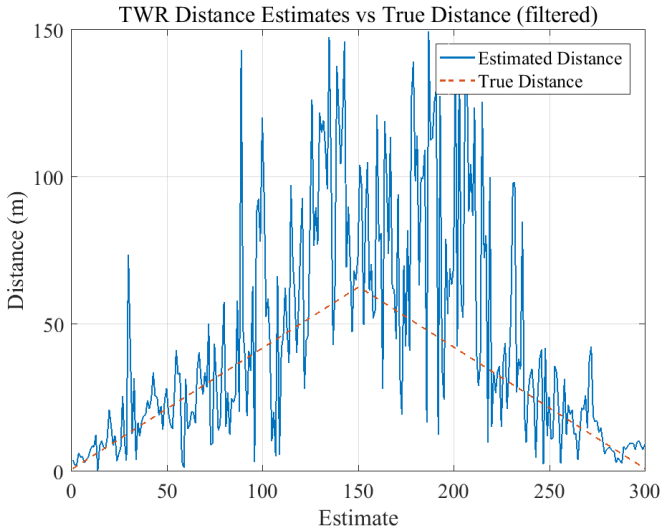

Fig. 38 Experimental TWR distance estimate samples compared to the true distance of 1 to 62.5 m

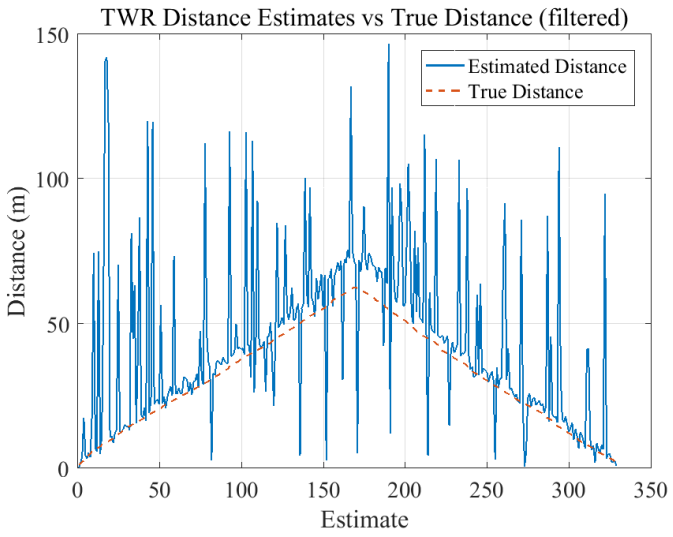

Fig. 39 Simulation TWR distance estimate samples compared to the true distance of 1 to 62.5 m

We conducted one more test in order to experimentally validate the simulated behavior of the 511 length code in Fig. 31 and Fig. 32 and to alleviate the unpredictable nature of the software AGC in multipath environments. We conducted this experiment using the same system parameters as Table 7 except we used the corrected order 9 polynomial Gold code and removed the AGC entirely. The full list of parameters can be seen in Table 8, and the test location can be seen in Fig. 40.

Table 8 Outdoor "Road Test" system parameters

Parameter	Value
Ranging device	E312
Sample rate	2 MHz
Symbol rate	1 MHz
Modulation	GFSK
Samples per symbol	2
Modulation sensitivity	2
Gaussian filter length	8
Center frequency	2.5 GHz
PN sequence	Gold code
PN maximal length	511 bits (corrected)
Truncated PN length	N/A
Signal-to-noise ratio	variable (no AGC)
Receive LPF cutoff	250 kHz
Ranging rate	10 Hz

Fig. 40 Outdoor "Road Test" TWR test location and procedure

We can see from the results in Fig. 41 that the range estimate has much less bias than the truncated code and no whole sample offset estimates. We also plot the range versus real-time reliability of each ranging estimate in Fig. 42 and can see the correlation between multipath fading and range deviation thanks to the stable front-end gain. However, without AGC there is a noticeable, albeit predictable, decrease in reliability due to a reduction in signal strength. Therefore, an easy way to filter out multipath error is to simply reject all estimates less than 80% reliability as shown in Fig. 43.

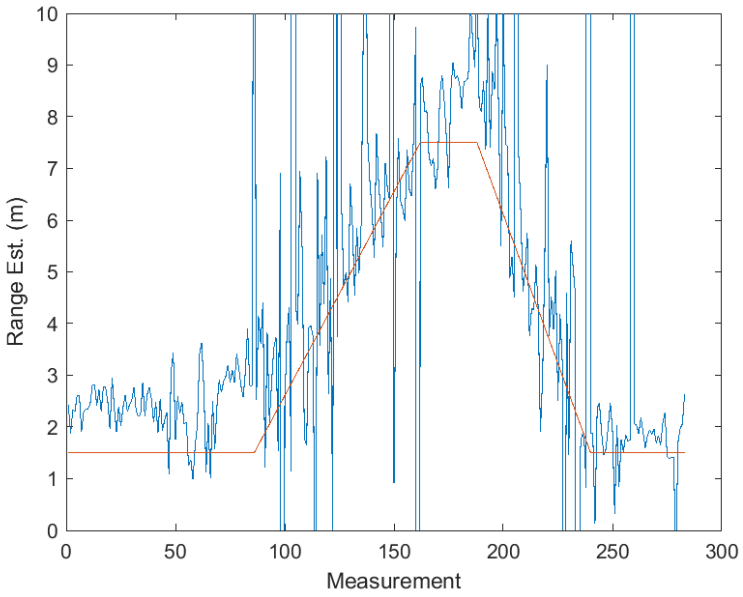

Fig. 41 Experimental TWR distance estimates versus the true distance

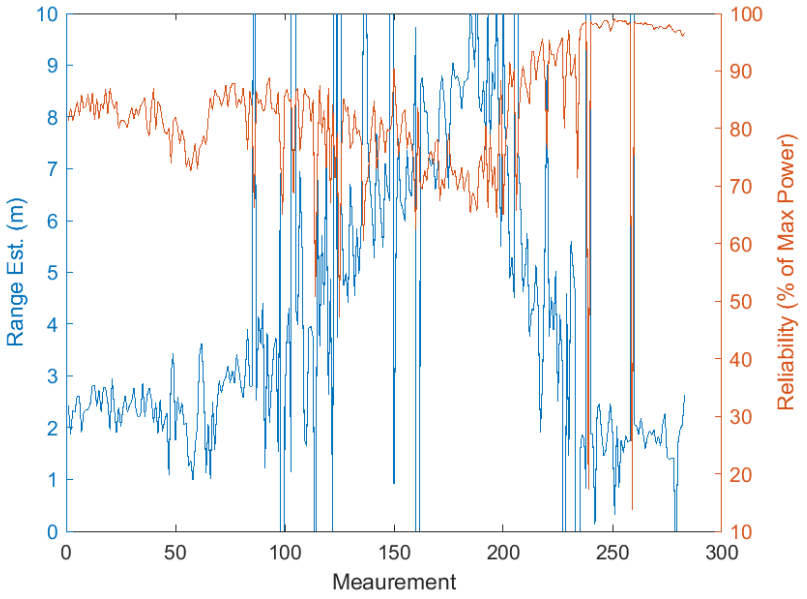

Fig. 42 Experimental TWR distance estimates versus range reliability

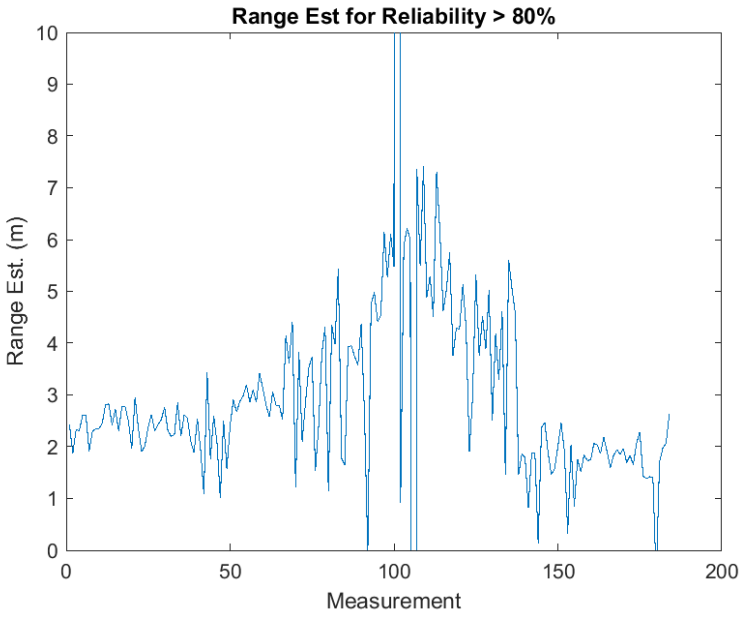

Fig. 43 Experimental TWR distance estimates with reliability greater than 80%

In order to improve range accuracy more substantially in a multipath environment, multiple options are available in literature.[15] The most simple approach is frequency

hopping,[28] where the ranging protocol attempts to range at different center frequencies, attempting to avoid frequency-selective fading that may occur on one of the bands. This is more difficult in an SDR context because the different center frequencies will have a different phase offset signature during calibration as described in Section 7. This means calibration will have to be performed for every frequency channel used during ranging.

Another popular method is channel estimation via deconvolution of the known ranging message. In the time domain, if the received signal is $y(t)$, the transmitted signal is $x(t)$, the channel impulse response is $h(t)$, and the noise is $z(t)$, then the received signal can be represented after sampling at F_s as

$$y[n] = x[n] \star h[n] + z[n]. \tag{23}$$

The frequency domain relationship is hence

$$Y[k] = X[k]H[k] + Z[k], \tag{24}$$

where $Y[k]$, $X[k]$, $H[k]$, and $Z[k]$ are the DFT of their respective discrete time domain signals. Therefore, the channel frequency information $H[k]$ can be estimated simply by dividing $Y[k]$ by $X[k]$. This estimate $\hat{H}[k]$ can be converted back to the time domain to get $\hat{h}[n]$, the estimated channel impulse response. This channel impulse response will give estimates of the multipath delay spread seen during that range estimate. However, the resolution of the channel is limited by the sample rate of the system F_s. This is because range accuracy is restricted to whole sample estimates obtained by choosing the earliest sample peak above some threshold, which is not desirable. However, the channel estimation can still be used to reject corrupted range estimates. If the channel estimate shows significant multipath response, it is likely that the estimate will be corrupted and the estimate can be rejected without further processing.

The last method, called **MU**ltiple **SI**gnal **C**lassification (MUSIC),[29] is a vector subspace super-resolution[30] method that relies on the covariant matrix and performs Eigenvector decomposition (EVD) to separate the frequency information of the various multipath components. The number of multipath signals should be known a priori to ensure there is not significant reduction in accuracy. The number of multipath components can be estimated by counting the number of peaks above a prede-

fined threshold in the channel impulse response estimate $\hat{h}[n]$. By taking the whole channel frequency response vector $\mathbf{H}$ and decomposing it into phase, amplitude, and noise components in the form

$$\mathbf{H} = \mathbf{UA} + \mathbf{Z} \tag{25}$$

where

$$\mathbf{U} = [\mathbf{u}(\tau_1), \ldots, \mathbf{u}(\tau_M)], \tag{26}$$

$$\mathbf{u}(\tau_m) = [1, e^{-j2\pi\Delta f_1 \tau_1}, \ldots, e^{-j2\pi\Delta f_{N-1}\tau_{M-1}}], \tag{27}$$

$$\mathbf{A} = [\alpha_1, \ldots, \alpha_M]. \tag{28}$$

Δf is the frequency sample spacing, τ_m is the m-th multipath delay component, N is the number of samples, and M is the total number of multipaths. The covariance matrix of $\mathbf{H}$ corresponds to

$$\mathbf{R}_H = E\{\mathbf{H}\mathbf{H}^H\} = \mathbf{U}\mathbf{R}_A\mathbf{U}^H + \sigma_z^2\mathbf{I}, \tag{29}$$

where $\mathbf{R}_A = E\{\mathbf{A}\mathbf{A}^H\}$ and σ^2 is the noise variance. If we take the $L \times L$ autocorrelation matrix $\mathbf{R}_H$ where $\{M < L < N\}$ and perform EVD, sorting the eigenvalues in decending order, the eigenvectors corresponding to the M largest eigenvalues span the signal subspace. The remaining $N - M$ eigenvectors span the orthogonal noise space. Finally, the MUSIC pseudo-spectrum is computed by

$$\hat{P}_{MU}(\theta) = \frac{1}{\sum_{i=N+1}^{M} |\mathbf{u}^H \mathbf{v}_i|^2}, \tag{30}$$

where $\mathbf{v}_i$ is the i-th noise eigenvector. The first value in the pseudo-spectrum above a predefined threshold is the first LOS ranging signal path. Even though the MUSIC method is very accurate, thanks to its ability to analyze the frequency content of the signal, the EVD operation is computationally intensive, especially for long signals, which can make implementation difficult in real-time systems.

12. Conclusion

In conclusion, we have demonstrated a real-time TWR protocol using the UHD application programming interface and implemented it on two USRP devices, the B200 and E312. Problems critical to proper implementation in an SDR environment, including timed sampling and RF hardware delay compensation, are discussed and solutions are demonstrated. We find that the protocol is accurate in a multipath free, controlled environment closely following simulation results. The main error sources were the truncated Gold code having suboptimal correlation properties, the internal PLL phase error, and expected multipath fading effects.[15] In addition, we observed that AGC adjustments and cold start conditions contributed to measurement variability. The truncated Gold code was corrected by replacing it with a shorter, full length code, while the correction of other error sources is left for future research.

13. References

1. Iliev N, Paprotny I. Review and comparison of spatial localization methods for low-power wireless sensor networks. IEEE Sensors Journal. 2015;15(10):5971-5987.

2. Lockspeiser JR, Don ML, Hamaoui M. Radio frequency ranging for swarm relative localization. Army Research Laboratory (US); 2017 Oct. Report No.: ARL-TR-6022.

3. Hamaoui M. Non-iterative mds method for collaborative network localization with sparse range and pointing measurements. IEEE Transactions on Signal Processing. 2018;67(3):568–578.

4. Allik BL, Hamaoui M, Don M, Miller C. Kalman filter aiding mds for projectile localization. In: Aiaa scitech 2019 forum; p. 1159.

5. Don ML. A hybrid code division and time division multiple access (cdma/tdma) communications network with localization via two-way ranging and direction of arrival. CCDC Army Research Laboratory Aberdeen Proving Ground United States, Tech. Rep. 2021;.

6. Don ML. A low-cost software-defined telemetry receiver. In: International foundation for telemetering;.

7. Don M, Ilg M. Advances in a low-cost software-defined telemetry system. In: International foundation for telemetering;.

8. Grabner MJ, Don ML, Zajicek J, Ilg MD, Hall R, Hallameyer JM, States CARLAPGU. A networked software-defined radio telemetry receiver. CCDC Army Research Laboratory Aberdeen Proving Ground United States, Tech. Rep. 2020;.

9. Don ML, Brown TG, Bukowski EF, States CARLAPGU. Wired signal time-stamping with a software-defined radio telemetry receiver. CCDC Army Research Laboratory Aberdeen Proving Ground United States, Tech. Rep. 2020;.

10. Don ML. The feasibility of radio direction finding for swarm localization. CCDC Army Research Laboratory Aberdeen Proving Ground United States, Tech. Rep. 2017;.

11. Ettus Research. Ettus Research, an NI Brand. https://www.ettus.com/; 2023 Accessed: 13 Oct. 2023.

12. Hanson DW. Fundamentals of two-way time transfers by satellite. In: Proceedings of the 43rd annual symposium on frequency control; p. 174–178.

13. Lanzisera S, Zats D, Pister KSJ. Radio frequency time-of-flight distance measurement for low-cost wireless sensor localization. IEEE Sensors Journal. 2011;11(3):837-845.

14. Van Trees HL, Bell KL, Tian Z. Detection estimation and modulation theory. Wiley; 2013.

15. Zekavat SA, Buehrer M. Handbook of position location: theory, practice and advances. IEEE Press; 2012.

16. Demmel J. Basic Issues in Floating Point Arithmetic and Error Analysis. 2019.

17. Analog Devices. RF Agile Transceiver AD9364. https://www.analog.com/media/en/technical-documentation/data-sheets/AD9364.pdf; 2014 Accessed: 13 Oct. 2023.

18. Ettus Research. USRP B200, Block Diagram. https://www.ettus.com/all-products/UB200-KIT/; 2023 Accessed: 13 Oct. 2023.

19. Ettus Research. USRP E312, Block Diagram. https://www.ettus.com/all-products/USRP-E312/; 2023 Accessed: 13 Oct. 2023.

20. Golomb SW, Gong G. Signal design for good correlation: for wireless communication, cryptography, and radar. Cambridge University Press; 2005.

21. Sarwate DV, Pursley MB. Crosscorrelation properties of pseudorandom and related sequences. Proceedings of the IEEE. 1980;68(5):593-619.

22. NAVSTAR GPS user equipment introduction. US Government Navigation Center; 1996.

23. Miao G. Fundamentals of mobile data networks. Cambridge University Press; 2016.

24. Specification GSS. Global Positioning System Standard Positioning Service Signal Specification, [S]. 1995.

25. IEEE 802.15.1 wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs). LAN/MAN Standards Committee; 2002 Apr.

26. Organick EI. A fortran iv primer. 1st ed. Addison-Wesley Publishing Company; 1966.

27. Corum S, Bonior JD, Qiu RC, Guo N, Hu Z. Evaluation of phase error in a software-defined radio network testbed. In: 2012 proceedings of ieee southeastcon; p. 1–4.

28. Watteyne T, Lanzisera S, Mehta A, Pister KSJ. Mitigating multipath fading through channel hopping in wireless sensor networks. In: 2010 ieee international conference on communications; p. 1–5.

29. Schmidt R. Multiple emitter location and signal parameter estimation. IEEE Transactions on Antennas and Propagation. 1986;34(3):276-280.

30. Barabell AJ. Performance comparison of superresolution array processing algorithms. revised. Massachusetts Institute of Technology Lincoln Lab; 1998.

List of Symbols, Abbreviations, and Acronyms

AGC: automatic gain control

C/A: Course/Aquisition

CPC: clock phase correction

CPU: central processing unit

DFT: discrete Fourier transform

EVD: eigenvector decomposition

FPGA: field-programmable gate array

GFSK: Gaussian frequency shift keying

GPS: global positioning system

IQ: in-phase/quadrature

LFSR: linear feedback shift register

LOS: line of sight

LPF: low-pass filter

MSps: megasamples per seconds

MUSIC: multiple signal classification

NRZ: non-return to zero

PLL: phase lock loop

PN: pseudo-noise

RF: radio frequency

RFFE: radio frequency front-end

RFIC: radio frequency integrated circuit

RMSE: root mean square error

RSSI: received signal strength indicator

SDR: software-defined radio

TWR: two-way ranging

UHD: USRP Hardware Driver

USRP: Universal Software Radio Peripheral

1 (PDF) DEFENSE TECHNICAL INFORMATION CTR
DTIC OCA

1 (PDF) DEVCOM ARL
FCDD RLB CI
TECH LIB

25 (PDF) DEVCOM ARL
FCDD RLA WE
B J ACKER
T G BROWN
M BROWN
S BUGGS
E BUKOWSKI
J COLLINS
B DAVIS
M DON
D EVERSON
J HALLAMEYER
M HAMAOUI
T HARKINS
B HART
M ILG
B KLINE
C MILLER
D PETRICK
K PUGH
S SCHMELTZER
N SCHOMER
F SHEDLESKI
B TOPPER
J ZAJICEK
FCDD RLA W
T SHEPPARD
FCDD RLA CL
F FRESCONI