Exploring the use of signals of opportunity for practical localization

Cheng, Chi

2015

Cheng, C. (2015). Exploring the use of signals of opportunity for practical localization. Master's thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/62929>

<https://doi.org/10.32657/10356/62929>

**NANYANG
TECHNOLOGICAL
UNIVERSITY**

**EXPLORING THE USE OF SIGNALS OF
OPPORTUNITY FOR PRACTICAL LOCALIZATION**

**CHENG CHI
SCHOOL OF ELECTRICAL AND ELECTRONIC
ENGINEERING**

2015

EXPLORING THE USE OF SIGNALS OF OPPORTUNITY FOR PRACTICAL LOCALIZATION

CHENG CHI

School of Electrical and Electronic Engineering

A thesis submitted to the Nanyang Technological University
in partial fulfilment of the requirement for the
degree of Master of Engineering

2015

Abstract

The Global Positioning System (GPS) provides position estimates on the Earth at anytime, anywhere and in any weather. However, to provide robust localization performance, GPS requires an unobstructed path to satellite signals. As such, GPS performance generally degrades or becomes non-existent in environments like indoors or in larger urban areas. So the use of non-localization purposed signals, commonly referred as Signals of Opportunity (SOP) and including signals such as radio (AM/FM, DAB) transmission tower, cellular/mobile phone network (GSM/3G) base stations, LEO satellite signals (Iridium/Orbcomm), and Wi-Fi access points are being considered as alternatives for position estimation.

Different signals have different signal structures, thus will be used at different ways. In this research, we will investigate properties of signals come from LEO Iridium satellites, GEO Inmarsat Satellite and airplanes. Specifically, we will explore the usage of time difference of arrival (TDOA) techniques on those signals of opportunity. Moreover, we also propose an all-wireless relaying architecture for improving the performance of TDOA based localization .

For this research, Universal Software Radio Peripherals (USRPs) are used for all experiments and implementations.

Acknowledgments

I would like to express the deepest appreciation to my advisor Prof. Tay Wee Peng, for his friendly and expert guidance during the last few years, and for giving me the opportunity to work on the project.

I would like to thank Dr. Francois Quitin for his invaluable help in understanding software defined radio. I have learnt a lot from his scientific thinking methodology, rigorous work attitude and his personality of generosity. Without his guidance and constant help this dissertation would not have been possible.

I also like to thank my friends in the reseach group: Jianhua Tang, Wuqiong Luo, Mei Leng, Yi Zhang, Wenjie Xu, Ruoyu Li and Wuhua Hu for the stimulating discussions, and for all the fun we have had in the last few years.

Table of Contents

Acknowledgments	iii
List of Figures	vi
List of Tables	viii
Chapter 1	
Introduction	1
1.1 Motivation	1
1.2 Objectives	2
1.3 Major Contributions of the Thesis	2
1.4 Organization of the Thesis	3
Chapter 2	
Background of Wireless Localization Techniques	4
2.1 Non-TDOA Localization Systems	4
2.1.1 TOA	4
2.1.2 AOA	5
2.1.3 RSS	5
2.2 TDOA Localization Systems	7
2.2.1 Fundamentals of TDOA	7
2.2.2 Common Problems in TDOA	8
Chapter 3	
Background of Software Defined Radio	10
3.1 USRP	10
3.1.1 WBX Daughterboard	12
3.1.2 GPS Disciplined Oscillator (GPSDO) Module	13
3.2 UHD	14
3.3 GNU Radio	15

Chapter 4	
Signals of Opportunity	17
4.1 Iridium Satellite Result	18
4.1.1 Iridium System Overview	18
4.1.2 Iridium Channel Characteristic	19
4.1.3 Outdoor Experiment Results	21
4.2 Inmarsat Satellite Result	23
4.2.1 Inmarsat System Overview	23
4.2.2 Outdoor Experiment Results	24
4.3 Automatic Dependent Surveillance Broadcast (ADS-B) Result . . .	29
4.3.1 ADS-B Signal Overview	29
4.3.2 Outdoor Experiment Result	30
4.3.3 Decoding ADS-B Signal	33
Chapter 5	
TDOA Performance	35
5.1 Iridium Result	36
5.2 Inmarsat Result	37
5.3 Island Wide Experiment Result	38
Chapter 6	
No-GPS Synchronization	47
6.1 USRP GPS Synchronization Error	48
6.2 Relaying Architecture for TDOA	49
6.3 Indoor Cable Experiment Result	52
6.4 Outdoor Experiment Results	54
6.4.1 1D Result Using Relaying Architecture	54
6.4.2 2D Result Using Relaying Architecture	55
Chapter 7	
Conclusion and Future Work	58
7.1 Conclusion	58
7.2 Future Work	59
7.2.1 Completely Remove GPS in Relaying Architecture	59
7.2.2 Explore Signal Characteristic of Broadcasting Signal Like Orbcomm, GSM, DVB-T	59
7.2.3 Combining IMU with TDOA estimation	59

List of Figures

2.1	TOA Illustration	5
2.2	AOA Illustration	6
2.3	TDOA Illustration	7
3.1	USRP in Receiving	11
3.2	USRP in Transmitting	11
3.3	USRP Block Diagram	13
3.4	WBX without UHD Corrections	14
3.5	GNU Radio Companion Example	16
4.1	Gpredict Main Window	18
4.2	Coverage Map of the Iridium System	19
4.3	TDMA Frame	20
4.4	Burst Structure	21
4.5	Iridium Frequency Domain Plot	22
4.6	Iridium Time Domain Plot	23
4.7	Iridium Packet Plot	23
4.8	Inmarsat I4 Series Coverage map	25
4.9	Inmarsat Frequency Domain Plot	27
4.10	Inmarsat Time Domain Plot	27
4.11	Inmarsat Red Packet Spectrum Plot	28
4.12	Inmarsat Green Packet Spectrum Plot	28
4.13	Planes around Singapore	30
4.14	ADSB Packet Format	30
4.15	ADS-B Time Domain Plot	31
4.16	Mode S Squitter Packet	32
4.17	Mode S Extended Squitter Packet	32
4.18	Mode S Position Squitter	33
4.19	Airplane Trajectory based on Decoded Positions	34
4.20	Mode S Velocity Squitter	34
5.1	Sharing Clock Reference	36
5.2	Iridium Co-site Experiment Setup	37
5.3	Iridium Packet Plot	38

5.4	Cross Correlation of Iridium Ring Alert Packet	39
5.5	Inmarsat Co-site Experiment Setup	40
5.6	Cross Correlation of Inmarsat Packets	41
5.7	Locations of These Three Locations on Map	41
5.8	Iridium Satellite 1: TDOA Results vs SGP4 Model	42
5.9	Iridium Satellite 1: TDOA Error	43
5.10	Iridium Satellite 2: TDOA Results vs SGP4 Model	43
5.11	Iridium Satellite 2: TDOA Error	44
5.12	Inmarsat Satellite: TDOA Results vs SGP4 Model	44
5.13	Inmarsat Satellite: TDOA Error	45
5.14	ADS-B: TDOA Results vs Decoded Positions	45
5.15	ADSB: TDOA Error	46
6.1	Setup for Measuring TDOA between USRPs	47
6.2	Error Between USRPs	48
6.3	Relaying Architecture Illustration	50
6.4	Relaying Architecture Explained in Detail	50
6.5	Cabled Experiment Setup.	53
6.6	Comparison between Measured Cables Lengths and True Cable Lengths	54
6.7	1D Experiment Setup	54
6.8	1D Experiment Result Using Relaying Architecture	55
6.9	Hyperboles corresponding to the TDOAs Estimations	56
6.10	Experimental TDOA Error for Outdoor Experiment	57
7.1	Localization System Flowchart	60

List of Tables

3.1	Summary of N210 Specifications	12
3.2	Summary of GPSDO Specifications	14
4.1	Summary of Iridium Communication System Specifications	20
4.2	Summary of Inmarsat Communication System Specifications	24
4.3	Summary of ADS-B Signal Specifications	29

Introduction

1.1 Motivation

Location information has become indispensable for many applications, including wireless sensor networks [1] and location based services [2]. A common localization method is the use of the Global Positioning System (GPS) to provide position coordinates. However, this technique requires a dedicated receiving device to receive and decode GPS signals, and GPS service degrades quickly when the signal is denied, impaired or otherwise unavailable [3]. Therefore, alternatives to GPS localization have been widely investigated, and localization using signals of opportunity has gained increasing interest recently [4, 5]. The signals of opportunity are generally public signals transmitted from an already established signal infrastructure for non-navigation purposes, including AM/FM radio signals, digital television signals, cellular communication signals, and WiFi signals. These signals conform to well-established standards and can be detected in most urban areas with relatively high signal-to-noise ratio (SNR). This motivates us to explore different signals of opportunity and to test their potential for localization purposes.

Various measurements can be extracted from signals of opportunity for localization purposes, including Received Signal Strength (RSS), Time of Arrival (TOA), and Time Difference of Arrival (TDOA). Since signals of opportunity are generally not designed for navigation purpose, it may be difficult to obtain the knowledge of certain characteristics like transmit power and transmit time. Compared with

RSS and TOA, TDOA is an attractive alternative since it can remove the ambiguity caused by unknown transmit time or unknown signal structure. Therefore, we focus on TDOA measurements in this research.

1.2 Objectives

The objective of this research is to explore the use of signals of opportunity for practical localization. This is of great importance when we want to navigate in environments where GPS is unavailable or GPS performance degrades severely.

To that end, this research evaluates the performance of several potential signals for TDOA estimations and proposes a relaying scheme for mitigating time synchronization errors in TDOA localization systems.

1.3 Major Contributions of the Thesis

The contributions of this thesis can be summarized as follow:

- We investigate the signal structures of Low Earth Orbit (LEO) Iridium satellites, Geostationary Earth Orbit (GEO) Inmarsat satellite and airplanes, and present the data packet format, modulation and multiplexing scheme of each signal.
- We perform experimental measurements to collect signals and evaluate their potential for localization using their TDOA estimation performance.
- We propose a relaying scheme for mitigating hardware delay errors found during field experiments.
- We conduct indoor and outdoor experiments to verify the performance of the relaying scheme.

1.4 Organization of the Thesis

The rest of this thesis is organized as follows. Chapter 2 gives an overview of existing wireless localization techniques. Chapter 3 describes the software defined radio receiver we use for receiving different signals of opportunity. In Chapter 4, we present the signal structures of signals from Iridium and Inmarsat satellites, and downlink signals from airplanes. We also present measurement results from our experiments using the software defined radio platform. Chapter 5 discusses the TDOA estimation performances for those potential signals. For Chapter 6, we propose a relaying scheme for improving the performance of TDOA estimation. Chapter 7 concludes the thesis and outlines the future works.

Background of Wireless Localization Techniques

Many results have been accomplished in the area of wireless localization techniques [6–9]. In this chapter, we will briefly describe some common localization techniques, and then we will focus on localization systems using TDOA.

2.1 Non-TDOA Localization Systems

In general, there are three techniques other than TDOA based technique for localizing a target: TOA based, Angle of Arrival (AOA) based and RSS based.

2.1.1 TOA

The idea of TOA [7] is simple. The distance can be determined by multiplying the signal propagation time from the source to the receiver by the speed of electromagnetic wave in the transmission medium. Many existing radiolocation systems use TOA, including the well-known GPS. An illustrative 2D localization example using TOA is shown in Figure 2.1. The intersection of the three circles is the location of the target.

Due to its simplicity, TOA based localization system is relatively easy to implement. However, accuracy of the system highly depends on clock errors between

Figure 2.1. TOA Illustration

the source and the receiver. To mitigate clock error, we will need additional measurement to estimate it as a bias and eliminate it from the measurements [10]. Moreover, the requirement that transmitting signal needs to have timestamp information also limits its usage scenarios.

2.1.2 AOA

AOA [9] is another popular localization solution. It has many real applications including geolocation of cell phones, nautical position fixing in and around coastal regions, etc. A special antenna array that can receive multiple signals from the sources is needed for measuring angle of arrival. The position of the source is then determined by the intersection of several signal direction lines. Figure 2.2 shows how target is being localized using AOA.

Unlike TOA technique, AOA doesn't require precise time synchronization between measurement units. However, the disadvantage is that antenna array is often big size and high cost.

2.1.3 RSS

Using RSS indicator for localization is one of the most common methods for practical systems. To use RSS measurement, we need to form a mathematical path loss model to describe the signal attenuation over distance from the source to the

Figure 2.2. AOA Illustration

receiver. Once we have the model, the distance can be determined straightforward from the pass loss Equation 2.1.

$$PL = PL_0 + 10\gamma \log_{10}\left(\frac{d}{d_0}\right) + n \quad (2.1)$$

where

- PL is total pass loss;
- PL_0 is path loss at reference distance of d_0 ;
- γ is pass loss exponent;
- n is a normal random variable with zero mean

The disadvantages of this technique are

- the system is highly sensitive to multipath fading and shadowing
- parameters in the path loss model need to be calibrated case by case

2.2 TDOA Localization Systems

TDOA [6] refers to the difference in propagation time from a transmitter to two distinct receivers. For a pair of nodes in 2D, the solution to the TDOA equation defines a hyperbola. Using three receivers at known locations, we can determine the location of a target in 2D environment from the intersection of the two hyperbolas formed between receiver pairs AB and AC. Illustration is in Figure 2.3.

Figure 2.3. TDOA Illustration

2.2.1 Fundamentals of TDOA

TDOA can directly obtained by correlating the signals from a pair of receivers and finding the maximum of the ambiguity function.

$$TDOA = \arg \max_{\tau} \sum_t r_1(t) r_2^*(t + \tau) \quad (2.2)$$

Equation 2.2 is the simplest case where we have assumed that clock frequency is not drifting with time. In practice, the clock is always not perfect. We will have to form an ambiguity function considering both TDOA and FDOA, and get

the TDOA/FDOA pair that maximizes the function value. The corresponding function is Equation 2.3.

$$TDOA/FDOA = \arg \max_{\tau, \omega} \sum_t r_1(t) r_2^*(t + \tau) e^{-j\omega t} \quad (2.3)$$

The estimator is unbiased and has a CRLB for locating the location of the peak of the ambiguity function [11].

$$\sigma_{TDOA} \geq \frac{1}{2\pi\sqrt{2}B_{rms}\sqrt{BT * SNR_{eff}}}$$

$$\sigma_{FDOA} \geq \frac{1}{2\pi\sqrt{2}T_{rms}\sqrt{BT * SNR_{eff}}}$$

where

- B_{rms} is effective bandwidth of the signal;
- T_{rms} is effective duration of the signal;
- BT is time bandwidth product;
- SNR_{eff} is effective SNR

2.2.2 Common Problems in TDOA

The accuracy of TDOA estimation depends on several factors such as receiver bandwidth, SNR of received signal, bandwidth of transmitted signal, multipath and time reference of different nodes.

- Receiver bandwidth: Higher bandwidth will result in better resolution when calculating the ambiguity function. Since the bandwidth is limited by the receiver hardware, we can try oversampling to smooth the resulted function and thus improve the resolution. For example, we can set sampling rate at 10 MHz for Universal Software Radio Peripheral (USRP), then oversample 10 times to give us a 100 MHz signal.

- SNR of received signal: Bad SNR signals will have a lower correlation peak. Sometimes, there is no peak in the ambiguity function when the SNR is too low. To solve this problem, we can try correlating longer signals.
- Transmitter bandwidth: Narrowband transmitted signal will give us a very wide peak in the ambiguity function, which is very hard to find the correct peak. Most of the time in practice, we cannot do anything about it but increase the length of the signal for correlating.
- LOS and multipath: Due to multipath, there will be multiple peaks in ambiguity function and the strongest peak is not always the LOS signal. For cases that we have knowledge of transmitted waveform, we can estimate the channel and extract the LOS signal.

Background of Software Defined Radio

Software defined radio [12] is a Radio Frequency (RF) transceiver where one or multiple operations that are traditionally implemented in hardware are done digitally on a Field-Programmable Gate Array (FPGA) or on a computer. These hardware components includes amplifiers, filters, modulators, demodulators and so on. A software defined radio can have flexible analog RF hardware that can be controlled through software, like tunable analog-to-digital (ADC) converter, tunable RF mixer. Since those hardware components' functionalities can be defined in software without difficulty, we can adjust a software defined radio system for different scenarios easily without making significant hardware changes.

In the following, we will cover some background of the popular software defined radio USRP with its companion driver Universal Hardware Driver (UHD). An open source freeware toolkit called GNU Radio will also be introduced.

3.1 USRP

USRPs are computer hosted software radios, products of Ettus Research [13]. The USRP product family is inexpensive and flexible, and is widely used for proof-of-concept implementation or actual transceivers.

Figure 3.1. USRP in Receiving

Figure 3.2. USRP in Transmitting

As a receiver, the USRP down-converts the RF signals and sends the baseband samples over an Ethernet link to a host computer, and several analog RF parameters can be controlled through software. Similarly, as a transmitter, the USRP up-converts the baseband signal from the host to RF, parameters can be adjusted by software. Also, it is possible to program the USRP internal FPGA using common tools like Xilinx ISE Design Suite [14]. The USRP can then be used as a stand-alone device, without the need of communicating with host computer.

The USRP model used in our research is USRP N210. It belongs to the high performance class of the USRP family of products. The N210 hardware is quite suitable for various applications including physical layer prototyping, cognitive radio, dynamic spectrum access and networked sensor deployment.

The N210 provides MIMO capability with high bandwidth and dynamic range. An Ethernet interface is used for connection between the host computer and the N210 hardware. Theoretically, we are able to transmit and receive at 50 MS/sec simultaneously in real time. A more detailed specification of the N210 is shown in Table 3.1.

Table 3.1. Summary of N210 Specifications

Parameters	Specification
ADC sample rate	100 MS/s
ADC resolution	14 bits
DAC sample rate	400 MS/s
DAC resolution	16 bits
Host sample rate (8/16 bits)	50/25 MS/s
Frequency accuracy	2.5ppm
With GPSDO	0.01ppm
Receive noise figure	5 dB
Power output	15 dBm

3.1.1 WBX Daughterboard

The USRP N210 can operate from DC to 6 GHz. The main reason is there's a wide range of daughterboards that are compatible with it. In our experiment, we choose WBX 50-2200 MHz Rx/Tx (40 MHz) as daughterboard since it covers the downlink of ADS-B signals from airplanes, Iridium satellites and Inmarsat satellite.

The block diagram of USRP N210 with WBX daughterboard is shown in Figure 3.3. Incoming signals attached to the standard SMA connector are mixed down using a direct-conversion receiver (DCR) to baseband I/Q components, which are sampled by a 2-channel, 100 MS/s, 14-bit ADC. The digitized I/Q data follows parallel paths through a digital down-conversion (DDC) process that mixes, filters, and decimates the input 100 MS/s signal to a user-specified rate. The down-converted samples can be represented in 16-bit or 32-bit. The choice is application dependent and usually limited by hardwares. In this thesis, 32-bit mode (16 bits for I and 16 bits for Q) is used. The samples can be passed to the host computer at up to 25 MS/s over a standard Gigabit Ethernet connection.

For transmission, baseband I/Q signal samples are synthesized by the host computer and pass to the USRP N210 at up to 25 MS/s over Gigabit Ethernet. The USRP hardware interpolates the incoming signal to 400 MS/s using a digital up-conversion (DUC) process and then converts the signal to analog with a dual-channel, 16-bit digital-to-analog converter (DAC). The resulting analog signal is then mixed up to a user specified carrier frequency.

Figure 3.3. USRP Block Diagram

The detail performance characteristic of WBX with N210 can be found at Ettus website [15]. As an example, we show the noise figure, IP2 and IP3 information of N210+WBX in Figure 3.4 when the receiver is operating at 1.6 GHz. We can see that the minimum noise figure is around 7 dB. This is acceptable if we receive ADS-B signals from airplanes, but we will have to put a low noise amplifier (LNA) before the USRP N210 to improve overall noise figure of the receiver system to receive satellite signals. We can calculate the overall noise figure of a receiver system from the Friiss formula $F_{receiver} = F_{LNA} + \frac{(F_{rest}-1)}{G_{LNA}}$ when cascading a LNA with WBX. For example, for LNA ZHL-1217MLN, the noise figure is 1.5 dB and gain is 30 dB for frequency 1200 - 1700 MHz. For WBX, we normally set the gain at 10 dB which gives us a noise figure of 20 dB. Hence the receiver system has an overall noise figure of 1.8 dB.

3.1.2 GPS Disciplined Oscillator (GPSDO) Module

Another important component in the USRP N210 is GPSDO module. This module can be used to discipline the USRP N210 reference clock to within 0.01 ppm of the worldwide GPS standard. The GPSDO also provides a pulse-per-second (PPS) signal with an 1-sigma error 50 ns of the UTC time when locked to GPS signal. The detail specification is in Table 3.2. The accuracy of the PPS signal will be highly related to the time synchronization errors in later experiments.

Figure 3.4. WBX without UHD Corrections

Table 3.2. Summary of GPSDO Specifications

Parameters	Specification
1 PPS Accuracy	50ns to UTC RMS (1-Sigma) GPS Locked
Holdover Stability	$< \pm 11 \mu\text{s}$ over 3 hour period at +25C
Sensitivity	Acquisition -144dBm, Tracking -160dBm
Warm Up Time / Stabilization Time	5 min at +25C to 1E-08 Accuracy
Frequency Output	10MHz
Frequency Stability Over Temperature	2.5E-08

3.2 UHD

UHD is the universal driver for USRP and contains firmware and FPGA image. After installing UHD on a computer, it comes with a series of useful commands and utilities. For example, one can use *uhd_usrp_probe* to query the USRP and see

the models specification and parameters. Another example is *uhd_fft*, which gives a quick and easy to use spectrum analyzer.

3.3 GNU Radio

Once the signal is down-converted and digitized, GNU Radio [16] can be used to perform all the signal processing. In the GNU Radio toolkit, we can have channel coding, filters, synchronization elements, modulators, and many other elements that are common in radio communication systems.

GNU Radio gives access to all of the USRP functionalities, and it includes a block based method for doing a series of signal processing. This is a typical example of GNU Radio flow graph. Most of the blocks in the picture are included in the GNU radio package by default. If you cannot find the block for your task, you can easily create a block using C++.

GNU Radio is easy to use. You can create a FM receiver in minutes by building up the blocks. Moreover, in GNU Radio, every block has a separate thread. This guarantees that the toolkit is also capable for implementing real-time, high throughput radio systems. Another advantage of GNU Radio is it has a good supporting community. You can easily get answers by asking questions on the mailing list.

Figure 3.5. GNU Radio Companion Example

Chapter 4

Signals of Opportunity

After our survey in frequency band from 80 MHz to 2 GHz, we have focused our research on several signal sources as potential beacons, including Iridium satellites [17–20], Inmarsat satellite [21, 22] and airplanes. Positions of the Iridium satellites and Inmarsat satellite can be predicted by using SGP4 model. Positions of airplanes can be decoded from their broadcasting downlink signal.

In this chapter, we will present some measurement results from these signal sources. A preliminary study on the signal structure (bandwidth, duration, frequency, time of transmission) of different sources is also provided.

All the data collections are based on USRPs. The program for controlling the USRP is either a C++ program based on UHD or a Python program based on GNU Radio.

To assist in receiving satellite signal, we have used an open source software Gpredict for real time satellite tracking and orbit prediction. Before each satellite signal collection experiment, we will use it to predict the time of future passes above Singapore and learn each pass in detail. The screenshot of its main window is shown in Figure 4.1. From the main window, we can see which satellite is coming in the near future, what is the trajectory of the current passing satellite and where are all the satellites in global view.

Figure 4.1. Gpredict Main Window

4.1 Iridium Satellite Result

4.1.1 Iridium System Overview

The Iridium satellite system [18] is a mobile communication system, which is designed to provide truly global voice and data communication services. Every satellite is orbiting at a height about 780 km with a speed around 7.5 km/sec. It takes 100 minutes and 28 seconds for each satellite to circle around the earth. The satellite view time for Singapore is around 15 minutes.

Each satellite is cross-linked to four other satellites: two satellites in the same orbit plane and two in an adjacent plane. Thus, the Iridium constellation consists 66 active satellites and 14 spares orbiting in a constellation of six polar planes. This constellation ensure that every region on the global is covered by at least one satellites at all times. The global coverage map is shown in Figure 4.2. In the figure, the coverage area of every Iridium satellite is shown as a circle.

The Iridium satellites communicate with ground mobile users with frequencies

Figure 4.2. Coverage Map of the Iridium System

in L band. The communication between the earth gateway and satellites are in the band between 29.1 GHz and 29.3 GHz for the up-link and in the band between 19.1 GHz and 19.6 GHz for the downlink [19]. The frequency band for communication between the satellites is between 22.55 GHz and 23.55 GHz.

Frequency band 1616 - 1626.5 MHz is allocated for Iridium communication system. There are 240 channels and each channel is separated by 41.67 KHz. A channel bandwidth of 31.5 KHz is used for data communication. Table 4.1 has the technical parameters of the Iridium satellite transmitter.

4.1.2 Iridium Channel Characteristic

For Iridium downlink, every Time Division Multiple Access (TDMA) frame is 90 ms. Each frame contains a 20.32 ms downlink simplex time slot, four uplink time slots and four downlink time slots, which provides the duplex channel capability. The TDMA frame is illustrated in Figure 4.3. The simplex time slot is used only for downlink and designed for ring alert and message channel. For TDOA localization, we will use this simplex time slot for cross correlating.

In Iridium's Frequency Division Multiple Access (FDMA) scheme [20], each

Table 4.1. Summary of Iridium Communication System Specifications

Parameters	Specification
Number of satellites	66
Number of orbit planes	6
Number of spot beams	48
Altitude	780 km
Orbital period	100 mins and 28 secs
Polarization	RHCP
Transmit power	1200 W
Satellite to user downlink	1616 - 1626.5 MHz
Satellite to gateway downlink	19.1 - 19.6 GHz
Gateway to satellite uplink	29.1 - 29.3 GHz
Access scheme	TDMA/FDMA
Channel bandwidth	31.5 KHz

Figure 4.3. TDMA Frame

frequency access is a 41.667 KHz band and assigned to be a duplex channel band or simplex channel band. For duplex channel, we are able to receive signal from satellite only if there is a communication happening between the satellite and a mobile terminal. In other words, the downlink signal is not always there. So we move our focus to simplex channels located between 1626.0 MHz and 1626.5 MHz. In these channels, there is a broadcasting channel centered at 1626.270833 MHz designated for ring alert message. The advantages of this channels are: 1) the signal is always available, ring burst appears every 4.32 seconds 2) every Iridium satellite uses this channel 3) the transmitting power for this channel is higher than other voice and data channels.

Iridium downlink signals are transmitted as bursts. Each burst has three segments: preamble, unique word and data. Preamble is just pilot tone signal, unique

word is binary phase-shift keying (BPSK) modulated signal and data is differential quadrature phase-shift keying (DQPSK) modulated and pulse shaped using a root-raised-cosine (RRC) filter with rolloff factor of 0.4. The structure is described in Figure 4.4.

Figure 4.4. Burst Structure

4.1.3 Outdoor Experiment Results

The process of Iridium signal acquisition involves a USRP N210 with WBX daughterboard, a laptop with GNU Radio software installed, a LNA (ZHL-1217MLN) from Mini-circuits with a DC power supply, an Iridium antenna, various SMA to SMA cables and connectors. RG-59/U coax was used for the connections between the LNA and the USRP input port. Data was transferred over a 1Gbps Ethernet cable from the USRP to the laptop.

The data collection was conducted on the roof of S2 in order to make sure there was a line of sight propagation between Iridium satellites and USRP receiver. We recorded data only after the USRP was locked to GPS signal. This is to guarantee that the USRP has a very accurate clock. The parameters we set for collecting Iridium:

- Center frequency: 1626.27 MHz
- Sampling rate: 10 MS/s
- Gain: 0 dB
- Duration: 20 seconds

Using the settings listed above, the USRP down-converted the RF signal to baseband signal directly and saved the data to hard drive. After we collected the data in binary format, we processed it offline using MATLAB.

Figure 4.5 is the frequency domain plot of the Iridium satellite signal. Since we sampled at 10 MS/s, we captured the whole 10 MHz band centered at 1626.27 MHz. Many signals that were out of Iridium signal band were captured as well. Hence, before plotting the time domain data, we filtered it thorough a low pass filter with a cutoff frequency of 100 KHz. Figure 4.6 shows the time domain plot of the 20 seconds filtered data. From the plot, we can see clearly there are packets appearing periodically. We find that the period is 4.32 seconds.

Figure 4.5. Iridium Frequency Domain Plot

If we zoom in the packet data as shown in 5.3, we can see a packet about 7 ms long. As we expected, the packet is divided into preamble and data. This confirm that we were receiving the Iridium signal.

Figure 4.6. Iridium Time Domain Plot

Figure 4.7. Iridium Packet Plot

4.2 Inmarsat Satellite Result

4.2.1 Inmarsat System Overview

Inmarsat is the world's first international and non-governmental Gateway Mobile Switching Centre (GMSC) operator and is still the only one to offer a mature

range of modern communications services to maritime, land, aeronautical and other mobile users [21, 22]. Currently, Inmarsat operates 10 satellites in geosynchronous orbit, which means their position appears to be fixed when viewed from the Earth. Satellites are positioned to transmit radio beams in two global configurations. Four of them covering the oceans and three covering the major landmasses. Their combined footprints provide seamless worldwide communications coverage, except in the extreme polar regions.

There are several Inmarsat satellites above Singapore. Since Inmarsat third series satellites are going to be decommissioned, we concentrate on receiving signal from the fourth generation of Inmarsat satellites (I4). There are three I4 satellites currently in operation, coverage map is shown in Figure 4.8:

- I4 Americas, at 98 degrees West
- I4 Europe, Middle East and Africa, at 25 degrees East
- I4 Asia Pacific, at 143.5 degrees East

Parameters of Inmarsat-4 communication systems are listed in Table 4.2.

Table 4.2. Summary of Inmarsat Communication System Specifications

Parameters	Specification
Number of satellites	10
Inclination angle	2.7°
Number of spot beams	5
Altitude	36000 km
Polarization	RHCP
Transmit power	2800 W
Satellite to user downlink	1525-1559 MHz
Access scheme	TDMA/FDMA
Channel bandwidth	200 KHz

4.2.2 Outdoor Experiment Results

For collecting Inmarsat signal, we used the same setup as for Iridium signal. The parameters we set for collecting I4-F1:

Alphasat coverage

Figure 4.8. Inmarsat I4 Series Coverage map

- Center frequency: 1531.3 MHz
- Sampling rate: 10 MS/s
- Gain: 0 dB
- Duration: 20 seconds

Compared to Iridium, Inmarsat is relatively easier to receive since it is a geo-stationary satellite and will always be present above Singapore. Figure 4.9 is the frequency domain plot of the I4-F1 satellite signal. Similar to Iridium signal, before plotting the time domain data, we filtered it through a low pass filter with a cutoff frequency of 150 KHz. Figure 4.10 shows the time domain plot of the 0.2 second filtered data. From the plot, we can see there were two types of packets, weak one marked in red and strong one marked in green. According to the GEO-Mobile Radio Interface Specifications [23], the weak packet is normal burst and the strong

packet corresponds to high margin burst.

To make sure that these two types of packets both come from I4-F1, we have analyzed them separately. Figure 4.11 and Figure 4.12 shows their spectrum separately. From the comparison, we can see that both packets have a bandwidth around 200 KHz, and green packet has a higher SNR than the red one. As we know, Inmarsat I4 channel bandwidth is 200 KHz. This suggests that the signal we have received came from Inmarsat I4.

Figure 4.9. Inmarsat Frequency Domain Plot

Figure 4.10. Inmarsat Time Domain Plot

Figure 4.11. Inmarsat Red Packet Spectrum Plot

Figure 4.12. Inmarsat Green Packet Spectrum Plot

4.3 Automatic Dependent Surveillance Broadcast (ADS-B) Result

4.3.1 ADS-B Signal Overview

ADS-B is a cooperative surveillance technology for tracking airplanes. Airplane determines its own position via Global Navigation Satellite System (GNSS) and periodically broadcasts this at frequency 1090 MHz. With ADS-B, airplanes are required to broadcast their position information to ground control tower and other airplanes. This is the downlink information we are going to use. Those control stations are also broadcasting valuable information for airplanes equipped with ADS-B receiver to use. Parameters of ADS-B signals are listed in Table 4.3.

Table 4.3. Summary of ADS-B Signal Specifications

Parameters	Specification
Number of airplanes	around 10
Altitude	around 10 km
Downlink	1090 MHz
Access scheme	TDMA
Channel bandwidth	1 MHz
Modulation	PPM

Singapore has one of the busiest airports in the world, which makes it a very good place to easily receive ADS-B signals. Figure 4.13 is a snapshot of the airplanes around Singapore at around 2pm. We can see that we should easily have 10 airplanes transmitting their positions and velocity every seconds.

For ADS-B [24], there are two types of data, Mode S squitter and Mode S extended squitter. The format is illustrated in Figure 4.14. They both have preamble part and data block part.

- Mode S squitter: contains a 56 us data block. In the data block, there is only information about the airplane's unique identifier. The frequency is 1/second.
- Mode S extended squitter: contains a 112 us data block. Depends on the squitter type, the data block contains different information. For example, if

Figure 4.13. Planes around Singapore

it is a position squitter, it contains information like latitude, longitude and altitude. If it is a velocity squitter, it contains the velocity information.

Figure 4.14. ADSB Packet Format

4.3.2 Outdoor Experiment Result

For collecting ADS-B signal, we only used USRP with a VERT 900 antenna. The parameters we used:

- Center frequency: 1090 MHz
- Sampling rate: 10 MS/s

- Gain: 15 dB
- Duration: 20 seconds

We have collected the data of ADS-B. The time domain plot is in Figure 4.15. Similar to signal from Inmarsat-4, there were also strong packets and weak packets. However, the strong packets were mode A/C signal, which had interference with mode S signal. The actual data bits were in those weak packets.

Figure 4.15. ADS-B Time Domain Plot

From time domain plot of the data, we can find Mode S squitter (c.f. Figure 4.16) and Mode S extended squitter (c.f. Figure 4.17). We can also see clearly the preamble at the beginning of the data packet from the figure. ADS-B signal is PPM modulated. We can demodulate the signal and decode position of the airplane from the demodulated data.

Figure 4.16. Mode S Squitter Packet

Figure 4.17. Mode S Extended Squitter Packet

4.3.3 Decoding ADS-B Signal

The protocol and format of ADS-B downlink signal is not encrypted, thus can be received and decoded by everyone. We wrote a simple ADS-B decoder using MATLAB. The decoding process can be summarized as follow:

1. use the preamble information to locate all the mode S squitter and find the start index of the packet
2. extract the packet and demodulate the data into bits
3. run CRC on the bits, if fail, flip one bit and re-run the CRC check
4. for all packets that pass the CRC, we find the subtype packets that provide position or velocity information, and decode the information according to packet specifications

Figure 4.18 and Figure 4.20 are example outputs of our MATLAB ADS-B decoder. From position squitter, we can have position data like latitude, longitude and altitude. From velocity squitter, we have speed data in three directions and accuracy level of the data. Figure 4.19 shows trajectories of several planes based on the decoded data.

```

odd_cprlat: 14344
odd_cprlon: 126152
odd_cpertime: 79274937
even_cprlat: 14581
even_cprlon: 33455
even_cpertime: 67980021
alt: 9.2737e+003
lat: 0.6677
lon: 105.2843
plane: '76CCD1'

```

Figure 4.18. Mode S Position Squitter

Figure 4.19. Airplane Trajectory based on Decoded Positions

```

ew_dir: 1
ew_velocity: 428
ns_dir: 0
ns_velocity: 62
vert_rate_source: 0
vert_rate_sign: 1
vert_rate: 8
cprtime: 70778981
accuracy: 'Error < 10m/s'
velocity: [-219.6678 31.3811 -2.2758]
plane: '76CCD1'

```

Figure 4.20. Mode S Velocity Squitter

TDOA Performance

In this chapter, we will show the results of several experiments we conducted for investigating the TDOA performance of the signals of opportunity.

To verify the cross correlation property of the signal, we have used two sets of equipments to collect Iridium signal at the same location. Specifically, we let the two USRP receivers share the same 10 MHz reference signal and PPS signal, and we used GPS time to trigger USRPs to start recording data. Figure 5.1 illustrates the setup. In this way, we have completely removed any TDOA or FDOA that may be caused by hardware. In this case, the ground truth for TDOA estimation is 0.

After the co-site experiments described above, we also present some results from island wide experiments. In the experiments, we measure TDOA performance by comparing the estimated TDOA from the ground truth TDOA. The estimated TDOA is from cross correlation of the received signals from different receivers. The way of getting the ground truth TDOAs depends on the type of the signals of opportunities. For Iridium and Inmarsat satellites, we can get the satellite positions from SGP4 model. For airplanes, we can decode the received signals and get the airplanes' positions. We know the locations of our receivers, and then we can calculate the TOA from the source of signal to every receiver. By taking the difference of TOAs, we get the ground truth TDOA.

Figure 5.1. Sharing Clock Reference

5.1 Iridium Result

The test setup is shown in Figure 5.2. Two receivers were placed side by side and sharing the same 10 MHz reference signal and PPS signal. For each receiver, the components were USRP N210 with WBX daughterboard, a laptop with GNU Radio software installed, a LNA (ZHL-1217MLN) from Mini-circuits with a DC power supply, an Iridium antenna, a SMA to SMA cables and connectors. The TDOA we wanted to measure was $t_1 - t_2$. The two Iridium antennas were placed nearly at the same location and receiving the signal from the same Iridium satellite, hence the expected value of $t_1 - t_2$ was close to 0 ns.

We used the setup to collect 30 sets of data and each data set was 10 seconds long. For processing data, we first detected where the Iridium packets were located in the 20 seconds duration. After that, we selected a 20 ms length window which covered one whole packet. As shown in Figure 5.3, the amplitude of the packet was higher than the noise amplitude. Hence, we can select the packet from the signal with a simple power detector. At the end, we oversampled the packet data 10 times to 100 MHz and filtered it with a low pass filter. The cross correlation result of one packet is plotted in Figure 5.4. We can see that there was a clear

Figure 5.2. Iridium Co-site Experiment Setup

peak around zero. From 30 sets of the experiment data, we found that the average of TDOA errors was 17 ns with a standard deviation of 110 ns.

As a comparison, we calculated the CRLB for the TDOA estimation. The CRLB can be estimated as follows [11]:

$$\sigma_{TDOA} = \frac{0.55}{B_s} * \frac{1}{\sqrt{BT * SNR}} \quad (5.1)$$

For Iridium experiment, received signal bandwidth B_s is 20 KHz, sampling rate B is 10 MHz, packet length T is 7 ms and SNR is around 5 dB. This gives us σ_{TDOA} to be 79 ns.

5.2 Inmarsat Result

We did the same experiment as for Iridium satellites to verify the cross correlation property of the signal. The setup was shown in Figure 5.5.

Figure 5.3. Iridium Packet Plot

We used the setup to collect 30 sets data and each data set was 10 seconds long. Compared to Iridium signal, it's easier for processing Inmarsat data since we did not need to detect where the packets were. From the recorded 10 seconds data, we directly selected a 50 ms length window which covered several Inmarsat packets. Then we oversampled the data 10 times to 100 MHz and filtered it with a low pass filter. The cross correlation result is plotted in Figure 5.6. We can see that there was a clear peak around zero. From 30 sets of our experiment data, we found that the average of TDOA was 19 ns with a standard deviation of 50 ns. For Inmarsat experiment, the received signal bandwidth B_s was 200 KHz, sampling rate B was 10 MHz, and SNR was around 5 dB. The data packet in Inmarsat signal was shorter than Iridium's. In a 50 ms length window, the total length T was about 700 us. This gave us a CRLB of 25 ns for TDOA estimation.

5.3 Island Wide Experiment Result

We have conducted outdoor experiments using three sets of USRP devices to receive signals from Iridium satellites, Inmarsat satellite and airplanes. The locations

Figure 5.4. Cross Correlation of Iridium Ring Alert Packet

of USRP receivers were obtained from Google Map. For satellite positions, we can calculate them from the SGP4 model. Hence, we can calculate TDOAs based on the satellite positions and receiver positions. For comparison, we treat these calculated TDOAs as true TDOAs. The estimated TDOAs were obtained by cross correlating received signals of the three receivers. For ADS-B signal, we have the true TDOAs by using the decoded airplane positions and receiver locations.

Three set of devices were placed at three locations, shown in Figure 5.7, and they started recording at the same GPS time. For each signal source, five successive TDOA measurements were taken, separated by 30 seconds.

Figure 5.5. Inmarsat Co-site Experiment Setup

- location-1 (L_1): near DSO, using USRP GPS.
- location-2 (L_2): N1 roof @ NTU, using USRP GPS.
- location-3 (L_3): S2 roof @ NTU, using USRP GPS.

For USRP GPS, observed errors range from 50 ns to 300 ns per device, which result in an expected TDOA errors at the order of 100 ns. Detail discussion about the USRP GPS error can be found at Section 6.1.

The results are shown in following Figures. Figure 5.8 and Figure 5.10 show results from two Iridium satellites. We can see that the estimated TDOAs from received signals are close to the true TDOAs. In order to see the magnitude of the error, we have plotted the errors in Figure 5.9 and Figure 5.11.

Figure 5.12 shows result for Inmarsat satellite. Unlike Iridium satellite's result, there are biases between estimated TDOAs and true TDOAs. The bias can be caused by the SGP4 model since the model tend to produce higher error for GEO satellites.

Figure 5.6. Cross Correlation of Inmarsat Packets

Figure 5.7. Locations of These Three Locations on Map

Figure 5.14 shows ADS-B result. We have plotted 9 airplanes on the Figure. We can see that the estimated trajectory and decoded trajectory are close to each other. To see the errors clearly, the TDOA errors are shown in Figure 5.15.

Figure 5.8. Iridium Satellite 1: TDOA Results vs SGP4 Model

Figure 5.9. Iridium Satellite 1: TDOA Error

Figure 5.10. Iridium Satellite 2: TDOA Results vs SGP4 Model

Figure 5.11. Iridium Satellite 2: TDOA Error

Figure 5.12. Inmarsat Satellite: TDOA Results vs SGP4 Model

Figure 5.13. Inmarsat Satellite: TDOA Error

Figure 5.14. ADS-B: TDOA Results vs Decoded Positions

Figure 5.15. ADSB: TDOA Error

Chapter 6

No-GPS Synchronization

When we did experiment using GPS time as the common timestamp between USRPs, we found that the time differences between USRPs were still in the order of 100 ns. This was due to hardware error of the GPSDO modules. We have measured the error between four USRPs, the error was quite random and visible even after 10 hours of warming up. Hence, this chapter would discuss a method we proposed to eliminate the hardware error between USRPs.

Figure 6.1. Setup for Measuring TDOA between USRPs

Figure 6.2. Error Between USRPs

6.1 USRP GPS Synchronization Error

In our experiment, all receiver nodes were synchronized using the embedded GPS modules. To record signal at the same time, we triggered the data logging of all the receivers simultaneously using GPS time. This was achieved by sending a timed data recording command to all the USRP receivers with a common GPS timestamp. Then every USRP would wait for its local clock to reach the timestamp we set. The local time of the USRPs were corrected every second by PPS signals that came from the GPS modules. The synchronization accuracy would depend on the quality of the PPS signals.

If the PPS signals were accurate with respect to the UTC time, or the time difference between two PPS signals was 0 ns, the expected TDOA was 0 ns between every pair of two USRP receivers. To confirm this, we did a test with two USRPs. We split the PPS signal from one USRP and shared it between these two USRPs. The input signals for the USRP receivers were equally split from a signal generator. The output signal of the signal generator was 1 MHz QPSK signal with carrier frequency at 1.6 GHz. Every USRP and signal generator was connected with an

1 meter cable. We started the data logging with timed command and set the sampling rate at 10 MHz. We recorded 50 ms second data every 30 seconds and repeated it for 50 times. The cross correlation results of these 50 sets data shown that the TDOA estimations were 0 ns. This also shown that when the PPS signals were well aligned, initiating the data logging of all receivers didn't introduce extra timing error, or the error can be ignored.

However, in actual experiment, every USRP used its own GPS module. In our lab experiment, we found that the time difference between two PPS signals from two GPS modules was in the order of 100 ns. The lab experiment was as follows. We split a 1 MHz QPSK signal from signal generator into four signals and passed the split signals to four USRPs through four 1 meter long cables. All the four USRPs were synchronized using the GPS modules. The carrier frequency was set at 1.6 GHz. The sampling rate was at 10 MHz. Then, the data logging was triggered with GPS time. We recorded 50 ms second data every 30 seconds and repeated this procedure for 10 hours. Then we estimated the TDOAs between every two USRPs based on the cross correlation result of the 50 ms data.

The result is shown in Figure 6.2. Each color represents a TDOA estimation between a pair of two USRP receivers (R1-R2, R1-R3, R1-R4). For the 10 hour period, we can see that the error was random. In Section 6.2, we will show how to eliminate this error.

6.2 Relaying Architecture for TDOA

In order to improve accuracy and eliminate this error, we propose a relaying architecture shown in Figure 6.3. Relays start measuring approximately at the same time, then each relay forwards the message to a central receiver after some fixed delay. See Figure 6.4 for more detailed illustration.

Here we will show how this relay works. Let $x(t)$ represents the unknown signal transmitted from the RF source. The propagation delay between the RF source and the i -th relay is given by τ_{i1} . The message received by the i -th relay is given

Figure 6.3. Relaying Architecture Illustration

Figure 6.4. Relaying Architecture Explained in Detail

by the following

$$r_i(t) = x(t - \tau_{i1}) \quad (6.1)$$

The i -th relay will sample the message at time T_{0i} . This starting time is relay dependent and would slightly differs for different relays. The sampled message received by the i -th relay is given by

$$r_i[l] = x(T_{0i} + \beta_i l T_s - \tau_{i1}) \quad (6.2)$$

where T_s is the sample rate and β_i is the clock skew of the i -th relay.

Then each relay will wait for its allotted time slot before forwarding the message

to the final receiver. The message transmitted by the i -th relay is

$$t_i = \sum_{l=-\infty}^{+\infty} x(T_{0i} + \beta_i l T_s - \tau_{i1}) \times u(t - \beta_i l T_s - T_{0i} - \beta_i T_{Di}) \quad (6.3)$$

where T_{Di} is the retransmission delay of the i -th relay, and $u(t)$ is the pulse shaping filter of the relay.

We represent the clock skew of the final receiver as β_R . The receiver will start sampling the message from relay i at time $T_{0R} + \beta_R T_{Di}$. The n -th sample of the signal received from relay i at the final receiver can be described as

$$r_R^i[n] = \sum_{l=-\infty}^{+\infty} x(T_{0i} + \beta_i l T_s - \tau_{i1}) \times g(T_{0R} + \beta_R T_{Di} + \beta_R n T_s - \beta_i l T_s - T_{0i} - \beta_i T_{Di} - \tau_{i2}) \quad (6.4)$$

where τ_{i2} is the propagation delay between the i -th relay and the final receiver, and $g(t) = u_t * u'(t)$ with $u'(t)$ being the pulse shaping filter at the receiver. If the pulse shaping filters are chosen appropriately and inter-symbol interference is canceled, we have $g(t) = \delta(t)$ where $\delta(t)$ is the Dirac function. In that case, Equation 6.4 can be simplified to

$$r_R^i[n] = x(T_{0R} + (\beta_R - \beta_i)T_{Di} + \beta_R n T_s - \tau_{i2} - \tau_{i1}) \quad (6.5)$$

If the clock skew $\beta_R = \beta_i = 1$, then Equation 6.5 can be further simplified to

$$r_R^i[n] = x(T_{0R} + n T_s - \tau_{i2} - \tau_{i1}) \quad (6.6)$$

which is independent of the relay measurement time T_{0i} .

For different nodes, the received samples at the receiver node will have identical offsets T_{0R} . The proposed architecture can thus successfully cancel out differences in node measurement time offsets if all clock skews are unity. The receiver then computes the ambiguity functions between the received messages $r_R^i[n]$ and $r_R^j[n]$

from node i and j . The index of the peak of the ambiguity function is equal to $\tau_{i2} - \tau_{i1} - \tau_{j2} - \tau_{j1}$. If τ_{i2} and τ_{j2} are known, the receiver can recover the original TDOA $\tau_{i1} - \tau_{j1}$.

We can see that the time errors introduced by the inaccurate PPS signals lead to different start recording time T_{0i} for every receiver i . After implementing this relaying architecture, we have cancelled out the T_{0i} .

6.3 Indoor Cable Experiment Result

The TDOA estimation setup was first ran in a controlled environment. We used a signal generator for the transmitter, which transmitted a random QPSK modulated signal. The relay nodes consisted of USRPs with WBX daughterboards. The WBX daughterboard can receive and transmit on two different frequency bands. The final receiver was a USRP with a TVRX2 daughterboard, which can receive signals on different frequency bands simultaneously.

The relays and receiver operated at a sampling rate of 10 MHz. The signal generator was transmitting a 1 MHz QPSK signal at 795 MHz. The relays recorded the received signal at 795 MHz and then forwarded the recorded signal to the final receiver at 755 MHz. Every relay delayed the received signal for a different amount of time. The length of the relayed signal was 10 ms.

We used only one relay and one receiver, and the relay-to-receiver link was a short wireless link that accounted for zero-TDOA. A short cable was used for the link between the transmitter and the relay. Cables of various lengths were used for the transmitter-to-receiver link. The setup was illustrated in Figure 6.5. By using cables to connect the transmitter with the relay/receiver, we avoided the problem of multipath (the relay and receiver were placed close to one another, such that the relay-to-receiver link had a very dominant line-of-sight and no multipath either). Figure 6.6 compared the estimated cable length with true cable length for different cable lengths.

The true cable lengths were obtained by measuring the cable delays with a

Figure 6.5. Cabled Experiment Setup.

vector network analyzer (VNA). The estimated cable length was calculated in the following way. We first estimated the TDOA between cable channel and wireless channel by cross correlating the two received signals. For the cable channel, the received signal was continuous. We filtered out a 10 ms signal from the beginning of the recording. For the wireless channel, the signal was delayed by a fixed amount of time. To get the corresponding signal for cross correlation, we filtered out a 10 ms signal after the delay period. We oversampled the 10 ms signal to 100 MHz before the cross correlation. After we got the estimated TDOA, we compensated the propagation delay in the short cable. The final result was the the propagation delay in the cable we wanted to measure. We converted the VNA measured cable lengths to nanoseconds so that we can regard the Y-axis as TDOA estimation error of the relaying architecture. We need to note that the propagation speed is different for different medium when converting length to time. For each cable length, ten measurements were taken.

The results in Figure 6.6 show the mean and 2σ -spread of the measurements. It can be seen that all measurements are within 10 ns of the reference measurement. It can be concluded that, in a controlled environment without multipath, a TDOA accuracy as low as 10 ns can be achieved with our relaying architecture.

Figure 6.6. Comparison between Measured Cables Lengths and True Cable Lengths

6.4 Outdoor Experiment Results

6.4.1 1D Result Using Relaying Architecture

We have done 1D localization experiments using the relaying architecture along the corridor. The setup is shown in Figure 6.7. Relays were R1 and R2. Rx was the final receiver to receive data from relay R1, relay R2 and transmitter Tx. Tx was the target we were trying to localize and being positioned at four different locations (indicated as green dots). The relays and receiver positions were fixed.

Figure 6.7. 1D Experiment Setup

Figure 6.8. 1D Experiment Result Using Relaying Architecture

The target was localized using TDOA estimation. Result is shown in Figure 6.8. Squares in the figure indicate true values while circles indicate estimated values. As an example, the distance between R1 and R2 is defined as follows. For R1, the signal path is Tx-R1-Rx; for R2, the signal path is Tx-R2-Rx. Hence, the distance between R1 and R2 is the difference between these two paths. We can see that, the estimation errors of this experiment were all within 10 meters.

6.4.2 2D Result Using Relaying Architecture

We have also done 2D localization experiments using the relaying architecture. Figure 6.9 show an experimental result for a full-wireless setup with three relay nodes and one receiver. For each transmitter location, ten successive TDOA measurements were taken, separated by 10 seconds. The nodes were placed such that there was a dominant LOS between the transmitter and each relay node, and between the relay nodes and the receiver nodes. However, the LOS was sometimes obstructed by the foliage of a tree or by people passing by during the experiment. With four nodes we had a total of six TDOAs between nodes, and each TDOA described a hyperbole between the two corresponding nodes.

The hyperboles corresponding to one transmitter location (and 10 successive measurements) are shown in Figure 6.9, where each colour corresponds to a different pair of nodes. The blue lines correspond to the TDOA between Rx and R1, the red lines correspond to RX and R2, the green lines correspond to Rx and R3, the cyan lines correspond to R1 and R2, the magenta lines correspond to R1 and R3, and the black lines correspond to R2 and R3. It can be seen that successive measurements might yield slightly different results, and the different hyperboles intersect close to the transmitter's location. The transmitter was moved to a 9 different locations, on a line between Rx and R1. The transmitter locations were separated by 5 m. At each location, ten TDOA measurements were taken, separated by 10 s.

The CDF of all the combined TDOA errors is shown in Figure 6.10. The TDOA error has a mean of -2 ns and a standard deviation of 28 ns. This error is attributed mostly to multipath induced errors: when the LOS is obstructed by foliage or people, the multipath components have a larger influence on the TDOA estimation and can easily induce errors in the TDOA estimation. However, in two thirds of the measurement, the error is below 10 m.

Figure 6.9. Hyperboles corresponding to the TDOAs Estimations

Figure 6.10. Experimental TDOA Error for Outdoor Experiment

Conclusion and Future Work

7.1 Conclusion

In this thesis, we have investigated the signal structures of LEO Iridium satellites, GEO Inmarsat Satellite and airplanes, and presented the data packet format, modulation and multiplexing scheme of each signal.

We have built a USRP based receiver, and have used it to perform experimental measurements to collect signals and evaluated their potential for localization using their TDOA estimation performance. For ADS-B signal, we have implemented an ADS-B signal decoder in MATLAB to get positions and velocities information from the signal.

At last, we have discussed GPS synchronization errors found in the embedded GPSDO modules of USRPs, and proposed a novel wireless TDOA estimation architecture for eliminating these synchronization errors. In the architecture, the time offset between different nodes is cancelled out by having each node forward its sampled data to a central receiver node, provided that the clock skews of different nodes are reasonably small. This architecture permits to have a TDOA error that is lower than using GPSDO synchronized nodes, especially in GPS-degraded environments. We also have implemented this architecture on USRPs and shown that the architecture can achieve errors below 10 ns in controlled environments. For outdoor experiments, we have shown that the TDOA errors of this relaying

architecture are less than 30 ns with high probability.

7.2 Future Work

7.2.1 Completely Remove GPS in Relaying Architecture

For the relaying architecture, we have used GPSDO module with USRP N210. The GPSDO is used to make sure there is zero clock skew and to set USRP time at the same time. In the future, we will use repeated transmission from relay node to receiver to estimate clock skew and then compensate the clock skew when estimating TDOA. Moreover, we will transmit a specially designed signal from the receiver to relays to trigger them to start measuring at the same time.

7.2.2 Explore Signal Characteristic of Broadcasting Signal Like Orbcomm, GSM, DVB-T

For signals of opportunity, we can also look at signal from Orbcomm satellite system, GSM signals [25, 26] and DVB-T [27]. These signals often comes from quite a large number of transmitters, which can provide a good signal geometry.

7.2.3 Combining IMU with TDOA estimation

Inertial measurement units (IMU) have been widely used for assisting navigation when the GPS signal is too weak to use. IMU usually contains accelerometer and gyroscope sensor to measure force and angular velocity [28]. IMU based localization normally have very high accuracy, but the error would accumulate after a period of time. For our case, we have signals from multiple sources like satellites, airplanes to get a position estimation based on TDOA method. Those measurements can be used to correct the accumulate error result from IMU. In summary, we can design a localization system which combines all the measurements from different beacons using dynamic filtering techniques [29, 30]. The flowchart of the system is shown in Figure 7.1.

Figure 7.1. Localization System Flowchart

Bibliography

- [1] A. Boukerche, H. Oliveira, E. F. Nakamura, and A. A. Loureiro, "Localization systems for wireless sensor networks," *Wireless Communications, IEEE*, vol. 14, no. 6, pp. 6–12, 2007.
- [2] P. Bellavista, A. Kupper, and S. Helal, "Location-based services: Back to the future," *Pervasive Computing, IEEE*, vol. 7, no. 2, pp. 85–89, 2008.
- [3] R. Zekavat and R. M. Buehrer, *Handbook of position location: Theory, practice and advances*. John Wiley & Sons, 2011, vol. 27.
- [4] D. Serant, P. Thevenon, M.-L. Boucheret, O. Julien, C. Macabiau, S. Corazza, M. Dervin, and L. Ries, "Development and validation of an ofdm/dvb-t sensor for positioning," in *Position Location and Navigation Symposium (PLANS), 2010 IEEE/ION*. IEEE, 2010, pp. 988–1001.
- [5] M. Bshara, U. Orguner, F. Gustafsson, and L. Van Biesen, "Robust tracking in cellular networks using hmm filters and cell-id measurements," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 3, pp. 1016–1024, 2011.
- [6] C.-R. Comsa, J. Luo, A. Haimovich, and S. Schwartz, "Wireless localization using time difference of arrival in narrow-band multipath systems," in *Signals, Circuits and Systems, 2007. ISSCS 2007. International Symposium on*, vol. 2, 2007, pp. 1–4.
- [7] I. Guvenc and C.-C. Chong, "A survey on toa based wireless localization and nlos mitigation techniques," *Communications Surveys & Tutorials, IEEE*, vol. 11, no. 3, pp. 107–124, 2009.
- [8] G. Mao, B. Fidan, and B. Anderson, "Wireless sensor network localization techniques," *Computer Networks*, vol. 51, no. 10, pp. 2529–2553, 2007.
- [9] R. Peng and M. L. Sichitiu, "Angle of arrival localization for wireless sensor networks," in *Sensor and Ad Hoc Communications and Networks, 2006*.

- SECON'06. 2006 3rd Annual IEEE Communications Society on*, vol. 1, 2006, pp. 374–382.
- [10] O. Jean and A. Weiss, “Passive localization and synchronization using arbitrary signals,” *Signal Processing, IEEE Transactions on*, vol. 62, no. 8, pp. 2143–2150, April 2014.
 - [11] S. Stein, “Algorithms for ambiguity function processing,” *Acoustics, Speech and Signal Processing, IEEE Transactions on*, vol. 29, no. 3, pp. 588–599, 1981.
 - [12] M. Dillinger, K. Madani, and N. Alonistioti, *Software defined radio: Architectures, systems and functions*. John Wiley & Sons, 2005.
 - [13] “Ettus research.” [Online]. Available: <http://www.ettus.com/home>
 - [14] “Xilinx ISE Design Suite.” [Online]. Available: <http://www.xilinx.com/support>
 - [15] “WBX 50-2200 MHz Rx/Tx.” [Online]. Available: <https://www.ettus.com/product/details/WBX>
 - [16] “GNU Radio.” [Online]. Available: <http://gnuradio.org/>
 - [17] C. E. Fossa, R. A. Raines, G. H. Gunsch, and M. A. Temple, “An overview of the iridium low earth orbit satellite system,” in *Aerospace and Electronics Conference, Proceedings of the IEEE*, 1998, pp. 152–159.
 - [18] K. Maine, C. Devieux, and P. Swan, “Overview of iridium satellite network,” in *WESCON/'95. Conference record. 'Microelectronics Communications Technology Producing Quality Products Mobile and Portable Power Emerging Technologies'*. IEEE, 1995, p. 483.
 - [19] S. R. Pratt, R. A. Raines, C. Fossa, and M. A. Temple, “An operational and performance overview of the iridium low earth orbit satellite system,” *Communications Surveys & Tutorials, IEEE*, vol. 2, no. 2, pp. 2–10, 1999.
 - [20] C. M. Shahriar, “Mitigation of interference from iridium satellites by parametric estimation and subtraction,” Ph.D. dissertation, Virginia Polytechnic Institute and State University, 2006.
 - [21] D. C. Morse, K. Griep, R. Deininger, D. Peters, and B. Snow, “Next generation fans over inmarsat broadband global area network (bgan),” in *Digital Avionics Systems Conference, 2004. DASC 04. The 23rd*, vol. 2, 2004.
 - [22] A. Franchi, A. Howell, and J. Sengupta, “Broadband mobile via satellite inmarsat bgan,” 2000.

- [23] “GEO-Mobile Radio Interface Specifications.” [Online]. Available: <http://www.etsi.org/>
- [24] “Sc-186 automatic dependent surveillance-broadcast.” [Online]. Available: <http://www.rtca.org/>
- [25] C. Drane, M. Macnaughtan, and C. Scott, “Positioning gsm telephones,” *Communications Magazine, IEEE*, vol. 36, no. 4, pp. 46–54, 1998.
- [26] V. Otsason, A. Varshavsky, A. LaMarca, and E. De Lara, “Accurate gsm indoor localization,” in *UbiComp 2005: Ubiquitous Computing*. Springer, 2005, pp. 141–158.
- [27] R. Saini and M. Cherniakov, “Dtv signal ambiguity function analysis for radar application,” in *Radar, Sonar and Navigation, IEE Proceedings-*, vol. 152, no. 3, 2005, pp. 133–142.
- [28] W. W.-L. Li, R. A. Iltis, and M. Z. Win, “Integrated imu and radiolocation-based navigation using a rao-blackwellized particle filter,” in *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*, 2013, pp. 5165–5169.
- [29] M. Sanjeev Arulampalam, S. Maskell, N. Gordon, and T. Clapp, “A tutorial on particle filters for online nonlinear/non-gaussian bayesian tracking,” *Signal Processing, IEEE Transactions on*, vol. 50, no. 2, pp. 174–188, 2002.
- [30] F. Gustafsson, F. Gunnarsson, N. Bergman, U. Forssell, J. Jansson, R. Karlsson, and P.-J. Nordlund, “Particle filters for positioning, navigation, and tracking,” *Signal Processing, IEEE Transactions on*, vol. 50, no. 2, pp. 425–437, 2002.