TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

Pedro Manuel Figueiredo e Silva

Signals of Opportunity for Positioning Purposes

Julkaisu 1601 • Publication 1601

Tampere 2018

Tampereen teknillinen yliopisto. Julkaisu 1601
Tampere University of Technology. Publication 1601

Pedro Manuel Figueiredo e Silva

Signals of Opportunity for Positioning Purposes

Thesis for the degree of Doctor of Science in Technology to be presented with due permission for public examination and criticism in Päätalo Building, Auditorium PA103, at Tampere University of Technology, on the 4th of December 2018, at 12 noon.

Tampereen teknillinen yliopisto - Tampere University of Technology
Tampere 2018

Doctoral candidate: Pedro Manuel Figueiredo e Silva, MSc
Laboratory of Electronics and Communications Engineering
Tampere University of Technology
Finland

Supervisor: Elena Simona-Lohan, Associate Professor
Laboratory of Electronics and Communications Engineering
Tampere University of Technology
Finland

Pre-examiners: Dragos Niculescu, Professor
Computer Science Department
Universitatea Politehnica București
Romania

Sanna Kaasalainen, Professor
Navigation and Positioning
National Land Survey of Finland
Finland

Opponent: Juan Jesús García Domínguez, Professor
Universidad de Alcalá
Spain

Sanna Kaasalainen, Professor
Navigation and Positioning
National Land Survey of Finland
Finland

ISBN 978-952-15-4267-1 (printed)
ISBN 978-952-15-4280-0 (PDF)
ISSN 1459-2045

Abstract

Over the last years, location-based services (LBS) have become popular due to the emergence of smartphones with capabilities of positioning their user's location on Earth at unprecedented speed and convenience. Behind such feat are the technological advances in global navigation satellite systems (GNSS), such as Galileo, Globalnaya Navigazionnaya Sputnikovaya Sistema (GLONASS), Global Positioning Service (GPS) and Beidou. The easiness of smartphones and the improvement of positioning technology has driven LBS to be at the core of many business models. Some of these business models rely on the user's location to pick him up on a car, relinquish a meal to him, offer insights on sports performance, locate items to be picked up on a warehouse, among many others.

While LBS are driving the need to continuously locate the user at higher degrees of accuracy and across any environment, be it in a city park, an urban canyon or inside a corporate office, some of these environments pose a challenge for GNSS. Indoor environments are particularly challenging for GNSS due to the attenuation and strong multipath imposed by walls and building materials. Such challenges and difficulties in signal acquisition have led to the development of solutions and technologies to improve positioning in indoor environments.

While there are several commercial systems available to fulfill the needs of most LBS in indoor environments, most of these are not feasible to deploy at a global scale due to their infrastructure costs. Hence, several solutions have sought to build upon existing infrastructure to provide positioning information.

Building upon existing infrastructure is what leads to the main topic of this thesis, the concept of signals of opportunity (SoO). A SoO is any wireless signal that can be exploited for a positioning purpose despite its initial design seeking to fulfill a different purpose. A few examples of these signals are IEEE 802.11 signals, commonly known as WiFi, Bluetooth, digital video broadcasting - terrestrial (DVB-T) and many of the cellular signals, such as long-term evolution (LTE), universal mobile telecommunications system (UMTS) and global mobile system (GSM).

The goal of this thesis is to address various challenges related to SoO for positioning. From the identification of SoO at the physical layer, how to merge them at the algorithmic level and how to put them in use for a cognitive positioning system (CPS).

Preface

This thesis is based on the research work carried out during the years 2013–2017 at the Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland.

First and foremost, I would like to thank Prof. Elena Simona-Lohan for offering me the opportunity to work under her supervision and guidance. It has been a pleasure to work with her and to follow her vision in the field of wireless positioning.

I am grateful to Prof. Dragos Niculescu and Prof. Sanna Kaasalainen for agreeing to act as the pre-examiners of my thesis. I also wish to thank Prof. Sanna Kaasalainen and Prof. Juan Jesús García Domínguez, for agreeing to act as the opponents at my defense.

I am most honored for all the financial support towards supporting my studies, training and execution of this thesis possible. The support given by the Marie Skłodowska-Curie Initial Training Network Multitechnology Positioning Professionals (MULTI-POS) which allowed my relocation to Finland and financial support for the course of three years. I would also like to thank the local doctoral schools for the organization of workshops and support with travelling costs, such as Graduate School in Electronics, Telecommunications and Automation (GETA), doctoral training network in Electronics, Telecommunications and Automation (DELTA) and the Inforte network.

I would also like to acknowledge the support of the the University of Nottingham, in particular the Geospatial Institute and Wirepas for hosting my academic and industry research visits during the MULTI-POS program.

Another token of appreciation goes to my project fellows and projects leaders, which in some sort became my family during the MULTI-POS years. I would like to thank the TUT MULTI-POS fellows, with whom I had most interaction and whose feedback was deeply important for me, Ondrej Daniel, Jussi Raassakka, Giorgia Ferrara and Alejandro Rivero. A big thank to all the other MULTI-POS fellows, with whom I exchanged several trips and stories over the last years, Enik, Maciej, Luis, Pekka, Anahid, Susana, Paolo, Markus, Arash and Ana. A special thank you to Jari Nurmi and Simona Lohan for helming and taking on the project.

For my time at TUT, I would like to thank my other colleagues for their friendship and activities after work. Their help and support was essential for my integration in the Finnish life and culture. A big thank you to Janis Werner, Joonas Säe, Markus Allen, Jaakko Marttila, Jukka Talvitie, Dani Korpi and Toni Levanen.

For my time at Wirepas, I would like to acknowledge a few of my coworkers for the obstacles we faced together as well as downtime we enjoyed together. Thank you Janne Valtanen, Ville Juven, Jukka-Pekka Partanen, Vesa Saarinen, Hannu Hirvi, Teemu Piroinen, Chunyan Pei, Juhani Rautalappi, Gary Horning, Kari Pihl and Florean Curticapean. A special appreciation to Ville Kaseva and Teppo Hemia for all the trust, acceptance and support throughout my research visit and continuation of my work at Wirepas.

I am indebted to all the gastroenterology medical staff I met over the last two decades. Their work and support has allowed me to be among my dearest friends and family.

For my parents, Manuel and Maria, my sister, Liliana and my closest friends, Eduardo Santos and Denis Surmann, a big thank you for your support, nurture and help over the last years.

Finally, for my soon-to-be wife, Laura Keski-Vähälä, thank you for all your support, dedication, patience and love.

Tampere, October 2018
Pedro Figueiredo e Silva

Table of Contents

Abstract i

Preface iii

List of Publications vii

Abbreviations ix

Symbols xi

1 Introduction 1
- 1.1 Background and motivation . . . 1
- 1.2 Objectives and scope of the thesis . . . 2
- 1.3 Thesis contributions and structure . . . 3
- 1.4 Author's contributions to the publications . . . 3
- 1.5 Other contributions by the author . . . 4

2 Signals of Opportunity 5
- 2.1 Overview . . . 5
- 2.2 Elements of a positioning system . . . 6
  - 2.2.1 Measurement layer . . . 6
  - 2.2.2 Algorithmic layer . . . 12

3 Spectrum Sensing 15
- 3.1 Background, state-of-the-art, and related work . . . 15
  - 3.1.1 Spectrum sensing . . . 16
  - 3.1.2 Cyclostationary . . . 17
  - 3.1.3 Related work . . . 18
- 3.2 Distinguishing signals in a mixture . . . 18
  - 3.2.1 Signal modelling . . . 18

3.2.2 Cyclostationary features . . . 20
3.2.3 Cyclic frequency detector . . . 22
3.2.4 Decision process . . . 23
3.3 Receiver design aspects . . . 24
3.3.1 Measurement setup . . . 25
3.3.2 Understanding the impact of undersampling on cyclostationary analysis . . . 26
3.4 Discussion . . . 31

4 Channel Impairments **33**
4.1 Background, state-of-the-art and related work . . . 33
4.1.1 Wireless propagation . . . 34
4.1.2 Fading . . . 34
4.1.3 Related work . . . 36
4.2 Impact of intra-system interference on BLE signals . . . 36
4.2.1 Measurement acquisition . . . 37
4.2.2 Model-fit evaluation . . . 37
4.2.3 Implications for ranging and trilateration . . . 42
4.3 Discussion . . . 46

5 Efficient positioning **47**
5.1 Background, state-of-the-art and related work . . . 47
5.1.1 Model-based and model-free approaches . . . 47
5.1.2 Fingerprinting . . . 48
5.1.3 Related studies . . . 50
5.2 Fundamental limits on SoO positioning . . . 50
5.2.1 Time-domain hybridization . . . 52
5.2.2 Power-domain hybridization . . . 54
5.3 Discussion . . . 60

6 Opportunities for Internet of Things **61**
6.1 Background, state-of-the-art and related work . . . 61
6.1.1 Related work . . . 61
6.1.2 An overview of IoT technologies . . . 62
6.2 IoT as enabler for future positioning systems . . . 64
6.3 Discussion . . . 65

7 Conclusions **69**
7.1 Summary . . . 69
7.2 Discussion and further development . . . 71

References **73**

Publications **85**

List of Publications

This thesis is a compound thesis based on the following six publications:

[P1] P. Figueiredo e Silva, O. Daniel, J. Nurmi, E.S. Lohan, "Cyclostationary features of downsampled 802.11g OFDM signal for cognitive positioning systems", in *Proceedings of IEEE ISWCS'2014 conference*, August 2014, Barcelona, Spain;

[P2] P. Figueiredo e Silva, G. Seco-Granados, and E.S. Lohan, "Receiver Architecture for Cognitive Positioning with CDMA and OFDM signals", in *Proceedings of IEEE International Conference on Localization and GNSS (ICL-GNSS 2015), June 2015*, Gothenburg, Sweden;

[P3] P. Figueiredo e Silva, A. Basiri, E.S. Lohan, J. Pinchin, C. Hill, T. Moore, "On the Impact of Intra-System Interference for Ranging and Positioning with Bluetooth Low Energy", in *Proceedings of 23rd International Conference on Advances in Geographic Information Systems: ACM SIGSPATIAL*, November 2015, Seattle WA, Unite States of America;

[P4] P. Figueiredo e Silva and E.S. Lohan, "Room-level indoor positioning with Wi-Fi and RFID fingerprints", in *Proceedings of 23rd International Conference on Advances in Geographic Information Systems: ACM SIGSPATIAL*, November 2015, Seattle WA, Unite States of America;

[P5] P. Figueiredo e Silva and E.S. Lohan, "Performance Considerations for Positioning with Signals of Opportunity", in *Proceedings of IEEE International Conference on Localization and GNSS (ICL-GNSS 2016)*, June 2016, Barcelona, Spain;

[P6] P. Figueiredo e Silva, V. Kaseva, E. Simona-Lohan, "Wireless Positioning in IoT: A Look at Current and Future Trends", in *Sensors*, 18(8):2470, 2018.

Abbreviations

AFH	Adaptive frequency hopping
AOA	Angle of arrival
BLE	Bluetooth low energy
CDMA	Code division multiple access
CPS	Cognitive positioning system
CR	Cognitive radio
CRLB	Crámer-Rao lower bound
DAOA	Differential angle of arrival
DRSS	Differential received signal strength
DVB-T	Digital video broadcasting - terrestrial
FAM	Fast Fourier transform accumulation method
GLONASS	Globalnaya Navigazionnaya Sputnikovaya Sistema
GNSS	Global navigation satellite systems
GPS	Global Positioning Service
GSM	Global mobile system
IMU	Inertial measurement unit
IoT	Internet of things
LBS	Location-based services
LTE	Long-term evolution
OFDM	Orthogonal frequency-division multiplexing
RFID	Radio-frequency identification
RMSE	Root mean square error
RSS	Received signal strength
RTT	Round trip time
SCF	Spectral correlation function
SNR	Signal to noise ratio
SoO	Signals of opportunity
SSCA	Strip spectrum correlation algorithm
TDOA	Time difference of arrival

TOA	Time of arrival
UMTS	Universal mobile telecommunications system
UWB	Ultra-wideband
V-TDOA	Virtual time difference of arrival
WCDMA	Wideband code division multiple access
WGN	White Gaussian noise

Symbols

I	Activity indicator
W	Activity detector's window
$\mathfrak{E}$	Activity margin to avoid overlapping cyclic frequencies
Θ	Angle between two vectors
θ	Angle of arrival of a signal
$\mathfrak{R}(t,\tau)$	Autocorrelation function
τ	Autocorrelation lag parameter
E_m	Average energy of a M-QAM data symbol
$\mathrm{E_b}$	Bit energy
$\mathcal{C}/N_0$	Carrier to noise ratio
$\mathrm{Y}(f)$	CDMA's Fourier transform
$\mathrm{y}(t)$	CDMA's signal representation
T_c	CDMA's chip interval
α	CDMA's cyclic frequencies
$\mathrm{p}(t)$	CDMA's pulse shape function
SF	CDMA's spreading factor
f_c	Chip rate
$\mathrm{c_k}(n)$	Chip value
$\mathcal{W}$	Combined fading component from the difference of two received signal strengths
$\mathbf{P}$	Coordinate in a 3D space
$\mathfrak{R}^{\gamma}(\tau)$	Cyclic autocorrelation function
$\mathcal{H}$	Decision hypothesis
$\Delta\theta$	Difference between two angles of arrival
$\Delta\mathrm{P_r}$	Differential received signal strength
d	Distance between an emitter and a receiver
$\mathrm{T_{obs}}$	Duration of spectrum segments
ψ_n	Error associated with simulated time measurements
$\mathcal{J}$	Fingerprint cost function

$\mathbf{F}$	Fingerprint vector
γ	Fundamental cyclic frequency
$\mathcal{L}$	Gaussian Likelihood
R	Geometric range
$\mathbf{L}$	Learning database
w	Log-normally distributed random variable which models the slow fading phenomenon
$\overline{F^2}$	Mean square bandwidth of the signal
μ	Mean value
$\mathbf{M}$	Measurement vector
$\Delta t_{\text{message}}$	Message processing time
$\text{z}(t)$	Mixture of two signals plus white Gaussian noise
A	Multiplicative constant normalizing OFMD's symbol energy
T_0	Network beacon period
$\text{N}_{\text{channels}}$	Number of channels available
N_{tags}	Number of tags competing for channel access
N	Number of OFDM subcarriers
f_N	Nyquist frequency
$\text{o}(t)$	OFDM's signal representation
β	OFDM's cyclic frequencies
T_{symbol}	OFDM's symbol period with cyclic prefix
$\text{q}(t)$	OFDM's pulse shaping functions
T_{U}	OFDM's symbol period without cyclic prefix
$\text{X}_n(k)$	OFDM symbol
η	Pathloss coefficient
C	Pathlosses imposed by the hardware chain
Φ	Phase difference between the received signals at two antenna elements
N_0	Power spectral density
$\mathfrak{P}$	Probability of picking an advertisement channel that is busy
$\text{Q}(f)$	Pulse shape Fourier transform
P_r	Received signal strength
t_{RT}	Return trip time
f_s	Sampling frequency
r	Separation between two antennas
$\mathcal{A}$	Set of CDMA cyclic frequencies
$\mathcal{B}$	Set of OFDM cyclic frequencies
ξ	Signal's energy
λ	Signal's wavelength
B	Signal's one-sided bandwidth
T	Signal's period
L_n	Simulated time measurements
$\mathfrak{S}^\gamma(f)$	Spectral correlation function
c	Speed of light
σ	Standard deviation
Δf	Subcarrier's frequency spacing

T_{GI}	Symbol guard interval
$\Delta\tau_k$	Time offset due to local oscillator drift
t	Time
$g(t)$	White Gaussian noise

CHAPTER 1

Introduction

Machine-made signals have allowed human population to develop efficient mechanisms to exchange information and knowledge.

Daily, we interact with many of these signals, such as WiFi, Bluetooth, cellular, TV and satellite signals with a given purpose, either to access the Internet, call another person, watch or listen the news or locate oneself on Earth.

The goal of this thesis is to identify such signals and understand how to identify and use them towards a positioning context.

1.1 Background and motivation

Location has always been an important aspect for human development. From the star navigation days, we have progressed towards a time where artificial satellites allow us to determine our location and time to an unprecedented degree of accuracy. While these satellites are mostly useful in outdoor environments, they are one of the key drivers for several applications, such as autonomous vehicles and aircrafts, smart agriculture, fleet management, smart tolling, among many other location-based services at a worldwide scale.

While outdoor environments have been the pinnacle of location-based services so far, indoor environments have remained a challenge. Global navigation satellite systems (GNSS) are unavailable in indoor environment due to strong multipath and attenuation imposed by the building materials. The difficulty in acquiring GNSS signals in indoor environments has fostered the creation and development of indoor specific systems, which allow for the determination of a user's location from an accuracy of several dozens of meters to just a few decimeters. There are several commercially available indoor positioning systems which rely on technologies such as WiFi [122, 126], Bluetooth low energy (BLE) [41,106,116], Internet of things (IoT) technologies [120,131,137] and ultra-wideband (UWB) [40, 103]. The problem behind these systems is the cost associated with creating and maintaining a dedicated service infrastructure. It would also be quite time consuming to roll out a worldwide infrastructure to provide users with a seamless mechanism to acquire their location worldwide.

One of the biggest hurdles for indoor environments is the cost of infrastructure. Infrastructure refers to all the equipment necessary to have in place for the system to offer a location of a user in a given environment. The infrastructure cost is bigger for higher accuracy and precision systems, since such systems rely on dedicated hardware and often require additional cabling to be added throughout the environment.

Overall, aiming for a seamless worldwide location in indoor environments, such as GNSS for the outdoors, would require building on existing infrastructure to keep costs low. This motivation is what has led the research community over the last years to explore existing opportunities available through wireless communication systems, due to their popularity in indoor environments, either corporate, commercial or residential. One key technology driver for this has been WiFi, which has sprouted throughout indoor environments to allow users to access the Internet or replace existing cable infrastructure. However, there are far more technologies other than WiFi, such as radio, digital radio, digital TV, 3G, 4G, Bluetooth. There are also several other IoT opportunities in the 2.4 GHz and sub-GHz spectrum, such as NB-IoT, SigFox, Wirepas, among other presented and discussed in chapter 6.

The above-mentioned signals create an opportunity to use them outside their initial purpose and derive useful information to locate a user seamlessly throughout any kind of environment. This is the key driver behind this thesis, where the goal is to look at the existing and future radio environment and look for what is known from now on as signals of opportunity (SoO).

This thesis tries to find answers to the following questions:

- Which signals among the available ones could be used?
- What are the limitations of available SoO in terms of positioning performance metrics?
- Which of the SoO features can be explored to support location and navigation?
- How would an opportunity receiver look like?
- How would a designer build a SoO-based positioning system?

1.2 Objectives and scope of the thesis

The main objective of this thesis is to study the applicability of SoO for wireless positioning. This includes looking at their properties in the time-frequency domain, allowing for their identification among other signals reaching a receiver and building enhanced cognitive positioning receivers with a focus on power preservation. In addition to this objective, this thesis also looks at a few aspects of interference and how it impacts the performance of a positioning algorithm. Moreover, this thesis investigates positioning algorithms to hybridize sensor data from multiple SoO. Finally, it draws a panorama on the status of several IoT technologies and on the needs and desires these impose during the design and construction of a positioning system.

1.3 Thesis contributions and structure

The main contributions of this thesis are enumerated below. The publications where these contributions were presented are shown in brackets.

1. Deriving a detection algorithm to infer the presence of 802.11 signals at sub-Nyquist rates [P1];
2. Providing a novel method to detect the presence of code division multiple access (CDMA) and orthogonal frequency-division multiplexing (OFDM) in a signal mixture [P2];
3. Proposing an architecture for a cognitive positioning system [P2];
4. Analyzing the impact of radio interference on the performance of a positioning algorithm based on BLE beacons [P3];
5. Analyzing the benefits in terms of the positioning performance by hybridizing multiple technologies, such as WiFi and radio-frequency identification (RFID) [P4–P5];
6. Providing insights on the design of a positioning system based on wireless communication systems, such as current and future WiFi and IoT systems [P6].

Publications [P1–P6] provide more details into the topics briefly described and presented in this thesis summary. Some of the notations and visual appearance of figures included in the thesis differ slightly from the associated publications.

This thesis is organized in three different parts. The first part consists of chapter 2 which provides an insight on the background of SoO. The second part consists of chapters 3 to 7, which contains the thesis contributions, namely on the realms of spectrum sensing, interference mitigation, efficient positioning, design of positioning systems and a summary. The third part is formed by a compilation of 6 publications by the thesis' author.

1.4 Author's contributions to the publications

The thesis topic was formulated by Assoc. Prof. Elena Simona-Lohan in the context of the EU FP7 Marie Skłodowska Curie project Multitechnology Positioning Professionals (MUTI-POS). Assoc. Prof. Elena Simona-Lohan has guided and contributed to all publications [P1–P6], where she was the main driver behind the publication ideas, providing support during the research formulation and while writing the manuscripts. The research work for most of the publications was carried out between 2013 and early 2016.

- In [P1] the thesis' author analyzed the measurements acquired by M.Sc. Ondrej Daniel with whom the paper was co-authored. The techniques and introduction of main concepts was written by the thesis's author, while M.Sc. Ondrej Daniel wrote other introductory parts and helped write the conclusions. The remaining

co-authors helped with the review of the document. The work was presented by the thesis' author;

- In [P2] the thesis' author created the simulation, wrote and presented the entirety of the paper with the help and feedback from the remaining co-authors;
- In [P3] the work was proposed by Prof. Terry Moore and PhD Anahid Basiri, PhD James Pinchin shared access to the hardware. The thesis' author acquired the field measurement data, which included the development of specific tools for the process. Moreover, the remaining analyses was performed by the thesis' author, who also wrote and presented the entirety of the document. The remaining co-authors helped with the review of the document;
- In [P4] the thesis's author developed the simulator and tools to analyze the measurement data set provided by Assoc. Prof. Elena Simona-Lohan. The paper was written and presented by the thesis' author;
- In [P5] the thesis's author developed the simulator, wrote and presented the manuscript;
- In [P6] the thesis' author and Assoc. Prof. Elena Simona-Lohan acquired the background information on the several technologies presented. Several simulations were developed and co created among both authors. Dr. Tech. Ville Kaseva contributed towards the discussion of the ideas and the review of the document.

1.5 Other contributions by the author

The author has also contributed actively to other studies in the area [10–12, 32, 49, 54, 83, 84, 107, 135]. These studies are not included in this compilation to preserve the compactness of the thesis. A brief description of the main contributions provided by the thesis' author is given instead:

- In [11] the thesis' author wrote the sections related to positioning with WiFi systems;
- In [107] the thesis's author helped with the simulation analysis and helped writing and reviewing the manuscript;
- In [10, 12, 54, 70, 83, 84] the thesis' author wrote some of the sections related to positioning with WiFi, RFID and BLE systems;
- In [135] the thesis' author helped with the manuscript preparation and presented the work;
- In [32, 49] the thesis' author helped with the review of the manuscript.

In addition to the academic work and under the scope of the MULTI-POS project, the thesis author contributed to the development of the local industry through a research visit of 8 months during 2016 (Wirepas Oy, Finland). This work has led to the creation and development of a positioning product [138].

CHAPTER 2

Signals of Opportunity

This chapter starts by introducing the concept of SoO for positioning. It continues by presenting an overview of several common signals and moves on the implications to use and exploit them in a positioning context.

2.1 Overview

As mentioned in chapter 1, SoO are any kind of signals which are used in a different context from what they were initially meant for. In other words, SoO for positioning are any signals whose initial intent was not for a positioning purpose, but which contain rich features or are ubiquitous enough to be useful in a positioning context. These are two of the main traits that ought to start an evaluation regarding which signals to exploit for the development of a positioning system.

Due to their extensive coverage in urban environments, the most common type of SoO to consider are WiFi and cellular signals. These signals were initially built and designed for telecommunication purposes, hence their classification as SoO. Table 2.1 presents a few relevant SoO together with some of their key physical layer parameters, which are relevant for positioning, such as bandwidth, carrier frequency and multiple access. In addition to machine made signals (see Table 2.1), it is also important to call attention to natural occurring fields, as well as artificial fields, such as geomagnetic fields and lighting patterns in indoor environments [4, 33, 36].

To apply these signals in a positioning context, first of all, it is necessary to extract from them a measurement to or from a reference point. Second, by associating this measurement with the known coordinates of such reference points, it is possible to obtain a position in the same reference frame. These two elements are the necessary inputs for a positioning system, which is defined in more detail in section 2.2.

Table 2.1: Machine-made signals of opportunity.

Signal	Frequency	Multiple access	Bandwith
802.11ad	60 GHz	OFDM	160 MHz
802.11ac	5.8 GHz	OFDM	160 MHz
802.11n	5 GHz	OFDM	40 MHz
802.11g	2.4 GHz	OFDM	20 MHz
802.11a	5 GHz	OFDM	20 MHz
802.11b	2.4 GHz	DSSS	20 MHz
Bluetooth	2.4 GHz	FHSS	1 MHz
Zigbee	2.4 GHz	DSSS	2 MHz
DVB-T	40-200MHz	OFDM	8 MHz
LTE	800, 900, 1800, 2600 MHz	OFDM	20 MHz
UMTS	900, 2100 MHz	CDMA	1.25 MHz
GMS	900, 1800 MHz	TDMA	200 kHz

2.2 Elements of a positioning system

In a positioning system, the position of its users is provided through the algorithms applied to measurements taken from the received signals. The basic blocks of such system are illustrated in Figure 2.1. Figure 2.1, depicts a positioning system, where the first block is the measurement layer and the second block is an algorithmic layer. The output of the system is a position or location update, which often corresponds to a coordinate point in a 2D or 3D space. The first block provides to the second block a set of measurements extracted from the received signals. Depending on the signal design, the measurement involves obtaining a power level, an angle or a time estimate. The most popular techniques are time of arrival (TOA), time difference of arrival (TDOA), angle of arrival (AOA) and received signal strength (RSS). For example, global navigation satellite systems rely on TOA to compute the distance of the mobile to each satellite in view [114]. In indoor systems, RSS is used frequently to provide an estimate of the user's position [79].

2.2.1 Measurement layer

The algorithmic block shown in Figure 2.1 depends on the type of measurement produced by the measurement layer. In this thesis, the measurements and corresponding algorithms are classified in three distinct domains, time, power and space. Each of these domains and their most important techniques are described in this section.

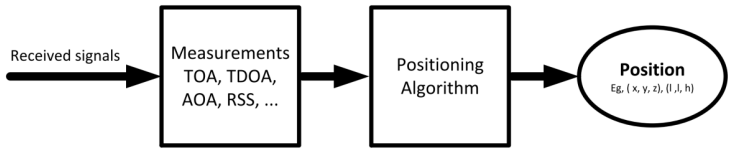


Figure 2.1: Basic elements of a positioning system.

Time domain

This section introduces several time domain measurements, which rely on a time reference to understand how much the signals have travelled between devices. The major drawback in time measurements is the necessity of having synchronized clocks, either at the receiver or at the transmitter side. The problem appears at how the clocks keep time. Higher precision clocks are expensive and thus unbearable for consumer minded applications.

Round trip time

Round trip time (RTT) measures the time a message takes to travel from the source to the destination and back. It does not require synchronization in the network, but it increases the complexity of the overall system, since it requires each node to transmit a message and wait for its return [95]. The distance between the emitter and the receiver, R,

$$\mathrm{R} = \frac{(t_{\mathrm{RT}} - \Delta t_{\mathrm{message}})\mathrm{c}}{2}, \tag{2.1}$$

is a function of the return trip time, t_{RT}, minus the time taken by the device to process the request, $\Delta t_{\mathrm{message}}$, times the speed of the medium, c, divided by two.

Time of arrival

TOA provides the system with the time taken by the signal to travel from the emitter to the receiver. The distance between the receiver and the emitter, R,

$$\mathrm{R} = t\mathrm{c}, \tag{2.2}$$

is the travel time, t, it takes for the message to arrive times the speed of propagation in the medium, which for electromagnetic waves is the speed of light, c.

Therefore, synchronization is necessary for an accurate computation of the distance, since small timing errors, such as millisecond, will result in several hundred meters of error.

Time difference of arrival

TDOA measures the difference in TOA, $t1 - t2$, from the emitter to two receivers,

$$\frac{\mathrm{R}_1}{c} - \frac{\mathrm{R}_2}{c} = t_1 - t_2, \tag{2.3}$$

where $\mathrm{R}_1, \mathrm{R}_2$ are the geometrical distance between the receiver and the emitter at times t_1 and t_2, respectively and c is the speed of light.

In TDOA, the goal is no longer to determine the arrival time of the emitter's signal, but instead to determine the difference in time at which the signal arrives at multiple receivers and by consequence inferring the relative position of the emitter [24].

One major drawback of TDOA is that it still relies on synchronized clocks by one of the parties involved in the process. Because of the synchronized clocks and its inherent cost, the measurements are often taken at the network side allowing for the end equipment to keep relying on cheaper components.

Virtual time difference of arrival

Virtual time difference of arrival (V-TDOA), [105], starts by assuming that the RF transmitter is synchronized to an absolute time reference and that it transmits a periodic beacon at every T_0 period. A receiver acquires the k^{th} beacon at time t_k, as describe by,

$$t_k = t_0 + 2\mathrm{T}_0 + \Delta t_k + \Delta\tau_k, \tag{2.4}$$

where Δt_k is the difference in propagation time, V-TDOA, between measurement 0 and measurement k, and $\Delta\tau_k$ is the time offset due to local oscillator drift between measurement 0 and measurement k.

The goal behind V-TDOA is to estimate Δt_k using the TOA measurements t_k despite of the local oscillator's offset $\Delta\tau_k$. However, the local oscillator's skew ought to be modelled to allow accurate V-TDOA measurements.

Space domain

In the space domain, techniques require the presence of specialized antennas or antenna arrays. This leads to challenges in terms of the hardware design regarding the physical separation and number of antennas in the array. Nevertheless, the most critical aspect in the space domain is to enable a precise discrimination of the angle of the incident signal. Precise angle information is important since the error in the measurement grows larger as the distance between emitter and receiver increases [35]. Besides that, strong multipath and lack of line of sight pose additional challenges when determining the principal wave front.

Angle of arrival

In AOA, determining the location of a device requires at least two angle measurements [141]. One measurement is also enough if another measurement from another domain, such as time or power, is used to infer the distance between the emitter and receiver.

Hence, for the n^{th} device, it is possible to describe its measurement at the receiver m as,

$$(x_n, y_n) = \mathrm{R}_m cos(\theta_m) + \mathrm{R}_m sin(\theta_m), \tag{2.5}$$

where R_m is the distance from m to n and θ the angle of arrival determined at m. A range measurement is obtained by solving the set of equations with regards to the unknown coordinates. For the determination of θ, an array of at least two elements is required and its determination follows,

$$\theta = cos^{-1}\left(\frac{\lambda}{2\pi \mathrm{r}}\Phi\right), \tag{2.6}$$

where Φ is the phase difference between the received signals at two antenna elements, λ is the wavelength at the operating frequency and r is the separation between antenna elements, fulfilling the inequality

$$\mathrm{r} \leq \frac{\lambda}{2}. \tag{2.7}$$

Differential angle of arrival

In this technique the estimation of the emitter's location is derived based on the difference of AOA between multiple emitters [5]. Differential angle of arrival (DAOA), $\Delta\theta$, is derived from AOA as,

$$\Delta\theta = \theta_x - \theta_y, \tag{2.8}$$

where θ_x and θ_y are the AOA acquired at the receiver from emitters x and y, respectively. DAOA's major drawback is the necessity of an additional measurement, which means that at least three observables are required for determining a 2D location. However, to its advantage, there is no longer a need to know the antenna's orientation.

Power domain

In the power domain, the observable is the RSS at a receiver's antenna. This is a metric that is feasible to extract from any system, since it is inherent to the signal propagation. However, due to the propagation impairments it is also one that is difficult to model. In addition to that, a lot of devices expose this information as an indicator, which maps to a representation of the RSS in a discrete scale. This poses errors in the interpretation of the incoming value as well as understanding what is the actual value that the emitter is producing. Despite its weaknesses, its availability from any system, without additional hardware requirements is its biggest advantage [79, 145].

Received signal strength

RSS has a fundamental relationship with distance which results from the decrease of power as its coverage area increases. Imagining a signal as a sphere whose center is at the emitter's antenna, as it travels through space, its surface scales as the square of the

radius, while its power decays with the square of the distance. Despite this relationship, the effects caused by channel impairments, system non linearities, either at the receiver's or transmitter's side, leads to a complex problem to model properly.

In short, RSS behavior varies greatly depending on its environment but regardless of that, the most popular models accepted follow empirical measurements, from which typical attenuation factors are derived for specific environments, such as offices, industrial factories, rural and residential areas [68].

The popular Log distance model for the path losses and shadowing is given by,

$$\mathrm{P_r} = \mathrm{P_r}(\mathrm{d_0}) - 10\eta \log_{10} \left(\frac{d}{\mathrm{d_0}}\right) + w, \tag{2.9}$$

where $\mathrm{P_r}(\cdot) < 0$ is the received signal power in logarithmic scale dependent on distance d, $\mathrm{d_0}$ is a reference distance (usually 1 m), $\eta > 0$ is the path-loss exponent and $w \sim log(\mathrm{N}(0, \sigma^2))$ is a log-normally distributed random variable which models the slow fading phenomenon (i.e. shadowing) and possible RSS measurements errors (e.g., due to quantization). Both, η and w are dependent on the propagation environment and are different for each device.

Differential received signal strength

If two emitters are placed away from the receiver and in similar propagation conditions, it is possible to assume that the channel impairments they suffer are similar. In differential received signal strength (DRSS), the subtraction of RSS equations for each emitter allows one to write the relationship to the user's location as [110],

$$\mathrm{P_{r1}}(d, f) - \mathrm{P_{r2}}(d, f) = 10\eta \log_{10} \left(\frac{\mathrm{d_2}}{\mathrm{d_1}}\right) + \Delta\mathrm{P_{r12}}(\mathrm{d_0}) + \mathcal{W}, \tag{2.10}$$

where $\mathrm{P_{r1}}(d_1, f)$ and $\mathrm{P_{r2}}(d_2, f)$ are the RSS between the receivers and the selected emitter, $\mathrm{P_{r12}}(\mathrm{d_0})$ is the difference between the apparent power at the reference distance $\mathrm{d_0}$, η is the pathloss coefficient assumed to be the same for both paths, d_i is the distance between the receiver and emitter i and $\mathcal{W}$ the combined fading component from each signal path.

Summary

Regardless of the domain, the location to be determined from a given set of measurements will only be as accurate as the measurements allow it to be. However, besides accuracy, there are other factors that come into play in the selection of a certain domain. Cost and complexity are often the main driver for the selection of the measurement domain, especially in resource constrained devices. To conclude this section, Table 2.2 presents a qualitative summary of the several techniques presented throughout Section 2.2.1.

Table 2.2: A qualitative summary of each measurement domain.

Measurement	Advantages	Disadvantages
TOA / RTT	High precision.	The necessity of having the emitters' and receivers' clocks' synchronized results in high hardware costs.
TDOA	The receiver's clock does not need to be synchronized.	Requires a synchronized network of access points.
V-TDOA	The receiver's clock does not need to be synchronized.	Susceptible to the emitter's jitter. The local oscillator needs to be considered through a local model.
AOA	Does not require synchronized emitters and offers a 2D location with a single receiver.	Requires specialized hardware such as antenna arrays.
DAOA	No longer depends on the antenna's orientation.	As in AOA, it requires dedicated hardware. Requires an extra measurement with respect to AOA for a positioning solution in the same positioning domain.
RSS / D**RSS**	Low cost and complexity since measurement is inherent to the system's operation.	Highly susceptible to fading phenomena as small changes in the environment lead to different power measurements. It is also dependent on the hardware manufacturer and on the measurement accuracy provided by it.

2.2.2 Algorithmic layer

The algorithmic layer, as seen in Figure 2.1, is responsible for using the provided measurements and translate that information into a set of coordinates. It is at this layer, that the system should consider the needs of the user. If the user requires an information about city block level, then the algorithmic layer should engage the system to provide him the most efficient measurement in terms of resource consumption. For such a lax accuracy requirement, a simple power measurement to the nearby base station ought to be enough. However, if the user needs an accurate and precise measurement, it should request a high performing measurement, such as a precise time measurement or the second best available.

Moreover, a cognitive positioning system (CPS) must not simply select a single measurement domain, instead it should aim to draw information from multiple domains with different degrees of certainty and quality. Only this will allow the CPS to provide a seamless positioning solution in indoor and outdoor scenarios. Therefore, as more SoO are considered it is important to understand how to proceed towards the hybridization of such different sources.

Measurement hybridization

If the data in use is commensurate, meaning both sensors are measuring the same physical phenomena, then the data can be directly combined [2]. In such cases, typical techniques involve classic estimation methods, such as Kalman filtering. Otherwise, when the sensor data is non-commensurate, the data must be fused at the feature/state vector or decision level.

For the non-commensurate case, feature level fusion involves the extraction of characteristic features that are relevant to the process under analysis. These features can then serve as an input to pattern recognition techniques, such as neural networks, clustering algorithms or template methods.

Decision level fusion means that the sensor information is combined after each sensor has made a preliminary determination of an entity's location, attributes, and identity. Examples of decision-level fusion methods include weighted decision methods, classical inference, Bayesian inference and Dempster-Shafer's method [2, 125].

Outdoor environments

The works in [16, 17, 30, 51, 61] show applications and methods of applying multiple sensor data with GNSS. Most of these studies focus on GNSS and inertial sensor units, while [30] also adds another sensor, a video camera. To merge this information, feature extraction is necessary before the fusion occurs. The study in [17] covers the usage of a particle filter for handling the fusion of several sensors with the possibility of having different observations models to handle, for example, sensor failures. An overview of several techniques for vehicle navigation is provided in [61].

The work in [44] further presents a real-time positioning system that is based on the tight integration of low-cost sensors and a consumer-grade GNSS receiver. The work in [96] presents a hybrid data fusion of GNSS measurements in conditions of poor signal coverage, such as urban canyons. This work relies on timing information from

the long-term evolution (LTE) system to aid when the number of available satellites is insufficient.

Indoor environments

The work in [144] presents a TDOA/RSS hybrid algorithm for localization using ultra-wide band. In [112], an inertial measurement unit (IMU) and RFID measurements are fused together with a tight Kalman filter where ranges are derived for both cases for the estimation phase.

The work in [8] proposes a hybrid system for WiFi and RFID measurements, discussing its potentials and limitations. In [115] inertial data is fused with WiFi data for indoor pedestrian navigation. [58] presents a joint estimation of range and angle measurements for systems using ultra-wide band signals on a real scenario with both line-of-sight and non-line-of-sight datasets.

In [80] a more specific application of data fusion is applied to smartphones, with the objective of enabling several location-based services. The same is seen in [142], where an indoor positioning system is evaluated in a supermarket scenario. The works in [8, 123] rely on Bluetooth beacons to enhance the performance of WiFi positioning systems. In [48] proposes a method to correct RSS-based position estimates from a Zigbee network with the help of a building graph model. The graph model consists of building information, movement model and rules which to use for the RSS filtering.

Seamless - Outdoor/Indoor environments

The work [133] proposes an architecture for fusing inertial, GNSS and WiFi sensors. A similar architecture is proposed in [87] where a barometer is added to improve the GNSS solution. The work in [37] looks at the benefit of observing multiple sensor data, such as LTE, WiFi and magnetometers and proposes a client-server architecture to provide a mechanism for the decision making, regarding which signals to trust in a given location. It also aims to solve inconsistency issues, such as when different systems report different locations of the users.

In [134] the work discusses how a seamless positioning system was built to accommodate visually impair people. It provides an overview of hybrid navigation methods, positioning techniques and lessons learned from building such system. The work in [50] discusses existing technologies for indoor positioning from a services point of view and how to switch between technologies when the scenarios change. The work [1] demonstrates the use of UWB as a complement to a cognitive radio technology (5G). The use of UWB is proposed to increase the accuracy of the system and to relieve the congestion on the licensed bands. It shows one of the trends in the hybridization of data, since the objective now is to understand which sensors to fuse and in which situations they should be merged.

So far, most authors have been focused in fusing a couple of technologies together to obtain a position solution but knowing which ones to select and when to use is still lacking more research.

CHAPTER 3

Spectrum Sensing

This chapter focus on the results in publications [P1, P2], where spectrum sensing techniques were used to detect the presence of OFDM and CDMA signals. It starts with a background introduction and progresses with the theoretical and simulation framework of detecting OFDM and CDMA signals based on their cyclostationarity features [P1] and moves on to practical considerations regarding the detection of IEEE 802.11g downsampled signals [P2].

In summary, the main contributions in this chapter consist of:

- Presentation of the detection algorithm derived in [P1] for the detection of 802.11 signals through downsampled samples;
- Summary of the method presented in [P2] to detect the presence of CDMA and OFDM in a signal mixture;
- Overview of the proposed receiver architecture to build upon the methods presented and described in this chapter and in [P1] and [P2].

3.1 Background, state-of-the-art, and related work

A cognitive radio (CR) is a device aware of its environment, allowing the coexistence with other radios that might lack cognition features [97]. The coexistence is guaranteed by monitoring the spectrum for unused frequency sub-bands [19, 139]. In some applications, knowing about its location is a valuable information for a CR. Unfortunately, it is not equally easy for a CR to obtain its location seamlessly across any environment, with indoor scenarios being particularly difficult ones. The reason behind the difficult in acquiring a location in indoor scenarios is related to the strong attenuation and multipath imposed by the environment. This places difficulties in acquiring a location estimate or location fix from widely available signals such as those coming from the GNSS. Consequently, it is important to seek better indoor positioning technology, to accommodate further CR enhancements as well as to enable other end user applications. Hence, it

is important to look at such environments, where cellular and WiFi signals are already widely deployed and make use of them for positioning purposes.

Enabling navigation through SoO, requires a device capable of simultaneously acquiring, tracking and decoding a multitude of signals, raising difficulties at the implementation level. Besides the physical limitations of current devices, power consumption is an important concern which does not benefit from adding extra sensors. Since CR and advanced signal processing techniques are becoming the norm for future telecommunication standards [6], it should be possible for positioning systems to build on the information made available by the cognition layer. Such information would allow a CR to manage more efficiently the hybridization of different sensor data [18, 82].

The idea of using SoO for positioning purposes has led the research community towards the concept of CPS [19–23, 109, 139]. These systems can understand the radio frequency spectrum and identify signals present in it. In a way, this is like what CRs are proposing for the communication protocols, however the main difference is that in CR, the idea is to optimize the spectrum efficiently. The spectrum optimization is done by allowing radio devices to operate in a band where they do not hold a license to operate in, as long as their operation does not interfere or degrade significantly the operation of the service intended for that frequency band [97]. CPS build on the same techniques for signal identification and detection but aim to understand the spectrum contents rather than simply understand if the spectrum is free or not. Knowing which signals are available in the spectrum is useful for positioning systems, as well as to the hardware controller, who might decide which signals are worthy to be acquired and tracked to fulfill the necessary location requirements.

3.1.1 Spectrum sensing

Spectrum sensing techniques are an important and useful background for CPS. This field has received the attention of the research community for several years and the works done by [60, 65, 139] serve as a good introduction, in the author's opinion, to this field. [60] discusses the main design challenges and requirements of a spectrum sensing system. The work done in [139] points out all the relevant radio spectrum and transmission opportunities, continuing further with an overview, comparison and discussion of the most common spectrum sensing algorithms in use. Some of the algorithms presented in [139] are further explained and presented along with other state of the art detectors in [65]. The work done in [65] provides an extensive overview on the most known spectrum sensing algorithms, such as:

- Energy detector;
- Cyclostationary-based detectors;
- Higher order moment detectors;
- Filterbank-based detectors;
- Multitaper detectors.

From the start, [65] describes why energy detection falls short for detection in noisy environments, where the signal to noise ratio (SNR) of the signal of interest is too low to be recognized by the energy detector [27, 38, 132]. The major drawback of the energy detector is that most of the times, the noise variance is not known, leading to an incorrect threshold level, resulting in a false detection. This is mostly known in the field as a SNR wall, which is the SNR limit to which the detector can provide accurate detection. Also, this is something that every detector suffers from, not only the energy detector. As mentioned in [65], the energy detector's SNR wall will be higher than some detectors that exploit known periodicities in the signals. Nevertheless, there are several approaches, mentioned in [67], to reduce the SNR wall for signal detectors.

Another approach to signal detection, which usually involves an increase in complexity, is the exploitation of second order statistics. Communication signals are possible to be identified with these statistics since they are considered colored signals, containing a non-flat power spectrum density. Indeed, this is caused by characteristics of the signals at hand and can be exploited in the detection stage to achieve better detection performance and even circumvent the issue of the SNR wall. It does not mean the detection will be possible at any SNR value, but only that the noise's statistics does not need to be properly known. In [65] the second order statistics methods are introduced using an OFDM signal, a popular modulation method in current wireless systems. A good introduction to second order statistics methods is also provided in [56], where it is shown how features for a simple pulse amplitude modulated signal appear due to a simple quadratic operation. These two works pave the way for cyclostationary-based methods.

In [65], the discussion continues with more specific detectors, that rely on structures of the sample co-variance matrix, blind detection, filterbank-based detectors and enters in other challenges and design questions in the field, such as cooperative spectrum sensing. Regarding cooperative spectrum sensing, where several sensors in different locations communicate between each other, the work done in [104] points out the main challenges, advantages and overhead when considering such situations.

3.1.2 Cyclostationary

Cyclostationary-based methods are one of the most popular methods in the field of signal detection and classification. This is mostly because the increase in complexity offers a good trade-off between detection accuracy and the decrease of the SNR wall, allowing for detection in noisy environments.

In both works presented in [56] and [57] it is possible to get a better understanding of cyclostationary theory and how it can be used to obtain useful features for detection purposes. The work in [57] is quite extensive, covering most of the applications of the cyclostationary, not only in the field of telecommunications, but also in other fields such as econometrics and biology.

Regardless of that, the cyclostationary methods are usually divided in frequency smoothing and time smoothing algorithms. The most efficient algorithms are the fast Fourier transform accumulation method (FAM) and strip spectrum correlation algorithm (SSCA), which belong to the time smoothing domain. While these two detectors are covered in [56], the work done in [111] describes booth of them with the necessary

detail for a correct and efficient implementation. An implementation of these methods is available in [31].

3.1.3 Related work

The work in [21] proposes a CPS that relies on two blocks, one that determines the necessary bandwidth to achieve a given accuracy and another that manages which spectrum is available to achieve that end goal. The CPS under proposal in [21], relies on TOA measurements to obtain the user's location. The work in [20] outlines and presents the multitude of cognition in several natural systems and brings the same methodology towards the cognitive radio, where a cognitive positioning system is presented that can adapt its accuracy requirements through different modes of operation. The work in [19] provides a comprehensive overview of cognitive radio for efficient communications, localization and radar systems.

The work in [130] proposes an enhancement to the CPS defined in [21] by increasing the bandwidth efficiency through the usage of multiple receiver antennas. The work presents a model based on the Crámer-Rao lower bound (CRLB) to derive the efficiency relationship to the number of antennas at the receiver and to model the accuracy of TOA measurements.

In [74], cellular CDMA signals are used in a positioning system built upon a software defined radio. Furthermore, it looks at experimental results from ground and aerial vehicles using the proposed receiver. The focus in [74] is placed upon the experiment setup and analysis of the clock biases as well as a comparison between the GNSS receiver pseudoranges and the ones obtained by the software defined radio.

3.2 Distinguishing signals in a mixture

Since there are plenty of SoO available to use, one of the goals of this thesis is to prove that it is indeed possible to distinguish, using cyclostationary-based methods, between CDMA and OFDM signals when mixed together in a baseband signal. This offers a fast way to understand the spectrum contents, without the need to wait for a decision from the dedicated hardware.

This section presents simulation results to distinguish between CDMA and OFDM signals. These signals are considered since they are commonly used by communication systems, such as IEEE 802.11ac/g/n/b signals. Recent studies show their applicability in the positioning field, through the usage of timing-based estimators [43, 117, 129].

3.2.1 Signal modelling

The simulation under presentation in this section consists of a mixture of two signals plus noise, $\mathrm{z}(t)$, denoted as,

$$\mathrm{z}(t) = \mathrm{y}(t) + \mathrm{o}(t) + \mathrm{g}(t), \tag{3.1}$$

where $\mathrm{y}(t)$ is a CDMA signal, $\mathrm{o}(t)$ an OFDM signal and $\mathrm{g}(t)$ is white Gaussian noise (WGN) of double-sided power spectral density equal to N_0. When $\mathrm{y}(t)$ or $\mathrm{o}(t)$ are

assumed to be absent in the spectrum, their representation is set to zero. For simplicity, the simulation assumes a channel with flat frequency response. These concepts could also be applied to other types of channels, such as frequency-selective channels.

The CDMA signal (see Figure 3.1 for an illustration of its spectrum), $\mathrm{y}(t)$, is given by,

$$\mathrm{y}(t) = \begin{cases} \mathrm{E_b} \sum_{n=-\infty}^{+\infty} \sum_{k=1}^{\mathrm{SF}} \mathrm{c_k}(n) p(t - k\mathrm{T}_c - n\mathrm{SF}\,\mathrm{T}_c), \\ 0, \text{ when signal absent,} \end{cases} \tag{3.2}$$

where $\mathrm{E_b}$ is the bit energy, $\mathrm{c_k}(n)$ is the chip value (+1 or -1) for k^{th} chip during n^{th} symbol, $\mathrm{p}(t)$, a pulse shaping function, which is taken as a rectangular pulse with amplitude one and width equal to the chip interval, T_c and SF is the spreading factor.

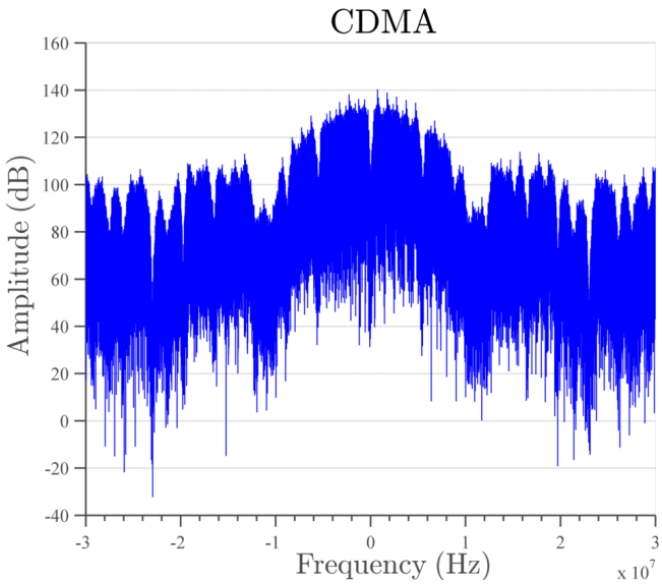


Figure 3.1: Example of a CDMA power spectrum.

As for the OFDM signal (see Figure 3.2 for an illustration of its power spectrum), $\mathrm{o}(t)$, is described by,

$$\mathrm{o}(t) = \begin{cases} \mathrm{A} \sum_{n} \sum_{k=0}^{\mathrm{N}-1} \mathrm{X}_n(k) e^{j2\pi k \Delta_f t} q(t - nT_U), \\ 0, \text{ when signal absent,} \end{cases} \tag{3.3}$$

where $\mathrm{A} = \sqrt{(\mathrm{N}\,\mathrm{T_U}\mathrm{E}_m)}$ is a multiplicative constant normalizing the OFDM symbol energy, N is the number of subcarriers, E_m is the average energy of M-QAM data symbols forming the OFDM symbols, $\mathrm{X}_n(k)$ is the n^{th} OFDM symbol expressed as a vector consisting of data symbols, and $\mathrm{q}(t)$, a pulse shaping function. $\mathrm{X}_n(k)$ is the

symbol period without the cyclic prefix. The total symbol period, T_{symbol}, is defined as

$$T_{symbol} = T_{GI} + T_U, \tag{3.4}$$

where T_{GI} is the duration of the guard interval, which is occupied by the cyclic prefix, plus the duration of the useful symbols, $T_U = \Delta f^{-1}$, which is chosen to guarantee orthogonality of the OFDM subcarriers for their given frequency spacing Δf. In the frequency domain, the signal occupies frequencies in the range $[-B, B]$ MHz.

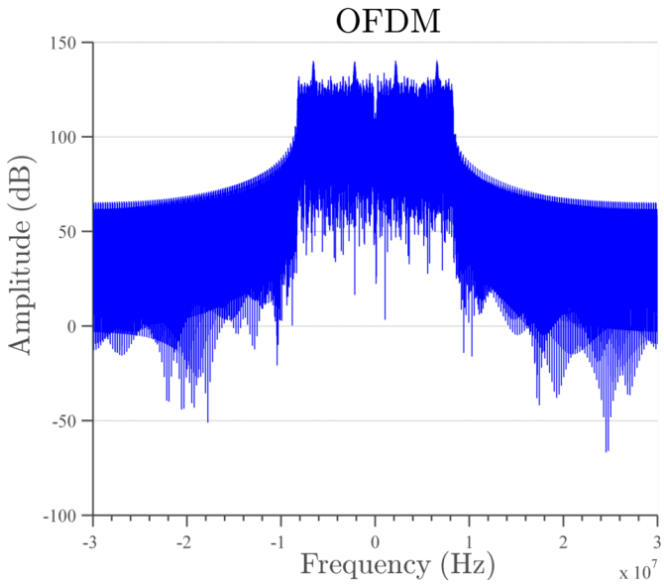


Figure 3.2: An example of an OFDM power spectrum.

3.2.2 Cyclostationary features

A signal $z(t)$ is wide-sense cyclostationary if its time-varying autocorrelation function $\Re(t, \tau)$ is periodic in time, t, for each lag parameter, τ. Hence, it can be represented as a Fourier series,

$$\Re(t, \tau) = E\{z(t)z^*(t + \tau) = \sum_{\gamma} \Re(t, \tau)^{\gamma}(\tau)e^{j2\pi\gamma t}, \tag{3.5}$$

where the sum is taken over multiples of fundamental cyclic frequency γ for which the cyclic autocorrelation function is defined as,

$$\Re^{\gamma}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} \Re(t, \tau)(t, \tau)e^{-j2\pi\gamma t}dt, \tag{3.6}$$

where T is the signal's period. The spectral correlation function (SCF) [57], $\mathfrak{S}^{\gamma}(f)$, is the Fourier transform of $\Re^{\gamma}(\tau)$ given as,

$$\mathfrak{S}^{\gamma}(f) = \int_{\mathbb{R}} \Re^{\gamma}(\tau)e^{-j2\pi f\tau}d\tau. \tag{3.7}$$

In [P1] and [P2] the FAM is used to estimate the SCF of the signals, with further reading available from [57, 111, 124]. A representation of the SCF in the frequency and cyclic domain is shown in Figure 3.3.

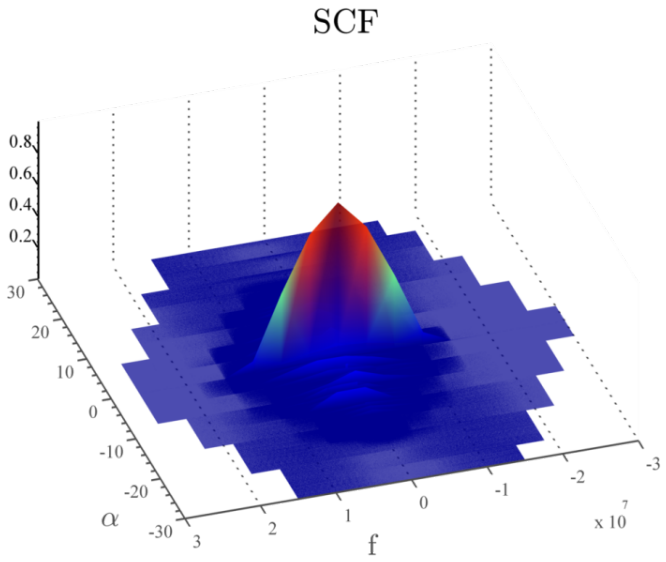


Figure 3.3: Example of a CDMA and OFDM SCF $\mathfrak{S}^{\gamma}(f)$ for $f_s = 60$ MHz, $\Delta\alpha = 1\exp{-05}$ f_s,$\Delta f = 0.1 f_s$.

Periodicities in the signal, such as those produced by the symbols or the repetitions of the spreading sequence are responsible for the appearance of spectral lines in the SCF domain. The location of such spectral lines is what is known as cyclic frequencies. When a signal has no well-defined periodicities, or, in other words, a signal is random, its SCF will be zero in all cyclic frequencies except for $\gamma = 0$. Figure 3.4 shows an example of a SCF for a mixture of CDMA and OFDM signals in noise. In Figure 3.4 the cyclic frequencies for the CDMA signal is shown as α_m and for the OFDM signal as β_m. The definition of α_m and β_m is presented over the following paragraphs.

The cyclic frequencies of interest are those specific to CDMA and OFDM signals, which for the first can be expressed [55, 82] as,

$$\mathfrak{S}^{\gamma}(f) \cong \mathrm{Y}(f)(f - \frac{\gamma}{2})\mathrm{Y}(f)^{*}(f + \frac{\gamma}{2}) \sum_{k=-\infty}^{\infty} \delta_{\left(\gamma - \frac{k}{\mathrm{T_{symbol}}}\mathrm{T}_c\right) \bmod 1} + \frac{\mathrm{N}_0}{\mathrm{E_b SF}}\delta_{\gamma}, \tag{3.8}$$

where $\mathrm{Y}(f)$ is the Fourier transform of $\mathrm{y}(t)$, $\delta_{(\gamma - \frac{k}{\mathrm{T}}\mathrm{T}_c) \bmod 1}$ the Kronecker delta function having value 1 when $(\gamma - \frac{k}{\mathrm{T}}\mathrm{T}_c) \bmod 1 = p$, $p \in \mathbb{Z}$ and zero otherwise, T_c is the chip interval length, T the symbol period. Its theoretical cyclic frequencies [55] are dependent on both the chip rate, f_c, and SF and are contained in $\mathcal{A}$,

$$\mathcal{A} = \{\alpha_0, \alpha_1, \cdots, \alpha_m\}, m \in \mathbb{Z}, \forall \alpha_m : \alpha_m \in \left\{ kf_c\ ,\ kf_c \pm n\frac{f_c}{SF} \right\}, k, n \in \mathbb{Z}. \tag{3.9}$$

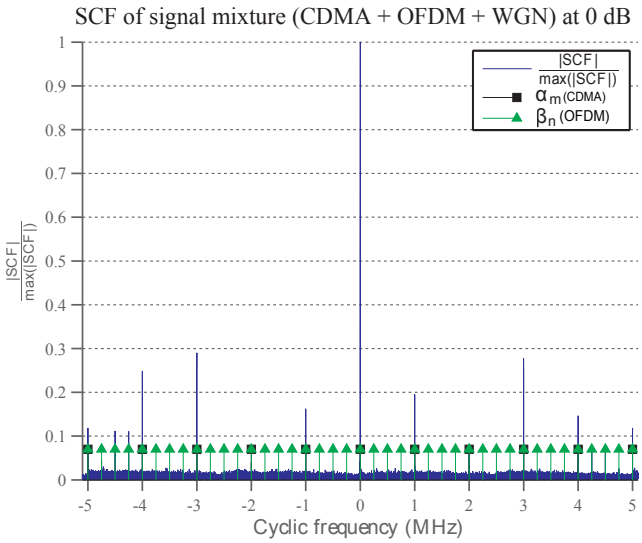


Figure 3.4: SCF section at frequency zero $\mathfrak{S}^{\gamma}(0)$.

The OFDM SCF [127] is estimated by,

$$\mathfrak{S}^{\gamma}(f) = \frac{\delta_r^2}{\mathrm{T}} \sum_{n=0}^{\mathrm{N}-1} \mathrm{Q}(f) \left(f - \frac{n}{\mathrm{T_{symbol}}} + \frac{\gamma}{2} \right) Q^* \left(f - \frac{n}{\mathrm{T_{symbol}}} - \frac{\gamma}{2} \right), \tag{3.10}$$

which is non-zero for every $\gamma = \frac{k}{\mathrm{T_{symbol}}}$ and zero otherwise and $\mathrm{Q}(f)$ is the Fourier transform of the pulse shape function. The OFDM theoretical cyclic frequencies are found to be in $\mathcal{B}$,

$$\mathcal{B} = \{\beta_0, \beta_1, \cdots, \beta_n\}, n \in \mathbb{Z}, \forall \beta_n : \beta_n \in \left\{ k \frac{1}{\mathrm{T_{symbol}}} \right\}, k \in \mathbb{Z}, \tag{3.11}$$

where each β_n location is related to the symbol period [88].

3.2.3 Cyclic frequency detector

Building on the knowledge of the cyclic frequencies, the work in [P2] proposes an algorithm to infer if CDMA or OFDM signals are present in a signal mixture. The algorithm works by considering a window, W, with center point at a cyclic frequency, γ_i, from either sets $\mathcal{A}$ or $\mathcal{B}$. The window's size is set to,

$$\mathrm{W} = [\gamma_i - \mathfrak{E}, \gamma_i + \mathfrak{E}] \tag{3.12}$$

where $\mathfrak{E}$ is set to a value that avoids overlapping with other cyclic frequencies of the signals being tested. If such condition is not met, the algorithm reports a false positive. Future work might address this issue or at least provide some insight to the correct size of the window, according to the resolution in the cyclic domain.

This resolution will impact the possible number of samples to acquire from the vicinity of γ_i therefore, in this study the condition was met and W is defined over the range $[\gamma_i - 0.0305, \gamma_i + 0.0305]$ Hz of the absolute value of the SCF. The range is defined over the previous and next 100 frequencies in the cyclic domain.

Using the samples taken from W, the algorithm takes the mean, μ, and standard deviation, σ, values of this region and computes an activity indicator, I, as,

$$\mathrm{I} = \frac{\sigma}{\mu}, \tag{3.13}$$

for each window centered in the cyclic frequencies under test, as seen in the right side of 3.5. Therefore, if a cyclic frequency is present and is contained in W, the peak value in the SCF at that location will significantly increase the value of the standard deviation and by consequence the value of the activity indicator I.

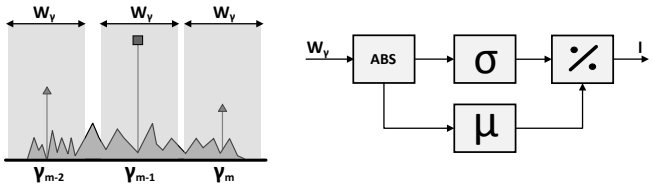


Figure 3.5: Algorithm's window for α_m (left) and detector's diagram block (right).

3.2.4 Decision process

The detection mechanism consists of feeding the cyclic frequencies from an SCF into a K out of M detector [136]. Hence by testing against the cyclic frequencies defined in sets $\mathcal{A}$ and $\mathcal{B}$, it is possible to infer the presence of a CDMA, OFDM or none of the signals present in the spectrum's digital representation.

However, as some cyclic frequencies are bound to overlap, the work in [P2] proposes a detection test over two stages. The detection bases its decision on the following hypotheses:

$$\mathcal{H}_{1.1} = \begin{cases} \text{CDMA and OFDM with AWGN} \\ z(t) = x(t) + y(t) + n(t), \end{cases} \tag{3.14}$$

$$\mathcal{H}_{1.2} = \begin{cases} \text{CDMA with AWGN,} \\ z(t) = x(t) + n(t), \end{cases} \tag{3.15}$$

$$\mathcal{H}_{1.3} = \begin{cases} \text{OFDM with AWGN,} \\ z(t) = y(t) + n(t), \end{cases} \tag{3.16}$$

$$\mathcal{H}_{0} = \begin{cases} \text{AWGN only,} \\ z(t) = n(t). \end{cases} \tag{3.17}$$

First, the test starts by evaluating the presence of M CDMA cyclic frequencies. If these are flagged by the detector as being present, then, the process is done for M OFDM

cyclic frequencies. If at this stage the detector also provides a positive response, then both CDMA and OFDM signals are present in the spectrum. Otherwise, only a CDMA signal would be present in the spectrum. Moreover, if the first test would be negative, then the decision would carry on by testing against M OFDM cyclic frequencies. In this case, a positive would point out that only an OFDM signals is present in the spectrum, whereas a negative would mean that only noise is available. A flowchart of the decision process is provided in Figure 3.6.

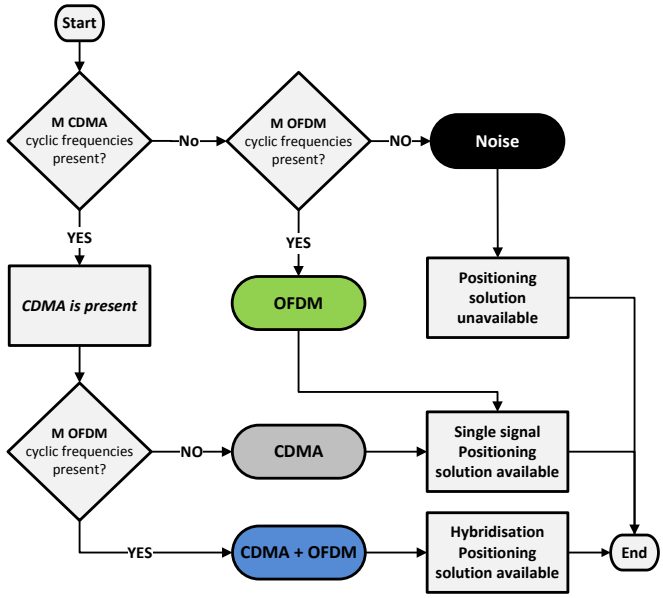


Figure 3.6: Cognitive positioning algorithm with SCF-based detection.

The cyclic frequency detector was also used in [P1] to detect the presence of IEEE802.11 signals using experimental data acquired through a USRP platform.

3.3 Receiver design aspects

The work in [P2] proposes a receiver architecture whose aim is to reduce the time of acquisition, tracking and demodulation of the incoming signals, in comparison to traditional approaches (see Figure 3.7.A).

The main difference between these two architectures is the presence of a spectrum sensing block, which provides relevant input to the CPS about the available signals. Thus, the CPS executes the signal selection based on this information exchange, controlling which acquisition, tracking and demodulation blocks to enable. This allows for better power management in the devices, which is further improved by the efficiency of the spectrum sensing detection methods. One practical example is discussed in [P1]. The work in [140] refers to the contribution in [P2] for comparison of experimental results.

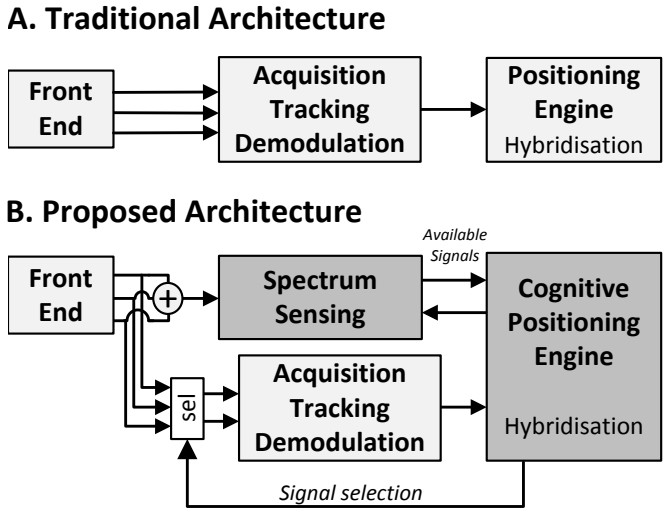


Figure 3.7: Cognitive positioning system.

3.3.1 Measurement setup

The work in [P1] relied on field measurements of 802.11g OFDM signals. The acquisition of such data was performed with a universal software radio peripheral (USRP) B210, with a standard 2.4 GHz 3 dBi omnidirectional antenna attached to it. Several acquisitions were performed at different sampling rates,

$$f_s = \left\{ 2f_N = 40, f_N = 20, \frac{1}{2} f_N = 10 \right\} \text{ MHz},$$

where $f_N = 2\text{B} = 20$ MHz is the signal's Nyquist rate. The signal under acquisition spans over the frequency range $[-\text{B}, \text{B}]$ MHz, where B is the one-sided bandwidth equal to 10 MHz. Hence, its Nyquist frequency is $10MHz$. Figure 3.8 illustrates the measurement setup.

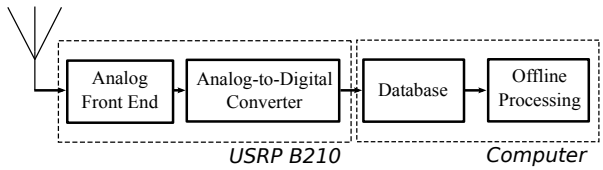


Figure 3.8: Setup used for the measurement of IEEE 802.11g OFDM signals.

3.3.2 Understanding the impact of undersampling on cyclostationary analysis

One of the main disadvantages of cyclostationary methods is the complexity burden associated with them, which is also dependent on the sampling rate used at the receiver. Most of the times, this sampling rate is high, to observe more easily the appearance of certain spectral lines. Using real measurement data, the study in [P1] aims to understand if cyclostationary properties are still preserved in undersampled signals, sampled at rates below the Nyquist rate. Since these properties seem to be still visible, this result means a reduction of the complexity through usage of lower sampling frequencies.

Effect of downsampling in cyclic properties

The measurement data from the measurement setup in Figure 3.8 was further split in T_{obs} ms segments. In [P1] T_{obs} was set to 10ms which was arbitrarily chosen to contain useful signal at each time.

Each of these time measurements were further fed into a cyclostationarity block to obtain the corresponding cyclic frequencies and investigate the impact of each sampling frequencies in the SCF defined by equation (3.11). The resulting spectrum, at 40 and 10 MHz, is presented in Figure 3.9, where several major spectral lines remain visible for both sampling frequencies.

However, the amplitude of the spectral lines change based on the sampling frequencies, with some intensifying and others diminishing towards the noise level. An example of such phenomena is visible in Figure 3.9 at 1 MHz.

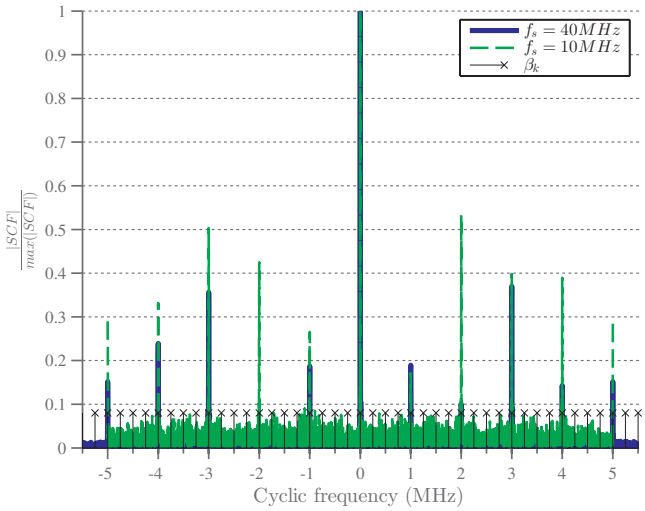


Figure 3.9: $\mathfrak{S}^{\gamma}(0)$ for measured data sampled at $f_s = 40$ MHz and $f_s = 10$ MHz.

Statistical behavior

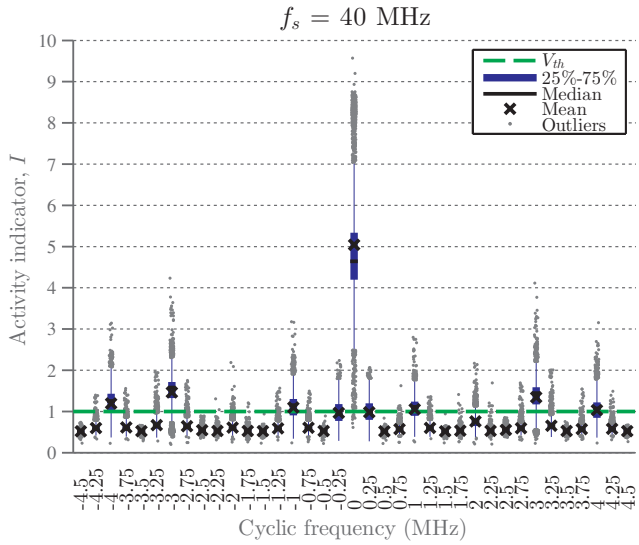
To further understand the impacts of the sampling frequencies in the cyclic frequencies, the work in [P1] proposes looking at the statistical behavior coming out of the activity indicator, I (as defined in equation 3.13). Hence, for each sampling frequency, Figures 3.10 - 3.11 present the boxplot of the values of the activity indicator I calculated over the cyclic frequency interval of (-5, 5) MHz. The boxplots contain the median, mean, the 25th and the 75th percentiles of the activity indicator I. The 25th percentile is defined by the box's lower edge while the upper edge corresponds to the 75th percentile. The Vth in the boxplot refers to the threshold used for calculating the probability of appearance seen in Figure 3.12 and later explained in section 3.3.2

Based on Figures 3.10 - 3.11, the value changes in the activity indicator I are mostly due to the cyclic frequencies located at integer values. In other location, the value of I remains close to the noise level activity of 0.5. It is also clear that for certain sampling frequencies, such as 10 MHz, the value of the activity indicator I is well above the threshold value for most of its cyclic frequencies at integer frequency values. This does not seem to be so evident for the other sampling frequencies.

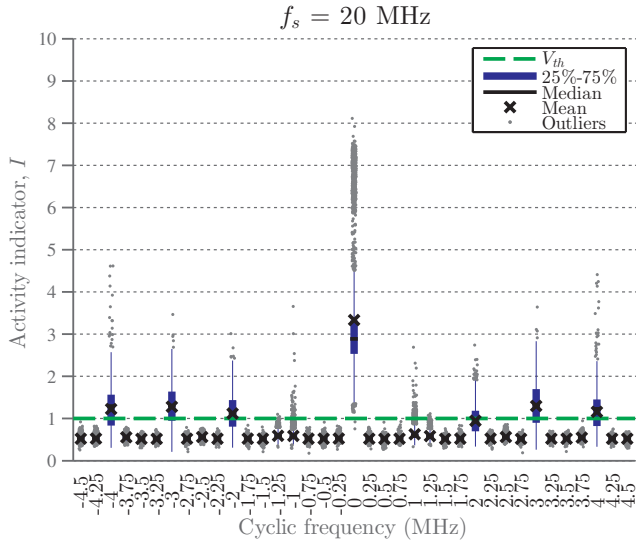
Overall, this observation should have an impact on setting the correct value of the threshold. While such mechanism was out of scope in [P1], it will play an important aspect in the correct classification of the spectrum contents as later presented in [P2].

Most frequent cyclic frequencies

Based on the results presented in Figures 3.10 - 3.11, the work in [P1] proposes looking also at the probability of appearance of cyclic frequencies. The motivation behind this is to allow further decision aids when determining the spectrum contents. In [P1], the probability of appearance of a cyclic frequency is defined as the number of times its value is above the threshold value of I for a set of N observation windows of T_{obs} ms duration. Figure 3.12 shows the probability of appearance for all the expected cyclic frequencies from $\mathcal{B}$ over N=5000 windows. It is visible from Figure 3.12 and Table 3.1 that the highest probability of appearance is associated to cyclic frequencies located at integer frequencies.



A



B

Figure 3.10: Boxplot of the activity indicator for $f_s = 40$ MHz (A) and $f_s = 20$ MHz (B).

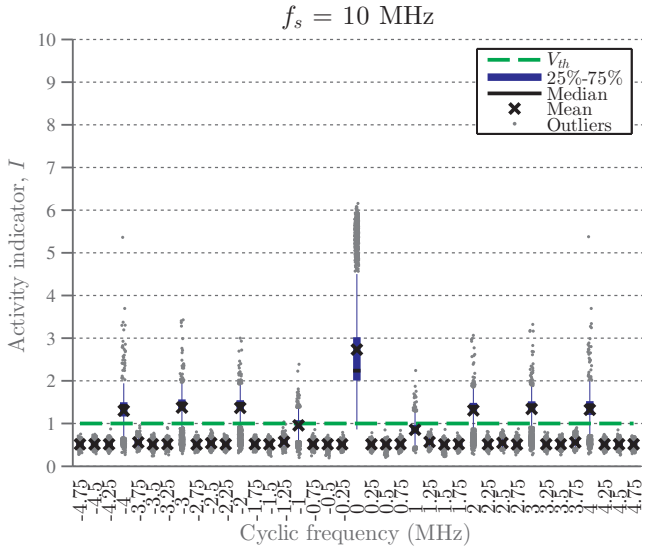


Figure 3.11: Boxplot of the activity indicator for $f_s = 10$ MHz.

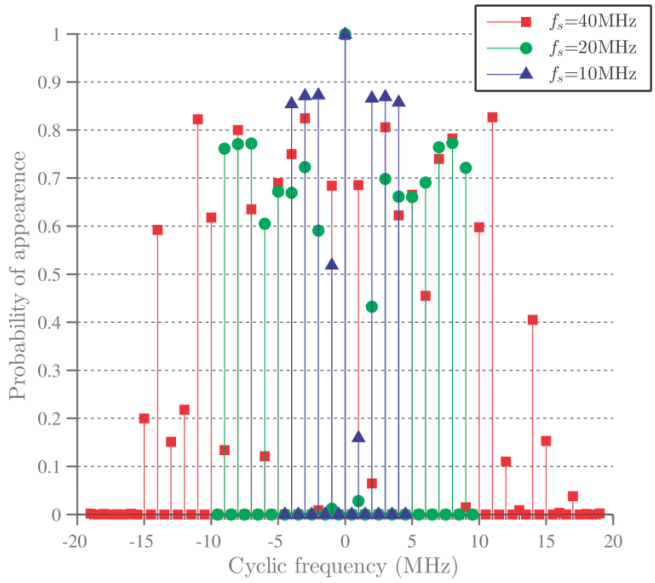


Figure 3.12: Probability of appearance for signals sampled by USRP, sampled at 40MHz, 20MHz, 10MHz.

Table 3.1: Probability of appearance of cyclic frequency.

	Sampling frequency		
	40 MHz	**20 MHz**	**10 MHz**
Cyclic frequency (MHz)	**Probability (%)**		
4	62	68	86
3	81	71	87
2	6	45	87
1	69	3	16
0	100	100	100
-1	68	1	52
-2	1	61	87
-3	82	74	87
-4	75	69	85

3.4 Discussion

This chapter covered an introduction to the contributions done by the thesis' author in the field of spectrum sensing. The chapter was divided in two parts. The first part introduced the background, state-of-the-art and parallel work. The second part provided a short summary of the author's contributions presented in [P1] and [P2], where the main goal was to detect the presence of CDMA or OFDM signals at the physical layer through a cyclostationarity framework. The reason to choose CDMA and OFDM signals came from the fact that they represent, at the physical layer, popular and commonly used telecommunication signals, such as WiFi and Bluetooth.

The contribution in [P1] demonstrated through an experimental setup that it is possible to infer the presence of a WiFi signal at sampling frequencies below the Nyquist rate. While such result was known from [124], the results in [P1] provide further experimental validation on an USRP platform, which has been cited by [140] for comparison of experimental results.

Besides the experimental validation, the work in [P1] relied on the algorithm presented and discussed further in [P2]. The algorithm in [P2] provided a simple mechanism to infer the detection of OFDM or CDMA signals.

While [P2] relied on actual measurement data acquired inside a typical office environment, the work did not focus on the possible interference and degradation of results imposed by other signals. Nevertheless, this is one of the reasons why cyclostationarity was picked as the framework, since its characteristics allow to distinguish overlapping signals in the spectrum.

Due to the complexity of the cyclostationarity methods, some of the benefits pointed out by the works in [P1] and [P2] are difficult to achieve with off the shelf hardware. For example, the trade-off between CPU power and battery savings might not justify such complex hardware loops in a CPS.

Nevertheless, the goal of a CPS would be to adapt itself to its environment, hence, understanding its radio environment will be of importance to maximize the usage efficiency of future hardware, providing a better user experience to the end user.

CHAPTER 4

Channel Impairments

This chapter focuses on how to deal with the degradation in signal quality imposed by radio interference in terms of a SoO positioning system. The chapter starts by presenting key aspects of radio propagation and interference, the phenomena of fading. There is a big emphasis on the intra-system interference mitigation as it was the main topic under discussion in [P3].

The main contributions discussed in this chapter consist of:

- Summary of the analysis done in [P3] regarding the impact of intra-system interference regarding the RSS of commercial BLE tags;
- Demonstration on how to compensate for the impact of intra-system interference and other channels impairments on ranging based on RSS measurements.

4.1 Background, state-of-the-art and related work

Interference is the process of two radio waves interacting with each other and producing a new signal with different amplitude and phase properties. Intra-system interference refers to interactions between signals belonging to the same system: they can be multiple copies of the same signals (e.g, multipath interference) or different signals belonging to the same system (e.g., multi-user interference). Inter-system interference is known as the interaction between radio waves from different systems. As an example, two WiFi signals intra-interfere with each other, while a WiFi and Bluetooth signal inter-interfere with each other.

The amount of interference is characterized by the change this interaction causes in the original signal. Understanding the effect of interference requires the understanding of the propagation environment and the effects the signals are subject to throughout their travel.

4.1.1 Wireless propagation

Propagation of a radio wave is the behavior exhibited by a radio wave as it travels away from its emitting source. In an ideal medium, known as free space, the losses follow the Friis equation given by,

$$\mathrm{P_r}(d, f) = \mathrm{P_t} - 10\log_{10}\left(\frac{4\pi f d}{\mathrm{c}}\right)^2, \tag{4.1}$$

where $\mathrm{P_r}(d, f)$ is the received power at distance d (m) for the operating frequency f (Hz), assuming a transmission power of $\mathrm{P_t}$ in dBm and a propagation in free space at the constant speed of light, c (m/s). However, due to the channel impairments two common ways to describe the behavior of a radio wave is through the Log distance model, as defined in equation (2.9) or through the recommended ITU model described by [68],

$$\mathrm{P_r}(d, f) = \mathrm{P_r}(\mathrm{d_0}) + \mathrm{C} - 20\log_{10}\ (f) - \eta\log 10(d) - w, \tag{4.2}$$

where $\mathrm{P_r}(\cdot) < 0$ is the received signal power in logarithmic scale dependent on distance d in dBm, $\mathrm{d_0}$ is a reference distance, C is a constant that models other system losses due, $\eta > 0$ is the path-loss exponent and $w \sim \mathrm{N}(0, \sigma^2)$ a normally distributed random variable which models the fading phenomenon. Both, η, w are dependent on the propagation environment and should be considered different for each path between receiver and transmitter.

Characterizing the propagation of a radio wave is not trivial and for more reliable models, one needs to look at more complex methods such as ray tracing. In the ray-tracing approach, multiple paths or rays are simulated from their origin until they are captured. A ray-tracing technique also includes simulating reflection and refraction of the rays in the surrounding environment. Nevertheless, while this technique does offer a clear benefit over the standard methods, it is resource consuming. Besides that, its effectiveness is also limited to the knowledge of the surrounding propagation environment, meaning that one needs to know exactly the building materials to have accurate refraction and absorption indexes.

4.1.2 Fading

Fading or small-scale fading describes the variations in the amplitude of a radio signal over a short path or period, so that large-scale path loss effects may be ignored [108]. The cause of fading is due to the interference between two or more versions of the transmitted signal which arrive at the receiver at slightly different times. The combination of these radio waves at the receiving antenna can result in a single signal which varies greatly in amplitude and phase from the one that was initially sent, depending on the relative propagation time and bandwidth of the transmitted signal.

According to [108], the most important effects caused by fading are:

- Rapid changes in signal strength;
- Random frequency modulation due to varying Doppler shifts on different multi-path signals;

- Time dispersion by multipath propagation delays.

In most telecommunication systems, fading happens due to the lack of line of sight between receivers and transmitters. This means that the arrival signal is a version of the original version that has suffered attenuation due to presence of an obstacle in this primary path. Nevertheless, even in line of sight conditions, fading still occurs, as the signals still gets reflected and refracted by the surrounding environment. However, in a line of sight condition it is expected that the signal over the primary path is the one with the highest received signal strength. In short, the major physical factors affecting fading are [108]:

- multipath propagation - objects and changes in the surrounding transmission environment contribute to constant changes of the signal's energy dissipation. This also results in the creation and propagation of multiple versions of the transmitted signal with random phases and amplitudes, resulting in fluctuations of the signal strength or distortion of the signals;
- relative speed of receiver to the transmitter - the relative speed between transmitter and receiver results in what is known as the Doppler shift. This associated with multipath propagation results in multiple signal paths with random frequency modulations;
- speed of surrounding objects - the motion of objects within the radio channel induce a time varying Doppler shift on multipath components. This effect is only relevant if the objects velocity is bigger than the receiver;
- transmission bandwidth of the signal - the bandwidth of the transmitted signal relates to how the channel affects it over a small local area. Depending on the coherence bandwidth of the channel, or simply the multipath bandwidth channel, which is a measure of the maximum frequency distance between two correlated frequencies, signals with a larger bandwidth will suffer distortion but their signal strength will likely not be affected as much.

In summary the combination of these effects results in multiple types of fading:

- Flat fading;
- Frequency Selective Fading;
- Fast fading;
- Slow Fading.

The first two types, flat and frequency selective fading are due to the multipath time delay spread, which results in time dispersion and frequency selective fading. Whereas the last two, fast and slow fading, result from the Doppler spread which results in frequency dispersion and time selective fading.

The presence of these channel impairments and the interference they impose on intra and inter-system signals, result in errors, biases and inaccuracies at the measurement

layer. For time-domain measurements, such errors in the measurement layer lead to delays or a miss-detection of the signal. For space-domain measurements, such errors can lead to several degrees of error, especially if what is detected by the receiver as the main path is a multipath signal and not the original one. Finally, in terms of power-domain measurements, the signal strength can vary greatly by the amount it is expected to change. This has a big effect on ranging techniques for beacon applications, which is discussed further in section 4.2.

4.1.3 Related work

The work in [93] provides experimental results from a fingerprinting approach relying on channel frequency response as the training feature, as proposed in [25]. The work in [93] proposes three distinct methods to increase the robustness of the fingerprints with regards to channel impairment effects.

The work in [71] looks at the impact of several wireless protocols on the operation of BLE devices in a hospital context. It also proposes and evaluates a mathematical model for the interference of wireless technologies on BLE enabled devices. Moreover, it offers recommendations on the spacing of the devices to minimize the symbol and packet error rate.

The work in [15] proposes a cooperative mechanism to prevent overlap of IEEE 802.15.4 and BLE (in connection mode) packets. The proposal mechanism relies on the tracking and adjustment of the periodic transmissions, based on the chance of collision wither with 802.15.4 or with BLE.

The work in [46] investigates the impact of BLE on WiFi fingerprinting-based indoor positioning systems. It looks at the signal characteristics of BLE, which due to its lower bandwidth is more susceptible to fast fading with respect to WiFi. It also provides a mechanism to mitigate multipath for the BLE signals and draws up an upper bound on the beacon settings and deployments to observe a clear benefit in terms of combined fingerprinting accuracy benefits.

The work presented in this chapter and based on [P3] offers an additional view on the characteristics of BLE signals and effects caused by intra-system interference. In addition, it provides a rule of thumb to minimize the impact of multipath interference on the determination of BLE ranges.

4.2 Impact of intra-system interference on BLE signals

The contribution in [P3] discusses the impact on intra-system interference on BLE signals. This study consisted of analyzing the RSS of multiple commercial BLE tags and its impact on a ranging technique to determine the distance from the emitters to the receiver.

BLE is an extension to the Bluetooth 4.x Core Specification, targeted to supporting IoT applications. It contains a new physical layer, advertisement mechanism, asynchronous connection-less MAC among other features to allow low cost and low power operation in the 2.4GHz band [13]. However, since the 2.4GHz band is a contested

band by many wireless technologies, BLE has a built-in mechanism to fight off major sources of interference, for example, WiFi. This mechanism is called adaptive frequency hopping (AFH). Despite that, intra-system interference is inevitable, especially in the connection-less mode, where the devices are simply advertising, in this mode, only 3 out of the 40 available channels are used for broadcasts.

Assuming N_{tags} BLE advertiser devices operating over a period of t seconds and sharing $N_{channels}$ channels, then, according to [59], the probability, $\mathfrak{P}$, that a channel is occupied is given by,

$$\mathfrak{P} = 1 - \left(\frac{N_{channels} - 1}{N_{channels}} \right)^{(N_{tags}-1)} . \tag{4.3}$$

While equation (4.3) assumes significant simplifications, such as the fact that devices are synchronized and the time between frequency hops is always the same, it does show the inherit limitation of the BLE protocol for large scale deployments. Such limitation appears from the small number of advertisement channels, which means that, as the number of devices in a single radio vicinity increases, higher is the probability of the devices causing intra-system interference with each other. Based on equation (4.3), the increase of probability when 3 BLE devices are broadcasting is approximately 56% and it increases to 94% when the number of devices increases to 8.

Overall, despite AFH's best effort to mitigate the interference with other in-band systems, it cannot fully solve the intra-system problem as described above. Therefore, the study in [P3] sets out to make an evaluation of the characteristics of RSS in different scenarios of strong and weak interference. More specifically, the tests were undertaken in two office environments, one inside an office room and another in an office corridor.

4.2.1 Measurement acquisition

Two different environments were used for the analysis in [P3]. One environment was in a closed office environment in Finland and the other in an office corridor in the UK.

Office room

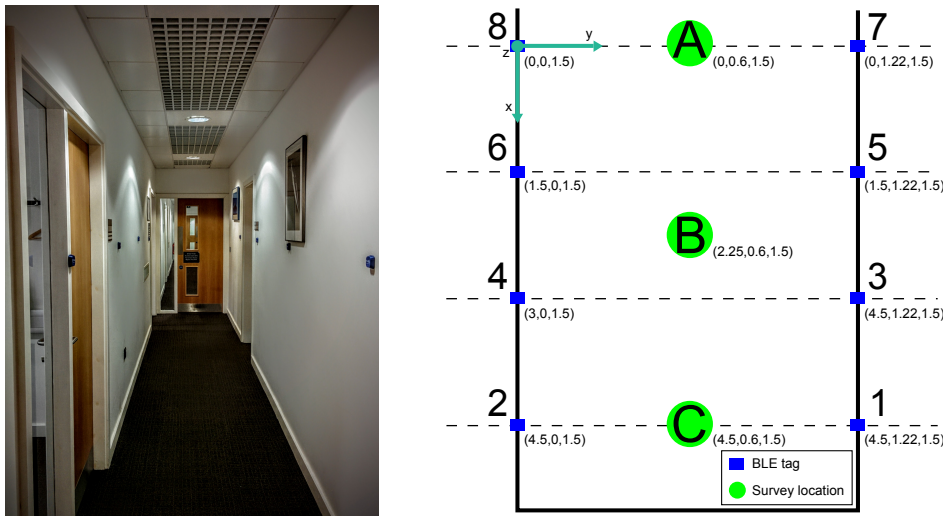
In the office room environment, a single BLE tag is set at distances of 0.05, 0.10, 0.5, 1, 1.5, 2, 2.5 and 3 meters from the receiver. The BLE reader was kept fixed, and the acquisition at each point lasted at least 30 minutes.

Office corridor

In the office corridor scenario, the eight tags were deployed in a regular grid, with a 1.5 meter distance, all at the same height of 1.5 m from the floor. The corridor environment is shown in Figure 4.1 along with a schematic of where the tags and the BLE reader were placed throughout the measurement acquisition.

4.2.2 Model-fit evaluation

The goal of the analysis in [P3] was to understand which model to be used in applications that require the knowledge of the BLE propagation signals. The root mean square error



A B

Figure 4.1: Corridor photo (A) and map (B) with tags and survey locations during the data acquisition.

(RMSE) is used as an indicator to the goodness of the fit, by comparing the mean observed value to the value reported by the model at that given distance.

The RMSE is defined as,

$$\mathrm{RMSE} = \sqrt{\frac{\sum_{i=0}^{N} (y_{\mathrm{observed}}^{(i)} - y_{\mathrm{expected}}^{(i)})^2}{N}}, \; N > 0 \tag{4.4}$$

where $y_{\mathrm{observed}}^{(i)}$ is taken as the mean of the power measurements and $y_{\mathrm{expected}}^{(i)}$ the value obtained through the fitted path loss model.

Tables 4.1 and 4.2 show the RMSE of the model fit for each of the two office environments considered. In both tables the log distance model is compared when the estimation of the path loss coefficient is done using an estimated value or the reported value by the tag ($\mathrm{P_r}(\mathrm{d_0}) = -77$ dBm is the value broadcast by the BLE tags). The estimated value is assumed to be the mean RSS at 1 m from the tag over more than one hour. The reported value is the transmit power reported by the protocol defined by the manufacturer.

Table 4.1 compares the fit of both models inside the office room in Finland. In this environment, a single tag was used throughout the study where its RSS was measured at several distances for periods of 30 minutes. Based on Table 4.1 the smallest RMSE is obtained when using the log distance model with estimated parameters. The worst fit seems to be for the log distance model when the tag's reported apparent power is considered. Regardless of that, the deviations can also be explained by the remaining error

Table 4.1: Model fit for the measurements of 1 tag acquired in Finland.

Distance (m)	RMSE (dB)		
	log dist model		ITU-R model
	$P_r(d_0) = -77dBm$ $\eta = 1.02$	$P_r(d_0) = -79.73dBm$ $\eta = 0.98$	$C = -24.76$ $\eta = 1.08$
0.50	0.95	1.87	4.60
1.00	3.59	0.87	3.78
1.50	8.57	5.91	6.74
2.00	7.69	5.07	4.42
2.50	8.95	6.37	4.58
3.00	5.33	2.78	0.05
Mean (dB)	**5.85**	**3.81**	**4.03**

Table 4.2: Model fit for the measurements of 1 to 8 tags acquired in the UK.

Distance (m)	RMSE (dB)					
	log dist model				ITU-R model	
	$P_r(d_0) =$ **-77 dBm** $\eta = 0.99$ **tags = 8**	$\eta = 0.97$ **tags = 1**	$P_r(d_0) =$ **-79.73 dBm** $\eta = 0.94$ **tags = 8**	$\eta = 0.96$ **tags = 1**	$C = -15.96$ $\eta = 1.09$ **tags = 8**	$C = -19.28$ $\eta = 1.00$ **tags = 1**
1.39	1.15	2.48	1.40	5.04	4.05	2.06
1.90	3.19	3.08	5.87	5.76	4.07	1.09
3.22	2.23	2.06	0.39	4.70	7.87	0.71
Mean (dB)	**2.19**	**2.54**	**2.55**	**5.17**	**5.33**	**1.29**

due to the variance of the measurements. Figure 4.2 shows a graphical representation of the three model fits alongside with the box plots for the measurement data.

Table 4.2 allows the same comparison for the office scenario in the UK. Three observations points defined with 1 and 8 tags broadcasting simultaneously and measurements done for 15 minutes. In this environment and contrary to what was observed in Table 4.1, the log distance model now offers the lowest RMSE when the 8 tags are broadcasting and the ITU-R model seems to perform better when a single tag is broadcasting.

Figures 4.3 - 4.4 show the box plot for the measurement data with 1 and 8 tags broadcasting, respectively. The fitted models are plotted on top of it. In both, the measurement data is skewed with only one balanced set in 4.4 for the measurement made at 3.2 m. In 4.2 most of the data sets are balanced which is not only related to the bigger observation period but also due to the differences in the propagation environment. While both play an important role in the degradation of the signal, the systems losses are estimated to be bigger in the closed office environment by approximately 10 dB (see value of C in Tables 4.1 and 4.2). Indeed, in the closed office environment there are many other objects present such as shelves located over the testing area.

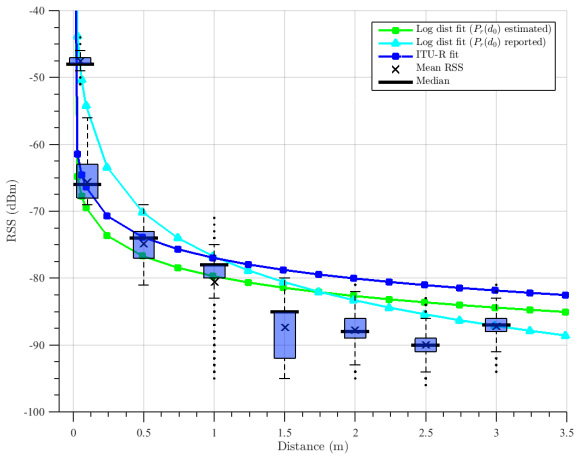


Figure 4.2: RSS fit for the office environment at TUT, with a single tag transmitting.

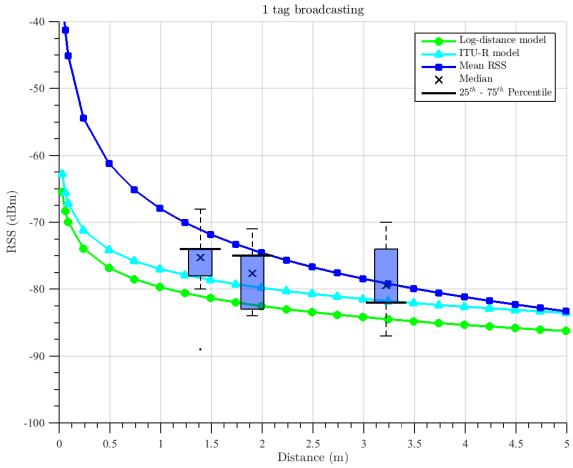


Figure 4.3: Measurement statistics with a single tag broadcasting, for the office corridor environment.

Nevertheless, besides the environment and the observation period, there is a clear offset in the fit of the ITU-R model when 8 tags are transmitting. The difference in the overall RMSE is approximately of 4 dB. Figure 4.5 shows the statistics for the RSS of tag 3 when up to 7 other tags were spread around it, spaced regularly on a half meter grid. The observations lasted over 3 hours.

Figure 4.5 shows that the RSS starts to show significant degradation once more than 3 tags are broadcasting. It is possible to see in Figure 4.5 a reduction in the mean and median values of the RSS up to 5 dB.

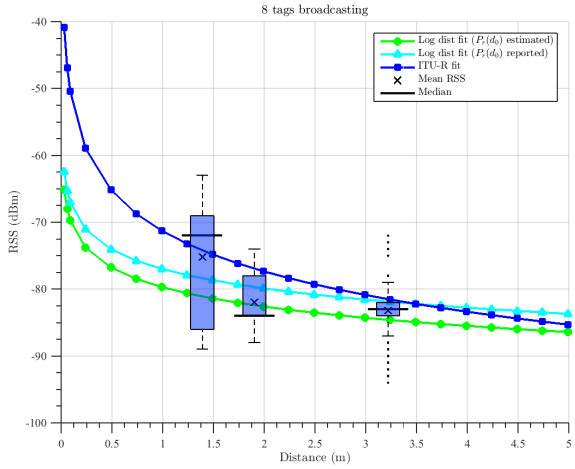


Figure 4.4: Measurement statistics with 8 tags broadcasting, for the office corridor environment.

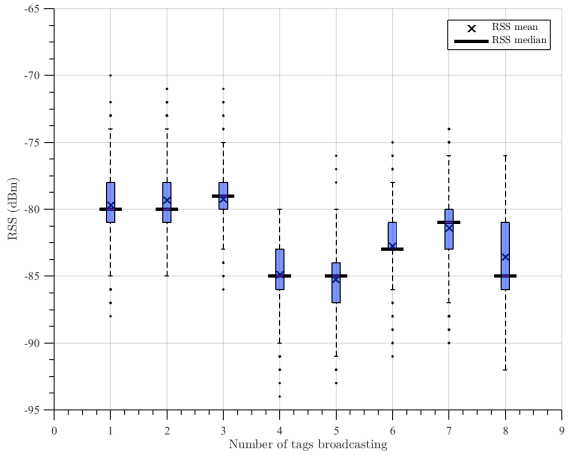


Figure 4.5: RSS values for tag 3 at 1 meter versus the number of tags broadcasting.

Another interesting observation is the one present in Figure 4.6 which shows the cumulative probability of the difference between the RSS at observation points A, B and C in the office corridor environment. In this figure it is also clear that there is a significant variability in the RSS when a larger number of tags is transmitting. It is even more interesting to see that the bigger variability occurs at point B, middle of the corridor (see Figure 4.1), where the difference in the RSS can reach 12 dB for about 20% of the data set. This is certainly due to the increase of multipath and reflections at this point. At point C the difference is also significant, but less noticeable than at

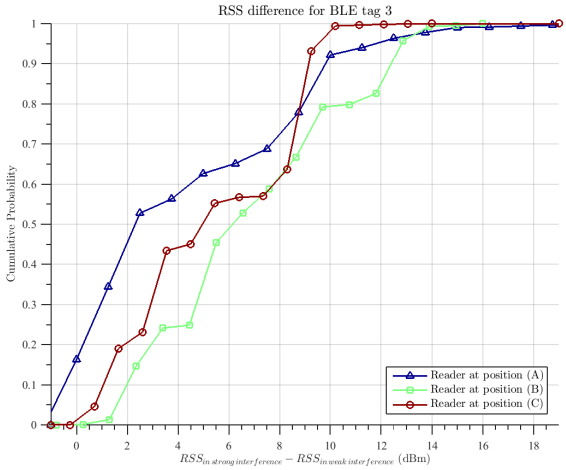


Figure 4.6: Difference between corridor points.

B, even though it is quite close to the end of the corridor. At point A the difference in RSS seems to be the normal fluctuation associated with shadowing.

Overall, based on the results presented in this section, it is possible to conclude that the environment has a significant impact on the fit of models and the translation of RSS into a distance. It was shown that for an office environment the best model to use was the ITU-R, while for the office corridor, the best fit was provided by the log distance model using the apparent power broadcast by the tags. All considered, the log distance model seems to be the one offering the best results and should be preferred for BLE ranging over the ITU-R model.

4.2.3 Implications for ranging and trilateration

In this thesis ranging refers to the act of translating an RSS measurement (or an average of several RSS measurements) into a distance. Trilateration refers to the process of finding the location resulting from the intersection of several ranges. Often this location is the result of a fit method, such as least squares.

In the field of indoor positioning, several applications can benefit from accurate path loss modeling, for example, such as the creation of probabilistic fingerprint databases. However, these models can also be used to obtain a distance instead of an expected RSS value. BLE is interesting for such an application since several manufacturers report the transmit power and not a manufacturer dependent indicator as in the case of WiFi. A distance is obtained by solving (4.2) and (2.9) with the values of the observed RSS.

Figure 4.7 shows the obtained distance from each of the models considered in the previous section in the closed office environment. The input to the model is an averaged RSS value with the last observed 2 seconds. It is clear from it that the several other tags broadcasting at the same time have a significant impact in the RMSE obtained for each of the models. With a single tag broadcasting, all the models achieve a sub meter

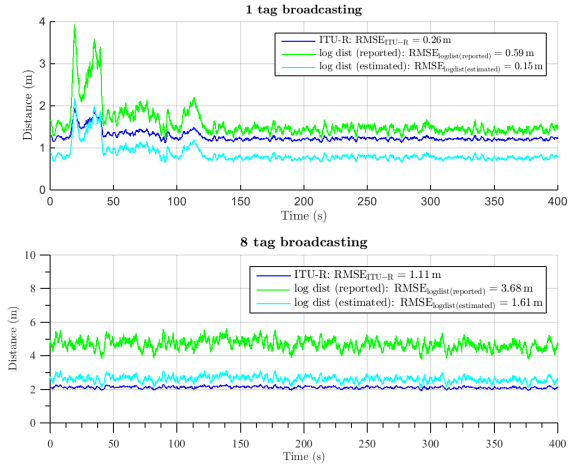


Figure 4.7: Ranging with BLE signal.

level accuracy, while the opposite is true when all 8 tags are broadcasting, increasing the RMSE significantly. Of attention is the degradation of the RMSE of the log distance model with the reported apparent power level. Its RMSE increases by more than 3 m while the RMSE for the other models increases, approximately, by one meter. This is in accordance with the values presented in Table 4.1, where the overall accuracy of the log distance model using the reported apparent power was the highest of the three. However, the ITU-R model is performing quite well considering the RMSE values in the same table, in particular when the 8 tags are broadcasting.

As expected, the impact of intra-system interference on ranging is significant and it shows the lack of accuracy such methods can have. Besides intra-system interference the lack of accuracy in ranging is also worse if other channel impairments are not mitigated in the path loss models. However, since ranging is a simple technique, this can be one easy way to get fast and coarse initial estimate on the location of the devices. Hence, if one would indeed like to use ranging based on RSS, it would be necessary to mitigate additional losses in the path loss models. Such feature would enable, as seen in Figure 4.8, a clear benefit in terms of accuracy, where for 8 simultaneous tags broadcasting, the ranging accuracy drops closer to the ones seen when only a single tag is broadcasting. However, mitigating such effects is not trivial and would require real time knowledge of the propagation conditions.

With ranging allowing for the determination of a distance to one of several tags, these distances can be put together in a trilateration problem to solve for the location of the BLE reader. In trilateration, the error will get amplified as the uncertainty grows with the inaccuracy of each range. To look at this problem, a simple setup was done in the UK where the BLE reader was placed in a corridor at locations A, B and C for 600 seconds at a time (see Figure 4.1). The reader's location was determined by solving for each tag the following nonlinear equation:

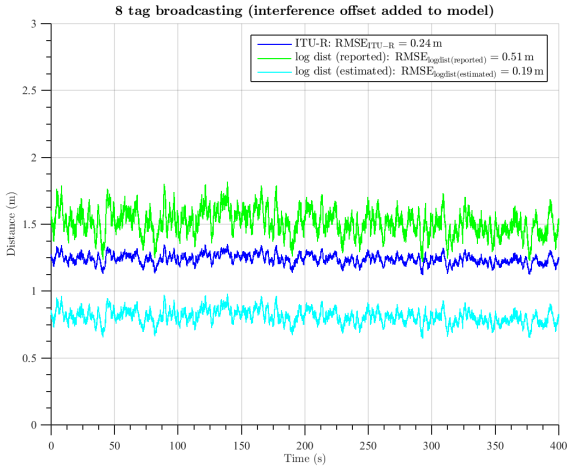


Figure 4.8: Mitigation of other tags interference.

$$\sqrt{(x_{\text{tag}}^{(i)} - \hat{x})^2 + (y_{\text{tag}}^{(i)} - \hat{y}) + (z_{\text{tag}}^{(i)} - \hat{z})} - L_{\text{tag}}^{(i)} = 0, \tag{4.5}$$

where $(x_{\text{tag}}^{(i)}, y_{\text{tag}}^{(i)}, z_{\text{tag}}^{(i)})$ are the known coordinates to the i-th tag, $(\hat{x}, \hat{y}, \hat{z})$ the unknown receiver position and $L_{\text{tag}}^{(i)}$ the distance to the i-th tag obtained through the path loss model.

Table 4.3 summarizes the RMSE of the receiver's location estimate at points A, B and C in a 2D (fixed height) and a 3D space with ranges derived from the log distance and ITU-R models. The overall accuracy is better for the 2D space as there is one less error component coming from the vertical axis (see right most column in Table 4.3). Despite that, the performance is similar for the estimates in 2D and 3D. Taking a look at the accuracy per model, it is possible to see that the log distance using the reported apparent power from the tags outperforms the other models.

All in all, calculating BLE ranges and solving the reader's location through trilateration seem to benefit most when the log distance model is used as the measurement's model. The addition of the apparent power in the BLE advertisements is also beneficial towards improving the overall performance of the positioning algorithm.

Table 4.3: RMSE values for 2D and 3D positioning in the office corridor at the UK.

	Model	$\text{RMSE}_\text{A}(m)$	RMSE_B (m)	RMSE_C (m)	$\text{Average}_{A,B,C}$
3D	ITU-R	1.83	2.17	1.31	1.77
	$\log \text{dist}_\text{reported}$	1.36	1.20	0.60	1.05
	$\log \text{dist}_\text{estimated}$	2.03	2.14	0.94	1.70
2D	ITU-R	1.68	2.05	1.11	1.61
	$\log \text{dist}_\text{reported}$	1.55	1.13	0.15	0.94
	$\log \text{dist}_\text{estimated}$	1.53	1.93	0.57	1.35

4.3 Discussion

The focus of this chapter was the contribution in [P3], where BLE intra-system interference is looked at empirically. The study in [P3] relied on two measurement campaigns, one executed in a small office room, while the other on a short section of a university corridor.

The results from the experiment carried out in the office room in Finland, showed that similar levels of performance for each model under consideration, whereas the results in the university corridor presented a better fit for the ITU-R model. In the first and second scenarios, the tags were oriented differently with respect to the receiver. In the office room trial, the tags were resting on a table while on the second trial they were glued to a wall on a higher plan than the receiver. This difference in placement and orientation certainly played a difference in the behavior of the signal, which contributed to the difference between results. The results in the office room were also more significantly attenuated by other environment elements and the multipath of the broadcasting tags themselves.

One other aspect, is that given the amount of tags, the probability of collision is still rather low. While the work in [P3] pointed out the nefarious contribution of intra-system interference, it also does so without looking at the physical level and in fact understand the amount of collisions that were indeed happening at that time.

While [P3] overlooks some of the physical channel phenomena, it discussed the benefit of quantifying the amount of intra-inference imposed by the environment. In [P3], for the office scenario under study, a compensation of -5 dBm in the signal allowed for an error reduction of up to 50%.

CHAPTER 5

Efficient positioning

This chapter focuses on the results from publications [P4, P5]. These publications look at the algorithmic layer, where measurements of multiple SoO are combined to provide an efficient positioning of a given user or device.

The main contributions in this chapter consist of:

- Theoretical discussion on the accuracy limitations for several SoO systems, including 3G and several WiFi systems;
- Analysis of results obtained from the simulator open sourced at [52, 53] and comparison against field measurements;
- Analysis on the improvement of the location performance by hybridizing Bluetooth and WiFi signals.

5.1 Background, state-of-the-art and related work

The term efficient positioning means that one tries to capitalize on the existing resources of the device, without causing a significant additional burden on it. Up until this chapter, the focus has been on identifying opportunities in the spectrum and propagation issues surrounding it. In this chapter, the focus falls on the usage of such opportunistic measurements and on the actual implementation and design of a positioning system based on them.

5.1.1 Model-based and model-free approaches

RSS exploitation is often categorized in two classes, a model-based and model-free approaches [34, 73].

In model-based approaches, the RSS is used to train the parameters of predefined propagation models, such as the one presented in equations (2.9) and (4.2). Furthermore, in a model-based approach, the RSS is translated into ranges and the estimation of the position determined through trilateration.

In model-free approaches, the RSS measurements are compared against a previously acquired database of RSS measurements. This database is known as a radio map, which contains the RSS observed for each point in space on a given environment. [34,73]. The work in [128] describes an approach to compress the fingerprint database using image compression techniques. The resulting database offers a smaller storage size and as a side effect it provides a significant improvement in the positioning performance.

5.1.2 Fingerprinting

Fingerprinting was initially introduced in [7] and has become the standard for indoor positioning services which build upon existing infrastructure [73]. Fingerprinting has no underlying requirement on the technology being measured, meaning it can be applied to any SoO, if it is possible to measure and map them to a physical location. Popular indoor positioning solutions rely on WiFi and natural occurring fields, such as the geomagnetic field [28, 33, 36, 45, 98, 102].

One of the major drawbacks of fingerprinting is that is requires two phases, commonly known as the training or learning phase and the online phase. In the training phase, distinct features at each location are collected and stored in a database, which later is used to compare received measurements against it.

Deterministic and probabilistic models

In deterministic models, the positioning problem is solved by acquiring information about the range between devices and solving for the unknowns. These ranges are the result of the observables made in the time, power or space domain. In a deterministic manner the essence of the problem is reduced to finding the set of arguments that minimizes the different between observations [34, 73].

In probabilistic models the positioning problem is solved by determining what is the most likely point where the user is located, through the means of a cost function [34,73].

Learning phase

The main goal of the learning phase is to build the learning or training database. The training database contains for each physical location a set of features observed at that location. The features can be any quantifiable quantity, such as light intensity, RSS from WiFi, Bluetooth, FM radio, geomagnetic fields, smell, temperature, pressure, among others. For the initial construction of such database, it is necessary to physically walk through the environment and make this one to one matching between local and world coordinates to a set of features.

Building the learning database

When building the learning database, the most fundamental requirement is to have a means of geo-referencing the measurements being acquired in the physical world. As common applications of fingerprinting are in indoor environments, it is impossible to rely on GNSS signals to provide us with an accurate coordinate in the global frame. Hence, it is mandatory to obtain coordinates in a local frame and afterwards translate

those to a global frame, if needed. One possibility to keep track of one's indoor location is to rely on IMU and reset them at known points to keep the measurement error low [115].

However, since in the end fingerprinting tends to rely on inaccurate and easily accessible measurements such as RSS, practical approaches are often favored when building the learning database. Nevertheless, if the operator, who is building the location database, is capable of understanding its location in the physical world, the construction of the database at each measurement point $\mathbf{P}$ consists of a measurement vector $\mathbf{M}$ defined as,

$$\mathbf{M} = [(\text{Addr}, \text{RSS})_1, (\text{Addr}, \text{RSS})_2, ..., (\text{Addr}, \text{RSS})_\text{N}], \tag{5.1}$$

which contains the RSS receive towards a given device identified by its MAC address, Addr_n.

Finally, the learning database is the collection of all measurement vectors defined as, $\mathbf{L}$,

$$\mathbf{L} = [(\mathbf{P}, \mathbf{M})_1, (\mathbf{P}, \mathbf{M})_2, ..., (\mathbf{P}, \mathbf{M})_\text{m}], \tag{5.2}$$

where $\mathbf{P}_i = [x_i, y_i, z_i]$ is the i-th point's coordinate and m the total number of measurement points. $\mathbf{P}_i$ is defined over a local reference frame with an origin point selected by the operator.

Online phase

The online phase consists of matching new observations with the ones stored in the training database. The new observations are provided by the user's equipment, which will need to have means of capturing the features of interest. For each observation reported by the user, a model-free network side algorithm will have to perform a database look-up, where it compares the incoming observation with each database entry that it deems relevant.

An important step in this phase is to decide on where the user is most likely to be at. It is quite likely that the lookup will provide several options of where the user is located, depending on the metrics used to rank the user's expected locations. A well-known method to acquire the most likely location of the user relies on the Gaussian likelihood presented in equation (5.3). For each $\mathbf{M}$ entry in the training database the likelihood of a user being at that given location is given by,

$$\mathcal{L}(\mathbf{P}_j, k) = \frac{1}{\sqrt{2\pi\sigma_k^2}} \exp\left(-\frac{\left(\mathbf{F}(k) - \mathbf{M}_j(\mathbf{P}_j, k)\right)^2}{2\sigma_k^2}\right), \tag{5.3}$$

where σ_k^2 is the variance associated with the fading phenomena and $\mathbf{P}_j$ a set of coordinates. $\mathbf{M}_j(\mathbf{P}_j, k)$ is the j^{th} fingerprint belonging to the k^{th} access node and $\mathbf{F}(k)$ is the reported measurement for each access node k.

After calculating the likelihood in equation (5.3) for each database entry, the cost function $\mathcal{J}$ is obtained by summing each individual logarithmic likelihood,

$$\mathcal{J}(\mathbf{P}_j) = \sum_{k=1}^{N} \log(\mathcal{L}(\mathbf{P}, k)). \tag{5.4}$$

The user's estimated location will then be the cost function's *arguments of the maxima*,

$$\hat{\mathbf{P}} = arg_{max_j}\{\mathcal{J}(\mathbf{P}_j)\}. \tag{5.5}$$

However, when it comes to select what is the user's final location, it is possible that there are many likely locations where to locate the user in. A simple approach is to pick the best X solutions and provide the user's location as the average of them, which is known as the k nearest neighbors algorithm [34].

Shortcomings

Overall the main benefit of fingerprinting is its simplicity and flexibility to build upon existing infrastructure. However, there are several challenges and disadvantages to tackle [3, 62, 66, 76, 94]. A known issue around it is that, due to the dynamics of the features it aims to capture, it is often necessary to re-acquire or continuously learn them. This has an implication on the cost of maintenance and operation of such system. Ideally, this learning ought to be kept automatic as new information is presented to the system. One approach, such as crowdsourcing of the data raises other security and privacy concerns, since it allows for the profile and tracking of individuals.

5.1.3 Related studies

The work in [85] presents a comparison between WiFi and RFID pathloss models. Moreover, it provides better insight on the fading and channel parameters for RFID signals, particularly in indoor scenario through an extensive field acquisition.

The work in [14] provides access to a fingerprinting database containing a multitude of signals, such as WiFi, Bluetooth, BLE as well as magnetic flux values. This contribution allows other researchers to compare their own algorithms and hybridization of signals against a common scenario.

The work in [91] discusses a similarity metric for a BLE-based fingerprinting. The metric under discussion in [91] is the Kendall Tau Correlation Coefficient and its performance is compared to the Euclidean distance method to determine the best fingerprints.

5.2 Fundamental limits on SoO positioning

When evaluating the performance of a positioning solution, it is important to understand how far it is from its nominal performance in a perfect evaluation scenario. Hence, the goal in [P5] was to use the CRLB to derive the minimum expected variance for time measurements coming from different SoO, such as wideband code division multiple access (WCDMA), 802.11b, 802.11g and 802.11ac. Hence, the study takes a look at the best any system could achieve with a combination of these systems, assuming that reliable TOA measurements are available for all of them.

In [P5] for each simulation point, timing measurements for each system, L_n, are determined to each n^{th}-emitter as,

$$\mathrm{L}_n = \frac{\mathrm{R}_n}{c} + \psi_n, \tag{5.6}$$

where R_n is the geometrical distance between the emitter and the receiver, cis the speed of light and ψ_n is the measurement error. R_n was determined in a 2D space to simplify the simulation problem.

The measurement error, ψ_n, was obtained from a normal distribution, with its variance set according to the CRLB and the expected carrier to noise ratio ($\mathcal{C}/N_0$) at the receiver's location.

The measurement's variance was drawn from the CRLB, which according to [72], is given as,

$$\mathrm{var}(\mathrm{L}_n) \geq \frac{1}{\frac{\xi}{\mathrm{N}_0/2}\overline{\mathrm{F}^2}} \Leftrightarrow \mathrm{var}(\mathrm{L}_n) \geq \frac{1}{\frac{C}{N_0/2\,\mathrm{T}}}\overline{\mathrm{F}^2}, \tag{5.7}$$

where, ξ is the signal energy, N_0 the noise spectral density, T the observation interval and $\overline{F^2}$ the mean square bandwidth of the signal, given as,

$$\overline{\mathrm{F}^2} = \frac{\int_{+\infty}^{-\infty} (2\pi \mathrm{f})^2 |\mathrm{S(f)}|^2 \mathrm{df}}{\int_{+\infty}^{-\infty} |\mathrm{S(f)}|^2 \mathrm{df}}, \tag{5.8}$$

where S(f) is the Fourier transform of $s(t)$.

The expected carrier to noise ratio is derived based on the ITU-R propagation model presented in equation (4.2).

Figure 5.1 shows the minimum achievable accuracy for WCDMA, 802.11b, 802.11g and 802.11ac measurements versus the signal's carrier to noise ratio ($\mathrm{C/N_0}$). Since WCDMA has the smallest bandwidth of all the signals under consideration, its variance is the highest of all.

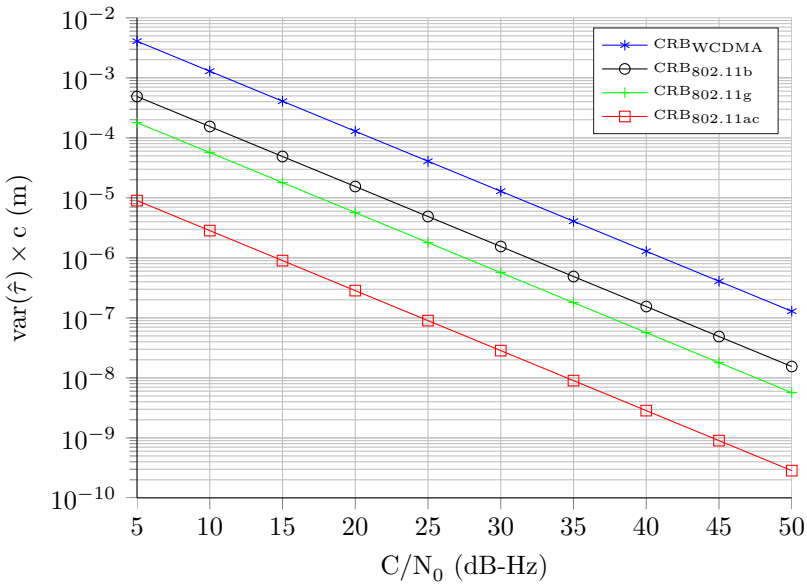


Figure 5.1: Crámer-Rao lower bounds for WCDMA and 802.11 ac/g/b.

5.2.1 Time-domain hybridization

The work in [P5] presented multiple scenarios where different combinations of WCDMA, 802.11b, 802.11g and 802.11ac were used together to obtain the user's estimated location. These allows to interpret the benefit of creating a CPS based on the observation of these signals and comparing the expected performance against positioning using solely measurements from a single technology, as shown in Figure 5.2. In Figure, WCDMA is one of the worst performing technologies since it is the one with the smallest bandwidth.

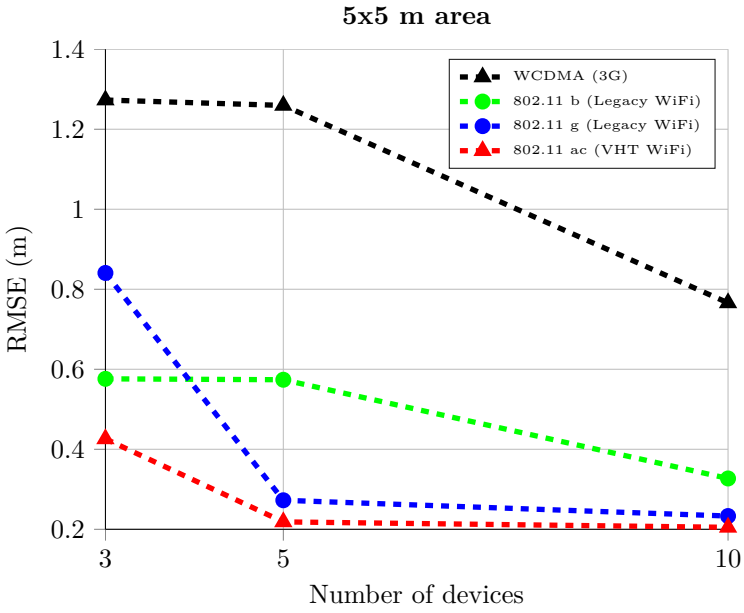


Figure 5.2: Positioning using a single technology of those identified in the legend.

Figures 5.3 - 5.4 show the benefit of observing WCDMA plus a multitude of observations from several 802.11 signals. More specifically, the thicker line with the circle marker represents the RMSE in meter obtained using only WCDMA, while the other lines represent the combination of WCDMA with a given amount of 802.11 signals. As an example, WCDMA + 3b means that N WCDMA emitters are available as well as 3 other 802.11b emitters. It is possible to conclude from these figures that assisting timing measurements of WCDMA with a few other technologies contributes to a significant performance improvement, especially between the 3 to 5 additional measurements. After that point, adding more measurements becomes redundant in the sense, that the contribution to an enhanced positioning performance is small.

In the end, when it comes to merge multiple SoO measurements and deciding on the design of a CPS which would be able to tackle all these measurements, the question boils down to which signals should it favor and to each point it should aim to track and rely on more measurements. While in [P5] all the measurements were ideal in the sense that they were not affected by strong channel impairments or other hardware non

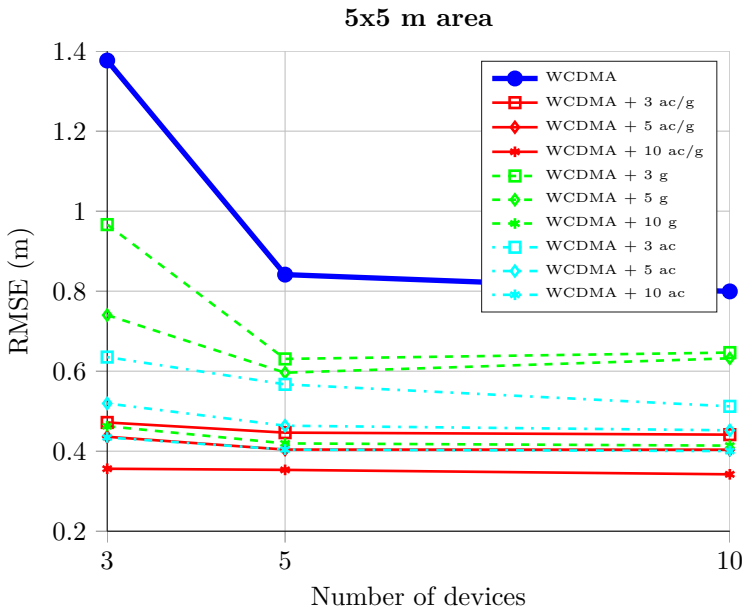


Figure 5.3: Positioning with multiple technologies: WCDMA, 802.11ac and 802.11g.

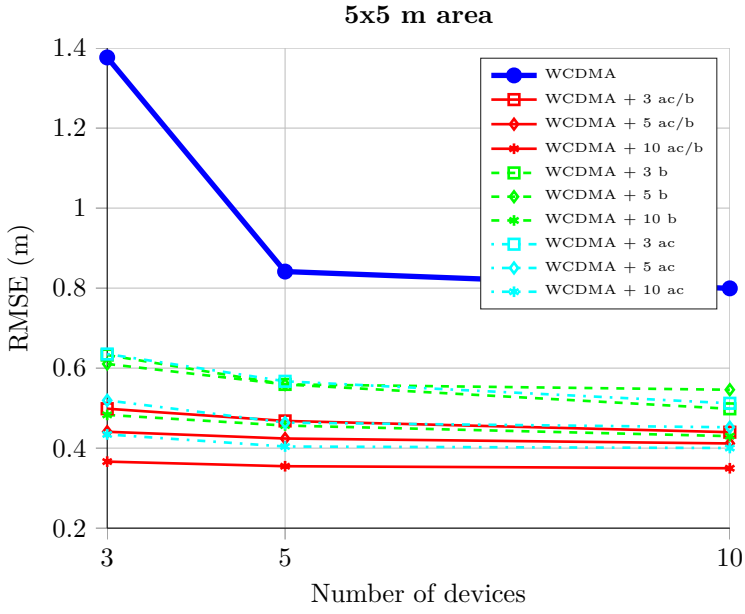


Figure 5.4: Positioning with multiple technologies: WCDMA, 802.11ac and 802.11b.

linearities, the fact is that in a real-case scenario these measurements would most likely show biases and measurement errors due to fading.

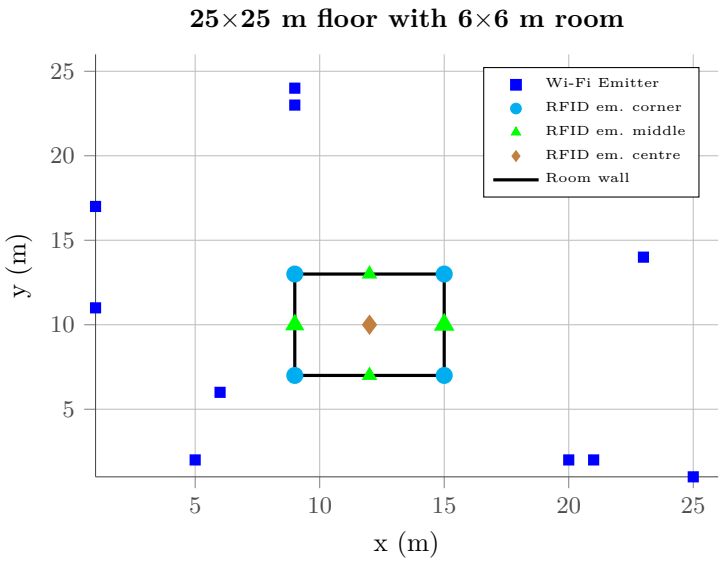


Figure 5.5: Simulated area and room.

5.2.2 Power-domain hybridization

This section tackles the hybridization of WiFi power measurements with measurements from BLE and RFID. This hybridization relies on fingerprinting to select the most probable location of the user according to a comparison between what the user's device is reporting and what has been acquired in the training phase.

Hybridization of WiFi and RFID measurements

In [P4] the discussion surrounded the hybridization of WiFi and RFID measurements through fingerprinting. This work relied on the simulation of these two signals and studies the contribution that observing RFID signals in two distinct scenarios, one where WiFi is widely available and another one where WiFi is scarcely available.

The main motivation behind this question was the fact that RFID signals have a limited coverage, since they rely on back-scattered signals, which means they have to transverse twice the same distance. The simulator developed and freely available in [P4] was modelled after the measurements taken in the studies [75, 85].

Simulated scenarios

The work sets out to follow [75] regarding the room dimensions and the placement of WiFi emitters on its exterior only. Figure 5.5 shows an example of a simulation scenario.

The simulation creates multiple sets of observations inside the room where, for each simulated random walk, RFID and WiFi measurements are generated according to their propagation model. Figures 5.6.A-B and 5.7.A-B both display accuracy curves. The curve makes the correspondence between the fraction of points whose average distance

error is smaller than that reported on the x-axis. The fractional value is obtained by calculating the number of points over which a location estimate is acquired P_n over the total amount of points defined in the random walk P_{total}. Since for some parts of the random walks some of the signals are unavailable, a location estimate for certain track points is not available, which results in some of the accuracy curves not reaching 1.

The RFID signals are particularly susceptible to multipath as they rely on back-scattered signals and directional antennas. Hence, it is impossible for a single reader to cover the entirety of the room, which means that for some parts of the room, there is simply no RFID coverage which causes the accuracy curves to converge at values below 1 as seen in Figures 5.6.A-B and 5.7.A-B. RFID's signal propagation is further discussed in [P4].

Despite the shortcomings of RFID, the motivation behind the work in [P4] was to identify if the observation of a limited signal, would indeed bring considerable benefits towards a WiFi-based positioning system. In this section we focus the presentation on a specific setup, where 4 RFID readers are placed in opposite sides of the room at varying WiFi access point densities.

The density of the Wi-Fi emitters was determined by numbers reported by several studies at university buildings in Finland, where reports show a density of 3-4 transmitters per 10 m^2 [118, 119]. Therefore, using this value, for the case of a high density Wi-Fi scenario, the environment is built with 24 Wi-Fi emitters, while 8 emitters were used for the medium to low density Wi-Fi scenario.

Figures 5.6.A-B showcase the error probability when the acquisition is done in a high density WiFi and in a low density WiFi scenario, respectively. From these two figures it is possible to conclude that even for a limited coverage signal such as RFID, its measurement provides a boost in performance when the amount of WiFi or other 2.4 GHz signals are present as well. At a ratio of 90%, the average error for the combined WiFi and RFID sees an improvement below 1m in Figure 5.6.A, while it is slightly over 3 m in Figure 5.6.B.

Experimental scenarios

From the same data set as [64], Figure 5.7.A and 5.7.B allow for a comparison with the simulation work depicted in Figure 5.6. Figure 5.7.A shows the accuracy curves for RFID, WiFi and RFID plus WiFi, where only one RFID emitter is placed in the middle section of the wall. Figure 5.7.B considers four RFID readers in the middle sections of the walls. In Figures 5.7.A-B, the WiFi only solution performs equally well in both situations. In Figure 5.7.A the presence of the RFID signal makes almost no difference in the overall performance. However, in Figure 5.7.B it is possible to see a performance improvement due to the presence of RFID. This is seen by the difference between the WiFi curve and the WiFi plus RFID curve, where the difference reaches over 1 m for low ratio values.

Hybridization of WiFi and BLE

In this last part, the focus is on the hybridization of WiFi and BLE signals. BLE signals are becoming more popular to connect small and inexpensive devices and have a role to aid positioning in indoor environments, as well as achieving the last shelf promotion of a

specific article or promotion. This makes these signals as another relevant measurement source to look for in terms of SoO and does pave the way for other 2.4 operating technologies in the same spectrum.

The data set in use for this study was collected via measurements at TUT were several BLE tags were deployed throughout the university corridors. From this data set it is interesting to understand what and if there is any relationship between RSS and the RMSE of a fingerprinting method. To understand this, Figure 5.8 draws the RSS against the RMSE of a ranked-based selection [92]. In this ranked-based selection, the top n most likely solutions are taken as the user's final location. It is possible to see from the Figure 5.8 that stronger RSS (less negative) do match with a better RMSE. In other words, it means that as the propagation fades, the RSS becomes more similar in the edges, making it more difficult to distinguish where the user is.

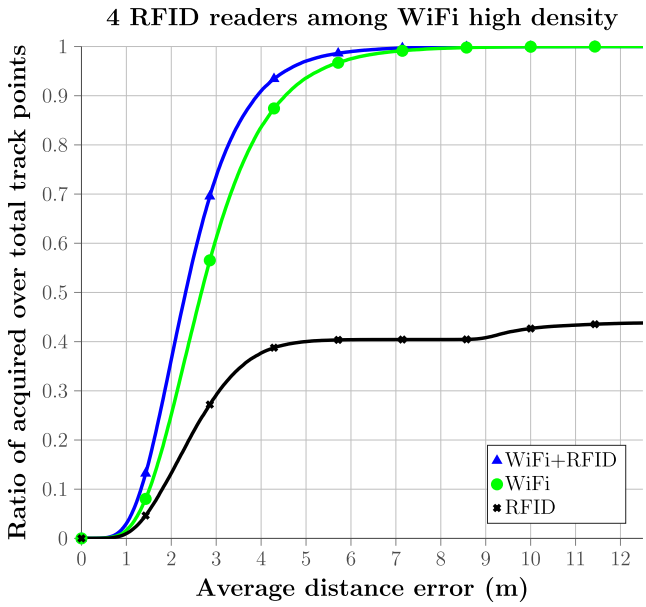
One of the major issues when merging data from several sources is the lack of uniformity in the actual reported value. A few preliminary studies reported in [63] have indicated that a cosine similarity approach can indeed lead to quite good results in comparison to a ranked based approach. The cosine similarity tackles this issue by assuming that two points are similar if the angles described between them are smaller. This is the reason why the metric fares quite well in comparison to the ranked based approach, as seen in Figure 5.10. Mathematically, the cosine similarity is given as,

$$\cos(\Theta) = \frac{\mathbf{A} \cdot \mathbf{B}}{||\mathbf{A}||||\mathbf{B}||}. \tag{5.9}$$

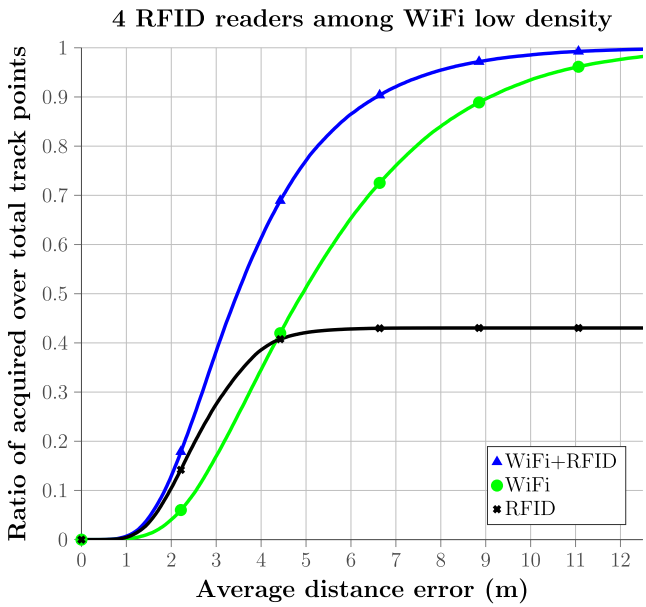
where Θ is the angle defined between the two vectors $\mathbf{A}$ and $\mathbf{B}$ of magnitude $||\mathbf{A}||$ and $||\mathbf{B}||$, respectively.

In equation (5.9) the similarity is applied to the set of heard RSS from the online phase against each set under the training database. Similar sets will have a similarity value closer to one, which means that the most likely location for the user to be in is the one where the cosine of the angle is one. This is identified by the star marked lined labeled sin weighted in Figure 5.9. Regarding the other CDFs in Figure 5.9, these consist of an hybrid approach as proposed in [64], considering BLE signals as another WiFi signals (in terms of fading variance) and the respective BLE and WiFi only measurement sets.

Figure 5.9 the user's location is derived as the average of the best 4 candidates, while on 5.10 the average is done over the top 10 candidates.

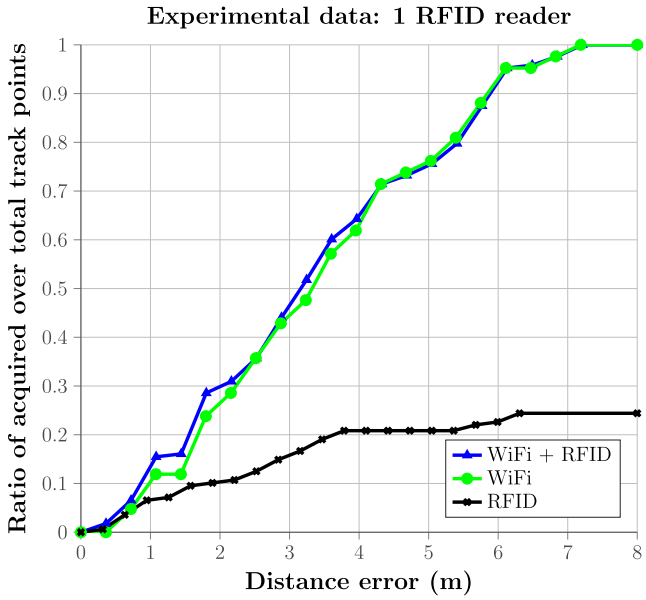


A



B

Figure 5.6: Accuracy curves with four RFID emitter in a high density WiFi (A) environment and in a low density WiFi (B) environment.



A

Figure 5.7: Experimental results using one RFID reader at a middle section of the wall (B) and four RFID readers (A).

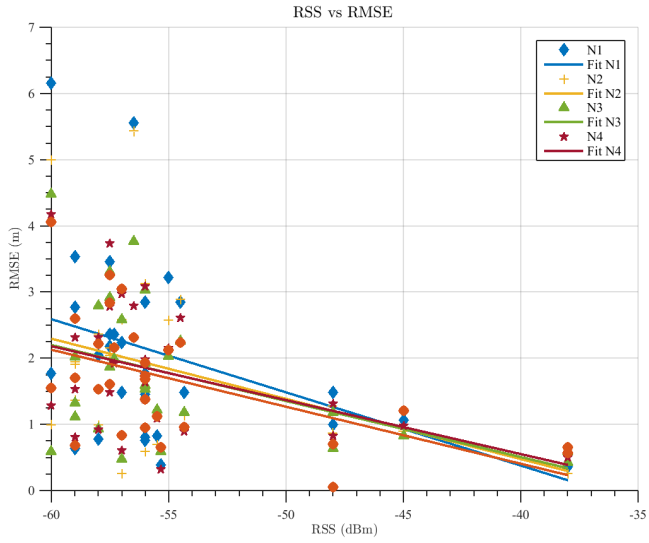


Figure 5.8: RMSE versus RSS.

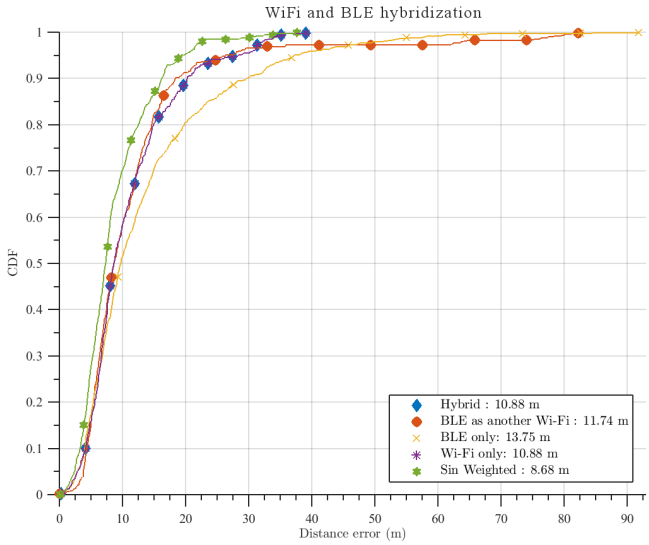


Figure 5.9: Cosine similarity.

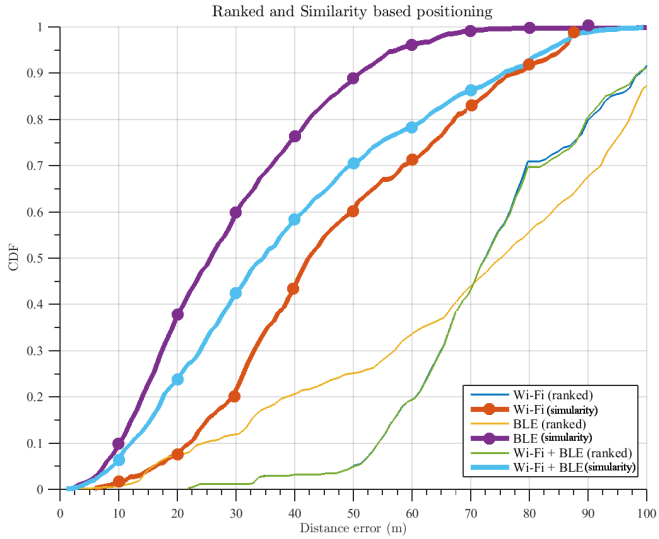


Figure 5.10: Cosine similarity versus ranked based approach.

5.3 Discussion

This chapter looked at contributions from [P4] and [P5], whose results relied on simulations built and made publicly available by the user [121]. To strengthen the simulation results, this chapter introduced results obtained from actual field measurements done in TUT, complementing the simulation results from [P4].

The work in [P5] was meant as purely theoretical and looked at the added benefit of observing multiple SoO. While it is well known that more independent and uncorrelated sources of measurements will enhance the system's performance, the motivation behind the study was to understand the performance gain assuming near-ideal scenarios. Despite the performance improvement in terms of using higher bandwidth signals, [P5] highlighted the small contributions that observing additional signals of that genre has on the overall performance. Hence, having a more diversified set of signals tends to offer the best trade-off between density and performance.

The work in [P4] looked at the benefit of measuring RFID signals in low and high density WiFi environments. The motivation was similar as in [P5], where the goal was to understand how worthy it was to observe certain signals. In the case of [P4], the RFID short propagation coverage was quite visible, which lead to poor in-room coverage. Acquisition of such weak signal was only relevant on an environment with low coverage of other SoO, such as WiFi.

The chapter ended with hybridization results of WiFi and BLE signals where there was a relationship between RMSE and RSS strength. It was seen that there was a proportional relationship between the device's proximity to the access point and the estimation error. The error was smaller when devices were closer to access points.

The hybridization results from WiFi and BLE presented a lower accuracy performance (see Figures 5.9) and 5.10), when compared to the results presented earlier in Section 5.2 (see Figures 5.7.A-B). A comparison between both cases showed that for the hybridization of WiFi and BLE, the average estimation error is approximately 10 m, while for the WiFi and RFID hybridization 90% of the points provided an error below 5m. Based on these values, the observation of an unique signal such as RFID was more valuable to the increase in accuracy than observing another signal with similar properties (BLE) as the main signal (WiFi).

CHAPTER 6

Opportunities for Internet of Things

This chapter presents the work in [P6], which contains a discussion about current IoT technologies and their place as current and future opportunities for CPS. The main contributions in this chapter consist of:

- Presentation of key physical and logical features of current and future IoT technologies.

6.1 Background, state-of-the-art and related work

Over the last years, there has been a trend to connect most of our daily devices and appliances to the Internet. There is clearly a trend in the consumer sector to allow the acquisition of any kind of metrics, wash cycle times, refrigerator temperature, automatic oven control, habit tracking, among many others. These are often systems that rely on simple radio protocols to achieve message passing in the most efficient way possible. Another drive and push for this kind of devices comes from the industry, where there is a trend to digitize time consuming processes, such as automated inventories, continuous tracking of environment parameters, automated lighting systems, among others. This chapter focus on the work in [P6].

6.1.1 Related work

In [100] the work focus on wireless sensor network and proposes a method based on the device's capabilities to obtain ranges and positioning groups of nodes taking part in certain message exchange. The work in [100] points out the benefits of positioning towards network management.

The work in [99] also in the realm of wireless sensor networks provides an overview of methods for positioning in GNSS-less networks. [99] proposes a method called local positioning system, which uses the nodes' capabilities for angle, range and motion estimation to position specific groups of nodes involved in particular message exchanges.

In [78] the authors focus on the LTE Machine type communications (LTE-M) and Narrow Band Internet of Things (NB-IoT) standards and their positioning capabilities. Another related study can be found in [77]. The focus in [77] is on indoor localization via improved RSS fingerprinting in generic IoT devices.

In [26] IoT positioning is looked at from the perspective of security, privacy and robustness of the localization technology. No positioning results are reported in there.

The work in [143] provides on overview of IoT positioning systems based on UWB solutions and their resilience towards spoofing attacks of their TOA measurements.

The work in [P6] provides, to the knowledge of the thesis author and co-authors, a comparative study between the positioning features of several IoT standards. Hence, it allows for interested parties to compare different technologies regarding key features for building positioning systems.

6.1.2 An overview of IoT technologies

The prospect of having so many connected devices means that there are many more opportunities to look out for in terms of SoO for positioning. Many of these opportunities are present in the 2.4 GHz band, but there are also others available at sub-GHZ and eventually at mmWave bands. Table 6.1 presents several IoT technologies with a focus on their signal characteristics.

The proposed approach to classify these technologies is seen in [P6] and consists of the following classes:

- licensed versus unlicensed bands: operation in a protected band, such as cellular bands;
- operating frequency bands: where each technology is matched to sub-GHz, GHz, or mmWave (with some technologies spreading over multiple ranges);
- protocols versus enablers: whether a technology is seen as a specific IoT communication protocol or a possible wireless positioning enabler;
- range: as Wireless Personal Area Network (WPAN), Local Area Network (WLAN) or Wide Area Network (WWAN);
- rate: as Low-Rate (LR) or High-Rate (HR);
- power: as Low-Power (LP) or High-Power (HP).

This classification makes several assumptions: in the range category, we consider WWAN for those protocols capable of delivering more than 10 km links, for rate we assume HR as those able to achieve an uplink above 10 Mbit/s and for power we assume LP all of those who can support at least non-routing devices on more than 2 years of battery.

Table 6.1: Summary of key physical layer parameters for several IoT protocols.

Technology	Frequency bands	Channel bandwidth (MHz)	Modulation type (UNB/NB/ SS/OFDM/UWB)
ANT+	GHz	1	NB
BLE mesh	GHz	1	NB
Dash7	sub-GHz	0.025, 0.200	NB
EC-GSM-IOT	sub-GHz	0.2	NB
EnOcean	sub-GHz	0.0625	NB
Ingenu	sub-GHz and GHz	1	SS
ISA101.11a	GHz	5	SS
LoRa	sub-GHz	0.125, 0.500	SS
LTE-M	sub-GHz and GHz	1.08, 1.4	OFDM
MiWi	sub-GHz and GHz	0.040, 0.250	NB
NB-IoT	sub-GHz and GHz	0.18	NB, OFDM
RFID	sub-GHz and GHz	0.2	NB
Sigfox	sub-GHz	0.2	UNB
Telensa	sub-GHz	0.1	NB
Thread	GHz	5	NB
Weightless-N	sub-GHz	0.2	UNB
Weightless-P	sub-GHz	0.0125	NB
Weightless-W	sub-GHz	5	SS
WirelessHART	GHz	0.25	SS
Wirepas	sub-GHz and GHz	0.126, 0.5	NB
WiSUN	sub-GHz and GHz	0.2 - 1.2	NB, SS and OFDM
ZigBee	sub-GHz and GHz	0.6, 1.2, 2	SS
ZigBee-NaN	sub-GHz	0.6, 1.2, 2	SS
Z-Wave	sub-GHz	0.2	NB

6.2 IoT as enabler for future positioning systems

One key aspect of a positioning system is that it will need to have a connection to an Internet backbone. This is required to pull assistance data for the positioning, such as the location of the infrastructure. It is also possible that the devices would be allowed to exchange this information among themselves, if they would have enough storage space to accommodate for that.

IoT technologies can become essential in this aspect as their main goal is to enable the connection and message passing among devices. Hence, besides being an interesting opportunity for future positioning systems, their unique system characteristics might also play a crucial role in terms of enabling such systems. These are not only physical layer characteristics, but also those belonging to higher OSI layers, such as:

Topology relates to message passing from one node to another and it dictates where the edge of the network is located, with two of the most common topologies being star and mesh. Star topologies are quite common in telecommunication technologies, where the access point or base station provide service to the other receivers. In a mesh topology, the receivers exchange messages between each other and the servicing device might change according to changes in the environment. From a positioning point of view, a mesh topology brings added value in terms of network reliability and extending the service coverage;

Range of an IoT system is important in the sense that it defines an upper bound of the positioning error, which cannot be larger than the communication range. For example, IoT systems with ranges of orders of meters are also expected to provide a meter-level positioning accuracy. It also has a relationship with the carrier frequency, as lower frequencies will allow for longer services ranges at the expense of power;

Positioning signaling or data exchange is the ability to use pilot signals or sequence of data packets to provide the location of nearby devices. This is important as it makes positioning an inherent aspect of the technology in use;

Roaming is the ability to provide continuity of service across multiple networks, owned or not by a single entity. As mobility is a keystone of most positioning applications, it is important to take note of this when looking at IoT systems. In this aspect, protocols such as Sigfox or Ingenu are at an advantage, as they operate similarly to cellular systems and offer service across multi continents. Despite that, even proprietary solutions start to provide open application interface specifications and open guest periods in the radio access, which facilitate the exchange of data across multiple vendors and technologies;

Network ownership raises security and privacy concerns, which are a strong requirement and must have in any current IoT system, especially as data access, transport and storage become more and more regulated by international and European bodies [42]. Several technologies allow the end user to build and operate its own network, but some technologies are aiming from the start to provide a bridge for data. Therefore, as these

manufactures keep their grasp on the network data, it is also more difficult to acquire information regarding the location of all serving points;

Power consumption is an important aspect for positioning applications. In the end, power consumption is a tradeoff between the latency an user expects to have its location updated and how much power it is willing to sacrifice. Despite that, network operations such as uplink and downlink data ought to be power efficient to keep consumption bounded by the number of location updates or attempts.

Several of these parameters are summarized on Table 6.2 in additional to other beneficial factors for positioning systems.

In terms of power consumption, it is typical for positioning services to require a powered infrastructure. However, there are indeed several industrial applications that would benefit from a fully battery-operated network or a network harvesting energy from surroundings (battery-less concept). Such applications are often found where an electricity network might not yet be present, e.g., construction sites, or for facility of service extension and maintainability.

In terms of positioning, most IoT systems are yet to offer specific signaling to support accurate measurements for this purpose. The Few of them have already raised interest in the academic field in terms of their positioning capabilities, as shown in the last column of Table 6.2. Most of these studies focus on RSS-based approaches, several of them relying on probabilistic methods such as fingerprinting. Few studies that focus on time-based and spatial-based approaches are mostly targeting current and future LTE derived signals, such as LTE-M and 5G, which are retaining some of LTE's positioning characteristics.

In addition, we have found that network-centric positioning solutions are being favored as opposed to device-centric ones. This mostly happens due to the limited resources at the end devices and gateways. However, this centralized architecture places an additional burden on the network capacity and latency as the number of devices grow and, for many of the systems under review will have difficulties accommodating real time location systems, especially due to the strict latency requirements of such systems. Integration with other higher capacity technologies, such as WiFi and 5G could solve some of this concern at the expense of per unit cost and power consumption. On the other hand, supporting positioning updates at sparse intervals ought to be feasible for many of them, which will certainly find its application in several niche markets, especially if the positioning system is supported fully by battery-powered networks over a span of multiple years.

6.3 Discussion

This chapter covered an overview of IoT technologies and their possible role in future CPS systems as they might function as additional SoO.

The discussion and presentation of current IoT technologies focused on key network parameters that considered important in a positioning context and in the signal detection realm. Overall, the biggest focus was placed on the physical and link layers with the discussion of parameters such as signal modulation, bandwidth and network topology.

Table 6.2: Summary of key technical specifications for several IoT protocols and IEEE 802.11∗ family protocols.

Technology	Network Topology	Network Type	Time-based [a] positioning	Power-based positioning	Space-based positioning	Achievable positioning accuracy	Most suitable domain	Accuracy studies
ANT+	mesh	LR/LP-WPAN	+,+++	+,+	++,++	Low	Power	
BLEmesh	mesh	LR/LP-WPAN	+,+++	+,+	++,+	Medium	Power	[34, 45, 86]
Dash7	star	LR/LP-WAN	+,+++	+,+	++,++	Low	Power or space	
EC-GSM-IOT	star	HR/LP-WAN	+,+++	+,+	++,++	Low	Power	
EnOcean	mesh	LR/LP-WAN	+,+++	+,+	++,++	Low	Power or space	
Ingenu /RPMA	star	LR/LP-WAN	+,+++	+,+	++,++	Medium	Power or space	
ISA101.11a	mesh	LR/LP-WPAN	+,+++	+,+	++,++	Medium	Power or space	
LoRa	star	LR/LP-WAN	+,++	+,+	++,++	Medium	Power	[47]
LTE-M	star	LR/LP-WAN	+,+	+,+	++,++	Medium	Time	[78]
MiWi	mesh	LR/LP-WAN	+,+++	+,+	++,++	Medium	Power	
NB-IoT	star	LP-WAN	+,+	+,+	++,++	Medium	Time	[78]
RFID	star	LP-WAN	+,+++	+,+	++,++	Medium	Power	[9, 64, 81, 89, 90]
Sigfox	star	LP-WAN	+,+++	+,+	++,++	Medium	Power	[69, 113]
Telensa	star	LP-WAN	+,+++	+,+	++,++	Low	Power or space	
Thread	mesh	LR-WPAN	+,+++	+,+	++,++	Medium	Power	
Weightless-N	star	LR/LP-WAN	+,+++	+,+	++,++	Medium	Power or space	
Weightless-P	star	LR/LP-WAN	+,+++	+,+	++,++	Low	Power or space	
Weightless-W	star	LR/LP-WAN	+,+++	+,+	++,++	Medium	Power	
WirelessHART	mesh	LR-WPAN	+,+++	+,+	++,++	Medium	Power	
Wirepas	mesh	HR-/LP-WLAN	+,+++	+,+	++,++	Medium	Power	
WiSUN	star,mesh	LR/LP-WPAN	+,+++	+,+	++,++	Medium	Power	
ZigBee/ZigBee-NaN	mesh	LR/LP-WPAN	+,+++	+,+	++,++	Medium	Power	[29, 39, 48, 101]
Z-Wave	mesh	LR/LP-WPAN	+,+++	+,+	++,++	Medium	Power or space	

[a] (+, +) : low impact, (++, ++) : medium, (+++, +++) : high impact

A major shortcoming in the study was the lack of presentation regarding the protocol level of each technology, which would have repercussions on how technologies operate in crowded and congested radio environments and their ability to perform message passing efficiently (capacity).

Overall, this chapter pointed out the fact that network-based positioning will most likely be a key aspect of future IoT-based positioning solutions. This was seen as a repercussion of the digitization of several industrial processes, where network ownership and data privacy are critical operational aspects. In such cases, future IoT networks can double as a communication infrastructure and offer positioning services. The role of power-based solutions for deriving the location of certain industrial assets was seen as valuable, as it imposes marginal impacts on the cost of the system when compared with other solutions based on time and spatial solutions. It was also observed that most IoT technologies are not offering any positioning specific signaling.

Based on this chapter and [P6], despite the difficulty in understanding all the local radio phenomena, RSS based positioning will nevertheless offer a cheap alternative for coarse based positioning. Other technologies, in the realm of time and space will cover higher accuracy demands, at the expense of battery consumption and higher unit cost.

CHAPTER 7

Conclusions

Signals of opportunity for positioning are those signals whose initial purpose was meant for other tasks, such as communications and data exchange. This thesis covered the concept of SoO and presented several studies surrounding this thematic, with a special attention in the indoor positioning field.

This chapter serves as a compilation of what was presented in the previous chapters and the main contributions provided by the studies under the scope of this thesis. Furthermore, this section ends with a discussion and ideas for future enhancement and improvement in the field of SoO for positioning.

7.1 Summary

The initial chapters, chapter 1 and 2, provided an overview of the whole thesis and the theoretical background approach for publications [P1–P6]. These first chapters defined the concept of SoO for positioning and provided several examples of commonly used signals and key physical layer parameters which serves as a means for identification in the later chapter 3. Chapter 2 also provided a classification of positioning techniques in the algorithmic layer in three distinct domains, power, space and time. The contributions on this thesis provided a discussion of several sets of results from the power domain.

Chapter 3 and publications [P1, P2] focused on the identification of SoO through their unique cyclostationarity features imposed by their physical layer representations. Section 3.1 provided a quick overview of several signal detection frameworks in signal processing, delving further in the realm of cyclostationarity. The cyclostationarity framework was the one chosen to identify two types of physical signal modulations, CDMA and OFDM. These two modulations were chosen as they cover several common signals available throughout most indoor and outdoor scenarios, such as Bluetooth and WiFi. Section 3.2 discussed the detection of CDMA and OFDM signals in a signal mixture. The work in [P1] contributed with a set of results confirming the possibility to apply the method later described in [P2] to distinguish CDMA and OFDM, as well as performing the detection at sub-Nyquist rates. Section 3.3 and publication [P2] described in further detail an algorithm to perform the detection of CDMA and

OFDM signals in a signal mixture and the role such algorithms could take in future CPS receivers.

Chapter 4 and publication [P3] looked at channel impairments problems with an intra-system interference case study presented for BLE systems. Section 4.1 laid the foundation for [P3], presenting key concepts in terms of radio propagation and channel impairment phenomena, in particular fading. Section 4.2 looked at in the intra-system phenomena and its effect on translating RSS into a range for a BLE system. The work in [P3] showed that such translation is mostly inaccurate and susceptible to several channel phenomena, like intra-system interference in the case of BLE. This phenomena, was seen to be visible in a small-scale experiment and to mitigate it, the work in [P3] suggested compensating the channel phenomena by understanding its contribution towards the degradation of the signal quality and applying it to the signal model. The conclusions in [P3] showed that such mitigation improve the quality of the ranges calculated based on the RSS information as well as sharing pre-calibrated measurements of the expected signal loss.

Chapter 5 and publications [P4, P5] focused at a theoretical and practical level on the benefits of acquiring multiple SoO. Section 5.1 provided an overview on popular positioning techniques, with interest placed in the fingerprinting method. Section 5.2 reviewed the results from [P4, P5]. The work in [P5] showed that while acquiring more independent sources of information leads towards a better accuracy, the accuracy trade-off in doing so is smaller if the measurement quality is equally good among these sources. Hence, the study in [P5] demonstrated that a CPS will benefit from acquiring at least a higher accuracy signal (higher bandwidth) in regions where lower accuracy (smaller bandwidth) signals proliferate. The work in [P4] provided an open source simulator to generate indoor scenarios for RFID and WiFi signals. The simulator allows the user to create room distributed over a pre-defined area with different degrees of WiFi density. The placement of RFID signals was contained to the room. The study showed that in the simulation and experimental based results, the observation of RFID signals only offered an accuracy gain when the density of WiFi signals was low.

Finally, chapter 6 and [P6] looked at the current technology landscape in terms of IoT technologies and discussed their fit towards the design of CPS. Section 6.1 identified several IoT technologies and their key physical aspects, as previously done for other SoO. Section 6.2 discussed several link layer parameters that were seen needed and relevant for IoT technologies aiming to offer the backbone for a positioning service. The IoT technologies discussed throughout chapter 6 were classified and placed in a comparison table. The aim of such table is to aid the decision making of system designers when picking a technology on which to build future CPS. Based on the observations of chapter 6 and [P6], IoT positioning systems will most likely tend to rely on inexpensive measurement layer solutions, such as those from the power domain. This domain is the one that will allow for the least impact on cost and battery life, as it will be an inherent functional parameter of the network. Whereas time and space solutions will provide enhanced positioning accuracy, the use case will in the end determine the most suitable domain and algorithms to use.

7.2 Discussion and further development

A future fully functional CPS will build on the understanding of its surrounding to capture and decode the necessary SoO to meet the necessary service levels that are required by its users. These requirements might change according to needs, requiring the adaptation of the radio interfaces for acquiring specific segments of the spectrum. Hence, understanding and characterizing the available SoO is important for such receivers and has been one of the main contributions of this thesis. This thesis has also contributed with valuable inputs regarding the selection of SoO and which ones to favor in terms of accuracy expectations.

The main challenges in terms of a CPS will be the channel phenomena affecting sections of the spectrum, which will cause simple solutions to malfunction. This is the case of power-based measurements, which will suffer greatly with the introduction of more and more radio interference, either from their own system or other systems. This phenomenon has been highlighted in this thesis, where mitigation at the signal model is discussed. Nevertheless, mitigation alone will not suffice, and better radio discipline will need to be looked after, especially as the IoT trend brings forward a massive number of connected devices.

As IoT increases the changes for future SoO signals, it also becomes clear that some of these signals could be even more useful if a global and distributed database could serve as the basis for future CPS. Having a public, distributed and regulated database with the location of multiple SoO's access points, would lead to a better quality of service and seamless localization throughout any environment.

In terms of quality of service for future CPS, RSS will remain as a relevant source of information, especially due to its low cost and small footprint in terms of resource utilization, but a rise of angle and timing approaches will become more common place as technology advances. Future cellular networks like 5G are looking at combination of angle and time-based methods to offer positioning services to its subscribers.

Nevertheless, while there are clear paths with respect to future trends in the accuracy domain, such as moving to higher accuracy domains as angle and time, the focus on minimizing the resource utilization will remain. In terms of resources, such as RAM and CPU, future devices will continue to see an upgrade as the silicon cost drops down, however in terms of battery, the utilization of the radio will remain a challenge. When to scan and how often to scan are costly actions that deplete the device's battery. Future advances in areas such as wake on radio and energy harvesting will allow for better energy preservation and management.

In a nutshell, this thesis has contributed with novel means of identifying SoO based on their physical layers characteristics as well as based on reduced observation of their spectrum and time properties. Furthermore, this thesis has contributed with a suite of tests regarding the use of SoO in indoor environments, based on simulations as well as on actual experimentation. This thesis has also contributed with a discussion surrounding future SoO (IoT technologies) and the choices that should be weighted when picking certain technologies towards a positioning context. Overall, the joint knowledge of this thesis aims to help the design of future positioning systems, CPS, built with a purpose of making the correct signal acquisition choices to meet the accuracy requirements while preserving the system's resources.

References

[1] A. A. Adebomehin and S. D. Walker, "Ultra-wideband signals for high-resolution cognitive positioning techniques in 5G wireless," in *2016 IEEE 37th Sarnoff Symposium*. IEEE, Sep. 2016, pp. 1–2.

[2] F. E. W. Alan N. Steinberg, Christopher L. Bowman, "Revisions to the jdl data fusion model," *Proc. SPIE*, vol. 3719, pp. 3719 – 3719 – 12, 1999.

[3] N. Alsindi, Z. Chaloupka, N. Alkhanbashi, and J. Aweya, "An empirical evaluation of a probabilistic RF signature for WLAN location fingerprinting," *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 3257–3268, 2014.

[4] A.R. Jimenez, F. Zampella, F. Seco, a.R. Jimenez, F. Zampella, F. Seco, A.R. Jimenez, F. Zampella, F. Seco, a.R. Jimenez, F. Zampella, and F. Seco, "Light-matching: A new signal of opportunity for pedestrian indoor navigation," *Int. Conf. Indoor Position. Indoor Navig.*, pp. 1–10, Oct. 2013.

[5] M. A. Aziz and C. T. Allen, "Experimental Results of a Differential Angle-of-Arrival Based 2D Localization Method Using Signals of Opportunity," *International Journal of Navigation and Observation*, vol. 2018, pp. 1–6, Mar. 2018.

[6] C.-I. Badoi, N. Prasad, V. Croitoru, and R. Prasad, "5G Based on Cognitive Radio," *Wireless Personal Communications*, vol. 57, no. 3, pp. 441–464, Jul. 2010.

[7] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *INFOCOM 2000*, vol. 00, no. c, 2000.

[8] A. Baniukevic, C. S. Jensen, and H. Lu, "Hybrid Indoor Positioning with Wi-Fi and Bluetooth: Architecture and Performance," in *2013 IEEE 14th Int. Conf. Mob. Data Manag.*, vol. 1. IEEE, Jun. 2013, pp. 207–216.

[9] M. R. Basheer and S. Jagannathan, "Localization of RFID Tags Using Stochastic Tunneling," *IEEE Transactions on Mobile Computing*, vol. 12, no. 6, pp. 1225–1235, Jun. 2013.

[10] A. Basiri, E. S. Lohan, T. Moore, A. Winstanley, P. Peltola, C. Hill, P. Amirian, and P. F. e Silva, "Indoor location based services challenges, requirements and usability of current solutions," *Computer Science Review*, vol. 24, pp. 1 – 12, 2017.

[11] A. Basiri, E. S. Lohan, P. Peltola, C. Hill, and T. Moore, "Overview of positioning technologies from fitness-to-purpose point of view," in *International Conference on Localization and GNSS 2014 (ICL-GNSS 2014)*. IEEE, Jun. 2014, pp. 1–7.

[12] A. Basiri, P. Peltola, P. Figueiredo e Silva, E. S. Lohan, T. Moore, and C. Hill, "Indoor positioning technology assessment using analytic hierarchy process for pedestrian navigation services," in *2015 International Conference on Location and GNSS (ICL-GNSS)*. IEEE, Jun. 2015, pp. 1–6.

[13] Bluetooth SIG Inc, "Bluetooth Technology," 2016. [Online]. Available: https://www.bluetooth.com/specifications/bluetooth-core-specificationhttps://www.bluetooth.com

[14] S. Bozkurt, A. Yazici, S. Gunal, U. Yayan, and F. Inan, "A novel multi-sensor and multi-topological database for indoor positioning on fingerprint techniques," in *2015 International Symposium on Innovations in Intelligent SysTems and Applications (INISTA)*. IEEE, Sep. 2015, pp. 1–7.

[15] O. Carhacioglu, P. Zand, and M. Nabi, "Time-domain cooperative coexistence of BLE and IEEE 802.15.4 networks," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, Oct. 2017, pp. 1–7.

[16] F. Caron, E. Duflos, D. Pomorski, and P. Vanheeghe, "GPS/IMU data fusion using multisensor Kalman filtering: introduction of contextual aspects," *Information Fusion*, vol. 7, no. 2, pp. 221–230, Jun. 2006.

[17] F. F. Caron, M. Davy, E. Duflos, and P. Vanheeghe, "Particle filtering for multisensor data fusion with switching observation models: Application to land vehicle positioning," *Signal Processing, IEEE*, vol. 55, no. 6, pp. 2703–2719, Jun. 2007.

[18] H. Celebi and H. Arslan, "Utilization of location information in cognitive wireless networks," *IEEE Wireless Communications*, no. August, pp. 6–13, 2007.

[19] H. Celebi and I. Guvenc, "Cognitive-radio Systems for Spectrum, Location, and Environmental Awareness," *IEEE Antennas and Propagation Magazine*, vol. 52, no. 4, pp. 41–61, 2010.

[20] H. Celebi, "Location awareness in cognitive radio networks," Ph.D. dissertation, University of South Florida, 2008.

[21] H. Celebi and H. Arslan, "Adaptive Positioning Systems for Cognitive Radios," in *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*. Ieee, Apr. 2007, pp. 78–84.

[22] H. Celebi and H. Arslan, "Enabling location and environment awareness in cognitive radios," *Computer Communications*, vol. 31, no. 6, pp. 1114 – 1125, 2008, advanced Location-Based Services.

[23] H. Celebi, H. Arslan, H. A. Hasari Celebi, H. Celebi, H. Arslan, H. A. Hasari Celebi, H. Celebi, H. Arslan, and H. A. Hasari Celebi, "Cognitive Positioning Systems," *IEEE Transactions on Wireless Communications*, vol. 6, no. 12, pp. 4475–4483, Dec. 2007.

[24] Y. T. Chan and K. C. Ho, "A simple and efficient estimator for hyperbolic location," *IEEE Transactions on Signal Processing*, vol. 42, no. 8, 1994.

[25] C. Chen, Y. Chen, Y. Han, H.-Q. Lai, and K. J. R. Liu, "Achieving Centimeter Accuracy Indoor Localization on WiFi Platforms: A Frequency Hopping Approach," *IEEE Internet of Things Journal*, pp. 1–1, 2016.

[26] L. Chen, S. Thombre, K. Jarvinen, E. S. Lohan, A. Alen-Savikko, H. Leppakoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, "Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[27] Y. Chen, "Improved energy detector for random signals in gaussian noise," *IEEE Transactions on Wireless Communications*, vol. 9, no. 2, pp. 558–563, Feb. 2010.

[28] A. D. Cheok and L. Yue, "A Novel Light-Sensor-Based Information Transmission System for Indoor Positioning and Navigation," *IEEE Trans. Instrum. Meas.*, vol. 60, no. 1, pp. 290–299, Jan. 2011.

[29] J. Cheon, H. Hwang, D. Kim, and Y. J. Y, "IEEE 802.15.4 ZigBee-Based Time-of-Arrival Estimation for Wireless Sensor Networks," *Sensors*, vol. 16, no. 2, 2016.

[30] T. Chu, N. Guo, S. Backén, and D. Akos, "Monocular camera/IMU/GNSS integration for ground vehicle navigation in challenging GNSS environments." *Sensors (Basel, Switzerland)*, vol. 12, no. 3, pp. 3162–85, Jan. 2012.

[31] E. L. Costa, "Detection and Classification of Cyclostationary Signals," Ph.D. dissertation, Naval Postgraduate School, 1996.

[32] O. Daniel, N. G. Ferrara, and P. M. Figueiredo e Silva, "Understanding the GNSS Signal Model," in *Multi-Technology Positioning*. Springer, Cham, 2017.

[33] D. Dardari, P. Closas, and P. M. Djuri, "Indoor Tracking: Theory, Methods,and Technologies," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 4, pp. 1263–1278, 2015.

[34] P. Davidson and R. Piché, "A Survey of Selected Indoor Positioning Methods for Smartphones," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 1347–1370, 2017.

[35] A. Dempster, "Dilution of precision in angle-of-arrival positioning systems," *Electronics Letters*, vol. 42, no. 5, p. 291, 2006.

[36] Z. Deng, Y. Yu, X. Yuan, N. Wan, and L. Yang, "Situation and development tendency of indoor positioning," *China Communications*, vol. 10, no. March, pp. 42–55, Mar. 2013.

[37] M. Di Felice, C. Bocanegra, and K. R. Chowdhury, "WI-LO: Wireless indoor localization through multi-source radio fingerprinting," in *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*. IEEE, Jan. 2018, pp. 305–311.

[38] F. F. Digham, M.-S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE International Conference on Communications*, vol. 5, pp. 3575–3579, 2003.

[39] Z. Dong, C. Mengjiao, and L. Wenjuan, "Implementation of indoor fingerprint positioning based on ZigBee," in *2017 29th Chinese Control And Decision Conference (CCDC)*, May 2017, pp. 2654–2659.

[40] Eliko, "Eliko." [Online]. Available: https://www.eliko.ee/

[41] Estimote, "Indoor location with bluetooth beacons and mesh," 2017.

[42] European Union, "EUR-Lex GPDR." [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX{%}3A32016R0679

[43] R. Exel, "Carrier-based ranging in IEEE 802.11 wireless local area networks," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, Apr. 2013, pp. 1073–1078.

[44] G. Falco, M. Nicola, and M. Pini, "Positioning Based on Tightly Coupled Multiple Sensors: A Practical Implementation and Experimental Assessment," *IEEE Access*, vol. 6, pp. 13 101–13 116, 2018.

[45] R. Faragher and R. Harle, "Location Fingerprinting with Bluetooth Low Energy Beacons," *IEEE Journal on Selected Areas in Communications*, vol. PP, no. 99, pp. 1–1, 2015.

[46] R. Faragher, R. Harle, and R. Faragher, "An Analysis of the Accuracy of Bluetooth Low Energy for Indoor Positioning Applications," *ION GNSS+*, pp. 201–210, 2014.

[47] B. C. Fargas and M. N. Petersen, "GPS-free geolocation using LoRa in low-power WANs," in *2017 Global Internet of Things Summit (GIoTS)*. IEEE, Jun. 2017, pp. 1–6.

[48] S. Fernández, D. Gualda, J. C. García, J. J. García, J. Ureña, and R. Gutiérrez, "Indoor location system based on zigbee devices and metric description graphs," in *2011 IEEE 7th International Symposium on Intelligent Signal Processing*, Sept 2011, pp. 1–5.

[49] N. G. Ferrara, O. Daniel, and P. M. Figueiredo e Silva, "MULTI-GNSS: facts and issues," in *Multi-Technology Positioning*. Springer, Cham, 2017.

[50] M. Ficco, F. Palmieri, and A. Castiglione, "Hybrid indoor and outdoor location services for new generation mobile terminals," *Personal and Ubiquitous Computing*, vol. 18, no. 2, pp. 271–285, Mar. 2013.

[51] P. M. Figueiredo, "Cycle Slip Detection and Correction Using Low Cost IMU Measurements," Master's thesis, Instituto Superior Técnico, University of Lisbon, 2012.

[52] P. Figueiredo e Silva, "silva / MULTI-POS WP 4.2 - Bitbucket." [Online]. Available: https://bitbucket.org/silva/multi-pos-wp-4.2/src

[53] P. Figueiredo e Silva, "silva / Open Access Bitbucket." [Online]. Available: https://bitbucket.org/silva/open-access/src

[54] P. M. Figueiredo e Silva and N. G. Ferrara, "Mapping the radio world to find us," in *Multi-Technology Positioning*. Springer, Cham, 2017.

[55] T. Fusco, L. Izzo, A. Napolitano, and M. Tanda, "On the second-order cyclostationarity properties of long-code DS-SS signals," *IEEE Transactions on Communications*, vol. 54, no. 10, pp. 1741–1746, Oct. 2006.

[56] W. A. Gardner, "Exploitation of spectral redundancy in cyclostationary signals," *Signal Processing Magazine, IEEE*, 1991.

[57] W. A. Gardner, A. Napolitano, and L. Paura, "Cyclostationarity: Half a Century of Research," *Signal Processing*, vol. 86, no. 4, pp. 639–697, Apr. 2006.

[58] C. Gentile, A. Braga, and A. Kik, "A Comprehensive Evaluation of Joint Range and Angle Estimation in Indoor Ultrawideband Location Systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2008, no. 1, p. 248509, 2008.

[59] E. Geraniotis and M. Pursley, "Error Probabilities for Slow-Frequency-Hopped Spread-Spectrum Multiple-Access Communications Over Fading Channels," *IEEE Transactions on Communications*, vol. 30, no. 5, pp. 996–1009, 1982.

[60] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: requirements, challenges and design trade-offs," *Communications Magazine, IEEE*, no. April, pp. 32–39, 2008.

[61] D. Gingras, "An Overview of Positioning and Data Fusion Techniques Applied to Land Vehicle Navigation Systems," 2009.

[62] F. Gustafsson and F. Gunnarsson, "Mobile positioning using wireless networks: Possibilities and fundamental limitations based on available wireless network measurements," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 41–53, 2005.

[63] S. Han, C. Zhao, W. Meng, and C. Li, "Cosine similarity based fingerprinting algorithm in WLAN indoor positioning against device diversity," *Communications (ICC), 2015 IEEE International Conference on*, vol. 2015-Septe, no. 61401119, pp. 2710–2714, Jun. 2015.

[64] M. Hasani, J. Talvitie, L. Sydanheimo, E.-S. Lohan, and L. Ukkonen, "Hybrid WLAN-RFID Indoor Localization Solution Utilizing Textile Tag," *IEEE Antennas and Wireless Propagation Letters*, vol. PP, no. 99, pp. 1–1, 2015.

[65] S. Haykin, D. J. Thomson, J. H. Reed, E. Axell, G. Leus, E. G. Larsson, and H. V. Poor, "Spectrum sensing for cognitive radio," *IEEE Signal Processing*, no. MAY 2012, pp. 101–116, 2009.

[66] V. Honkavirta, T. Perala, S. Ali-Loytty, and R. Piche, "A comparative survey of WLAN location fingerprinting methods," in *2009 6th Workshop on Positioning, Navigation and Communication*, vol. 2009. IEEE, Mar. 2009, pp. 243–251.

[67] N. Hoven, R. Tandra, and A. Sahai, "Some fundamental limits on cognitive radio," in *Allerton Conference in Commununication, Control, and Computing*, Monticello, 2004.

[68] ITU-R, "Recommendation ITU-R P.1238-7," 2012.

[69] T. Janssen, M. Weyn, and R. Berkvens, "Localization in Low Power Wide Area Networks Using Wi-Fi Fingerprints," *Applied Sciences*, vol. 7, no. 9, p. 936, Sep. 2017.

[70] Jordi Conesa, Antoni Pérez-Navarro, Joaquin Torres-Sospedra, and Raul Montoliu, Eds., *Geographical And Fingerprinting Data For Positioning And Navigation Systems: Challenges, Experiences and Technology Roadmap*, 1st ed. ELSEVIER ACADEMIC PRESS, 2018.

[71] H. Karvonen, K. Mikhaylov, M. Hämäläinen, J. Iinatti, and C. Pomalaza-ráez, "Interference of Wireless Technologies on BLE Based WBANs in Hospital Scenarios," *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 0–4, Oct. 2017.

[72] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1993.

[73] A. Khalajmehrabadi, N. Gatsis, and D. Akopian, "Modern wlan fingerprinting indoor positioning methods and deployment challenges," *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, pp. 1974–2002, thirdquarter 2017.

[74] J. Khalife, K. Shamaei, and Z. M. Kassas, "Navigation With Cellular CDMA Signals-Part I: Signal Modeling and Software-Defined Receiver Design," *IEEE Transactions on Signal Processing*, vol. 66, no. 8, pp. 2191–2203, Apr. 2018.

[75] K. Koski, E. Koski, T. Bjorninen, A. A. Babar, L. Ukkonen, L. Sydanheimo, and Y. Rahmat-Samii, "Practical read range evaluation of wearable embroidered UHF RFID tag," in *Proceedings of the 2012 IEEE International Symposium on Antennas and Propagation*. IEEE, Jul. 2012, pp. 1–2.

[76] C. Laoudias, C. G. Panayiotou, and P. Kemppi, "On the RBF-based Positioning using WLAN Signal Strength Fingerprints," *Small*, pp. 93–98, 2010.

[77] K. Lin, M. Chen, J. Deng, M. M. Hassan, and G. Fortino, "Enhanced Fingerprinting and Trajectory Prediction for IoT Localization in Smart Buildings," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1294–1307, Jul. 2016.

[78] X. Lin, J. Bergman, F. Gunnarsson, O. Liberg, S. M. Razavi, H. S. Razaghi, H. Rydn, and Y. Sui, "Positioning for the Internet of Things: A 3GPP Perspective," *IEEE Communications Magazine*, pp. 1–7, 2017.

[79] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 37, no. 6, pp. 1067–1080, Nov. 2007.

[80] J. Liu, R. Chen, L. Pei, R. Guinness, and H. Kuusniemi, "A hybrid smartphone indoor positioning solution for mobile LBS." *Sensors (Basel, Switzerland)*, vol. 12, no. 12, pp. 17 208–33, Jan. 2012.

[81] T. Liu, Y. Liu, L. Yang, Y. Guo, and C. Wang, "BackPos: High Accuracy Backscatter Positioning System," *IEEE Transactions on Mobile Computing*, vol. 15, no. 3, pp. 586–598, Mar. 2016.

[82] E. S. Lohan, J. Lundén, G. Seco-Granados, V. Koivunen, T. Potential, W. A. Cognitive, and P. Framework, "Cyclic frequencies of GNSS signals and their potential within a cognitive positioning framework," *ION journal of Navigation*, 2013.

[83] E.-S. Lohan and P. Figueiredo E Silva, "User traces analysis based on crowdsourced data," in *2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017*. IEEE, 2017.

[84] E.-S. Lohan, P. Figueiredo E Silva, A. Basiri, and P. Peltola, "Location Based Services analysis through Analytical Hierarchical Processes - an e-health-based case study," in *Multi-Technology Positioning*. Springer, Cham, 2017.

[85] E. S. Lohan, K. Koski, J. Talvitie, and L. Ukkonen, "WLAN and RFID Propagation channels for hybrid indoor positioning," in *Int. Conf. Localization GNSS 2014 (ICL-GNSS 2014)*. IEEE, Jun. 2014, pp. 1–6.

[86] E.-S. S. Lohan, J. Talvitie, P. Figueiredo e Silva, H. Nurminen, S. Ali-löytty, and R. Piché, "Received Signal Strength models for WLAN and BLE-based indoor positioning in multi-floor buildings," in *2015 International Conference on Location and GNSS (ICL-GNSS)*. Gothenburg: IEEE, Jun. 2015, pp. 1–6.

[87] J. F. M. Lorga, P. F. Silva, J. S. Silva, T. F. R. da Silva, M. S. Nunes, F. D. Nunes, and F. M. G. Sousa, "GNSS hybridization for indoor positioning," *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pp. 1–13, Dec. 2010.

[88] J. Lunden and V. Koivunen, "Spectrum Sensing in Cognitive Radios Based on Multiple Cyclic Frequencies," in *Cognitive Radio Oriented Wireless Networks and Communications*, 2007.

[89] H. Ma and K. Wang, "Fusion of RSS and Phase Shift Using the Kalman Filter for RFID Tracking," *IEEE Sensors Journal*, vol. 17, no. 11, pp. 3551–3558, Jun. 2017.

[90] H. Ma, Y. Wang, K. Wang, and Z. Ma, "The Optimization for Hyperbolic Positioning of UHF Passive RFID Tags," *IEEE Transactions on Automation Science and Engineering*, vol. 14, no. 4, pp. 1590–1600, Oct. 2017.

[91] Z. Ma, S. Poslad, J. Bigham, X. Zhang, and L. Men, "A BLE RSSI ranking based indoor positioning system for generic smartphones," in *2017 Wireless Telecommunications Symposium (WTS)*. IEEE, Apr. 2017, pp. 1–8.

[92] J. Machaj, P. Brida, and R. Piche, "Rank based fingerprinting algorithm for indoor positioning," in *2011 International Conference on Indoor Positioning and Indoor Navigation*. IEEE, Sep. 2011, pp. 1–6.

[93] E. R. Magsino, I. W.-H. Ho, and Z. Situ, "The effects of dynamic environment on channel frequency response-based indoor positioning," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, Oct. 2017, pp. 1–6.

[94] L. Mailaender, "On the CRLB scaling law for Received Signal Strength (RSS) geolocation," *2011 45th Annual Conference on Information Sciences and Systems, CISS 2011*, pp. 2–7, 2011.

[95] R. Mautz, "Indoor positioning technologies," Ph.D. dissertation, ETH Zurich, 2012.

[96] C. Mensing, S. Sand, and A. Dammann, "GNSS Positioning in Critical Scenarios: Hybrid Data Fusion with Communications Signals," *2009 IEEE International Conference on Communications Workshops*, no. 2, pp. 1–6, Jun. 2009.

[97] J. Mitola and G. Q. Maguire, "Cognitive Radio: Making Software Radios More Personal," in *IEEE Personal Communications*, vol. 6, no. 4, 1999, pp. 13–18.

[98] V. Moghtadaiee, A. G. Dempster, and S. Lim, "Indoor localization using FM radio signals: A fingerprinting approach," *2011 International Conference on Indoor Positioning and Indoor Navigation*, pp. 1–7, Sep. 2011.

[99] D. Niculescu, "Positioning in ad hoc sensor networks," *IEEE Network*, vol. 18, no. 4, pp. 24–29, July 2004.

[100] D. Niculescu and B. Nath, "Localized positioning in ad hoc networks," in *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.*, May 2003, pp. 42–50.

[101] C. W. Ou, C. J. Chao, F. S. Chang, S. M. Wang, G. X. Liu, M. R. Wu, K. Y. Cho, L. T. Hwang, and Y. Y. Huan, "A ZigBee position technique for indoor localization based on proximity learning," in *2017 IEEE International Conference on Mechatronics and Automation (ICMA)*, Aug. 2017, pp. 875–880.

[102] V. Pasku, A. De Angelis, M. Dionigi, G. De Angelis, A. Moschitta, and P. Carbone, "A Positioning System Based on Low Frequency Magnetic Fields," *IEEE Transactions on Industrial Electronics*, vol. 0046, no. c, p. 1, 2015.

[103] Posxyz, "Pozyx - centimeter positioning for arduino." [Online]. Available: https://www.pozyx.io/

[104] N. Pratas, N. R. Prasad, A. Rodrigues, and R. Prasad, "Cooperative spectrum sensing: State of the art review," in *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*. Ieee, Feb. 2011, pp. 1–6.

[105] F. Quitin, Z. Madadi, and W. P. Tay, "RF transmitter geolocation based on signal periodicity: Concept and implementation," in *IEEE International Conference on Communications*, vol. 2015-Septe. IEEE, Jun. 2015, pp. 4593–4598.

[106] Quuppa, "Quuppa," http://quuppa.com/. [Online]. Available: http://quuppa.com/

[107] M. L. Rahman, P. Figueiredo e Silva, and E.-S. Lohan, "Cyclostationarity-based spectrum sensing properties for signals of opportunity," in *2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, Oct. 2014, pp. 390–395.

[108] T. S. Rappaport, *Wireless communications : principles and practice*. Prentice Hall PTR, 2002, vol. 2.

[109] J. Raquet and R. K. Martin, "Non-GNSS radio frequency navigation," in *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, Mar. 2008, pp. 5308–5311.

[110] R. Rashidzadeh and M. Ahmadi, "Differential access points for indoor location estimation," *2009 IEEE International Conference on Electro/Information Technology*, pp. 256–259, 2009.

[111] R. S. Roberts, W. A. Brown, and H. H. Loomis, "Computationally efficient algorithms for cyclic spectral analysis," *Signal Processing Magazine, IEEE*, 1991.

[112] A. R. J. Ruiz, "Accurate pedestrian indoor navigation by tightly coupling foot-mounted IMU and RFID measurements," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 1, pp. 178–189, 2012.

[113] H. Sallouha, A. Chiumento, and S. Pollin, "Localization in long-range ultra narrow band IoT networks using RSSI," in *2017 IEEE International Conference on Communications (ICC)*. IEEE, May 2017, pp. 1–6.

[114] S. Sand, C. Mensing, S. Ancha, and G. Bell, "Communications and GNSS based navigation: A comparison of current and future trends," in *2007 16th IST Mobile and Wireless Communications Summit*. IEEE, Jul. 2007, pp. 1–5.

[115] J. Seitz, L. Patiño-studencka, B. Schindler, S. Haimerl, J. G. Boronat, S. Meyer, and J. Thielecke, "Sensor Data Fusion for Pedestrian Navigation Using WLAN and INS," *Proceedings of Gyro Technology Symposium 2007*, pp. 1–10, 2007.

[116] Senion, "Indoor Positioning for Offices - Senion | Indoor Positioning System." [Online]. Available: https://senion.com/indoor-positioning-for-office/

[117] M. Shafiee, "WiFi-based fine timing assistance for GPS acquisition," 2013.

[118] S. Shrestha, J. Talvitie, and E. S. Lohan, "Deconvolution-based indoor localization with WLAN signals and unknown access point locations," in *2013 13th Int. Conf. ITS Telecommun.*, Nov. 2013.

[119] S. Shrestha, J. Talvitie, and E. S. Lohan, "On the fingerprints dynamics in WLAN indoor localization," in *2013 13th International Conference on ITS Telecommunications (ITST)*. IEEE, Nov. 2013, pp. 122–126.

[120] Sigfox, "Sigfox - The Global Communications Service Provider for the Internet of Things (IoT)," 2017. [Online]. Available: https://www.sigfox.com/en/sigfox-geolocation

[121] P. F. e. Silva and P. Peltola, "piTiming." [Online]. Available: https://bitbucket.org/silva/pitiming

[122] Sky Hook, "SkyHook Products." [Online]. Available: http://www.skyhookwireless.com/products/

[123] M. R. Song, J. Y. Moon, and S. H. Bae, "Efficient Indoor Positioning By Hybrid Algorithm," *Science & Engineering Research Support soCiety*, vol. 25, pp. 118–122, 2013.

[124] C. M. Spooner, A. N. Mody, J. Chuang, and M. P. Anthony, "Tunnelized cyclostationary signal processing: A novel approach to low-energy spectrum sensing," in *IEEE Military Communications Conference*. Ieee, Nov. 2013, pp. 811–816.

[125] A. N. Steinberg and C. L. Bowman, *Handbook of multisensor data fusion*. CRC Press, 2001.

[126] Streetpath.com, "Steerpath indoor positioning and navigation SDK."

[127] P. Sutton, K. Nolan, and L. Doyle, "Cyclostationary Signatures in Practical Cognitive Radio Applications," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 13–24, Jan. 2008.

[128] J. Talvitie, "Algorithms and Methods for Received Signal Strength Based Wireless Localization," *Tampere University of Technology. Publication*, vol. 1365, 2016.

[129] Technische Universität Ilmenau and Institute of Electrical and Electronics Engineers, *Wireless Communication Systems (ISWCS 2013), Proceedings of the Tenth International Symposium on : date: 27-30 August 2013*. [VDE Verlag], 2013.

[130] R. Thomas and B. Maharaj, "Towards a bandwidth efficient cognitive positioning system," *Electronics Letters*, vol. 48, no. 12, p. 736, 2012.

[131] Trackinno, "IoT Solutions for Asset Management - Trackinno."

[132] H. Urkowitz, "Energy Detection of Unknown Deterministic Signals," *Proceedings of the IEEE*, vol. 55, no. 4, 1967.

[133] G. A. Vecchione, D. Palenzuela, M. Toledo, J. J. R. de Cáceres, D. Kubrak, Y. Capelle, G. Seco, J. López-Salcedo, P. Tiley, A. Consoli, D. Jiménez-Baños, and G. López-Risueño, "Dingpos, a gnss-based multi-sensor demonstrator for indoor navigation: Preliminary results," in *IEEE/ION Position, Location and Navigation Symposium*, May 2010, pp. 113–121.

[134] S. Wagner, N. Fet, M. Handte, and P. J. Marrón, "An approach for hybrid indoor/outdoor navigation," in *Proceedings - 2017 13th International Conference on Intelligent Environments, IE 2017*, vol. 2017-Janua. IEEE, Aug. 2017, pp. 36–43.

[135] W. Wang, P. Figueiredo e Silva, and E. S. Lohan, "Investigations on mobility models and their impact on indoor positioning," in *International Workshop on Mobile Entity Localization and Tracking in GPS-less Environments*, Seattle, USA, 2015.

[136] P. Williams, "Evaluating the state probabilities of M out of N sliding window detectors," DSTO Aeronautical and Maritime Research Laboratory, Tech. Rep., 1998.

[137] Wirepas, "Asset Management with Wirepas Mesh | Wirepas." [Online]. Available: https://wirepas.com/products-and-services/assets/

[138] Wirepas, "Technology - Wirepas." [Online]. Available: https://wirepas.com/connectivity/technology/

[139] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[140] G. C. Zanuz, J. M. Winter, I. Muller, J. L. T. Garzon, J. C. Netto, and C. E. Pereira, "Identification of IEEE 802.11g and IEEE 802.15.4 signals using energy and cyclostationarity detection approach," in *2016 1st International Symposium on Instrumentation Systems, Circuits and Transducers (INSCIT)*. IEEE, Aug. 2016, pp. 55–60.

[141] L. Zhang, C. Tao, and G. Yang, "Wireless positioning: fundamentals, systems and state of the art signal processing techniques," *InTech, Rijeka, Croatia*, 2011.

[142] W. Zhang, Y. Wang, L. Chen, Y. Liu, and Y. Rao, "A Hybrid Indoor Positioning Approach for Supermarkets," *Service-Oriented Computing-*, pp. 306–316, Nov. 2013.

[143] Y. Zhang, L. Deng, and Z. Yang, "Indoor positioning based on FM radio signals strength," in *2017 First International Conference on Electronics Instrumentation & Information Systems (EIIS)*. IEEE, Jun. 2017, pp. 1–5.

[144] D. Zhu and K. Yi, "A Hybrid TDOA / RSS Localization Algorithm Based on UWB Ranging in Underground Mines," *International Conference on Electronic Commerce, Web Application, and Communication*, pp. 402–407, 2011.

[145] H. Zou, B. Huang, X. Lu, H. Jiang, and L. Xie, "Standardizing location fingerprints across heterogeneous mobile devices for indoor localization," in *2016 IEEE Wireless Communications and Networking Conference*. IEEE, Apr. 2016, pp. 1–6.

Publications

Publication 1

P. Figueiredo e Silva, O. Daniel, J. Nurmi, E.S. Lohan, "Cyclostationary features of downsampled 802.11g OFDM signal for cognitive positioning systems," in *Proceedings of the IEEE International Symposium on Wireless Communication Systems (ISWCS)*, Barcelona, Spain, August 2014. DOI: 10.1109/ISWCS.2014.6933490

Cyclostationary features of downsampled 802.11g OFDM signal for cognitive positioning systems

Pedro Figueiredo e Silva*, Ondrej Daniel*, Jari Nurmi and Elena-Simona Lohan
Department of Electronics and Communications Engineering,
Tampere University of Technology, Finland
{pedro.silva, ondrej.daniel, jari.nurmi, elena-simona.lohan}@tut.fi
* Authors contributed in the same manner to this paper

***Abstract*—In cognitive positioning systems, spectrum sensing methods play an important role to understand the surrounding spectrum. Due to their good performance under noisy environments, cyclostationary methods are commonly used to characterise the received signals. These methods require a higher computational cost and high sampling rates [1]. With that in mind, this paper uses real measurement data, acquired in an office environment, at different sampling rates, including rates below the Nyquist rate. The motivation is to show that the implementation burden of these methods can be reduced by using lower sampling frequencies, since the cyclic properties of the signals are still visible.**

***Index Terms*—Cognitive positioning systems, downsampling, cyclostationary, signals of opportunity.**

I. INTRODUCTION

Spectrum sensing and signal identification methods are essential building blocks of cognitive radio and cognitive positioning systems. In cognitive radio the detection objective is primarily to infer whether the primary user's signal is absent, in order to better utilize the available spectrum resources by secondary users' signals. In cognitive positioning systems, the information about available spectrum resources is continuously delivered to the cognitive positioning engine, which attempts to exploit it in order to fulfill the localisation requirements of the user or system. As an example, if there are unused parts of the spectrum, a request to extend the bandwith of the navigation signals under use could be done by the cognitive positioning engine [2]

As opposed to the spectrum sensing methods, the identification methods can reveal more details about the available signals. Knowing which particular types of signals are present in the spectrum surrounding a receiver can be exploited, for example, to improve the accuracy of its localisation. Furthermore, the cognitive positioning systems may profit from the fact that the number of navigation signals, as well as signals of opportunity present in the spectrum, has increased significantly over the last years. The proliferation of these signals means an opportunity for positioning systems to provide its users with seamless operation throughout indoor and outdoor environments. However, exploiting all these signals in parallel can be too computationally demanding. Hence, it is important to select only the most relevant signals with respect to the current localisation requirements. If a method allowing the signal identification of the spectrum without using a standard procedure (acquisition, tracking, and demodulation) is incorporated in a positioning system, it can lead to faster operational times with a smaller power footprint. Fig.1 presents an example of a cognitive positioning system, where the spectrum sensing block provides to the cognitive positioning engine, necessary information regarding the spectrum. This information is used by the cognitive positioning engine to control the entire system and fulfill the local positioning requirements. Over this paper, the focus falls solely in the spectrum sensing block.

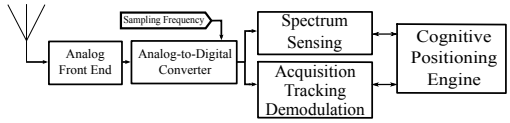


Fig. 1. An example of a cognitive positioning architecture.

A common approach to sense, as well as, to identify signals in the spectrum relies on their cyclostationarity properties. Such properties appear due to periodicities present in the signals, imposed by, for example, modulation, coding, spreading, among others. It can be inferred that these features vary for different signals, allowing their identification and classification. The mathematical tool describing the cyclostationarity properties is called Spectral Correlation Function (SCF). An advantage of using cyclostationarity-based methods is that it can distinguish between wide sense stationary noise and useful user's signals, since the noise does not exhibit periodic features. However, they also require more computational resources.

Currently, OFDM signals are relatively ubiquitous in the spectrum, since they are being used in several wireless networks systems, such as LTE and WiFi and have shown good positioning capabilities. In the particular case of LTE, pilot signals are already being thought to improve its positioning capabilities, on top of its communication purposes [3], [4]. As for WiFi signals, studies using timing [5], [6] and power information [7] have also shown the potential of these signals for navigation purposes.

The objective of this paper is to show that the periodic features of the SCF of IEEE 802.11g OFDM signals, measured

978-1-4799-5863-4/14/$31.00

in an office environment, are still visible and detectable when using sampling frequencies below the Nyquist rate. It has been reported that high sampling frequencies are usually necessary to observe cyclic frequencies [1], however the work in [8] suggests that sampling frequencies below Nyquist rates can still be used to identify the signals based on cyclostationary features. Besides this, the reduction in sampling frequencies leads to a lower complexity [9], by a factor proportinal to the downsampling factor, which is important from an implementation point of view.

II. Cyclostationarity

A signal $x(t)$ is wide-sense cyclostationary if its time varying autocorrelation function $R(t,\tau)$ defined as,

$$R(t,\tau) = E\{x(t)x^*(t+\tau)\}, \tag{1}$$

is periodic in time, t, for each lag parameter, τ. Hence, it can be represented as a Fourier series,

$$R(t,\tau) = \sum_{\beta} R^{\beta}(\tau)e^{j2\pi\beta t}, \tag{2}$$

where the sum is taken over integer multiples of fundamental cyclic frequency β, for which cyclic autocorrelation function is defined as,

$$R^{\beta}(\tau) = \lim_{T\to\infty}\frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} R(t,\tau)e^{-j2\pi\beta t}dt. \tag{3}$$

The SCF, $S^{\beta}(f)$, is the Fourier transform of R^{β} and is given as,

$$S^{\beta}(f) = \int_{\mathbb{R}} R^{\beta}(\tau)e^{-j2\pi f\tau}d\tau. \tag{4}$$

In this paper the fast Fourier transform Accumulation Method (FAM) is being used to estimate the SCF of the IEEE 802.11g OFDM signal. Other methods can be used and should provide comparable results and further information can be found in [8]–[10].

A. IEEE 802.11g cyclostationary properties

The cyclostationary properties of the IEEE 802.11g OFDM signal appear due to the pilots and cyclic prefix present in the signal's design. From a mathematical point of view, the IEEE 802.11g signal, $y(t)$, can be seen as,

$$y(t) = A\sqrt{E_s}\sum_{n}\sum_{k=1}^{N} X_n(k)e^{j2\pi k\Delta f t}h(t-nT_U), \tag{5}$$

where $A = (NT_UE_d)^{-1/2}$ is a multiplicative constant normalizing the OFDM symbol energy, E_s represents the average energy of OFDM symbols, N is the number of subcarriers, E_d is the average energy of 16-QAM data symbols which form the OFDM symbols, X_n is n-th OFDM symbol expressed as a vector consisting of N data symbols, and $h(t)$ represents a unity rectangular pulse on the interval $[0, T_U)$ and zero otherwise. The signal is further extended through the cyclic prefix. In the frequency domain, the signal occupies frequencies in the range $[-B, B]$ MHz, where B is the one-sided bandwith equal to 10 MHz. Hence, the signal's Nyquist rate is $f_N = 2B = 20$ MHz and, in this case, the Nyquist frequency is $10MHz$.

Under the FAM implementation, the cyclic frequencies are dependent on the symbol duration [11]. Theoretically, the cyclic frequencies, β_k, of such a signal are determined by,

$$\beta_k = \frac{1}{T_{symbol}}\cdot k, k\in\mathbb{Z}, \tag{6}$$

where the symbol period, $T_{symbol} = T_{GI} + T_U$, consists of guard interval, T_{GI}, which is occupied by cyclic prefix and duration of useful symbol, $T_U = \Delta_f^{-1}$, which is chosen to guarantee orthogonality of OFDM subcarriers for their given frequency spacing Δ_f.

B. Probability of appearance

From the previous discussion, it is expected that the cyclic frequencies will appear at well defined positions. Therefore, to understand which of these cyclic frequencies are more frequent in the SCF, the probability of appearance is defined as the number of times a given cyclic frequency is distinguishable over several input data windows. Distinguishing cyclic frequencies is done by using an activity indicator, [12], [13], I, computed as,

$$I = \frac{\sigma}{\mu}, \tag{7}$$

where the mean, μ, and standard deviation, σ, are obtained from a segment of the input window's absolute SCF, centered at each cyclic frequency, β_k. For each β_k the segment is taken over the region $[\beta_k - 0.01f_s, \beta_k + 0.01f_s]$, where f_s is the sampling frequency. It is also assumed that over this region only one β_k is present. This metric offers a χ-square test of the segment samples' distribution, which is true when only noise is present at the input. Therefore, if a cyclic frequency is present, the resulting outlier allows for its identification. This is done by comparing the value of I to the defined threshold V_{th}, which is, approximately, two times the value observed when noise only is present. This information can be further exploited by a signal detector to identify the present of one or more signals, however, this paper aims to offer an insight on which cyclic frequencies might be considered for such goal.

III. Measurement of IEEE 802.11g OFDM signals

Real IEEE 802.11g OFDM signals were captured using an inexpensive (below €1000) acquisition hardware platform. The platform is called Universal Software Radio Peripheral (USRP) B210. Its main components include RF integrated circuit AD9361 consisting of two channel transceiver with integrated 12 bit DACs/ADCs and Spartan 6 FPGA. Moreover, it incorporates a programmable analog filter which is automatically sets the appropriate bandwidth for the given sampling rate, minimising the effect of antialising. No additional RF

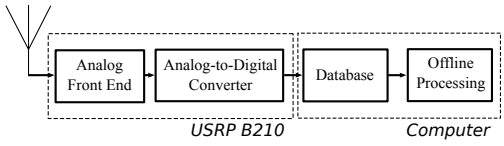


Fig. 2. Setup used for the measurement of IEEE 802.11g OFDM signals.

hardware was used besides a standard 3 dBi omnidirectional antenna working in 2.4 GHz band. The received signals were captured at sampling rates,

$$f_s = \left\{ 2f_N = 40, f_N = 20, \frac{1}{2} f_N = 10 \right\} \text{ MHz}, \qquad (8)$$

and stored in a computer for subsequent off-line processing. Some relevant parameters are summarised in table I.

The signals were measured in corridors and offices in Tietotalo building at Tampere University of Technology. Individual 802.11 frames captured in those signals do not keep a constant SNR value. However, it was roughly estimated that the SNR varies in range from 3 to 16 dB, where SNR is defined as the ratio of powers of useful signal and noise. Fig.2 illustrates the setup used for the measurements.

A. Effect of downsampling in cyclic properties

In order to investigate the possibility of using downsampled signals for cyclic features detection, the input data was split in 10 ms segments. These segments were used in the cyclostationary algorithm to investigate the behaviour and presence of the cyclic frequencies expected from (6). The length of this segment was arbitrary chosen in order to contain useful signal at each time. Since the measurements were made in an office environment, the high density traffic should fulfill this assumption.

Fig.3 shows an example of the SCF of the 10 ms time windows, at different sampling frequencies, 40MHz and 10MHz, respectively. In both cases it can be seen that the downsampling keeps the cyclic frequencies in the expected positions, but the values are slightly changed. This is particularly visible when comparing the values at 1 MHz. It is also possible to observe in the figure, that most cyclic frequencies, expected from (6), are not visible or its value too low and considered as noise.

B. Statistical behaviour

Fig.4-6 show a box plot containing the value of I, (7), for the segment defined over the cyclic frequencies contained in the interval $(-5, 5)$ MHz, for sampling frequencies 40 MHz, 20 MHz and 10 MHz, respectively. These figures allow a better understanding of how the value of I is changing throughut time for each cyclic frequency expected from (6). The boxplots show the median value (central mark in the box) and mean of I at the given cyclic frequencies, as well as the 25th and 75th percentiles, defined by the box lower and upper edges, respectively. The minimun and maximum values are represented by the vertical lines extended from the box and remaining dots mark the outliers, defined as the observations with values abov 3σ. The threshold used for the later probabilities of appearance is also plotted for reference.

TABLE I
PARAMETERS USED IN THE MEASUREMENT AND PROCESSING OF THE IEEE 802.11G SIGNALS.

Parameter	*Value*
Number of random trials, T	5000
Activity threshold, $V_{\mathbf{th}}$	1
Observation time	10 ms
Cyclic resolution	$1e^{-4} \times f_s$ Hz
Frequency resolution	$0.1 \times f_s$ Hz
Bandwidth (two-sided), 2B	20 MHz
Modulation	16-QAM
Number of carriers, N	64
Symbol interval, $\mathbf{T_{symbol}}$	$4\,\mu$s
Sub-carrier spacing, $\mathbf{\Delta_f}$	$B/N = 312.5$ kHz
Guard interval, $\mathbf{T_{gi}}$	$\Delta_f^{-1}/4$ s
First cyclic frequency, β_1	250 kHz

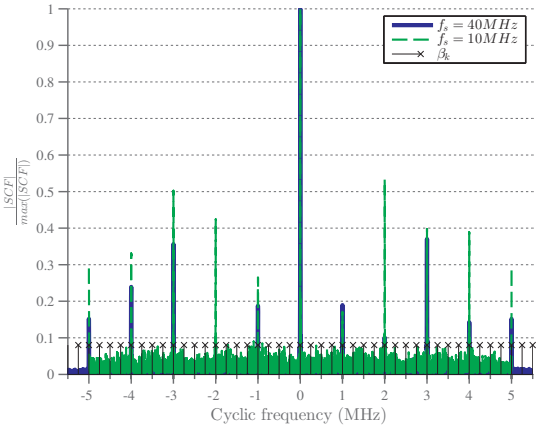


Fig. 3. $S^{\beta}(0)$ for measured data sampled at $f_s = 40$MHz and $f_s = 10$MHz.

One main conclusion from these figures is that the cyclic frequencies at integer values are the ones causing the biggest changes in the value of I. Otherwise, the mean of I remains close to 0.5 as it has also been observed when only noise is present at the input. It is also interesting to note that almost all the values of I, for 10 MHz sampling frequency, are clearly above the defined the threshold. While for the other sampling frequencies this only happens at some cyclic frequencies, such as 3 MHz. Regardless of that, the threshold can be tweaked which will have impact on the porbability of identifying the cyclic frequencies, however the proper way to set this value is outside the scope of this paper.

C. Most frequent cyclic frequencies

Supporting the discussion above, the probability of appearence at integer cyclic frequencies is obtained by counting

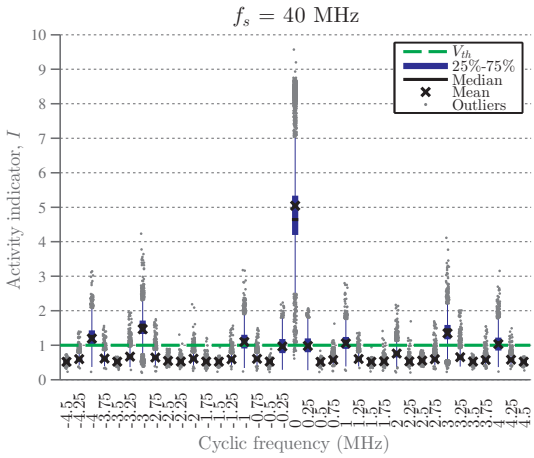


Fig. 4. Boxplot of the activity indicator for $f_s = 40$MHz.

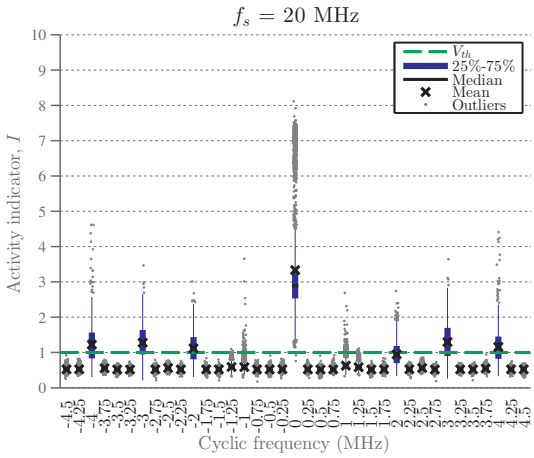


Fig. 5. Boxplot of the activity indicator for $f_s = 20$MHz.

the number of times the cyclic frequency is present in the 5000 input data windows of 10 ms duration. In Fig.7 the probability of appearence for all the expected cyclic frequencies from (6) is shown. This figure shows, as expected from the previous discussion, that the cyclic frequencies with higher probability of appearance are located at integer frequencies. Table II contains the probability of appearence for these cyclic frequencies located inside the region $(-5, 5)$ MHz.

IV. Conclusion

Over this paper, a stream of IEEE 802.11g signals, acquired by an USRP B210 in an office environment, was used to investigate the behaviour of cyclic frequencies when downsampling the input signal. The motivation behind this is to reduce the complexity of the cyclostationary methods, since the number of samples is reduced.

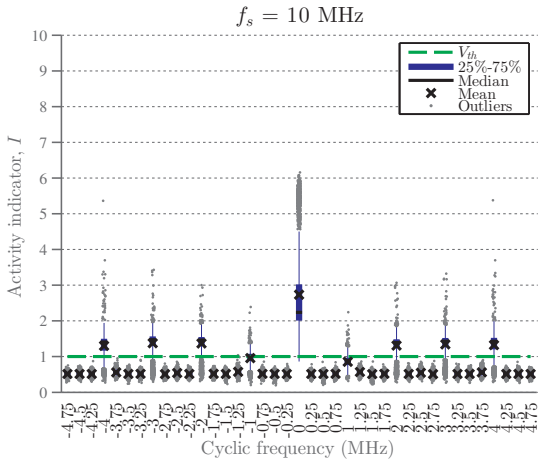


Fig. 6. Boxplot of the activity indicator for $f_s = 10$MHz.

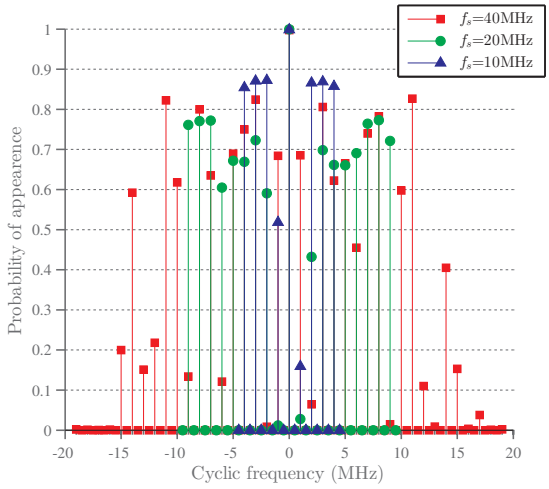


Fig. 7. Probability of appearence for signals sampled by USRP, sampled at 40MHz, 20MHz, 10MHz.

TABLE II
PROBABILITY OF APPEARANCE FOR CYCLIC FREQUENCIES IN UNDERSAMPLED SIGNALS FROM USRP.

Sampling frequency	**40MHZ**	**20MHZ**	**10MHZ**
***Cyclic frequency* (MHz)**	**Probability %**		
4	62	68	86
3	81	71	87
2	6	45	87
1	69	3	16
0	100	100	100
-1	68	1	52
-2	1	61	87
-3	82	74	87
-4	75	69	85

The main conclusions from this paper are that cyclic spectral analysis can be used to identify the presence of a IEEE 802.11g OFDM signal, since this signal exhibits clear cyclic peaks at n MHz, $n \in \mathbb{Z}$. Besides that, even when using a reduced sampling frequency, such as $0.5 f_N$, cyclic frequencies can still be identified. Therefore, sampling frequencies below the Nyquist rate can be chosen in order to design a reliable signal detector, however the design and performance of such detector has not been considered over this study.

ACKNOWLEDGMENT

This work was financially supported by EU FP7 Marie Curie Initial Training Network MULTI-POS (Multi-technology Positioning Professionals) under grant nr. 316528.

The authors express their gratitude to the Academy of Finland (project 256175 "Cognitive Approaches for Location in Mobile Environments") for its additional financial support for this research work.

REFERENCES

[1] E.-S. Lohan, J. Lundén, G. Seco-Granados, V. Koivunen, T. Potential, W. A. Cognitive, and P. Framework, "Spectral Patterns of BOC-Modulated Signal Mixtures for Cognitive Positioning," *ION journal of Navigation, [in press]*, 2013.

[2] H. Celebi and H. Arslan, "Cognitive Positioning Systems," *IEEE Transactions on Wireless Communications*, vol. 6, no. 12, pp. 4475–4483, Dec. 2007.

[3] J. A. del Peral-Rosado, J. A. Lopez-Salcedo, G. Seco-Granados, F. Zanier, P. Crosta, R. Ioannides, and M. Crisci, "Software-Defined Radio LTE Positioning Receiver Towards Future Hybrid Localization Systems," *31st AIAA International Communications Satellite Systems Conference*, Oct. 2013.

[4] R. Montalban, J. A. Lopez-Salcedo, G. Seco-Granados, and A. L. Swindlehurst, "Power allocation approaches for combined positioning and communications OFDM systems," *2013 IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 694–698, Jun. 2013.

[5] T. Ohlemueller, F. Winkler, and E. Grass, "Radio localization in OFDM networks using the round trip phase," *2010 7th Workshop on Positioning, Navigation and Communication*, pp. 23–27, Mar. 2010.

[6] A. Gaber and A. Omar, "A Study of TDOA Estimation Using Matrix Pencil Algorithms and IEEE 802 . 11ac," 2012.

[7] K. Wu, J. Xiao, Y. Yi, and D. Chen, "CSI-Based Indoor Localization," *Parallel and Distributed Systems*, vol. XX, no. X, pp. 1–11, 2013.

[8] C. M. Spooner, A. N. Mody, J. Chuang, and M. P. Anthony, "Tunnelized Cyclostationary Signal Processing: A Novel Approach to Low-Energy Spectrum Sensing," in *IEEE Military Communications Conference*. Ieee, Nov. 2013, pp. 811–816.

[9] R. Roberts, W. Brown, and H. Loomis, "Computationally Efficient Algorithms for Cyclic Spectral Analysis," *Signal Processing Magazine, IEEE*, 1991.

[10] W. A. Gardner, A. Napolitano, and L. Paura, "Cyclostationarity: Half a Century of Research," *Signal Processing*, vol. 86, no. 4, pp. 639–697, Apr. 2006.

[11] J. Lunden and V. Koivunen, "Spectrum Sensing in Cognitive Radios Based on Multiple Cyclic Frequencies," in *Cognitive Radio Oriented Wireless Networks and Communications*, 2007.

[12] E. Guenterberg, H. Ghasemzadeh, R. Jafari, and R. Bajcsy, "A Segmentation Technique Based on Standard Deviation in Body Sensor Networks," in *Engineering in Medicine and Biology Workshop*, 2007.

[13] A. Benbasat and J. Paradiso, "An Inertial Measurement Framework for Gesture Recognition and Applications," *Gesture and Sign Language in Human-Computer Interaction*, 2002.

Publication 2

P. Figueiredo e Silva, G. Seco-Granados, and E.S. Lohan, "Receiver Architecture for Cognitive Positioning with CDMA and OFDM signals," in *Proceedings of the International Conference on Localization and GNSS (ICL-GNSS)*, Gothenburg, Sweden, June 2015. DOI: 10.1109/ICL-GNSS.2015.7217153

Receiver Architecture for Cognitive Positioning with CDMA and OFDM signals

Pedro Figueiredo e Silva*, Gonzalo Seco-Granados** and Elena Simona-Lohan*
* Department of Electronics and Communications Engineering, Tampere University of Technology, Finland
{pedro.silva,elena-simona.lohan}@tut.fi
** Signal Processing for Communications and Navigation (SPCOMNAV), Universitat Autònoma de Barcelona, Spain
gonzalo.seco@uab.es

***Abstract*—This paper proposes a cognitive positioning architecture. This architecture uses cyclostationary analysis to understand the contents of the spectrum surrounding the receiver and exploit this information for activating the necessary tracking and demodulation loops. This paper assumes the presence of CDMA and OFDM signals. The results show the performance of the spectrum sensing technique used along with the expected positioning accuracy.**

***Index Terms*—Cognitive positioning architecture, spectrum sensing, signals of opportunity, approximate maximum likelihood.**

A cognitive radio (CR) is a device aware of its environment, allowing the coexistence with other radios that might lack cognition features [1]. The coexistence is guaranteed by monitoring the spectrum for unused frequency subbands [2], [3]. In some cases, the CR may need to know its location. However, while a position fix is easy to obtain in an outdoor environment, indoor environments are particularly difficult for current positioning technologies, such as global navigation satellite systems (GNSS). Consequently, there is a need for better indoor navigation, at a reasonable price. In indoor environments cellular and Wi-Fi signals are already widely deployed, their use for indoor positioning systems is an alternative to other dedicated systems. The main purpose of Wifi and celular signals is to provide data and voice communication links, therefore they are known as signals of opportunity (SoO) when used in a navigation context.

Enabling navigation through SoO, requires a device capable of simultaneously acquiring, tracking and decoding a multitude of signals, raising difficulties at the implementation level. Besides the physical limitations of current devices, the power consumption is another concern, and it does not benefit from adding extra sensors. Since cognitive radios and advanced signal processing techniques are becoming the norm for future telecommunication standards [4], it should be possible for positioning systems to tap into this cognition layer. With such information, these systems could manage the existing hardware and provide more efficient hybridisation of different sensor data [5], [6].

The architecture proposed in this paper, aims to speed up the acquisition, tracking and demodulation of the incoming signals in comparison to the traditional approach illustrated in Fig. 1.A. To fulfil that objective, the signals at the input of the front end are merged in a single digital representation and fed

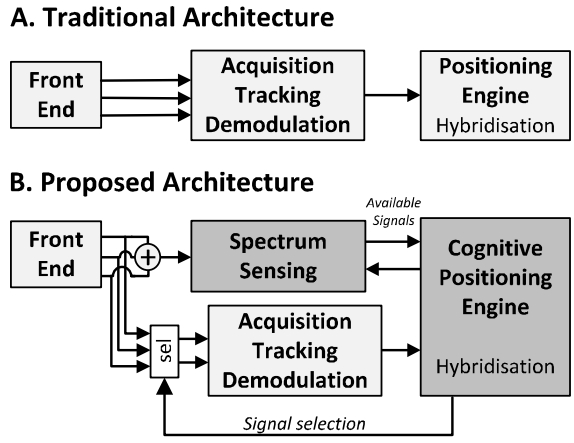


Fig. 1. Example of a possible cognitive positioning system.

to the spectrum sensing block Fig. 1.B. These signals can be, for example, Wi-Fi, Bluetooth, RFID, LTE, as well as other signals and the goal of the block is to identify which signals are present in the spectrum at a given time. This information is carried over to the cognitive positioning engine, which is responsible for performing the signal selection for the acquisition and tracking stages. The reason of performing such signal selection is either to increase the performance requirements or improve the power and resource usage of the device. Later on, this is exemplified with an example where different number of orthogonal frequency-division multiplexing (OFDM) and code division multiple access (CDMA) emitters are used to determine the location of a mobile receiver.

I. Proposed architecture

The following discussion focuses on signal detection and signals using their cyclostationary features, at the cognitive positioning engine. CDMA and OFDM signals are considered due to their popularity in current and future communication systems. Besides that, the authors of [7], [8] have found them suitable for positioning based on timing and received signal strength (RSS) estimates [9], [10].

A. Signal model

CDMA and OFDM signals are assumed to be present in the surrounding spectrum of a receiver, such as the one depicted in Fig. 1.B, and at the spectrum sensing block input, their representation is given by $z(t)$,

$$z(t) = d(t) + m(t) + n(t), \tag{1}$$

where $d(t)$ is a CDMA signal, $m(t)$ a OFDM signal and $n(t)$ is white Gaussian noise (WGN) of double-sided power spectral density equal to $\frac{N_0}{2}$. If either one of the signals is absent during a period of time, their representation is set to zero. For clarity, the channel is assumed to have flat frequency response, but the ideas can be extended to frequency-selective channels as well.

The CDMA signal, $d(t)$, is given by,

$$d(t) = \begin{cases} E_c \sum_{n=-\infty}^{+\infty} \sum_{k=1}^{\mathrm{SF}} c_k(n) p(t - kT_c - nJT_c) \\ 0, \text{ when signal absent,} \end{cases} \tag{2}$$

where E_c is the chip energy, SF is the spreading factor, $c_k(n)$ is the chip value (+1 or -1) for k^{th} chip during n^{th} symbol, $p(t)$, a pulse shaping function, T_c the chip interval.

As for the OFDM signal, $m(t)$, is described by,

$$m(t) = \begin{cases} A \sum_{n} \sum_{k=0}^{N-1} X_n(k) e^{j2\pi k \Delta_f t} q(t - nT_U) \\ 0, \text{ when signal absent,} \end{cases} \tag{3}$$

where $A = \sqrt{(NT_U E_m)}$ is a multiplicative constant normalising the OFDM symbol energy, N is the number of subcarriers, E_m is the average energy of M-QAM data symbols which forms the OFDM symbols, $X_n(k)$ is n-th OFDM symbol expressed as a vector consisting of I data symbols, and $q(t)$, a pulse shaping function. T_U is the symbol period before being extended with the cyclic prefix. With the introductuion of the cyclic prefix, the total symbol period, T_{symbol}, is defined as

$$T_{\text{symbol}} = T_{GI} + T_U, \tag{4}$$

where T_{GI} is the duration of the guard interval, which is occupied by the cyclic prefix, plus the duration of the useful symbols, $T_U = \Delta_f^{-1}$, which is chosen to guarantee orthogonality of the OFDM subcarriers for their given frequency spacing Δ_f. In the frequency domain, the signal occupies frequencies in the range $[-B, B]$ MHz.

B. Cyclostationary features

A signal $z(t)$ is wide-sense cyclostationary if its time varying autocorrelation function $R(t, \tau)$ is periodic in time, t, for each lag parameter, τ. Hence, it can be represented as a Fourier series,

$$R(t, \tau) = E\{z(t) z^*(t + \tau)\} = \sum_{\gamma} R^{\gamma}(\tau) e^{j2\pi\gamma t}, \tag{5}$$

where the sum is taken over multiples of fundamental cyclic frequency γ for which the cyclic autocorrelation function is defined as,

$$R^{\gamma}(\tau) = \lim_{T \to \infty} \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} R(t, \tau) e^{-j2\pi\gamma t} dt. \tag{6}$$

The spectral correlation function (SCF) [11], $S^{\gamma}(f)$, is the Fourier transform of R^{γ} given as,

$$S^{\gamma}(f) = \int_{\mathbb{R}} R^{\gamma}(\tau) e^{-j2\pi f \tau} d\tau. \tag{7}$$

Periodicities in the signal, such as those produced by the symbols or the repetitions of the spreading sequence are responsible for the appearance of spectral lines in the SCF domain. The locations of the spectral lines are referred to as cyclic frequencies. When the signal is purely random, as it is the case with AWGN, the value of the SCF is zero for every cyclic frequency, except at $\gamma = 0$. An example of SCF for a mixture of CDMA and OFDM signals with noise is shown in Fig. 2, where α_m and β_m are the cyclic frequencies for each signal type, respectively, which are defined in the following paragraphs.

In the context of this study, the cyclic frequencies of interest are those specific to CDMA and OFDM signals. For the CDMA signal the SCF can be expressed [6], [12] as

$$S^{\gamma}(f) \cong D(f - \frac{\gamma}{2}) D^*(f + \frac{\gamma}{2}) \sum_{k=-\infty}^{\infty} \delta_{\left(\gamma - \frac{k}{T_{\text{symbol}}}\right) T_c \bmod 1} + \frac{N_0}{E_c \mathrm{SF}} \delta_{\gamma}, \tag{8}$$

where $D(f)$ is the Fourier transform of $d(t)$, $\delta_{(\gamma - \frac{k}{T_{\text{symbol}}} T_c) \bmod 1}$ the Kronecker delta function having value 1 when $(\gamma - \frac{k}{T_{\text{symbol}}} T_c)\, mod\, 1 = p, p \in \mathbb{Z}$ and zero otherwise, T_c is the chip interval length, T_{symbol} the symbol period. Its theoretical cyclic frequencies [12] are dependent on both the chip rate, f_c, and SF and are contained in $\mathcal{A}$,

$$\mathcal{A} = \{\alpha_0, \alpha_1, \cdots, \alpha_m\}, m \in \mathbb{Z}, \tag{9}$$

$$\forall \alpha_m : \alpha_m \in \left\{ k f_c \,,\; k f_c \pm n \frac{f_c}{SF} \right\} \wedge k, n \in \mathbb{Z}. \tag{10}$$

The OFDM SCF [13] is estimated by,

$$S^{\gamma}(f) = \frac{\delta_r^2}{T} \sum_{n=0}^{N-1} Q\left(f - \frac{n}{T_{\text{symbol}}} + \frac{\gamma}{2}\right) Q^*\left(f - \frac{n}{T_{\text{symbol}}} - \frac{\gamma}{2}\right), \tag{11}$$

which is non-zero for every $\gamma = \frac{k}{T_{\text{symbol}}}$ and zero otherwise and $Q(f)$ is the Fourier transform of the pulse shape function. The OFDM theoretical cyclic frequencies are found to be in $\mathcal{B}$,

$$\mathcal{B} = \{\beta_0, \beta_1, \cdots, \beta_n\}, n \in \mathbb{Z}, \tag{12}$$

$$\forall \beta_n : \beta_n \in \left\{ k \frac{1}{T_{\text{symbol}}} \right\} \wedge k \in \mathbb{Z}, \tag{13}$$

where each β_n location is related to the symbol period [14].

The proposed detector requires the knowledge of both $\mathcal{A}$ and $\mathcal{B}$. For that reason, parameters for both signals need to be known by the algorithm. Regarding the CDMA signal, the

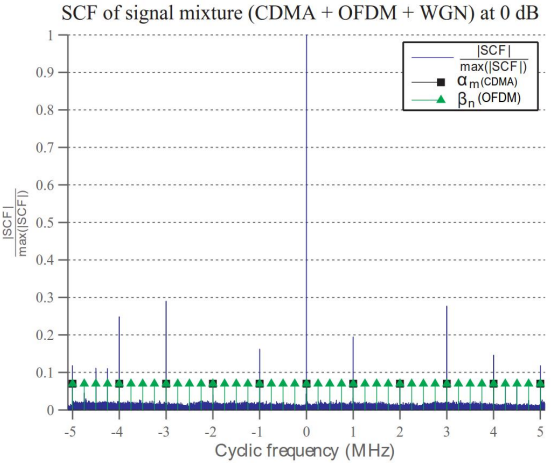


Fig. 2. Section of the SCF at frequency zero $S^{\alpha}(0)$.

chip rate and spreading factor are necessary. As for OFDM signal, the total number of carriers and bandwidth.

C. Feature detector

The proposed feature detector, inspired in [15] and [16], determines if certain cyclic frequencies are present or not in the SCF. The algorithm starts by defining several windows, $\mathbf{W}$, over the absolute value of the SCF. These windows are placed over the SCF at specific cyclic frequencies, γ,

$$\boldsymbol{W} = [\gamma_i - \epsilon, \gamma_i + \epsilon] \tag{14}$$

and with ϵ set to a value that guarantees, γ_i is the only cyclic frequency present (Table I). This is the input to the algorithm (Fig. 3). Afterwards, the algorithm computes the standard deviation, σ, and mean, μ, within each window. The ratio between the standard deviation and the mean result in an activity indicator, I,

$$I = \frac{\sigma}{\mu}, \tag{15}$$

which is compared to a threshold, V_{th}, to decide whether a cyclic frequency is present or not. When no cyclic frequency is present the values over $\boldsymbol{W}$ remain close to zero, as per definition of the SCF. Therefore, from (15) is understandable that for in case of a cyclic frequency, the standard deviation will significantly increase the value of I, since the mean will be less sensitive to this outlier. When cyclic frequencies are absent in $\boldsymbol{W}$, the value of I is consistent throughout the windows and relates the mean and variance of the χ^2 distribution of $\boldsymbol{W}$. $\boldsymbol{W}$ is χ^2 distributed, due to the absolute square (magnitude) operation. For a more robust approach, a goodness of fit to the χ^2 distribution should be done [17]. When the test fails, no cyclic frequency should be present in $\boldsymbol{W}$.

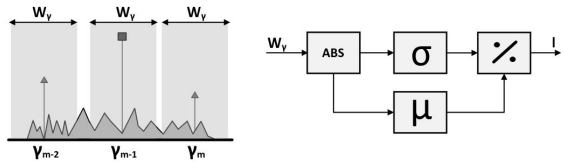


Fig. 3. Algorithm's window (left) and detector's diagram block (right).

D. Decision process

The detection mechanism is used to test the presence of certain cyclic frequencies in sets $\mathcal{A}$ and $\mathcal{B}$. This information is used by a K out of M detector [18] to point out whether a CDMA or an OFDM signal is present or not. Since some of the cyclic frequencies might overlap, as it is the case in this work, the detection is performed over two stages. Therefore, the decision about whether a signal is present or not is taken following the flow chart in Fig. 4, where the following definitions have been used:

$$\mathcal{H}_{1.1} = \begin{cases} \text{CDMA and OFDM with AWGN} \\ z(t) = x(t) + y(t) + n(t), \end{cases} \tag{16}$$

$$\mathcal{H}_{1.2} = \begin{cases} \text{CDMA with AWGN,} \\ z(t) = x(t) + n(t), \end{cases} \tag{17}$$

$$\mathcal{H}_{1.3} = \begin{cases} \text{OFDM with AWGN,} \\ z(t) = y(t) + n(t), \end{cases} \tag{18}$$

$$\mathcal{H}_{0} = \begin{cases} \text{AWGN only,} \\ z(t) = n(t), \end{cases} \tag{19}$$

the decision of whether a signal is present and the sub-sequent positioning options is done by the process in Fig. 4.

In more detail, a CDMA signal is present if no OFDM cyclic frequencies are detected in the set $\mathcal{B} - (\mathcal{B} \cap \mathcal{A})$. If cyclic frequencies are observed in such a set it means that an OFDM signal is also present in the mixture. However, both signals are only present if K cyclic frequencies from both $\mathcal{B}$ and $\mathcal{A}$ are detected.

In this approach, it is not possible to look only at the exclusive set of CDMA cyclic frequencies, since the set $\mathcal{A} - (\mathcal{B} \cap \mathcal{A})$ is an empty set.

E. Hybridisation algorithm

Time of arrival (TOA) positioning methods became quite popular in the navigation field due to several systems, such as the global positioning service (GPS), however their main disavantage is the requirement of a synchronised network. For example, for GNSS the satellites are synchronised through the ground control stations and the receiver clock offset is estimated along with the position estimates. In mobile telecommunications systems, the synchronisation is provided by the control at the base stations.

In this paper, an approximate maximum likelihood (AML) approach is used to solve a 2D position estimate of a receiver [19]. Lack of synchronisation is assumed among CDMA and

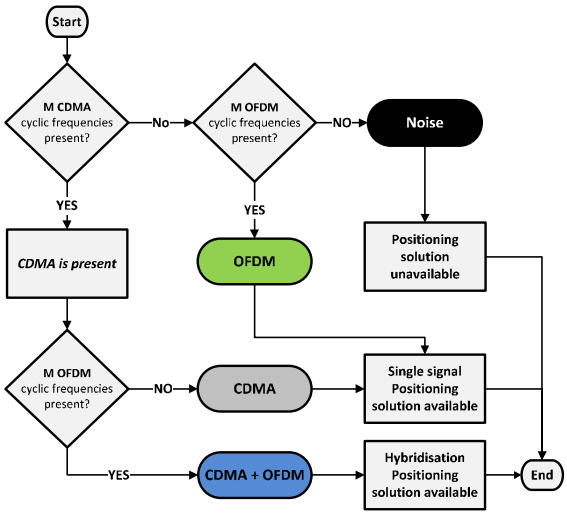


Fig. 4. Cognitive positioning algorithm with SCF-based detection.

OFDM emitters, but each emitter of the same technology is assumed to be synchronised. In addition, CDMA and OFDM measurements are considered to have different levels of quality, with OFDM leading to more noise time-delay estimates.

Assuming the presence of N_E emitters, E, the distance, r_i, between them and the receiver is given by,

$$r_i = \sqrt{x - x_i)^2 + (y - y_i)^2},\ i = 1, 2, ..., N_E. \tag{20}$$

The measured distances are given by,

$$l_i = r_i + \varepsilon_i, i = 1, 2, ..., N_E \tag{21}$$

where, ε, represents the timing errors associated with the underlying signal used to compute the pseudoranges l_i. Therefore, the magnitude of ε is set from a normal distribution with zero mean mean and variances σ_{CDMA} and σ_{OFDM}, depending on whether a CDMA or an OFDM signal is used. TOA estimators with CDMA offer better performance than TOA estimators with OFDM, thus the assumption of $\sigma_{OFDM} > \sigma_{CDMA}$ [20]. Nevertheless, this is not a requirement for the algorithm to work. The essential is that different signals will have different noise variances.

A TOA vector, $\boldsymbol{T}$, can be obtained by diving (21) by the speed of the medium, v, resulting in,

$$\boldsymbol{T} = \frac{\boldsymbol{r}}{v} + \frac{\boldsymbol{\varepsilon}}{v} = \boldsymbol{T}^0 + \boldsymbol{\varepsilon}, \tag{22}$$

where,

$$\boldsymbol{r} = [r_1, ..., r_{N_E}]^T = \boldsymbol{r}(\boldsymbol{\Theta}),\ \boldsymbol{\Theta} = [x, y], \tag{23}$$

and

$$\boldsymbol{\varepsilon} = [\varepsilon_1, ..., \varepsilon_{N_E}]^T. \tag{24}$$

The conditional probability density function of $\boldsymbol{T}$ given $\boldsymbol{\Theta}$ is given by,

$$f(\boldsymbol{T}|\boldsymbol{\Theta}) = (2\pi)^{-\frac{N_E}{2}} (\det \boldsymbol{Q})^{-1/2} \exp\left\{-\frac{J}{2}\right\}, \tag{25}$$

where,

$$J = \left[\boldsymbol{T} - \frac{\boldsymbol{r}(\boldsymbol{\Theta})}{v}\right]^T \boldsymbol{Q}^{-1} \left[\boldsymbol{T} - \frac{\boldsymbol{r}(\boldsymbol{\Theta})}{v}\right], \tag{26}$$

and

$$\boldsymbol{Q} = \mathbb{E}[\boldsymbol{\varepsilon}\boldsymbol{\varepsilon}^T] = \text{diag}[\sigma_1 \cdots \sigma_{N_E}]. \tag{27}$$

The maximum likelihood estimate of the receiver position is the Θ that minimises J [19], which can be obtained as follows,

$$\begin{aligned} &\boldsymbol{A}\boldsymbol{\Theta} = \boldsymbol{b} \Leftrightarrow \\ \Leftrightarrow &2 \begin{bmatrix} \sum g_i x_i & \sum g_i y_i \\ \sum h_i x_i & \sum h_i y_i \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \sum g_i (s + K_i - l_i^2) \\ \sum h_i (s + K_i - l_i^2) \end{bmatrix}, \end{aligned} \tag{28}$$

where,

$$s = \quad x^2 + y^2, \qquad K_i = x_i^2 + y_i^2, \tag{29}$$

$$g_i = \frac{x - x_i}{\sigma_i^2 r_i (r_i + l_i)},\ h_i = \frac{y - y_i}{\sigma_i^2 r_i (r_i + l_i)}, \tag{30}$$

with (x, y) the receiver estimated location and (x_i, y_i) the location of each emitter.

In an AML algorithm, there is at least one $\boldsymbol{\Theta}$ which corresponds to the minimum value of J. For that reason, the AML can provide a position estimate when only two measurements are available. The lack of synchronisation leads to a wider uncertainty region. However, in this paper, the problem is solved by computing the value of J for the entire grid. The global minimum and a local minimum closest to the mean location of the emitters is used to compare the performance of estimation of $\boldsymbol{\Theta}$. This offers a baseline of how good the AML can performe, when iteratively solving 28.

II. Results

Table I provides the most relevant parameters used throughout the simulations. The SCF was estimated using the fast Fourier transform accumulation method (FAM) [11], [21].

A. Probability of detection

Fig. 5 shows the probability of detection for OFDM signals versus the signal to noise ratio (SNR), considered as the ratio between signal and noise powers.

Fig. 5 compares hypotheses $\mathcal{H}_{1.1}$ through $\mathcal{H}_{1.3}$. The probability is obtained by counting how many times K, $K = 5$, cyclic frequencies are observed in the SCF, for each simulation iteration. The total number of simulation iterations is present in Table I. The noise-only case has been omitted since its probability is close to zero.

Similar results have been obtained for CDMA signal detection, the only observed exception was that the CDMA signal curves start at a lower SNR level (-3 dB).

B. Positioning performance

Table II and Table III provide results on the expected performance of the proposed architecture. These tables contain the root mean square error (RMSE) over 10^4 iterations in a

TABLE I
SIMULATION PARAMETERS

Common parameters	
Number of random trials, T	5000
Activity threshold, V_{th}	0.75
Observation time	2 ms
Cyclic resolution, $\Delta\alpha$	0.5 μHz
Window length, ϵ	$100\Delta\alpha$
Frequency resolution	0.1 Hz
Sampling frequency, f_s	40 MHz
Receiver filter bandwith, B_T	20 MHz
CDMA parameters (IEEE 802.11b)	
Modulation	DQPSK
Chip rate, f_c	11 MHz
Data rate, f_b	2 MHz
Spreading Sequence	Barker code (11 chips), [22], [23]
OFDM parameters	
Modulation	16-QAM
Number of carriers, N	64
Symbol period, T_{symbol}	4 μs
Sub-carrier spacing, Δ_f	$B/N = 312.5$ kHz
Guard interval, T_{gi}	$\Delta_f^{-1}/4$ s
Useful symbol period, T_U	Δ_f^{-1} s
Pilot power boost	+3 dB [24]
Bandwith	20 MHz

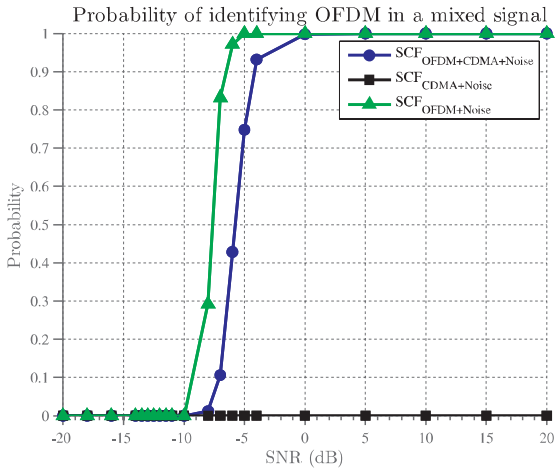


Fig. 5. Probability of detection under $\mathcal{H}_{1.1} - \mathcal{H}_{1.3}$.

25 by 25 m square room. In every iteration the emitters and user positions were obtained from an uniform distribution. To simplify the problem, it was considered that the CDMA and OFDM sytems were synchronised among each other, but a clock bias to the receiver is still present. This bias was assumed to be bigger for OFDM emitters. The position estimate is taken in Table II as the global minimum and in Table II as the local minimum closest to the mean location of the emitters.

In both tables, the addition of more emitters, in general, leads to an accuracy improvement, eg, over the diagonal of the tables. In some cases, the addition of more emitters,

TABLE II
ROOT MEAN SQUARE ERROR FOR AML ALGORITHM, WITH $\sigma_{CDMA} = 1$ AND $\sigma_{OFDM} = 10$ OVER 10^4 RUNS INSIDE A 25×25 M GRID AND A CLOCK BIAS OF 2 AND 8 M RESPECTIVELY. GLOBAL MINIMUM CONSIDERED FOR THE POSITION ESTIMATE.

RMSE (m)	Number of OFDM emitters $N_{BS_{OFDM}}$						
		0	**1**	**2**	**3**	**4**	**5**
Number of CDMA emitters $N_{BS_{CDMA}}$	**0**	-	-	11.82	10.97	10.26	9.74
	1	-	**9.56**	8.56	7.96	7.78	7.51
	2	**5.90**	**5.82**	**5.53**	**5.47**	**5.47**	**5.54**
	3	3.60	3.85	4.00	**4.10**	4.19	4.21
	4	**2.95**	**3.12**	**3.31**	**3.38**	**3.52**	**3.63**
	5	2.70	2.83	2.95	3.05	3.17	**3.31**

TABLE III
ROOT MEAN SQUARE ERROR FOR AML ALGORITHM, WITH $\sigma_{CDMA} = 1$ AND $\sigma_{OFDM} = 10$ OVER 10^4 RUNS INSIDE A 25×25 M GRID AND A CLOCK BIAS OF 2 AND 8 M RESPECTIVELY. MINIMUM TAKEN AS THE CLOSEST TO THE MEAN BASE STATIONS POSITIONS

RMSE (m)	Number of OFDM emitters $N_{BS_{OFDM}}$						
		0	**1**	**2**	**3**	**4**	**5**
Number of CDMA emitters $N_{BS_{CDMA}}$	**0**	-	-	10.78	9.72	8.85	8.23
	1	-	**7.37**	7.32	6.68	6.33	5.97
	2	**5.74**	**4.91**	**4.56**	**4.37**	**4.30**	**4.27**
	3	3.31	3.22	3.15	**3.13**	3.15	3.15
	4	**2.46**	**2.42**	**2.50**	**2.50**	**2.56**	2.60
	5	2.08	2.12	2.17	2.18	2.24	**2.33**

especially with noisy OFDM emitters, seems to lead to a higher RMSE (see the values along the diagonal of the tables). However, most of these differences are quite small, which means it is safe to assume that by adding more noisy emitters the performance should improve or remain approximately the same.

III. CONCLUSION

This paper proposes a cognitive positioning architecture for CDMA and OFDM signals. The architecture relies on a spectrum sensing block to detect the presence of CDMA and OFDM signals in the surrounding spectrum. The proposal suggests the use of cyclostationary algorithms to distinguish the signals present in an unique digital representation. The paper provides results that show how such signals could be distinguished, by suggesting a simple detection and decision algorithm. This detection would be useful to activate only the required acquisition loops, allowing the receiver to save energy and computational resources.

After a successful characterisation of the spectral contents, the cognitive positioning system utilises this information to extract from the signals timing information to compute TOA measurements. After that, assuming the locations of the emitters to be known, an AML algorithm combines the information from several SoO emitters. The performance of the algorithm was studied by comparing the estimate obtained from the global minimum and the minimum closest to the mean location of the emitters over the entire grid space.

In the end, the goal of this architecture is to use the cognition layers appearing in future communications standards

and use this information to improve user positioning and resource management of the mobile devices.

ACKNOWLEDGMENT

This work was financially supported by EU FP7 Marie Curie Initial Training Network MULTI-POS (Multi-technology Positioning Professionals) under grant nr. 316528.

The authors express their gratitude to the Academy of Finland (project 256175 "Cognitive Approaches for Location in Mobile Environments") for its additional financial support for this research work.

REFERENCES

[1] J. Mitola and G. Maguire, "Cognitive Radio: Making Software Radios More Personal," in *IEEE Pers. Commun.*, vol. 6, no. 4, 1999, pp. 13–18.

[2] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surv. Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[3] H. Celebi and I. Guvenc, "Cognitive-radio Systems for Spectrum, Location, and Environmental Awareness," *IEEE Antennas Propag. Mag.*, vol. 52, no. 4, pp. 41–61, 2010.

[4] C.-I. Badoi, N. Prasad, V. Croitoru, and R. Prasad, "5G Based on Cognitive Radio," *Wirel. Pers. Commun.*, vol. 57, no. 3, pp. 441–464, Jul. 2010.

[5] H. Celebi and H. Arslan, "Utilization of Location Information in Cognitive Wireless Networks," *IEEE Wirel. Commun.*, no. August, pp. 6–13, 2007.

[6] E. S. Lohan, J. Lundén, G. Seco-Granados, V. Koivunen, T. Potential, W. A. Cognitive, and P. Framework, "Cyclic frequencies of GNSS signals and their potential within a cognitive positioning framework," *ION J. Navig.*, 2013.

[7] R. Exel, "Carrier-based ranging in IEEE 802.11 wireless local area networks," in *2013 IEEE Wirel. Commun. Netw. Conf.* IEEE, Apr. 2013, pp. 1073–1078.

[8] M. Shafiee, "WiFi-based Fine Timing Assistance for GPS Acquisition," http://theses.ucalgary.ca/handle/11023/1101, 2013.

[9] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Trans. Syst. Man Cybern.*, vol. 37, no. 6, pp. 1067–1080, 2007.

[10] D. Zhang, F. Xia, and Z. Yang, "Localization technologies for indoor human tracking," in *Int. Conf. Futur. Inf. Technol.*, no. 60903153, Busan, 2010. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5482731

[11] W. A. Gardner, A. Napolitano, and L. Paura, "Cyclostationarity: Half a Century of Research," *Signal Processing*, vol. 86, no. 4, pp. 639–697, Apr. 2006.

[12] T. Fusco, L. Izzo, A. Napolitano, and M. Tanda, "On the second-order cyclostationarity properties of long-code DS-SS signals," *IEEE Trans. Commun.*, vol. 54, no. 10, pp. 1741–1746, Oct. 2006.

[13] P. Sutton, K. Nolan, and L. Doyle, "Cyclostationary Signatures in Practical Cognitive Radio Applications," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 13–24, Jan. 2008.

[14] J. Lunden and V. Koivunen, "Spectrum Sensing in Cognitive Radios Based on Multiple Cyclic Frequencies," in *Cogn. Radio Oriented Wirel. Networks Commun.*, 2007.

[15] E. Guenterberg, H. Ghasemzadeh, R. Jafari, and R. Bajcsy, "A Segmentation Technique Based on Standard Deviation in Body Sensor Networks," in *Eng. Med. Biol. Work.*, 2007.

[16] A. Benbasat and J. Paradiso, "An Inertial Measurement Framework for Gesture Recognition and Applications," in *Gesture Sign Lang. Human-Computer Interact.*, 2002.

[17] H. O. Lancaster and E. Seneta, *Chi-Square Distribution*. John Wiley & Sons, Ltd, 2005. [Online]. Available: http://dx.doi.org/10.1002/0470011815.b2a15018

[18] P. Williams, "Evaluating the state probabilities of M out of N sliding window detectors," http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA348378, DSTO Aeronautical and Maritime Research Laboratory, Tech. Rep., 1998.

[19] Y. Chan, "Exact and approximate maximum likelihood localization algorithms," *IEEE Trans. Veh. Technol.*, vol. 55, no. 1, pp. 10–16, 2006. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1583909

[20] H. Sayed, A. Tarighat, and N. Khajehnouri, "Network-Based Wireless Location," *IEEE Signal Process. Mag.*, no. July 2005, pp. 24–40, 2005.

[21] R. Roberts, W. Brown, and H. Loomis, "Computationally Efficient Algorithms for Cyclic Spectral Analysis," *Signal Process. Mag. IEEE*, 1991.

[22] L. A. N. Man, S. Committee, and I. Computer, *Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications IEEE Computer Society*, 2012, vol. 2012, no. March.

[23] T. Lee and A. Al-Banna, "Spectral Signatures and Interference of 802.11 Wi-Fi Signals with Barker Code Spreading," *New Front. Dyn. Spectr. Access Networks*, no. 1, pp. 672–675, 2005.

[24] S. R. Schnur, "Identification and Classification of OFDM Based Signals Usng Preamble Correlaton and Cyclostationary Feature Extraction," Master thesis, Naval Postgraduate School, 2009.

Publication 3

P. Figueiredo e Silva, A. Basiri, E.S. Lohan, J. Pinchin, C. Hill, T. Moore,, 'On the Impact of Intra-System Interference for Ranging and Positioning with Bluetooth Low Energy," in *Proceedings of the 23rd International Conference on Advances in Geographic Information Systems (ACM SIGSPATIAL)*, Seattle, WA, USA, ©November 2015 https://10.1145/2830571.2830573

On the Impact of Intra-System Interference for Ranging and Positioning with Bluetooth Low Energy

Pedro Figueiredo e Silva
Dpt. of Electronics and Comm. Eng.
Tampere University of Technology
Tampere, Finland
pedro.silva@tut.fi

Anahid Basiri
The University of Nottingham,
The United Kingdom
anahid.basiri@nottingham.ac.uk

Elena Simona Lohan
Dpt. of Electronics and Comm. Eng.
Tampere University of Technology
Tampere, Finland
elena-simona.lohan@tut.fi

James Pinchin
The University of Nottingham,
The United Kingdom
james.pinchin@nottingham.ac.uk

Chris Hill
The University of Nottingham,
The United Kingdom
chris.hill@nottingham.ac.uk

Terry Moore
The University of Nottingham,
The United Kingdom
terry.moore@nottingham.ac.uk

ABSTRACT

This paper focuses on the study of intra-system interference for ranging and positioning applications using Bluetooth Low Energy (BLE). While BLE tries to avoid interference with other protocols in the same frequency band, such as Wi-Fi, the intra-system interference is unavoidable, either due to multipath or simultaneous transmissions in the same channel. This study shows that intra-system interference contributes with a deviation of approximately 5 dBm in the Received Signal Strength (RSS) and by taking this into account the ranging and positioning accuracy can be significantly improved. The study uses data collected from two different environments.

Categories and Subject Descriptors

D.2.1.3 [**Reusable Software**]: Reuse models

Keywords

Bluetooth Low Energy (BLE), Received Signal Strength (RSS), Interference, Indoor Positioning

1. INTRODUCTION

The Global Navigation Satellite System (GNSS) is the most widely-used positioning technology for outdoor use, however in deep urban canyons and indoor environments GNSS may fail to provide the positioning service due to stronger multipath, signal attenuation and blockage [7, 8]. In these environments other opportunistic signals, such as Wi-Fi are commonly used for positioning. However, in addition to the privacy concerns and the high power consumption, the positioning accuracy provided by Wi-Fi is highly correlated with the density of Wi-Fi access points. Hence, indoor localization is still a big challenge for many Location Based Services (LBS) applications, such as emergency and safety, navigation and tracking [3].

Lately, BLE has been enabling several indoor LBS applications thanks to its low power consumption and cheap hardware. Its popularity is growing, particularly where beacons are being deployed throughout the environment, to broadcast location specific information. These beacons are the BLE devices, most of the times, operating with batteries with a life span of months or even years, depending on its duty cycle. However, the major disadvantage of the BLE is the operation in the crowded 2.4 GHz band [2], where other systems, such as Wi-Fi, interfere with the BLE signals. Besides the interference from other systems, the number of available channels for the operation of BLE signals is limited. This limit is particularly small when the devices are operating in the advertisement mode, where 3 channels are available for broadcasting the advertisement packets. This is the case for BLE beacons. For that reason, this study investigates the interference caused by other beacons and its impact on received signal strength applications.

2. BLUETOOTH LOW ENERGY

BLE is designed for lower power operation, low complexity and cost. BLE devices operate according to several profiles defined by the Bluetooth SIG. These define how a device behaves in a particular application, e.g. the heart rate monitor or the battery level indicator. The Generic Attribute Profile (GATT) is a common profile adopted by the majority of BLE applications allowing them to receive and send short pieces of data, known as attributes, over a BLE link. These profiles are used to define specific protocols on top of it, such as Apple's iBeacon [1, 2].

For medium access, BLE relies on Adaptive Frequency Hopping (AFH) to avoid interference from other systems, for example, Wi-Fi, operating in the same frequency band [1].

DOI: http://dx.doi.org/10.1145/2830571.2830573
MELT '15, November 03-06, 2015, Bellevue, WA, USA

BLE operates over forty channels, with a 2 MHz bandwidth, three of which are being reserved for advertisement packets, for device discovery and connection establishment purposes. While a BLE device can operate under several modes, however this paper is focus on the unconnected mode. In this mode, the BLE devices are operating, exclusively, over three advertisement channels. While in a connected mode, the devices would use the advertisement channel for discovery and to establish connection, with the remaining channels being used for data exchange.

Even though AFH minimises the interference to other systems, it cannot guarantee the lack of interference from other Bluetooth devices. This would be more critical if the BLE devices operate solely in advertisement mode, as the number of channels is reduced to three, as it increases the likelihood of picking a channel where another beacon is already sending an advertisement packet. These three channels are located at 2.402, 2.426 and 2.480 GHz.

As reported in [4], for s BLE devices operating solely in the advertisement mode and sharing n advertisement channels, the probability that at a given time t the given channel will be occupied will be given by,

$$\mathrm{P} = 1 - \left(\frac{n-1}{n}\right)^{(s-1)}. \quad (1)$$

For $n = 3$ there is a 56% chance of picking a channel that is occupied by another BLE beacon and with $n = 8$ the probability increases to 94%. However, this assumes a simplified scenario where the devices are synchronised with each other and the time between jumps is considered to be the same. however in real world applications, the random delays in the hopping structure can reduce this probability, but in a massive deployment of such devices, interference between each other will inevitability happen.

3. PATH LOSS MODELS

This study uses two path loss models, the ITU-R model defined as,

$$\mathrm{P_r}(d) = \mathrm{P_t} + \mathrm{C} - 20\log_{10}\left(\frac{4\pi f}{c}\right) - 20\eta\log_{10}(d) + v \quad (2)$$

and the log distance model described by,

$$\mathrm{P_r}(d) = \mathrm{P_r}(\mathrm{d_0}) - 10\eta\log_{10}\left(\frac{d}{\mathrm{d_0}}\right) + w, \quad (3)$$

where $\mathrm{P_r}(d)$ is the RSS at a given distance d in meters, $\mathrm{P_t}$ the transmission power, f the operating frequency in Hertz, η is a constant that models additional losses in the path of the signal, $v, w \sim \log(\mathrm{N}(0, \sigma^2))$, are log-normal distributed random variable which model the slow fading phenomenon.

Both models offer an equivalent interpretation to the expected RSS at a given distance, but the ITU-R tries to take into account all the losses in the signal's path, while the log distance model, assumes an apparent transmission power, $\mathrm{P_r}(\mathrm{d_0})$, at a reference distance, $\mathrm{d_0}$. For that reason, the meaning of η differs in both models. For the ITU-R model, this parameter must be bigger than 1, since that represents the free space propagation. For the log distance model, this value has to be bigger than 0. Therefore, C is a constant that models additional system losses for the ITU-R model, while in the log distance model, it is lumped together with the apparent power.

Both models are used to fit measurement data obtained at Tampere University of Technology in Finland and at University of Nottingham in the UK. The beacons were deployed on regular grids over a corridor and over a table in a closed office room. For the first one, 8 beacons were deployed every 1.5 m from each other and from the floor, while for the later one, a single beacon was deployed at several distances from the receiver; 0.10, 0.5, 1, 1.5, 2, 2.5 and 3 meters from the receiver. The data from the beacons were captured using a laptop running Ubuntu 14.04. The beacons were manufactured by Kontakt.io and left at their default transmission power (-12 dBm) [5].

Using the models (2) and (3), tables 1 and 2 show the root mean square error (RMSE) for each environment and model. The RMSE is defined as,

$$\mathrm{RMSE} = \sqrt{\frac{\sum_{i=0}^{N}(y_{\mathrm{observed}}^{(i)} - y_{\mathrm{expected}}^{(i)})^2}{N}},\ N > 0 \quad (4)$$

where $y_{\mathrm{observed}}^{(i)}$ is taken as the mean of the measurements and $y_{\mathrm{expected}}^{(i)}$ the value obtained through the fitted path loss model.

In both tables the columns contain the RMSE for the log distance model and the ITU-R model. However, since the BLE beacons report the apparent power, the log distance column is divide in two. In the first column, the reported apparent power of -77 dBm is used in (3), while the second column shows the results when the apparent power in (3) is set to -79.73 dBm. This value is the measured mean RSS value, over 1 hour, for a single beacon (beacon 3) at 1 meter distance.

Table 1: Fit of the two models for the measurement data obtained in Finland

Distance (m)	RMSE (dBm)		
	log dist		ITU-R
	$\mathrm{P_r}(\mathrm{d_0}) = -77$dBm $\eta = 1.02$	$\mathrm{P_r}(\mathrm{d_0}) = -79.73$dBm $\eta = 0.98$	$\mathrm{C} = -24.76$ $\eta = 1.08$
0.50	0.95	1.87	4.60
1.00	3.59	0.87	3.78
1.50	8.57	5.91	6.74
2.00	7.69	5.07	4.42
2.50	8.95	6.37	4.58
3.00	5.33	2.78	0.05
Mean	**5.85**	**3.81**	**4.03**

Table 2: Fit of the two models for the measurement data obtained in the UK.

Distance (m)	RMSE (dBm)					
	log dist				ITU-R	
	$\mathrm{P_r}(\mathrm{d_0}) = -77$ dBm $\eta = 0.99$ beacons = 8	$\mathrm{P_r}(\mathrm{d_0}) = -77$ dBm $\eta = 0.97$ beacons = 1	$\mathrm{P_r}(\mathrm{d_0}) = -79.73$ dBm $\eta = 0.94$ beacons = 8	$\mathrm{P_r}(\mathrm{d_0}) = -79.73$ dBm $\eta = 0.96$ beacons = 1	$\mathrm{C} = -15.96$ $\eta = 1.09$ beacons = 8	$\mathrm{C} = -19.28$ $\eta = 1.00$ beacons = 1
1.39	1.15	2.48	1.40	5.04	4.05	2.06
1.90	3.19	3.08	5.87	5.76	4.07	1.09
3.22	2.23	2.06	0.39	4.70	7.87	0.71
Mean	**2.19**	**2.54**	**2.55**	**5.17**	**5.33**	**1.29**

Table 1 compares the fit of the log distance model and ITU-R model for the office room, where a single beacon (beacon 3) RSS was measured at several distances for periods of 30 minutes. The overall RMSE is the smallest for the log distance model with the estimated apparent power. With the ITU-R the overall RMSE is approximately the same and the worst fit happens when the apparent power is set to the reported value.

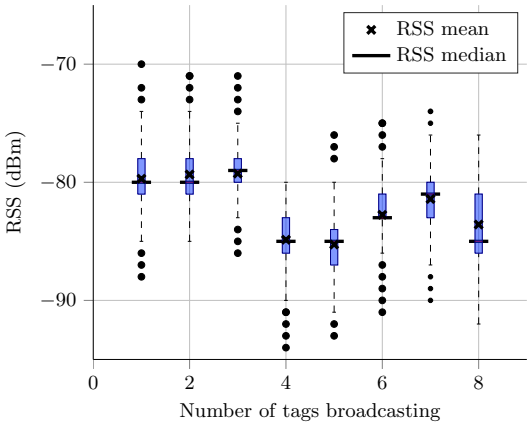


Figure 1: RSS values for beacon 3 at 1 meter versus the number of beacons broadcasting.

Table 2 shows the results in the office corridor, where data was collected for periods of 15 minutes in three different points. The acquisition was done with 1 and 8 beacons in advertisement mode. In contrast with office scenario, here, the log distance model with the reported apparent power is now the one with the lowest overall RMSE. While the fit with the log distance still offers an accurate fit for the case where 8 beacons are transmitting, it is quite poor when solely one is transmitting. On the other hand the ITU-R error for only one beacon is low, approximately 1 dBm error.

To understand the impact of other beacons on the RSS value of a single beacon, Fig. 1 shows the statistics for the RSS of beacon 3 when up to 7 other beacons are spread around it. The 7 other beacons are regularly spaced on a half meter grid around it and the observations lasted over 3 hours.

From Fig. 1 there seems to be no relevant degradation of the signal up to the presence of three beacons. Above this number, i.e. 3, the mean value drops by 4 dBm. With 4, 5 and 8 beacons broadcasting simultaneously, the mean and median values are approximately 5 dBm lower than for cases 1, 2 and 3. With 6 and 7 beacons broadcasting there are changes of 3 dBm and 1 dBm in the metrics, respectively. More interestingly, with 3 simultaneous beacons, the value is increased by 1 dBm, which is probably due to channel phenomena specific to that observation period. Therefore, with more than 3 beacons on advertisement mode, there is a degradation of the RSS that can reach up to 5 dBm.

Application for ranging and positioning

Many applications of the indoor positioning, such as creation of probabilistic fingerprint databases, can benefit from accurate path loss models. Since BLE, unlike Wi-Fi, can report the transmit power, rather than a manufacturer dependent indicator, such models can calculate the distance by solving (2) and (3) with the values of the observed RSS. Fig. 2 shows the distance from the beacon to the receiver in the closed office environment, using (2) and (3). The input to the model is an averaged RSS value with the last observed 2 seconds. With the addition of more beacons there is a

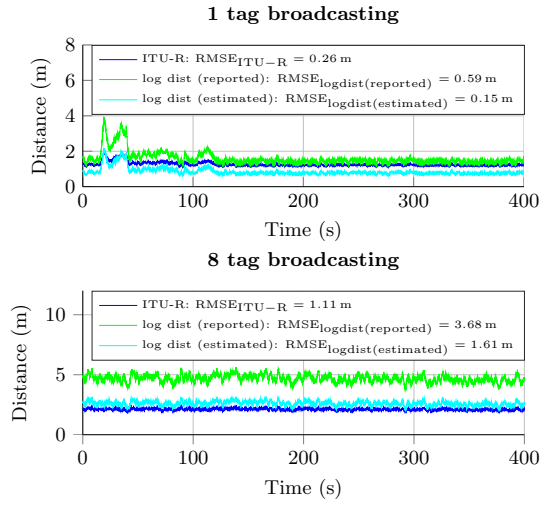


Figure 2: Ranging to beacon 3 with 1 and 8 beacons broadcasting.

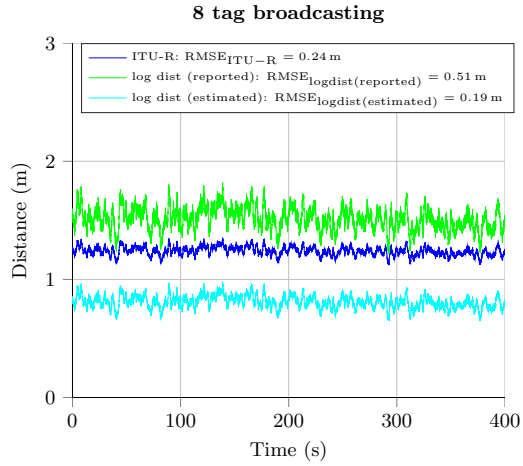


Figure 3: Ranging to beacon 3 with 8 beacons broadcasting and interference offset added to model.

significant impact in the RMSE for each model. With a single beacon broadcasting all the models achieve a sub meter level accuracy, while the opposite is true when all 8 beacons are broadcasting, increasing the RMSE significantly. Of particular interest is the degradation of the RMSE of the log distance model with the reported apparent power level by the beacons. Its RMSE increases by more than 3 m while the RMSE for the other models increases, approximately, by one meter.

However, if the interference contribution is taken into account by summing to the left side of (2) and (3) an addition term I = -5 dBm, the accuracy of the ranging approximates

the one observed when a single beacon is broadcasting, as seen in Fig. 3.

For positioning applications there are more challenges to tackle, since the lack of line of sight will reduce the RSS further, for example due to people and environment objects [6]. For example, in this study, the data was collected in the UK during off hours, with the receiver set at the beginning of corridor (A), middle of the corridor (B) and end of the corridor (C). The position of the receiver is obtained by solving and minimizing the following non linear equation for each beacon,

$$\sqrt{(x^{(i)}_{\text{beacon}} - \hat{x})^2 + (y^{(i)}_{\text{beacon}} - \hat{y}) + (z^{(i)}_{\text{beacon}} - \hat{z})} - L^{(i)}_{\text{beacon}} = 0 \quad (5)$$

where $(x^{(i)}_{\text{beacon}}, y^{(i)}_{\text{beacon}}, z^{(i)}_{\text{beacon}})$ are the known coordinates to the i-th beacon, $(\hat{x}, \hat{y}, \hat{z})$ the unknown receiver position and $L^{(i)}_{\text{beacon}}$ the distance to the i-th beacon obtained through the path loss model.

Table 3 contains the RMSE of the positioning in 2D (assuming the height is known) and 3D of the receiver's location, using ranges to the 8 available beacons. These results are a mean over 1000 observations. With no surprise, the RMSE values are better in most cases for the 2D positioning, however the difference between them is almost none in some cases, for example, at point B the results are quite the same in both scenarios. The overall performance, mean of the three points, (last column) for 3D is quite similar for the ITU-R model and the log distance using the estimated apparent power. With the log distance model using the reported apparent power, the performance increases by 70%, with the RMSE decreasing from 1.7 m to 1 m. For the 2D case, the best performance is still achieved by the log distance model using the reported apparent power, but now the performance is slightly worse when using the ITU-R model.

With the introduction of the interference offset in the models, the overall accuracy improves significantly by more than 50% in some cases, for either a positioning in 3D or 2D. This also shows, that the estimated interference offset can be calibrated in a different scenario from where it is used.

Table 3: RMSE (m) values for 2D and 3D positioning in the office corridor at the UK.

	Model	RMSE_{A} (m)	RMSE_{B} (m)	RMSE_{C} (m)	$\text{RMSE}_{\text{Modelmean}}$ (m)
3D	ITU-R	1.82	2.14	1.30	1.75
	$\log \text{dist}_{\text{rep.}}$	1.35	1.18	0.60	1.04
	$\log \text{dist}_{\text{est.}}$	1.95	2.18	0.95	1.69
2D	ITU-R	1.75	2.07	1.19	1.67
	$\log \text{dist}_{\text{rep.}}$	1.52	1.24	0.22	0.99
	$\log \text{dist}_{\text{est.}}$	1.61	2.01	0.67	1.43
3D (interf. corrected)	ITU-R	1.20	1.21	1.35	1.25
	$\log \text{dist}_{\text{rep.}}$	0.47	0.57	0.57	0.54
	$\log \text{dist}_{\text{est.}}$	0.79	1.05	1.32	1.05
2D (interf. corrected)	ITU-R	1.21	1.20	1.31	1.25
	$\log \text{dist}_{\text{rep.}}$	0.47	0.57	0.57	0.53
	$\log \text{dist}_{\text{est.}}$	0.79	1.06	1.32	1.06

4. CONCLUSION

This paper focuses on the study of the signal behaviour for BLE devices, under two office environments. The study focuses on the interference caused between beacons in advertisement mode, where more than three beacons cause a deviation on the RSS of, approximately, 5 dBm.

In addition, this paper compares two path loss models to identify the best fit to the measured data. It was seen that the log distance model, using an apparent power equal to the one reported to the beacons, was performing better in most situations than the log distance model with an estimated apparent power and the ITU-R model. When applying the models for ranging purposes, it was possible to see that the ITU-R and the log distance model using an estimated apparent power were indeed performing better in a closed office scenario, particularly when all the 8 beacons were broadcasting. In the office corridor, where the ranges were used to position the reader, all the three models performed in a similar manner, but the log distance model using the reported apparent power, did manage to outperform the other two. It was also seen, that taking the 5 dBm offset into account leads to a better positioning and ranging performance in either of the scenarios.

In the end, this paper shows that intra-system interference has a negative effect in the observed RSS and path-loss dependent applications, such as ranging and positioning. This effect can be removed by taking it into account in the path loss models, which should hold across different scenarios. Future studies should focus on mechanisms to monitor and compensate for intra-system interference.

Acknowledgment

This work was financially supported by EU FP7 Marie Curie Initial Training Network MULTI-POS (Multi-technology Positioning Professionals) under grant nr. 316528. The authors express their gratitude to the Academy of Finland (project 250266 "Cognitive Approaches for Location in Mobile Environments") for its additional financial support for this research work.

Open Access

The data and scripts used for this study are available at https://goo.gl/GHlSbK, under a CC 4.0 license.

5. REFERENCES

[1] Bluetooth SIG. Specification of the Bluetooth System, 2014.

[2] J. DeCuir. Introducing Bluetooth Smart: Part I: A look at both classic and new technologies. *IEEE Consum. Electron. Mag.*, 3(1):12–18, Jan. 2014.

[3] Z. Deng, Y. Yu, X. Yuan, N. Wan, and L. Yang. Situation and development tendency of indoor positioning. *China Commun.*, 10(3):42–55, Mar. 2013.

[4] E. Geraniotis and M. Pursley. Error Probabilities for Slow-Frequency-Hopped Spread-Spectrum Multiple-Access Communications Over Fading Channels. *IEEE Trans. Commun.*, 30(5):996–1009, 1982.

[5] Kontakt.io. Kontakt.io Beacon Datasheet v2.0. Technical report, 2014.

[6] K. Liu. Signal processing techniques in network-aided positioning: a survey of state-of-the-art positioning designs. *IEEE Signal Process. Mag.*, 22(4):12–23, July 2005.

[7] C. Mensing, S. Sand, and a. Dammann. GNSS Positioning in Critical Scenarios: Hybrid Data Fusion with Communications Signals. *2009 IEEE Int. Conf. Commun. Work.*, (2):1–6, June 2009.

[8] G. Seco-Granados, J. A. López-Salcedo, D. Jiménez-Baños, and G. López-Risueño. Challenges in Indoor Global Navigation Satellite Systems. *IEEE Signal*, (February):108–131, 2012.

Publication 4

P. Figueiredo e Silva and E.S. Lohan, "Room-level indoor positioning with Wi-Fi and RFID fingerprints," in *Proceedings of the 23rd International Conference on Advances in Geographic Information Systems (ACM SIGSPATIAL)*, Seattle, WA, USA, ©November 2015 ACM https://10.1145/2830571.2830579

Room-level Indoor Positioning with Wi-Fi and RFID Fingerprints

Pedro Figueiredo e Silva
Dpt. of Electronics and Comm. Eng.
Tampere University of Technology
Tampere, Finland
pedro.silva@tut.fi

Elena Simona Lohan
Dpt. of Electronics and Comm. Eng.
Tampere University of Technology
Tampere, Finland
elena-simona.lohan@tut.fi

ABSTRACT

This paper shows the advantages and limitations of combining RFID and Wi-Fi technology for estimating the location of a user in an indoor environment. The paper relies on a simulated environment, with one or several RFID readers being deployed inside a room and several Wi-Fi devices spread, exclusively, around the surrounding area. The parameters of the simulated environment were drawn from a real measurements.

Categories and Subject Descriptors

D.2.m [**Software Engineering**]: Miscellaneous—*reusable software*

General Terms

Design, Performance, Theory

Keywords

Wi-Fi, RFID, fingerprinting

1. INTRODUCTION

This study considers RFID due to its popularity in various indoor scenarios, such as commuting hallways, office buildings, schools, hospitals, among others [2]. It is an attractive signal for indoor positioning and tracking, since it offers, contactless communication, non line-of-sight readability, compactness and low cost [3]. Passive elements are particularly attractive as they can be used to mark a wide range of objects, *e.g.*, clothes, but raise more privacy concerns. However, the coverage of this technology is, by definition, smaller than traditional Wi-Fi networks [4, 3, 2] as the information is carried in the back-scattered power.

The aim of this study is to understand how RFID emitters, deployed inside a room, improve the performance of a Wi-Fi based indoor positioning method taking into account low and high density Wi-Fi scenarios. In addition to this, the study offers advice for possible deployment of such system, regarding the best location for the RFID emitters and the environment where they should be deployed. Furthermore, the software developed for this study is available at [1].

MOBIQUITUOUS '15 Coimbra, Portugal

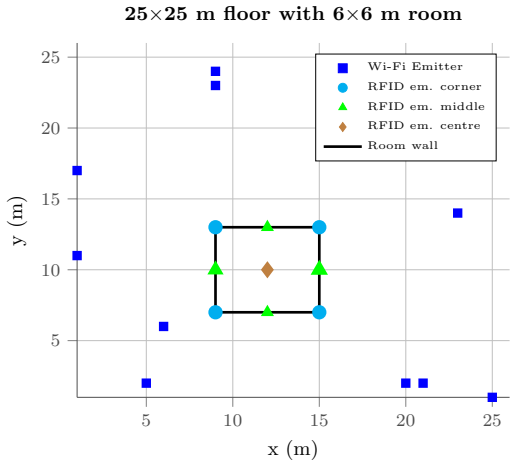


Figure 1: Simulated area and room.

2. SIMULATION DESCRIPTION

The simulation is done over a $M_1 \times N_1$ m area with a room of $M_2 \times N_2$ m randomly placed inside this area. In this simulation M_1 and N_1 were set to 25 m and M_2 and N_2 to 6 m. The simulation defines several user paths inside the room, where RFID emitters are deployed in different configurations, as shown in Fig. 1. The Wi-Fi emitters are exclusively deployed on the outside of the room, with a density according to the studies carried out in university buildings in Finland [7, 6]. For high density scenarios the number of Wi-Fi emitters was set to 24 and 8 for low density scenarios. The user movement follows a random walk [5] model with 1 meter fixed steps. For each scenario, the simulation defines 1000 paths of 100 steps in inside the room.

Regarding the RFID, the simulator assumes the user is wearing a passive tag, being tracked by the network. For this paper, up to four readers are deployed inside the room at specific locations. These readers are responsible for capturing the back-scattered power sent by the antenna or tag placed at the user. The tag can be placed, for example, directly in the garments of the user [2]. Afterwards, the

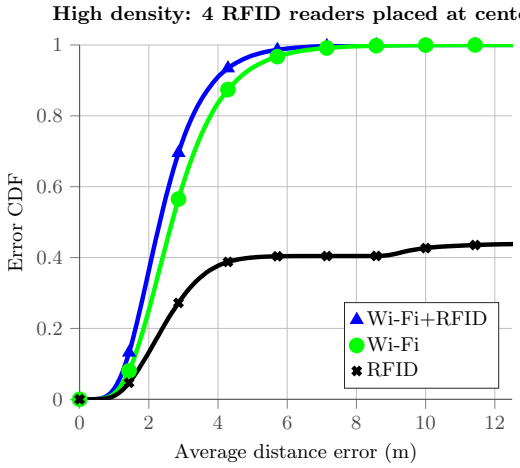


Figure 2: Average error probability using four RFID emitter configurations.

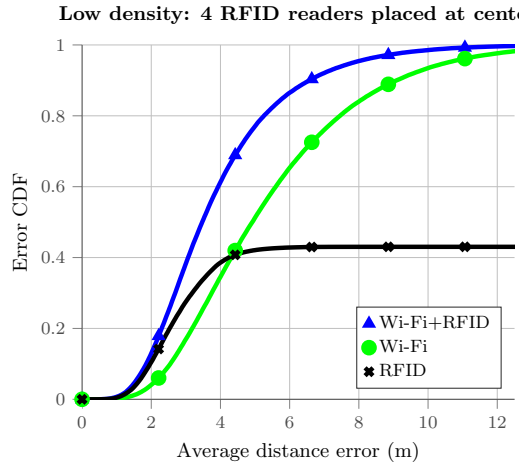


Figure 3: Average error probability using one RFID emitter configurations.

read values are communicated over a network with possible synchronization issues left out of this study. The backscatteredpower of RFID has been modeled according to the real-field measurement analysis in [2, 4, 3].

3. RESULTS AND CONCLUSIONS

In high density Wi-Fi environments (Fig. 2), the combination of Wi-Fi and RFID fingerprints leads to an estimation error below 4 m for 95% of the times when using Wi-Fi and RFID, compared to 85% of the times when only Wi-Fi is used. For low density Wi-Fi environments (Fig. 3), the presence of in-room emitters leads to a significant accuracy improvement. An estimation error below 4 m is reported 70% of the times when Wi-Fi and RFID are used, in comparison to 30% of the times when only Wi-Fi is used.

Hence, the deployment of RFID emitters for hybrid Wi-Fi-RFID localization is highly recommended in low density Wi-Fi environments (e.g., density below 1 emitter per 50 m^2), because, in such scenarios, the accuracy is expected to improve by 40%. Table 1 summarises the root mean square error for the several configurations considered over a larger number of environments. Also, while in the table the configuration with RFID only is showing better performance than Wi-FI for some scenarios, one should take into mind that the coverage area of the technology is smaller.

Table 1: Root mean square error per location for 50 low density scenarios

Location and number of RFID readers	Root mean square error (m)		
	Proposed Wi-Fi+RFID	Wi-Fi only	RFID only
Corner, 1	4.90	5.12	2.94
Middle, 1	4.59	5.09	7.70
Center, 1	4.61	5.16	6.21
Corner, 4	4.59	5.10	3.48
Middle, 4	3.39	5.09	4.19
Center, 4	3.45	5.14	3.57

Acknowledgment

The authors are thankful to the Academy of Finland (project 250266), EU (project 250266 "Cognitive Approaches for Location in Mobile Environments") and EU FP7 Marie Curie Initial Training Network MULTI-POS (Multi-technology Positioning Professionals) under grant nr. 316528 for the financial support of this work.

4. REFERENCES

[1] P. Figueiredo e Silva. An indoor positioning simulator, 2014. http://goo.gl/GHlSbK.

[2] M. Hasani, J. Talvitie, L. Sydanheimo, E. Lohan, and L. Ukkonen. Hybrid WLAN-RFID Indoor Localization Solution Utilizing Textile Tag. *IEEE Antennas Wirel. Propag. Lett.*, 2015.

[3] K. Koski, E. Koski, T. Bjorninen, A. A. Babar, L. Ukkonen, L. Sydanheimo, and Y. Rahmat-Samii. Practical read range evaluation of wearable embroidered UHF RFID tag. In *Proc. 2012 IEEE Int. Symp. Antennas Propag.*, July 2012.

[4] E. S. Lohan, K. Koski, J. Talvitie, and L. Ukkonen. WLAN and RFID Propagation channels for hybrid indoor positioning. In *Int. Conf. Localization GNSS 2014 (ICL-GNSS 2014)*, June 2014.

[5] D. Shiffman. *The Nature of Code*. Magic Book Project, 2012.

[6] S. Shrestha, J. Talvitie, and E. S. Lohan. Deconvolution-based indoor localization with WLAN signals and unknown access point locations. In *2013 13th Int. Conf. ITS Telecommun.*, Nov. 2013.

[7] S. Shrestha, J. Talvitie, and E. S. Lohan. On the fingerprints dynamics in WLAN indoor localization. In *2013 13th Int. Conf. ITS Telecommun.*, Nov. 2013.

Publication 5

P. Figueiredo e Silva and E.S. Lohan, "Performance Considerations for Positioning with Signals of Opportunity," in *IEEE Proc. of the International Conference on Localization and GNSS (ICL-GNSS 2016)*, Barcelona, Spain, June 2016. DOI: 10.1109/ICL-GNSS.2016.7533864

Performance Considerations for Positioning with Signals of Opportunity

Pedro Figueiredo e Silva and Elena Simona-Lohan
Department of Electronics and Communications Engineering, Tampere University of Technology, Finland
{pedro.silva, elena-simona.lohan}@tut.fi

***Abstract*—This paper presents a study on the benefit of observing several signals of opportunity for positioning purposes. Several static emitters are placed over a defined area where an user is moving and acquiring measurements to each of these emitters. The simulation considers that the user is capable of acquiring time of arrival measurements from several wireless protocols, such as WCDMA, 802.11b, 802.11g and 802.11ac. The variance in the measurements is modelled through the Crámer-Rao bound and a propagation model for each technology. As conclusions, this paper discusses the benefits of using multiple signals of opportunity in the context of positioning and how much the positioning performance is affected by considering different measurements combinations from several wireless technologies.**

***Index Terms*—Cramér-Rao Lower Bound, signals of opportunity, approximate maximum likelihood.**

I. Intrduction

Location based services have pushed the need to localize user's in any environment, either in urban canyons or indoor facilities, such as office buildings, hospitals, schools among others [1], [2]. While global navigation services are commonly relied on for providing the location of an user, these services are meant to be used in obstruction-less environments and a clear view of the sky. For that reason, positioning with signals of opportunity, any signal designed for something else than positioning, aims to be an alternative to complement the existing positioning services [3], [4].

The proliferation of Wi-Fi networks has contributed to the appearance of several techniques for estimating the location of an user. Fingerprinting is one of the most widely used approaches [5], whose popularity arises from the fact that the required infrastructure is already in place and no significant investments are required [6], [7]. However, one of its disadvantages is the requirement of a prior training phase, which can be expensive and difficult to deal with.

Therefore, relying on one stage estimators, such as those that employ angle of arrival, time of arrival and time difference of arrival measurements is more desirable. This is the motivation for the study, which focuses on time of arrival measurements to obtain the location of a mobile receiver [8].

The goal of the study is to provide a bound for the performance of a positioning system, which is assumed to rely on time of arrival measurements of several widely available wireless protocols, such as Wi-Fi and UMTS signals. This work is of interest, for example, for future microlocation for the Internet of things [9] or for energy-efficient cooperative opportunistic positioning systems [10]

II. Related work

Related works can be found for example in [11]–[14].

In [11], a similar problem of hybrid localization with heterogeneous networks is addressed. The authors combine cellular and WiFi signals with TOA, AOA and RSS and the focus is only on the overall performance, rather than on the incremental performance of adding one additional system or emitter at a time, as done here.

In [12] the authors compare the Wi-Fi-based positioning with UMTS-based positioning by using RSS measurements, but the two systems are not considered together. They conclude that similar indoor accuracies can be achieved with Wi-Fi and UMTS when RSS measurements are used.

The work in [14] looks into positioning with a 3GPP-LTE signal and what is the gain obtained by considering several signals of opportunity, such as digital television and Wi-Fi. When aided by signals of opportunity, the gain in accuracy was seen to be 40 % to 70% better than standalone positioning with 3GPP-LTE. These gains were observed for scenarios with more than 40 user equipments and 1 to 4 additional signals of opportunity, respectively.

III. Simulation

In this study, the simulation model assumes the existence of several Wi-Fi signals, based on the standards IEEE 802.11ac/b/g (simply refered as 802.11ac/b/g from now on) and WCDMA signals, based on UMTS signals. Table I summarises a few key parameters of each technology, including the signal structure type, OFDM and CDMA and bandwidth. The simulation assumes an environment where several emitters, from each of these technologies, are randomly distributed inside a defined area.

TABLE I
Signals under consideration

Signal	Type	Bandwidth (MHz)
802.11ac	OFDM	60
802.11g	OFDM	20
802.11b	CDMA	22
WCDMA	CDMA	5

For the given area, the user movement is modeled through a random walk in a two dimensional space [15], with a fixed step length of one meter. Each new position, $\mathrm{X}(t)$, at simulation time, t, was obtained by summing a movement vector, $\mathrm{M}(s)$,

to the previous position. The movement vector is randomly chosen by drawing the step decision variable s, from a random integer generator. Hence, the movement model is defined by,

$$\mathrm{X}(t) = \mathrm{X}(t-1) + \mathrm{M}(s), \text{where } s = \{1,2,3,4\}, \quad (1)$$

and,

$$\mathrm{M}(s) = \begin{cases} (-1,0) & , \text{ if } s = 1, \\ (1,0) & , \text{ if } s = 2, \\ (0,-1) & , \text{ if } s = 3, \\ (0,1) & , \text{ if } s = 4. \end{cases} \quad (2)$$

On each new location, the timing measurements, L_n, to each nth-emitter are computed by assuming their location known as well as the variance in the measurement error. Hence, L_n is obtained by

$$\mathrm{L}_n = \mathrm{R}_n + \epsilon_n, \quad (3)$$

where R_n is the geometrical distance to the emitter and ε_n is the measurement error. R_n is obtained by,

$$R_n = \sqrt{(x^{(i)}_{\text{emitter}} - x_{\text{user}})^2 + ((y^{(i)}_{\text{emitter}} - y_{\text{user}})^2} \quad (4)$$

where $(x_{\text{user}}, y_{\text{user}})$ are the coordinates of the user at a given time and $(x_{\text{emitter}}, y_{\text{emitter}})^{(i)}$ the position for the i-th emitter.

The measurement noise, ϵ_n, is modelled through a normal distributed distribution, with its variance set according to the Crámer-Rao lower and the expected carrier to noise ratio ($\mathrm{C/N_0}$) at the receiver's location. Regarding the variance, the Crámer-Rao lower bounds are computed using the result in [16], where the variance for an unbiased estimator for range measurements is given as,

$$\mathrm{var}(\hat{\tau}_0) \geq \frac{1}{\frac{\varepsilon}{\mathrm{N_0}/2}\overline{\mathrm{F^2}}} \Leftrightarrow \quad (5)$$

$$\Leftrightarrow \mathrm{var}(\hat{\tau}_0) \geq \frac{1}{\frac{C}{\mathrm{N_0}/2\,\mathrm{T}}}\overline{\mathrm{F^2}}, \quad (6)$$

where, ε is the signal energy, N_0 the noise spectral density, T the observation interval and $\overline{F^2}$ the mean square bandwidth of the signal, given as,

$$\overline{\mathrm{F^2}} = \frac{\int_{+\infty}^{-\infty} (2\pi \mathrm{F})^2 |\mathrm{S(F)}|^2 \mathrm{dF}}{\int_{+\infty}^{-\infty} |\mathrm{S(F)}|^2 \mathrm{dF}}. \quad (7)$$

Fig.1 shows the expected accuracy for the signals under consideration, WCDMA, 802.11b, 802.11g and 802.11ac, plotted against the signal's carrier to noise ratio ($\mathrm{C/N_0}$). As expected, the WCDMA is the signal showing the worst performance for timing estimates, since it is the one with the smallest bandwidth. A narrow band signal in the frequency domain equates to a larger signal in the time domain, which is undesirable for positioning purposes. Since the receiver relies on the correlation of the incoming signal with a locally generated replica to obtain a time of arrival (TOA) measurement, the larger or flatter this area is, the worse the timing estimate will be.

Therefore, besides considering each signal design individually, regarding its transmission power and bandwidth, the simulator also relies on the ITU-R propagation model to describe the expected $\mathrm{C/N_0}$ at the receiver [17]. The ITU-R model is derived from the Friis equation and given as,

$$\mathrm{P_r}(d) = \mathrm{P_t} + \mathrm{L} - 20\log_{10}\left(\frac{4\pi f}{c}\right) - 20\eta\log_{10}(d) + v, \quad (8)$$

where the RSS at a distance of d (meters) is given by $\mathrm{P_r}(d)$, the device's transmission power by $\mathrm{P_t}$, the operating frequency in Hertz as f, the propagation speed, considered as the speed of light in vacuum, as c, losses in the path of the signal are translated into η while L are other system losses. The model considers a slow fading phenomenon, described by the log-normal distributed random variable $v \sim \mathrm{N}(0, \sigma^2)$.

While the ITU-R model is used for the propagation loss, the noise component is modelled as thermal noise [17]. Fig.2 presents a diagram with the steps taken by the simulator in order to provide a measurement for the given location of the user. Afterwards, this measurement is used to estimate the user's location.

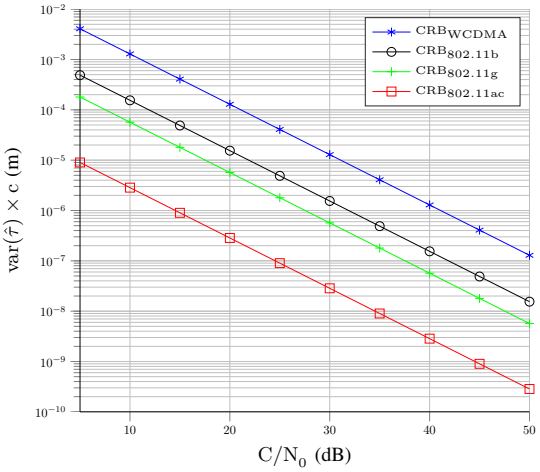


Fig. 1. Crámer-Rao lower bounds for WCDMA and 802.11 ac/g/b

Since the goal of the simulation is to infer the accuracy in a best case scenario, the network is assumed to be synchronized, meaning that no clock bias or offset is modelled and added to the measurement. Therefore, one should keep in mind that in a real system, these constrains would not hold. Nevertheless, they can give a clear image of the relative performance of the different considered approaches.

IV. Estimation

By using the measurements acquired at each point the user moves to (Fig.2), the simulation estimates the location of the user, (x, y), through an approximate maximum likelihood (AML) [18], [19]. Hence, assume each of these measurements, as in (3), define the measurement vector, $\mathbf{r}$, given as

$$\mathbf{r} = [\mathrm{L}_1, \mathrm{L}_2, \ldots, \mathrm{L}_n], \quad (9)$$

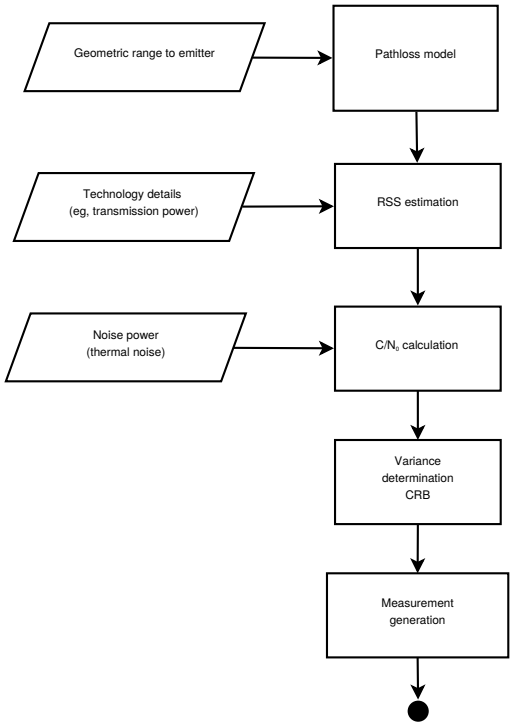


Fig. 2. Workflow for measurement generation

with n being the number of available emitters.

Assuming a vector of TOA as,

$$\mathbf{T} = [\mathrm{t}_1, \ldots, \mathrm{t}_n], \tag{10}$$

$$\mathbf{T} = \mathbf{T}_0 + \mathbf{e}, \tag{11}$$

where $\mathbf{T}_0$ is the vector of true TOA, and $\mathbf{e}$ is a vector of additive measurement errors, assumed independent random variables with a with a zero mena Gaussian distribution. The covariance matrix of $\mathbf{e}$ is given as,

$$\mathbf{Q} = \mathrm{E}\{\mathbf{e}\mathbf{e}^T\} = \mathrm{diag}(\sigma_1^2, \ldots, \sigma_n^2). \tag{12}$$

Finally, let $\mathbf{\Theta}$ be,

$$\mathbf{\Theta} = [x, y]. \tag{13}$$

Approximate Maximum Likelihood

The maximum likelihood (ML) estimate is the $\mathbf{\Theta}$ that minimizes the Jacobian $\mathbf{J}$ in the probability density function of $\mathbf{T}$ given $\mathbf{\Theta}$,

$$f(\mathbf{T}/\mathbf{\Theta}) = (2\pi)^{\frac{N}{2}} (\det\mathbf{Q})^{-\frac{1}{2}} \exp\left(-\frac{\mathbf{J}}{2}\right). \tag{14}$$

Setting the gradient of $\mathbf{J}$ with respect to $\mathbf{\Theta}$ to zero, gives the two ML equations

$$\sum_{i=1}^{n} \frac{(r_i - \delta_i)(x - x_i)}{r_i} = 0, \tag{15}$$

$$\sum_{i=1}^{n} \frac{(r_i - \delta_i)(y - y_i)}{r_i} = 0. \tag{16}$$

Due to the non linearity of (16), the AML solution, as presented in [18], in matrix form can be represented as,

$$2\begin{bmatrix} \sum_{i=1}^{n} g_i x_i & \sum_{i=1}^{n} g_i y_i \\ \sum_{i=1}^{n} h_i x_i & \sum_{i=1}^{n} h_i y_i \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{n} g_i (s + k_i - \delta_i^2) \\ \sum_{i=1}^{n} h_i (s + k_i - \delta_i^2) \end{bmatrix}, \tag{17}$$

where,

$$g_i = \frac{x - x_i}{r_i(r_i + \delta_i)}, \tag{18}$$

$$h_i = \frac{y - y_i}{r_i(r_i + \delta_i)}. \tag{19}$$

The AML treats (17) as a set of linear equations. Starting from an initial (x, y), it first computes g_i, h_i, and the least squares for (x, y) from (17), in terms of s. Putting them into

$$s = x^2 + y^2, \tag{20}$$

leads to a quadratic in s. Therefore, the correct root needs to be chosen. For that to happen the AML acts differently on three scenarios, one root is positive, both roots are positive and both roots are either negative or imaginary. For the first case, the root with a positive value is taken as the value to replace s in the least squares solution of (17). For the second case, the favored root is the one providing a smaller $\mathbf{J}$. On the third case, it takes the absolute values of the real parts.

After k iterations, the AML will have k values of $\mathbf{J}$ and in the end, the one that provides the smallest value of $\mathbf{J}$ [18], [19].

V. Results

This section covers a set of illustrative results obtained through the simulator. The first results show a direct consequence from the fact that narrow band signals provide an overall lower accuracy regarding timing estimates. This is seen through Fig.3 where the root mean square error is plotted against the number of emitters available for a given technology. As expected, the lowest RMSE is obtained by using 802.11ac emitters and the biggest RMSE when only WCDMA emitters are present.

Since the study sets out to understand the benefit of observing and exploiting several technologies, Fig.4 - 6 illustrate the benefit of obtaining measurements from additional emitters. In each figure, the thicker line with a circle marker represents the RMSE in meter obtained using only several WCDMA emitters, while the remaing lines represent the RMSE obtained when merging WCDMA with N other emitters of a different technology. As an example, WCDMA + 3b means that N WCDMA emitters are availalbe (read from the x axis) as well as 3 other 802.11b emitters.

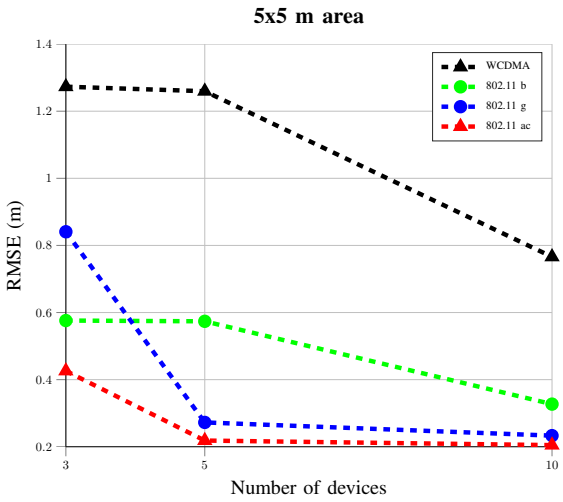


Fig. 3. Positioning using a single technology

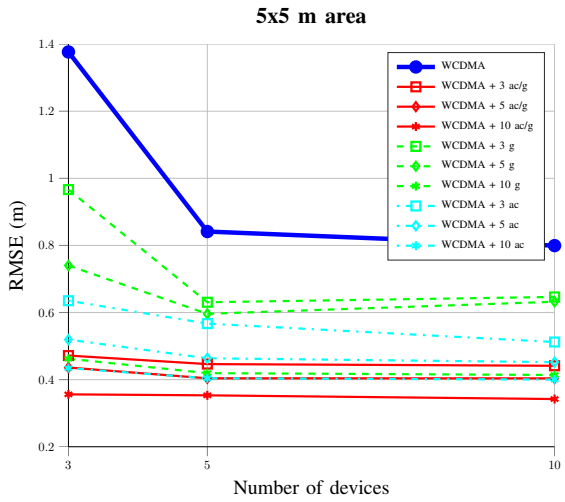


Fig. 4. Positioning with WCDMA, 802.11ac and 802.11g

Fig.4 shows the benefit in the performance of a system that uses primarily WCDMA and when available uses either 802.11g, 802.11ac or both. As it can be seen from the plot, the curve is obtained when both 802.11ac and 802.11g are combined together with WCDMA. Furthermore, one can also observe that when using WCDMA with 10 emitters of 802.11ac. There is no necessity of using more emitters of 802.11g, since the achievable performance is the same. However, using 10 802.11g emitters with WCDMA achieves the same performance when 3 emitters of 802.11ac and 802.11g are available. Even though 802.11ac provides more accurate measurements, it does not offset the fact that with 10 emitters, the system still has more 4 distinct measurements. Moreover, when merging WCDMA with a single other technology, regardless of the one that is picked, going from 3 to 5 emitters results in a significant improvement in performance. On the contrary, when WCDMA is merged with the other two technologies, the increase in the number of emitters has little impact on the overall performance of the system. Bottom line, the main conclusions to draw from this plot are the fact that increasing the number of observables is desirable in general, but the cost of adding and managing those does not translate to a significant increase improvement on the overall performance.

Fig.5 follows a similar approach, but now WCDMA is merged with the other technologies in this simulation with higher variance, 802.11b and 802.11g. As expected, the results also show better performance when the full number of emitters is used. It also shows the combination with 802.11g is less accurate than the one with 802.11b. This difference is particularly noticeable when 3 emitters of each technology are available, with the difference fading as the number increases. As for the best achievable performance, this seems to be attainable when using WCDMA in addition to 10 other 802.11g. The combination of the three technologies seems to fare equally well. Overall, the addition of 802.11b and 802.11g improves the performance of the system, but in some circumstances 802.11b provides the best performance.

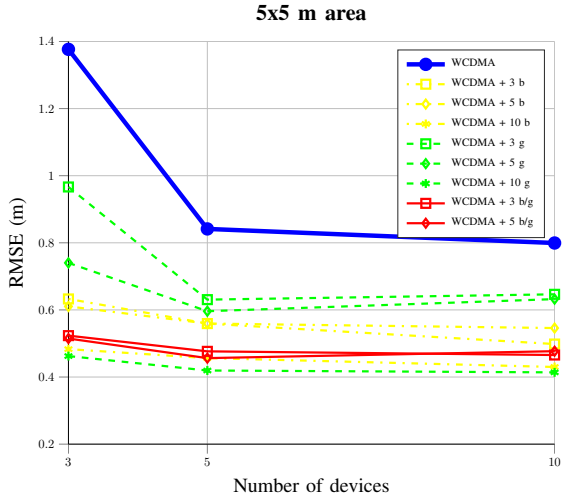


Fig. 5. Positioning with WCDMA, 802.11b and 802.11g

Fig.6 presents WCDMA measurements, being merged with the next less accurate measurement, 802.11b and with the more accurate timing measurements from 802.11ac. The best performance is achieved when the three technologies are all merged together. From the plot one can see that adding 3 emitther from either 802.11b or 802.11ac seems to provide a similar performance. This means the WCDMA is setting a

limit on the performance of the system.

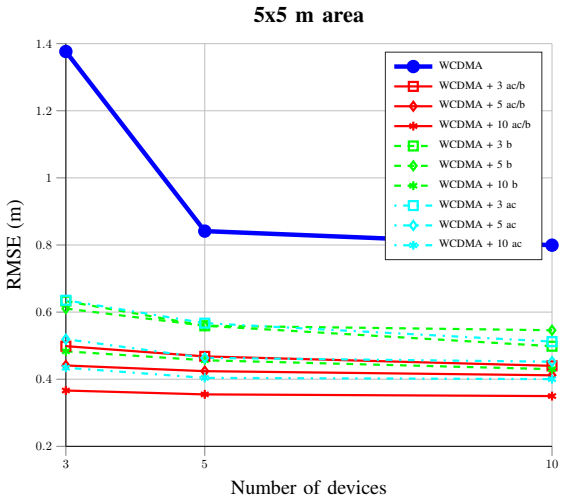


Fig. 6. Positioning with WCDMA, 802.11ac and 802.11b

In the end, all these plots, Fig.4 - 6, show that increasing the number of observables leads to an increase in performance. However, for some combinations of technologies, this benefit might not be worth the added complexity in terms of power consumption or processing power, due to the higher bandwidth of the signals, such as preferring 5 additional measurement from a 802.11g source rather than 3 from a 802.11ac one (Fig.6). Besides that, the signal structure should also be taken into account, for example, OFDM signals are prone to phane noise and frequency offset.

VI. Conclusions

This paper has presented a study on the impact of merging several TOA measurements for different signals of opportunity, WCDMA, 802.11b, 802.11g and 802.11ac. The measurements were acquired from a simulator which derives the timing estimates from the Crámer-Rao lower bounds for each signal. In addition to that, the simulator uses a propagation model to match the received signal power to the distance the user is from the receiver. Furthermore, the simulator assumes all the systems to be synchronised, which, in reality, would be difficult to achieve. Therefore, the results provide an insight on the best case scenario that a user could experience.

As main conclusions, while adding more emitters is often desirable, the benefit in the overall accuracy is small and in some situations less accurate systems might lead to the same or comparable results. In particular, the paper shows that when observing 5 emitters of 802.11b, the overall accuracy is equivalent to the one when 10 emitters of 802.11ac are available.

Overall, for a practical system relying on signals of opportunity, some combinations, pointed out in the paper, might not be worth pursuing since it will require more resources from the user device for little added benefit in the system's performance.

It is therefore of utmost importance to first perform a theoretical analysis, as the one illustrated here in order to pre-evaluate the possible positioning gain by using multiple emitters from heterogeneous systems. Only if the gain is large enough, the hybridization of signals from heterogeneous networks should be employed, otherwise a single system may still bring enough benefit with a lower complexity.

Open Access

The data and scripts used for this study are available at https://goo.gl/GHlSbK, under a CC 4.0 license.

Acknowledgment

This work was financially supported by EU FP7 Marie Curie Initial Training Network MULTI-POS (Multi-technology Positioning Professionals) under grant nr. 316528. The authors also express their warm thanks to the Academy of Finland (project 250266) for its financial support

References

[1] M. Ficco, F. Palmieri, and A. Castiglione, "Hybrid indoor and outdoor location services for new generation mobile terminals," *Pers. Ubiquitous Comput.*, vol. 18, no. 2, pp. 271–285, mar 2013.

[2] Juniper Research, "Location Based Services Market Driven by Context Aware Mobile Services," 2014.

[3] G. Seco-Granados, J. A. López-Salcedo, D. Jiménez-Baños, and G. López-Risueño, "Challenges in Indoor Global Navigation Satellite Systems," *IEEE Signal*, no. February, pp. 108–131, 2012.

[4] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of Wireless Indoor Positioning Techniques and Systems," *IEEE Trans. Syst. Man Cybern. Part C (Applications Rev.*, vol. 37, no. 6, pp. 1067–1080, nov 2007.

[5] J. Raquet and R. K. Martin, "Non-GNSS radio frequency navigation," in *2008 IEEE Int. Conf. Acoust. Speech Signal Process.* IEEE, mar 2008, pp. 5308–5311. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4518858

[6] V. Honkavirta, T. Perala, S. Ali-Loytty, and R. Piche, "A comparative survey of WLAN location fingerprinting methods," in *2009 6th Work. Positioning, Navig. Commun.* IEEE, mar 2009, pp. 243–251.

[7] A. Farshad, M. K. Marina, and F. J. Garcia, "A microscopic look at WiFi fingerprinting for indoor mobile phone localization in diverse environments," in *Int. Conf. Indoor Position. Indoor Navig.* IEEE, oct 2013, pp. 1–10.

[8] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Trans. Syst. Man Cybern.*, vol. 37, no. 6, pp. 1067–1080, 2007.

[9] F. Zafari, I. Papapanagiotou, and K. Christidis, "Micro-location for Internet of Things equipped Smart Buildings," *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2015. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7120085

[10] K. Dhondge, H. Park, B.-Y. Choi, and S. Song, "Energy-Efficient Cooperative Opportunistic Positioning for Heterogeneous Mobile Devices," in *2012 21st Int. Conf. Comput. Commun. Networks*. IEEE, jul 2012, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6289296

[11] U. Birkel and M. Weber, "Indoor localization with UMTS compared to WLAN," in *2012 Int. Conf. Indoor Position. Indoor Navig.* IEEE, nov 2012, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6418933

[12] A. Yassin, M. Awad, and Y. Nasser, "On the hybrid localization in heterogeneous networks with lack of hearability," in *ICT 2013*. IEEE, may 2013, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6632158

[13] Y. Shen and M. Z. Win, "Fundamental Limits of Wideband Localization - Part I: A General Framework," jun 2010. [Online]. Available: http://arxiv.org/abs/1006.0888

[14] A. Dammann, S. Sand, and R. Raulefs, "On the Benefit of Observing Signals of Opportunity in Mobile Radio Positioning," in *Proc. 2013 9th Int. ITG Conf. Commun. Coding*, vol. 9, 2013.
[15] D. Shiffman, *The Nature of Code*. Magic Book Project, 2012.
[16] S. M. Kay, "Fundamentals of Statistical Signal Processing : Est imat ion Theory."
[17] ITU-R, "Recommendation ITU-R P.1238-7," 2012.
[18] Y. Chan, "Exact and approximate maximum likelihood localization algorithms," *IEEE Trans. Veh. Technol.*, vol. 55, no. 1, pp. 10–16, 2006.
[19] M. Zhaounia, M. Adnan Landolsi, and R. Bouallegue, "Hybrid TOA/AOA Approximate Maximum Likelihood Mobile Localization," *J. Electr. Comput. Eng.*, vol. 2010, no. 1, pp. 1–5, 2010.

Publication 6

P. Figueiredo e Silva, V. Kaseva, E. Simona-Lohan, "Wireless Positioning in IoT: A Look at Current and Future Trends," in Sensors, July 2018. DOI: 10.3390/s18082470

sensors

MDPI

Article

Wireless Positioning in IoT: A Look at Current and Future Trends

Pedro Figueiredo e Silva [1,2,*], Ville Kaseva [2] and Elena Simona Lohan [1]

[1] Laboratory of Electronics and Communications Engineering, Tampere University of Technology, Korkeakoulunkatu 3, Tampere 33720, Finland; elena-simona.lohan@tut.fi
[2] Wirepas, Visiokatu 4, Tampere 33720, Finland; ville.kaseva@wirepas.com
* Correspondence: pedro.figs.silva@gmail.com

Received: 30 May 2018; Accepted: 25 July 2018; Published: 30 July 2018

Abstract: Connectivity solutions for the Internet of Things (IoT) aim to support the needs imposed by several applications or use cases across multiple sectors, such as logistics, agriculture, asset management, or smart lighting. Each of these applications has its own challenges to solve, such as dealing with large or massive networks, low and ultra-low latency requirements, long battery life requirements (i.e., more than ten years operation on battery), continuously monitoring of the location of certain nodes, security, and authentication. Hence, a part of picking a connectivity solution for a certain application depends on how well its features solve the specific needs of the end application. One key feature that we see as a need for future IoT networks is the ability to provide location-based information for large-scale IoT applications. The goal of this paper is to highlight the importance of positioning features for IoT applications and to provide means of comparing and evaluating different connectivity protocols in terms of their positioning capabilities. Our compact and unified analysis ends with several case studies, both simulation-based and measurement-based, which show that high positioning accuracy on low-cost low-power devices is feasible if one designs the system properly.

Keywords: Internet of Things (IoT); wireless positioning; indoor location

1. Introduction

Nowadays, the amount of connected wireless devices is growing, e.g., smart watches, smart light bulbs, smart toothbrushes, smart coffee mugs, etc. The trend in the information technology industry is towards connecting and extracting analytics from a variety of inter-connected wireless devices.

While many IoT applications have so far focused on the consumer realm, more and more industrial applications are also appearing, such as utilities measurement (e.g., water, electricity and gas), industrial lighting, logistics and smart agriculture. Enabling such industrial applications means that IoT networks need to support large amounts of devices, multiple years of operation on battery, different latency requirements and low costs per unit.

We believe that, on top of the communications and reliability requirements of a wireless link, many IoT applications will require or benefit from knowing the location of certain devices. Such location information will be needed seamlessly, both indoors and outdoors, and without the battery-draining Global Navigation Satellite Systems (GNSS) chipsets. The need for localization and tracking appears not only from the network management point of view, but also from a business perspective, driving new business models and new business avenues.

Nevertheless, enabling or creating a positioning system with an IoT network is not a trivial task. The reason behind this is that industrial applications seek a low per unit cost of their IoT devices, which results in devices with very limited hardware components, such as CPU, memory and battery.

The limited hardware has an impact on the number of devices that a single device can serve and how fast it can process network and application requests. However, while CPU and memory will have an important impact on the scale of the network, the biggest challenge for enabling a positioning system lies on the proper management of the devices' radio.

The need for proper radio management becomes evident as there are devices with known coordinates which will broadcast specific payloads on a regular basis and other devices whose locations are to be determined, which will need to scan the spectrum frequently. Hence, too frequent broadcasting will lead to spectrum congestion and increased packet collision, whereas frequent scanning leads to high battery consumption, which is particularly problematic for battery-operated devices.

Overall, the biggest challenge to tackle for an IoT positioning network is to balance the power consumption against the performance of the system. A very reactive system will have to rely on frequent scanning and broadcasting of its members, which means that devices will need to draw large quantities of power. A low reactive system will draw less power with devices scanning very seldom.

The goal of this paper is to provide an insight on positioning capabilities of the current IoT technologies and other relevant IoT-enabling wireless technologies, such as WiFi. The paper starts by classifying three domains of positioning and discussing the main shortcomings of each of these domains for IoT devices. It then classifies the different IoT solutions according to six classification criteria and it provides a discussion on the main system parameters relevant to positioning and tracking purposes. This discussion acts as a basis for comparison between the different IoT wireless solutions. To further complement this discussion, we present positioning results based on simulation-based scenarios and field experiments with a platform built on top of the Wirepas Mesh connectivity solution. In the end, we provide a short summary and conclusions of our findings.

2. Related Work

At this moment, to the best of the authors' best knowledge, there are no comprehensive comparisons in the literature between different IoT protocols in terms of their positioning capabilities. There are, however, other studies that compare specific IoT technologies and which look at IoT from the communications point of view, as well as studies focusing on positioning with a particular technology, such as narrow-band IoT (NB-IoT) or BLE. In this section, we highlight the related work from literature studies.

A survey of localization methods for 5G, having a short section also on IoT positioning has been recently published as a white paper in COST action CA15104 [1]. It has also been emphasized in this paper that localization will become a key component of future 5G systems and it has been pointed out that accurate future localization solutions in 5G should exploit the multipath and non-line-of-sight information and should put more emphasis on heterogeneous data fusion mechanisms. However, such advanced solutions would also increase the power consumption on the devices and are not well-suited for the majority of IoT systems. By distinction with the work in [1], our paper focuses mostly on low-cost low-power consumption IoT solutions.

The authors in [2] focus on the Long-Term Evolution (LTE) Machine type communications (LTE-M) and Narrow Band Internet of Things (NB-IoT) protocols and their positioning capabilities. It was shown in [2] that at 46 dBm power of the transmit AN, positioning accuracy goes to around 10 m and that NB-IoT protocol supports better positioning accuracy than LTE-M protocol. A related study can be found in [3]. The focus in [3] is on indoor localization via improved received signal strength (RSS) fingerprinting in generic IoT devices. The results are based on 802.11$n/b/g$ signals where location errors below 5 m are achieved in more than 50% of the studied cases.

In [4], the authors investigate a time-domain based positioning with additional frequency hopping for the NB-IoT system. The obtained positioning accuracy is down to 30–50 m under strong signal-to-noise ratio conditions, and it deteriorates quickly for medium and low signal-to-noise ratios.

A study complementary to our work is found in [5], where IoT positioning is looked at from the perspective of security, privacy and robustness of the localization technology. No positioning results

were reported in the study. Another complementary study is found in [6] in which the authors focused on existing and emerging software and hardware platforms for IoT applications, but positioning was not part of that study. IoT positioning has recently been considered in [7] from the point of view of spoofing resistance in time of arrival (TOA) ultra-wideband (UWB) for IoT systems.

Other complementary comprehensive studies, focusing solely on the communication aspects of IoT, are found for example in [8,9].

3. Designing an IoT Positioning System

In its essence, a positioning system translates a set of measurements from well-known reference points into a coordinate pair. The reference points, known as anchors in localization terminology or Access Nodes (AN) in IoT terminology, act as a means for the device of interests, a mobile or an IoT tag, to be in a local or global reference frame. Depending on who makes the measurements, the positioning is considered to be network centric (i.e., when the anchors make the positioning-related measurements) or device centric (i.e., when the IoT end nodes or tags perform the positioning-related measurements).

These two types of positioning have very different implications on security and privacy, which should always be carefully considered regarding the final application. For example, privacy-preserving positioning solutions are easier to be achieved in a device-centric approach than in a network-centric approach as the device would not need to disclose its position to the network.

3.1. Positioning Domains

In terms of measurements, there are multiple domains from which they can be extracted from, as long as there are means to do so in the devices. For that reason, we briefly present three of the main domains we consider of interest for an IoT positioning system:

- Power or signal strength-based;
- Time-based;
- Space-based.

Other domains, such as natural or artificial fields, e.g., geo-magnetic field, light, sounds, or smell are out of the scope of our study, but could also serve as relevant sources of information for future IoT positioning systems.

The following subsections provide a short summary of main challenges in each of these three positioning domains and their system-wide impacts.

3.1.1. Power Domain

Signal strength measurements are derived from the protocol operation, which most of the times results in a measurement of no additional cost to the device and battery consumption. However, positioning solutions in the power domain must tackle several challenges, in particular those related to the fast fluctuations of the Received Signal Strength (RSS) or of the backscattered power (BP), due to fading and shadowing caused by the surrounding environment. One key factor to model the RSS measurements relies on the possibility of understanding, with a given degree of accuracy, how the signal power changes in its surrounding environments. The signal power models as a function of the distance between the transmitter and the receiver are known as path-loss models, [10,11]. A typical empirical Log distance model is the single-slope path loss model [11]:

$$\mathrm{P_r}(d) = \mathrm{P_r}(\mathrm{d_0}) - 10\eta \log_{10}\left(\frac{d}{\mathrm{d_0}}\right) + w, \tag{1}$$

where $\mathrm{P_r}(\cdot) < 0$ is the received signal power in logarithmic scale dependent on distance d, $\mathrm{d_0}$ is a reference distance (usually 1 m), $\eta > 0$ is the path-loss exponent and $w \sim log(\mathrm{N}(0, \sigma^2))$ is a log-normally distributed random variable that models the slow fading phenomenon and possible

RSS measurements errors (e.g., due to quantization). Both η and w are dependent on the propagation environment and are typically dependent on the device type and environment type. In addition, w can depend on factors such as device orientation and the amount of people present in the measurement area at the time of acquisition.

In terms of an IoT positioning system, the fact that one can extrapolate this information directly from the communication's signal, which means that there is no additional cost for the device. In terms of battery, the cost will depend on the amount of positioning location requests demanded per second. Ideally, if the requirement is to have an opportunistic location, based on the sporadic communication of the device, acquiring the RSS-based positioning will have no impact on the battery life. However, if the device or the infrastructure will have to listen periodically for a specific pilot signal, acquiring the RSS-based positioning will cause further demands in terms of battery consumption. One limitation of RSS-based approaches is that some current IoT standards support only a coarse RSS measurement (e.g., in steps of 6 dB), which can adversely impact the positioning accuracy, as the noise variance σ^2 will increase.

Another interesting aspect of the RSS measurements is that, based on simulations, RSS-based positioning errors are shown to be frequency independent (as shown later in Figure 1). However, one would expect different levels of location-based service at different frequency ranges. The frequency ranges can be coarsely divided into three categories: sub-GHz (i.e., carrier frequencies less than 1 GHz), GHz (1 to 30 GHz) and mmWave (above 30 GHz). The scattering becomes more prominent as frequency increases, thus one would expect different target positioning accuracy according to the frequency range. In addition, as the operating frequency increases, the antenna's effective area is smaller, and the signal coverage decreases. This is possible to see in Figure 2 where the ideal signal propagation in drawn over a 100 by 100 square area, based on the Friis equation and assuming zero system gains, G,

$$\mathrm{P_r}(d) = \mathrm{P_t} + G + 20\log_{10}\left(\frac{\mathrm{c}}{f4\pi}\right) - 20\log_{10}(d) \quad (2)$$

where $\mathrm{P_t}$ is the transmission power, f the operating frequency and c the speed of light.

Based on the signal's behavior, it is easy to understand that a sparser infrastructure at higher frequencies will likely result in a degradation of the positioning performance (as shown later in Figure 1).

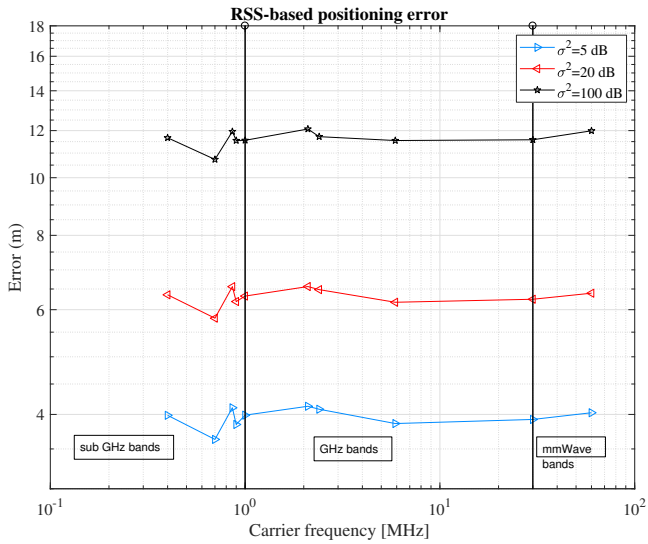


Figure 1. Comparative analysis of RSS-based estimates at various carrier frequencies and various AN densities.

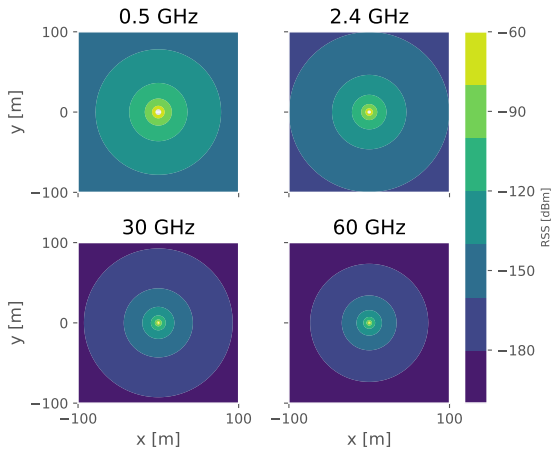


Figure 2. Ideal radio signal propagation at 0.5, 2.4, 30 and 60 GHz.

3.1.2. Time Domain

Positioning estimation based on timing information is based on estimating the time-of-arrival (TOA) or the time-difference-of-arrival (TDOA) from three or more fixed access nodes and then converting those timing estimates into distances. For example, 3D location based on TOA is possible with three synchronized measurements from three known devices. The goal is to solve the following set of equations and find out the node's location, $\xi_n = (x_n, y_n, z_n)$, assuming that $\xi_a = (x_a, y_a, z_a)$ are known coordinates:

$$\mathbf{L}_n = \sqrt{(\xi_a - \xi_n)^2}. \tag{3}$$

For TDOA, the range is now a difference of ranges, based on the TOA at the measurement device. Hence, the TDOA from a node n to a measurement device m would be written as

$$\mathbf{L}_{nm} = \mathbf{L}_n - \mathbf{L}_m. \tag{4}$$

Due to this difference, the range measurement is free of errors imposed by the measurement device's clock, since it cancels out when subtracting the two TOA measurements.

Overall, the time measurements require synchronized clocks, either at the receiver or at the transmitter side, leading to a significant burden on device cost. This does not play well for IoT applications, which are driven by the need of having low-cost devices.

It is also important to keep in mind the relationship between bandwidth and accuracy for TOA measurements. This is illustrated in Figure 3, where the positioning error is plotted against the available channel bandwidth at different Signal-to-Noise Ratio (SNR) values. Clearly, sub-m positioning accuracy with time-based approaches is achievable only with high bandwidths (of the order of 100 MHz), but it is very challenging for narrowband and ultra-narrowband systems even at very high SNR.

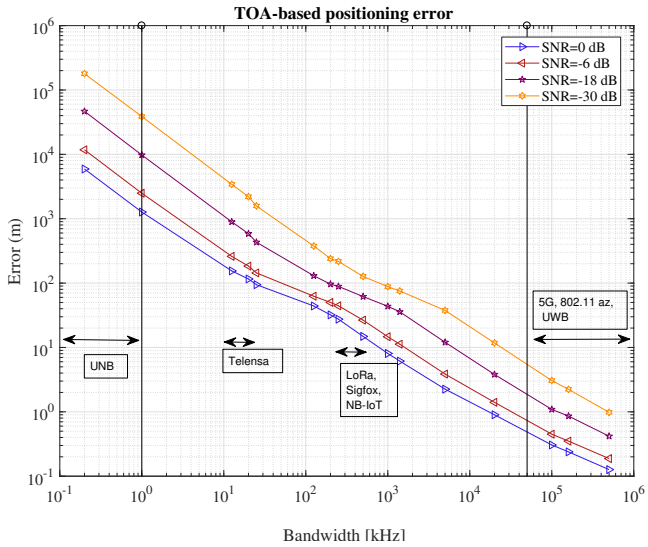


Figure 3. Comparative analysis of TOA-based position estimates at various bandwidths.

3.1.3. Space Domain

In the space domain, the ranges are estimated by measuring the angle (or direction) of arrival (AoA) for the signal of interest. Often, this is done by the means of an antenna array or a sectorized antenna. For a given device n, it is possible to describe its measurement at m as

$$(x_n, y_n) = r_m cos(\theta_m) + r_m sin(\theta_m), \tag{5}$$

where r_m is the distance from m to n and θ the angle of arrival determined at m. Hence, by solving for the unknown coordinates, one can obtain a range estimate.

In summary, AoA is particularly interesting for IoT, as the major constraint for achieving angle measurements relies only on the antenna design. However, its major drawback is that the error increases with the distance to the transmitter, which means that a small deviation in the angle results in a large error for the devices at the service edge.

3.2. IoT Classifications

While there are several domains from where to extract measurements for building knowledge of a device's location, several limitations arise from the actual IoT system that is built upon. The goal of this subsection is to introduce the IoT technologies, by classifying them into six main categories (see Figure 4):

- *Licensed versus unlicensed*: which refers to the operation in a protected band, such as cellular bands versus operation in unlicensed bands, such as industrial, scientific and medical (ISM) bands;
- *Operating frequency bands*: which refers to the carrier frequency of each IoT technology; here, we divide the frequency spectrum into three parts: sub-GHz, GHz, and mmWave bands. Some IoT technologies spread over multiple ranges;
- *Protocols versus enablers*: which refers to whether a technology is seen as a specific IoT communication protocol or a possible wireless positioning enabler;
- *Range-based classification*: which refers to short-, medium-, or long-range operation;

- *Rate-based classification*: which refers to Low-Rate (LR) or High-Rate (HR) data rates. Typically, most IoT connectivity solutions are meant for LR high delay applications, while solutions such as WiFi and 5G cover HR and low latency applications;
- *Power-based classification*: which refers to Low-Power (LP) versus High-Power (HP) operation. Typically, LP approaches go hand in hand with LR approaches, while HP approaches go hand in hand with HP approaches. In LP operation, the devices can function for several years on batteries.

We make the following assumptions: in the range category, we consider long-range for those protocols capable of delivering more than 10 km links; for the rate category, we assume HR as those able to achieve an uplink above 10 Mbit/s and, for power consumption category, we assume as LP all those IoT systems who can support at least non-routing devices on more than two years of battery.

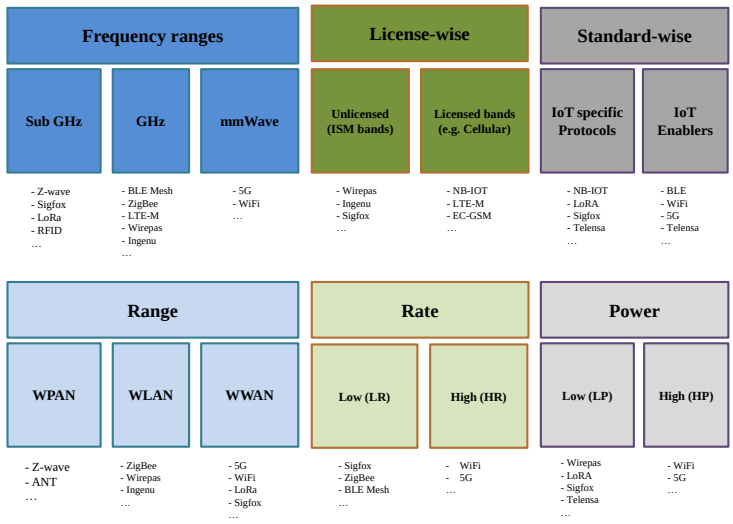


Figure 4. Classification of IoT networks.

3.3. IoT System Parameters

This subsection discusses the relevant parameters for a positioning fit in an IoT system.

Topology relates to a message passing from one node to another and the possibility to discover new nodes in the network. The network topology, illustrated in Figure 5, has a significant impact on how nodes with known locations are discovered by others. On a mesh topology, any node can be set as a reference node, whereas, on a star topology, only the access nodes can be defined as such. The density of the fixed nodes also plays an important role in the location accuracy. For example, a denser network with a well-spread distribution of nodes is likely to provide a better location accuracy than a network with few reference nodes all placed in the same direction from the device to be located. An IoT network typically has a star or mesh topology. In a star topology, devices can only talk to their parent device, while, in a mesh topology, nodes can exchange messages between each other. Star topologies are susceptible to single points of failure, since losing the connection to the parent means that the node will be outside the network. In a mesh topology, if a link fault occurs, the device can look for any other neighbor to connect to. Thus, mesh networks provide better coverage and, implicitly, they are likely to offer better positioning accuracy than star networks;

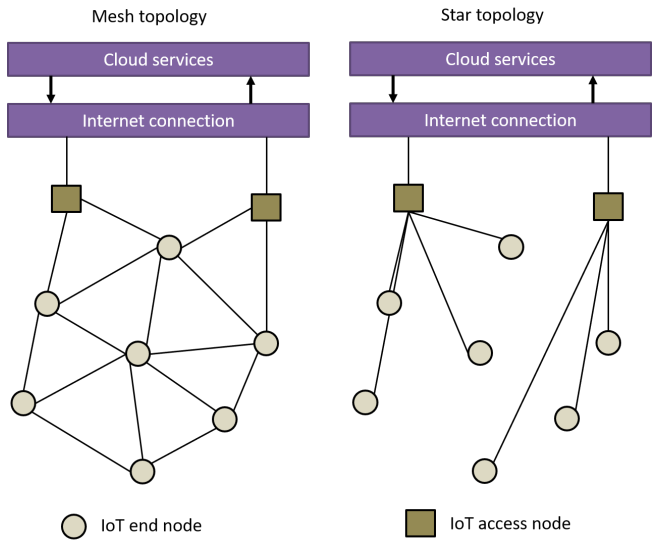


Figure 5. Comparison of a simplified IoT mesh and star network topology.

Range of an IoT system is important in the sense that it defines an upper bound of the positioning error, which cannot be larger than the communication range. In this aspect, mesh-capable networks have a better footing for positioning purposes as any device can extend service without the need to have specific and dedicated infrastructure;

Channel bandwidth is directly related to the achievable accuracy in positioning when a TOA-based estimation is used. The Crámer–Rao lower bound for any unbiased estimator [12] of a time delay τ_0 of a signal S is given as

$$\mathrm{var}(\hat{\tau}_0) \geq \frac{1}{\frac{\varepsilon}{N_0/2}\frac{\int_{-\infty}^{+\infty}(2\text{ß}f)^2|\mathrm{S}(f)|^2df}{\int_{-\infty}^{+\infty}|\mathrm{S}(f)|^2dt}}, \tag{6}$$

where ε is the signal energy, N_0 the noise spectral density and $\int_{-\infty}^{+\infty}(2\text{ß}f)^2|\mathrm{S}(f)|^2df$ is the mean square bandwidth of the signal. However, since we have do not have all the necessary information to accurately determine each IoT signal's spectrum density, we provide instead the multipath resolution or time-frequency resolution defined as follows:

$$\Delta t \geq \frac{2\pi}{\Delta w}. \tag{7}$$

Equation (7) determines how the time duration Δt and the spectral bandwidth $\Delta\omega$ relate to each other. The spectral bandwidth is defined as the bandwidth that includes most of the signal's energy. In this study, we assume it to be equal to the channel bandwidth. Overall, what both Equations (6) and (7) show is that, for time-based approaches, it is favorable to have signals with high SNR and short time duration (i.e., higher bandwidth);

Carrier frequency is inversely proportional to the signal wavelength and to the path losses exhibited by the signal. As we move from sub-GHz carriers towards mmWave carriers, the path losses are stronger and stronger, which results in smaller communication ranges. The differences in

path losses are due to a multitude of phenomena, but, as frequency increases, they are especially due to the smaller effective area of the devices' antennae. Overall, combining lower carrier frequencies and mesh topologies results in an enhanced service coverage;

Modulation types in IoT systems rely on various digital modulation types, from Ultra Narrow Band (UNB), defined as systems with bandwidths below 1 kHz, to Ultra Wide Band (UWB) modulations, i.e., bandwidths above 500 MHz. In addition, spread spectrum (SS) or Orthogonal Frequency Division Multiplexing (OFDM) modulations are also widely encountered. The modulation type plays a big role in the achievable positioning accuracy when TOA, TDOA, or AOA methods are used, but it has little or no impact when RSS methods are used. Certain modulation-based characteristics can be exploited for positioning purposes. For example, this is the case of SS signals (e.g., LoRa, ZigBee, etc.), where the spreading pseudo-random sequence can be used to infer the signal's travel time in a similar fashion to GNSS;

Positioning signaling or data exchange is the ability to use either pilot signals or sequences of data packets to provide the location of nearby devices. However, few of the existing IoT technologies support positioning-related signaling, except for most of the cellular IoT technologies (e.g., NB-IoT), which rely on the observed time difference of arrival (OTDOA), introduced in the LTE radio. Apart from the cellular IoT technologies, the future WiFi 802.11az standards also showcase a dedicated data exchange regarding the time-of-flight information to determine the location of its devices;

Roaming is the ability to provide continuity of service across multiple networks, owned or not by a single entity. As mobility is a keystone of most positioning applications, it is important to take note of this when looking at IoT systems. In this aspect, protocols such as Sigfox or Ingenu are at an advantage, as they operate similarly to cellular systems and they offer service across multi continents. Despite that, even proprietary solutions start to provide open application interface specifications and open guest periods in the radio access, which facilitate the exchange of data across multiple vendors and technologies;

Network ownership raises security and privacy concerns. Security is becoming a strong requirement in IoT systems, especially as the data access, transport and storage become more and more regulated by international and European bodies [13]. Technologies such as Ingenu and Sigfox own the entirety of the network, meaning that the transportation of data is under their full responsibility. Thus, positioning solutions enabled by such systems will be protected by the system provider, as the infrastructure device's location will not be known to the user;

Power consumption is a main topic for all IoT technologies. For positioning applications, low-power consumption is crucial for the viability of several systems, especially when the goal is to continuously track and monitor inexpensive items. For example, low-power consumption is mandatory in several use cases from the logistics and construction sectors.

3.4. Comparing IoT Technologies and IoT Enablers

After discussing the positioning domain and the main system parameters relevant to positioning, here we present two comparative tables between 29 IoT solutions (see Tables 1 and 2), whose goal is to sum up the key points mentioned so far and to enable an easy comparison between the different technologies. Throughout the rest of this subsection, our goal is to make comparisons and drive the reader towards a better understanding of how a certain technology would fare as the backbone of a positioning system, in a GNSS-free case.

Table 1 presents for each technology, from left to right, the network topology, network type, the impact of each measurement domain on the device battery life and cost, the achievable positioning accuracy, the most suitable domain and reported accuracy studies.

The first column maps each technology's topology to either a star or mesh topology.

The second column presents the network type, where each entry starts with the rate, power consumption and maximum operating range offered by the technology (see section). The operating range has a correlation with the frequency bands in Table 2.

The third column presents the impact on battery consumption and device cost for each measurement domain in discussion. While most of the technologies do not offer such capabilities, this classification assumes that it would be possible to couple the necessary measurement units to provide such information. Hence, the classification of low impact $(+)$, medium $(++)$ or high impact $(+++)$ are based on what the authors expect to be the addition burden in terms of device cost and battery burden. The power domain is seen to be the one with the smallest impact, due to the fact that it would be easily available to all of these technologies.

The fourth column provides a qualitative indicator for the expected accuracy based on what the technology currently offers. When available, this information is based on the related studies.

The fifth column states the most suitable measurement domain to use with each technology. The domain is attributed based on the technology's signal characteristics presented in Table 2 and its current capabilities.

Table 2 describes each technologies' key physical aspects, such as frequency bands, channel bandwidth and modulation type.

Positioning services often have a high demand for power consumption. Operating a positioning based infrastructure is often tied to the need of having a fully plugged-in (powered) infrastructure. However, there are several industrial applications that would benefit from a fully battery-operated network, especially where an electricity network might not yet be present, e.g., construction sites, or for facility of service extension and maintainability.

In terms of positioning, we found that most IoT systems are yet to offer specific signaling to support accurate measurements for localization. Few of the existing IoT systems have already raised interest in the academic field in terms of their positioning capabilities, as shown in the last column of Table 1. Most of the existing studies focus on RSS-based approaches and several of them rely on low-cost probabilistic methods requiring an underlying path loss model. Few studies that focus on time-based and space-based approaches are mostly targeting the current and future cellular IoT signals, derived from LTE, such as LTE-M, which are retaining some of LTE's positioning characteristics such as positioning-specific signaling. In addition, future 5G networks are likely to rely on time-based and space-based positioning approaches. Our paper further contributes with additional results based on RSS and time-based approaches as shown in the next sections.

Table 1. Summary of key positioning related aspects for several IoT protocols and IEEE 802.11∗ family protocols.

			Impact on (Battery, Device Cost) per Domain [1]					
Technology	**Network Topology**	**Network Type**	**Time-Based Positioning**	**Power-Based Positioning**	**Space-Based Positioning**	**Achievable Positioning Accuracy [2]**	**Most Suitable Domain**	**Accuracy Studies**
5G	star	HR/HP-Short range	+, +	+,+	+,+	High	Time	[14,15]
ANT+	mesh	LR/LP-Short range	+,+++	+,+	++,++	Low	Power	
BLEmesh	mesh	LR/LP-Short range	+,+++	+,+	++,+	Medium	Power	[11,16,17]
Dash7	star	LR/LP-Long range	+,+++	+,+	++,++	Low	Power or Space	
EC-GSM-IOT	star	HR/LP-Long range	+,+++	+,+	++,++	Low	Power	
EnOcean	mesh	LR/LP-Long range	+,+++	+,+	++,++	Low	Power or Space	
Ingenu /RPMA	star	LR/LP-Long range	+,+++	+,+	++,++	Medium	Power or Space	
ISA101.11a	mesh	LR/LP-Short range	+,+++	+,+	++,++	Medium	Power or Space	
LoRa	star	LR/LP-Long range	+,++	+,+	++,++	Medium	Power	[18]
LTE-M	star	LR/LP-Long range	+,+	+,+	++,++	Medium	Time	[2]
MiWi	mesh	LR/LP-Long range	+,+++	+,+	++,++	Medium	Power	
NB-IoT	star	LR/LP-Long range	+,+	+,+	++,++	Medium	Time	[2]
RFID	star	LR/LP-Short range	+,+++	+,+	++,++	Medium	Power	[19–23]
Sigfox	star	LR/LP-Long range	+,+++	+,+	++,++	Medium	Power	[24,25]
Telensa	star	LR/LP-Long range	+,+++	+,+	++,++	Low	Power or Space	
Thread	mesh	LR/LP-Short range	+,+++	+,+	++,++	Medium	Power	
Weightless-N	star	LR/LP-Long range	+,+++	+,+	++,++	Medium	Power or Space	
Weightless-P	star	LR/LP-Long range	+,+++	+,+	++,++	Low	Power or Space	
Weightless-W	star	LR/LP-Long range	+,+++	+,+	++,++	Medium	Power	

Table 1. *Cont.*

Technology	Network Topology	Network Type	Impact on (Battery, Device Cost) per Domain [1]			Achievable Positioning Accuracy [2]	Most Suitable Domain	Accuracy Studies
			Time-Based Positioning	Power-Based Positioning	Space-Based Positioning			
WirelessHART	mesh	LR/LP-Short range	+,+++	+,+	++,++	Medium	Power	
WiFi802.11af	star	HR/HP-Long range	+ , +	+,+	++,++	High	Time	
WiFi802.11ah/HaLoW	star	LR/LP-Long range	+,+	+,+	++,++	High	Time	
WiFi802.11az	star	HR/HP-Short range	+,+	+,+	++,++	High	Time	
WiFi802.11p (V2X)	mesh	HR/HP-Short range	+,+	+,+	++,++	High	Time	[26,27]
Wirepas	mesh	HR-Long range	+,+++	+,+	++,++	Medium	Power	
WiSUN	mesh	LR/LP-Long range	+,+++	+,+	++,++	Medium	Power	
ZigBee/ZigBee-NaN	mesh	LR/LP-Long range	+,+++	+,+	++,++	Medium	Power	[28–30]
Z-Wave	mesh	LR/LP-Long range	+,+++	+,+	++,++	Medium	Power or Space	

[1] (+, +): low impact, (++, ++): medium, (+++, +++): high impact; [2] assuming implementation without external sensors, such as GNSS.

Table 2. Summary of key physical layer parameters for several IoT protocols.

Technology	Frequency Bands	Channel Bandwidth (MHz)	Modulation Type (UNB/NB/ SS/OFDM/UWB)
5G	GHz, mmWave	<100	OFDM
ANT+	GHz	1	NB
BLE mesh	GHz	1	NB
Dash7	sub-GHz	0.025, 0.200	NB
EC-GSM-IOT	sub-GHz	0.2	NB
EnOcean	sub-GHz	0.0625	NB
Ingenu	sub-GHz and GHz	1	SS
ISA101.11a	GHz	5	SS
LoRa	sub-GHz	0.125, 0.500	SS
LTE-M	sub-GHz and GHz	1.08, 1.4	OFDM
MiWi	sub-GHz and GHz	0.040, 0.250	NB
NB-IoT	sub-GHz and GHz	0.18	NB, OFDM
RFID	sub-GHz and GHz	0.2	NB
Sigfox	sub-GHz	0.2	UNB
Telensa	sub-GHz	0.1	NB
Thread	GHz	5	NB
Weightless-N	sub-GHz	0.2	UNB
Weightless-P	sub-GHz	0.0125	NB
Weightless-W	sub-GHz	5	SS
WirelessHART	GHz	0.25	SS
WiFi802.11af	sub-GHz	8	OFDM
WiFi802.11ah	sub-GHz	1, 2, 4, 8, 16	OFDM
WiFi802.11az	GHz, mmWave	20, 40, 60, 80, 160	OFDM
WiFi802.11p (V2X)	GHz	10	OFDM
Wirepas	sub-GHz and GHz	0.126, 0.5	NB
WiSUN	sub-GHz and GHz	0.2–1.2	NB, SS and OFDM
ZigBee	sub-GHz and GHz	0.6, 1.2, 2	SS
ZigBee-NaN	sub-GHz	0.6, 1.2, 2	SS
Z-Wave	sub-GHz	0.2	NB

In addition, we have found that network-centric positioning solutions are being favored as opposed to device-centric ones, which is often related to the limited resources at the end nodes. However, a centralized architecture places an additional burden on the network capacity and latency as the number of devices grow. For many of the IoT systems, a centralized architecture will have difficulties accommodating real-time location systems, especially due to the strict latency requirements of such systems. Integration with other high-capacity technologies, such as WiFi and 5G, could decrease the latency at the expense of per unit cost and power consumption. The support of positioning updates at very sparse intervals ought to be feasible for many IoT technologies, which will certainly find its application in several niche markets, especially if the positioning system is supported fully by battery-powered networks over a span of multiple years.

To further complement our study, we end with a perspective on what the achievable positioning accuracy is. The next two sections focus on measurement-based and simulation-based studies, respectively. We introduce simulation-based results from two systems whose performance was difficult to find as benchmarks in the existing literature, namely IEEE 802.11az and LoRa. Then, we present measurement-based results from an office environment of a positioning system built on top of the Wirepas' mesh solution.

4. Simulation-Based Performance Metrics

4.1. Case Study 1: 802.11az IoT Enabler, Simulation-Based Results, Time Domain

In 802.11az, a position estimate is obtained by solving the hyperbolic location based on the measured TOA t_{A_a} at the mobile side from several ANs, where a is the AN index, $a = 1, \ldots, N_{AN}$.

$$t_{A_a} = t_s + \frac{d(Tag, AN_a)}{c} + \sum_{a=2}^{N_AN} \left(\frac{d(AN_{a-1}, AN_a)}{c} + t_f \right), \quad (8)$$

where t_s is the starting time of transmission from one AN in the network, taken arbitrarily as the first AN (AN_1), c is the speed of light, $d(Tag, AN_a)$ is the geometric distance between the mobile device and the a-th AN, $a = 1, \ldots, N_{AN}$, t_f is the forwarding time of the signaling message between two access nodes, and $d(AN_{a-1}, AN_a)$ is the geometric distance between the $a-1$-th AN and a-th AN. With several noisy observations of the measured time of arrivals, the IoT device can compute its position (as well as the unknown t_s). It is assumed that the AN positions and the forwarding time are known and transmitted in the signaling message. In addition to that, a minimum of four synchronized access points are needed to estimate the four unknowns (x, y, z, t_s), with the (x, y, z) the device location.

To understand an achievable location performance, we defined a simulation over a square area of 0.4 km^2 at the highest bandwidth available (160 MHz). We observe in Figure 6 that this solution would be able to offer sub-meter accuracies 80% of the times when at least seven ANs are available.

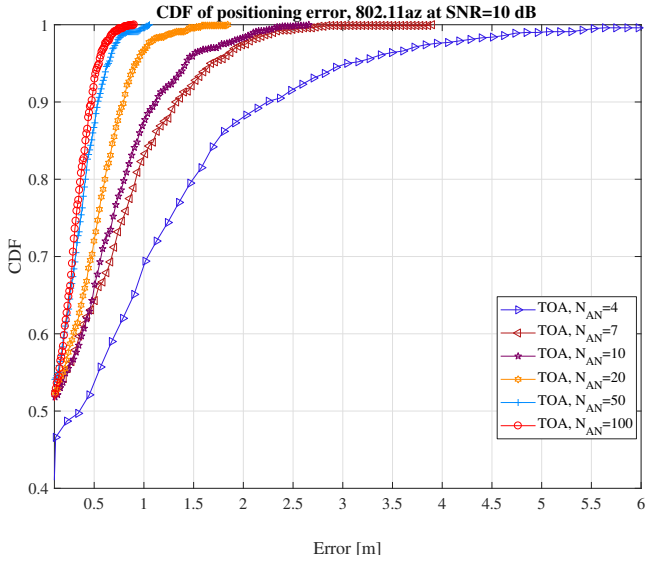


Figure 6. Example of 802.11az performance at various number of access nodes at signal to noise ration (SNR), SNR = 10 dB.

4.2. Case-Study 2: LoRa, Simulation-Based Results, Time Domain

A chirp spread spectrum (CSS) system with a 125 kHz bandwidth and a spreading factor of 7 was used in the simulations. It was assumed that we have a single-floor square indoor area of 200 m $\times$ 200 m size, in which N_{AN} access nodes are distributed uniformly, with N_{AN} between 3 and 100. Ten thousand Monte Carlo iterations were used to generate randomly the position of the ANs and of the IoT device. The positioning was based on TOA principle, where the TOA was estimated based on the correlation between the incoming signal and a reference CSS code. The results are shown in Figure 7 in terms of cumulative distribution function (CDF) of error, for a different number of LoRA access nodes, respectively. For three access nodes and at an SNR = -18 dB, the positioning error is higher than 50 m in more than 50% of cases. On the other hand, with 100 access nodes distributed in the 0.4 km^2 area, we can reach below 10 m accuracy in more than 50% of cases.

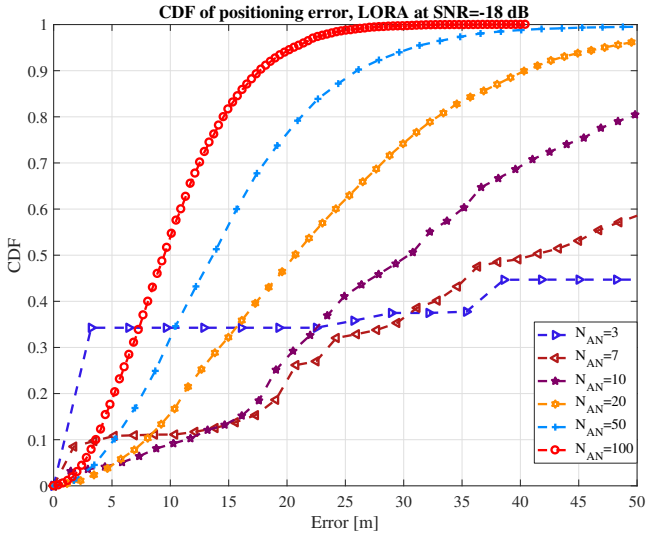


Figure 7. Example of LoRa performance at various numbers of access nodes.

5. Measurement-Based Performance Metrics with Wirepas IoT Platform

This section presents experimental results from an IoT positioning system built with Wirepas IoT mesh solution. The results presented in this section that were obtained are Wirepas' offices and are based on power measurements.

The environment where measurements took place, with a total area of 180 m^2 (10 by 18 meters), is a typical work environment with few small rooms and a large open areas (see Figure 8). Several battery powered operated devices were placed across the floor extending the network coverage in and outside the rooms. Some of these devices acted as known reference points while others as tracked devices. The reference points are identified in Figure 8 as routing devices (blue squares) and the measurement devices as yellow dots. All the devices were operating in the 2.4 GHz using Nordic's NRF51 as the radio chipset.

In this setup, the measurement devices were statically collecting information about network beacons' broadcast periodically by the routing devices. The information about the routing devices' beacons, as seen by the measurement devices, was sent regularly towards the network sink. In turn, the network sink and gateway communicated the measurements to a positioning engine running on a local computer. The position engine provided a location estimate based on the known location of the routing devices and the RSS observed by the measurement devices. A location estimate was calculated

by one-shot runs of a weighted centroid algorithm, meaning that no average or filtering were applied to the location estimates. However, the RSS measurements were averaged over a window of time to mitigate the channel propagation effects.

In addition to a location estimate on a global or local reference frame, the position engine also provided an area-based location. The area-based location consists of matching the location estimate to a set of geographical areas of interest (shaded areas in Figure 8). For a device to be in such area, it meant that its location estimate was found to be inside the geographic area defined by the four coordinate points of each area.

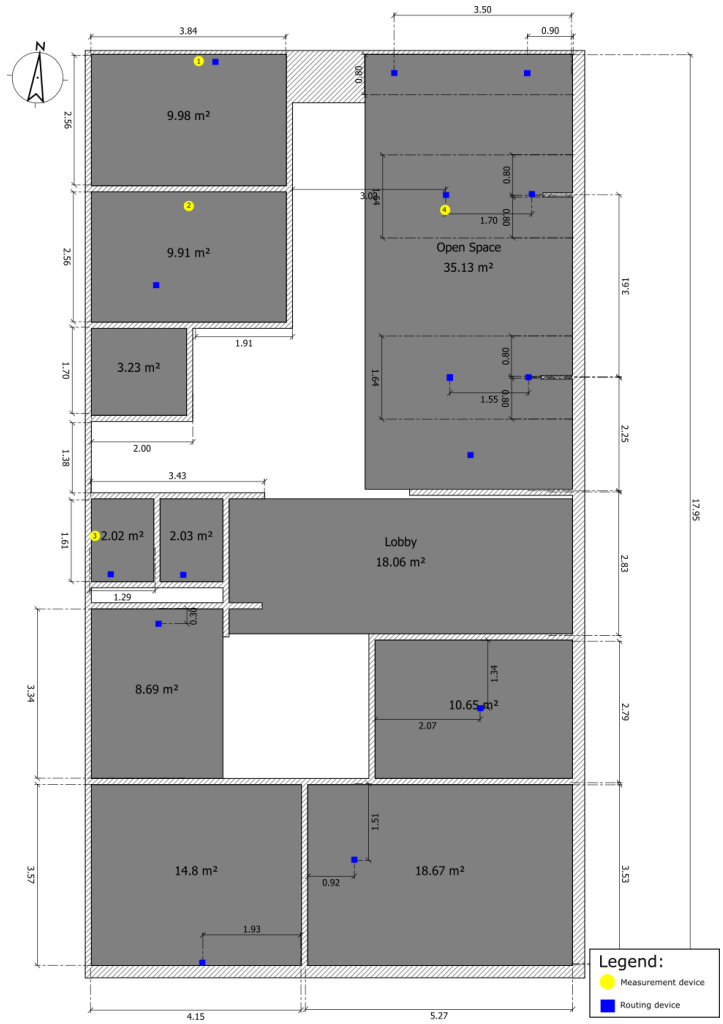


Figure 8. Office environment where the measurements were acquired.

The results on Table 3 show the probability of correctly classifying the measurement devices in the areas of interest. The percentage is calculated by summing the amount of location estimates in the node's correct area versus the total amount of location estimates in any other area of interest.

The results on Table 3 show that, during a day, the devices were correctly located inside the logical area where they were known to be at more than 90% of the time.

Table 3. Experimental results with an IoT testbed using Wirepas connectivity with 60 fixes per second and static nodes.

Area (m^2)	Office Hours	Outside Office Hours	All Day
	% of Correct Location Area Classification		
10	95.41	89.47	91.16
10	96.16	97.59	97.18
2	91.56	94.85	93.90
3	96.76	99.20	98.50
Mean	95.51	95.61	95.57

6. Conclusions

We believe positioning is important not only for IoT end applications, but also to support network self-management. Our paper addresses the lack of comprehensive studies comparing IoT solutions and their fit-for-positioning applications. The paper first covered three possible measurement domains from which IoT devices could derive their location. Afterwards, we focused on classification of the IoT solutions and we discussed several system parameters that should be considered when designing a positioning system. We concluded our study with a comparative table and discussion between multiple IoT and other wireless solutions. We also provided an overview of achievable system performance with unique results for three positioning systems built on top of IEEE 802.11az, LoRa and Wirepas, respectively.

Overall, based on our study, we conclude that power-domain positioning currently offers the best trade-off between implementation cost and positioning accuracy for low-power systems. Dedicated positioning signaling as well as space-based approaches are some of the feasible ways to push for higher accuracy and still offer low-power operation. Cooperation with other wireless technologies, such as WiFi and 5G, could allow for mobility support and ability to operate at large scales when low-power operation is not critical.

Author Contributions: Conceptualization, P.F.eS. and V.K.; Funding acquisition, E.-S.L.; Investigation, P.F.eS.; Software, P.F.eS. and E.-S.L.; Supervision, V.K. and E.-S.L.; Writing—Review and Editing, P.F.eS., V.K. and E.-S.L.

Funding: This work has been partly supported by EU FP7 Marie Curie Initial Training Network MULTI-POS (Multi-technology Positioning Professionals) under Grant No. 316528 and by the Academy of Finland, project numbers 303576 and 313039.

Conflicts of Interest: Two of the authors are currently full time employees at Wirepas. Regardless of their relationship with Wirepas, the authors have kept the reporting objective and fair for all the technologies under examination. Furthermore the authors have not received any additional financial incentive to execute or complete this work. Wirepas contributed with hardware for the activities performed in this report which was part of the research visit arranged within the MULTI-POS project.

References

1. Pedersen, T.; Fleury, B.H. *Whitepaper on New Localization Methods for 5G Wireless Systems and the Internet-of-Things*; COST Action CA15104; Danish National Research Database: Aalborg, Denmark, 2018.
2. Lin, X.; Bergman, J.; Gunnarsson, F.; Liberg, O.; Razavi, S.M.; Razaghi, H.S.; Rydn, H.; Sui, Y. Positioning for the Internet of Things: A 3GPP Perspective. *IEEE Commun. Mag.* **2017**, *55*, 179–185. [CrossRef]
3. Lin, K.; Chen, M.; Deng, J.; Hassan, M.M.; Fortino, G. Enhanced Fingerprinting and Trajectory Prediction for IoT Localization in Smart Buildings. *IEEE Trans. Autom. Sci. Eng.* **2016**, *13*, 1294–1307. [CrossRef]
4. del Peral-Rosado, J.A.; López-Salcedo, J.A.; Seco-Granados, G. Impact of frequency-hopping NB-IoT positioning in 4G and future 5G networks. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017; pp. 815–820.
5. Chen, L.; Thombre, S.; Järvinen, K.; Lohan, E.; Alén-Savikko, A.; Leppäkoski, H.; Bhuiyan, M.; Bu-Pasha, S.; Ferrara, G.; Honkala, S.; et al. Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey. *IEEE Access* **2017**, *5*, 8956–8977. [CrossRef]

6. Singh, K.; Kapoor, D. Create Your Own Internet of Things: A survey of IoT platforms. *IEEE Consum. Electron. Mag.* **2017**, *6*, 57–68. [CrossRef]
7. Zhang, P.; Nagarajan, S.G.; Nevat, I. Secure Location of Things (SLOT): Mitigating Localization Spoofing Attacks in the Internet of Things. *IEEE Internet Things J.* **2017**, *4*, 2199–2206. [CrossRef]
8. Al-Sarawi, S.; Anbar, M.; Alieyan, K.; Alzubaidi, M. Internet of Things (IoT) communication protocols: Review. In Proceedings of the 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 17 May 2017; pp. 685–690.
9. Raza, U.; Kulkarni, P.; Sooriyabandara, M. Low Power Wide Area Networks: An Overview. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 855–873. [CrossRef]
10. Zanella, A. Best Practice in RSS Measurements and Ranging. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2662–2686. [CrossRef]
11. Lohan, E.S.; Talvitie, J.; e Silva, P.F.; Nurminen, H.; Ali-Löytty, S.; Piché, R. Received signal strength models for WLAN and BLE-based indoor positioning in multi-floor buildings. In Proceedings of the 2015 International Conference on Location and GNSS (ICL-GNSS), Gothenburg, Sweden, 22–24 June 2015; pp. 1–6.
12. Kay, S. *Fundamentals of Statistical Signal Processing: Estimation Theory*; Prentice-Hall, Inc.: Upper Saddle River, NJ, USA, 1993.
13. European Union. *EUR-Lex General Data Protection Regulation*; European Union: Brussels, Belgium, 1998–2018.
14. Koivisto, M.; Costa, M.; Hakkarainen, A.; Leppanen, K.; Valkama, M. Joint 3D Positioning and Network Synchronization in 5G Ultra-Dense Networks Using UKF and EKF. In Proceedings of the 2016 IEEE Globecom Workshops, Washington, DC, USA, 4–8 December 2016; pp. 1–7.
15. Levanen, T.; Talvitie, J.; Wichman, R.; Syrjälä, V.; Renfors, M.; Valkama, M. Location-aware 5G communications and Doppler compensation for high-speed train networks. In Proceedings of the 2017 European Conference on Networks and Communications (EuCNC), Oulu, Finland, 12–15 June 2017; pp. 1–6.
16. Faragher, R.; Harle, R. Location Fingerprinting With Bluetooth Low Energy Beacons. *IEEE J. Sel. Areas Commun.* **2015**, *33*, 2418–2428. [CrossRef]
17. Davidson, P.; Piché, R. A Survey of Selected Indoor Positioning Methods for Smartphones. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1347–1370. [CrossRef]
18. Fargas, B.C.; Petersen, M.N. GPS-free geolocation using LoRa in low-power WANs. In Proceedings of the 2017 Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6.
19. Basheer, M.R.; Jagannathan, S. Localization of RFID Tags Using Stochastic Tunneling. *IEEE Trans. Mob. Comput.* **2013**, *12*, 1225–1235. [CrossRef]
20. Hasani, M.; Talvitie, J.; Sydänheimo, L.; Lohan, E.S.; Ukkonen, L. Hybrid WLAN-RFID Indoor Localization Solution Utilizing Textile Tag. *IEEE Antennas Wirel. Propag. Lett.* **2015**, *14*, 1358–1361. [CrossRef]
21. Liu, T.; Liu, Y.; Yang, L.; Guo, Y.; Wang, C. BackPos: High Accuracy Backscatter Positioning System. *IEEE Trans. Mob. Comput.* **2016**, *15*, 586–598. [CrossRef]
22. Ma, H.; Wang, K. Fusion of RSS and Phase Shift Using the Kalman Filter for RFID Tracking. *IEEE Sens. J.* **2017**, *17*, 3551–3558. [CrossRef]
23. Ma, H.; Wang, Y.; Wang, K.; Ma, Z. The Optimization for Hyperbolic Positioning of UHF Passive RFID Tags. *IEEE Trans. Autom. Sci. Eng.* **2017**, *14*, 1590–1600. [CrossRef]
24. Sallouha, H.; Chiumento, A.; Pollin, S. Localization in long-range ultra narrow band IoT networks using RSSI. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
25. Janssen, T.; Weyn, M.; Berkvens, R. Localization in Low Power Wide Area Networks Using Wi-Fi Fingerprints. *Appl. Sci.* **2017**, *7*, 936. [CrossRef]
26. Cruz, S.B.; Abrudan, T.E.; Xiao, Z.; Trigoni, N.; Barros, J. Neighbor-Aided Localization in Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2693–2702. [CrossRef]
27. Kalverkamp, G.; Schaffer, B.; Biebl, E. OFDM-Based Ranging Approach for Vehicular Safety Applications. In Proceedings of the 2013 IEEE 78th Vehicular Technology Conference (VTC Fall), Las Vegas, NV, USA, 2–5 September 2013; pp. 1–5.
28. Ou, C.W.; Chao, C.J.; Chang, F.S.; Wang, S.M.; Liu, G.X.; Wu, M.R.; Cho, K.Y.; Hwang, L.T.; Huan, Y.Y. A ZigBee position technique for indoor localization based on proximity learning. In Proceedings of the 2017 IEEE International Conference on Mechatronics and Automation (ICMA), Takamatsu, Japan, 6–9 August 2017; pp. 875–880.

29. Dong, Z.; Mengjiao, C.; Wenjuan, L. Implementation of indoor fingerprint positioning based on ZigBee. In Proceedings of the 2017 29th Chinese Control and Decision Conference (CCDC), Chongqing, China, 28–30 May 2017; pp. 2654–2659.
30. Cheon, J.; Hwang, H.; Kim, D.; Jung, Y. IEEE 802.15.4 ZigBee-Based Time-of-Arrival Estimation for Wireless Sensor Networks. *Sensors* **2016**, *16*, 203. [CrossRef] [PubMed]

Tampereen teknillinen yliopisto
PL 527
33101 Tampere

Tampere University of Technology
P.O.B. 527
FI-33101 Tampere, Finland

ISBN 978-952-15-4267-1
ISSN 1459-2045